UNIVERSITÄT ZU LÜBECK

**Aus dem Institut für Theoretische Informatik**
**der Universität zu Lübeck**
**Direktor: Prof. Dr. Till Tantau**

# IT-Sicherheit in der Kritischen Infrastruktur BOS-Leitstelle

Inauguraldissertation
zur
Erlangung der Doktorwürde
der Universität zu Lübeck

Aus der Sektion Informatik / Technik

vorgelegt von
Jens Christiansen
aus Malsch

Lübeck, 2025

1. Berichterstatter: Prof. Dr. Rüdiger Reischuk

2. Berichterstatter: Prof. Dr. André Calero Valdez

Tag der mündlichen Prüfung: 25.09.2025

Zum Druck genehmigt. Lübeck, den 06.10.2025

# Inhaltsverzeichnis

# Danksagung

Mein besonderer Dank gilt meinem Betreuer Herrn Prof. Dr. Rüdiger Reischuk für die unkomplizierte und zielführende Unterstützung.

Dem Fachverband Leitstellen (FVLST), allen voran den amtierenden und ehemaligen Vorsitzenden Marc Gistrichovsky und Achim Hackstein sowie dem gesamten Vorstand danke ich für die finanzielle und praktische Unterstützung, vor allem bei der Adressierung der Umfrage an die Leitstellenvertreter.

Ebenso gilt mein Dank den Mitgliedern der AG Technik des Fachverbandes Leitstellen, der AG Leitstelle der Deutschen Gesellschaft für Rettungswissenschaften (DGRe) und dem Referat 7 der Vereinigung zur Förderung des Deutschen Brandschutzes (vfdb) für die stetigen fachlichen Austausch.

Ein weiterer besonderer Dank gilt den Unternehmen CKS Systeme, Eurofunk Kappacher, Sinus Nachrichtentechnik sowie Vomatec Innovations für die Rückmeldungen bei der Herstellervalidierung.

# Zusammenfassung

Die Leitstellen von Rettungsdienst, Feuerwehr und Polizei unterliegen hinsichtlich rechtlicher und organisatorischer Vorgaben sowie Finanzierung den Bundesländern bzw. den Kommunen. Bedingt durch die föderalen Strukturen besteht keine Einheitlichkeit hinsichtlich technischer Ausstattung, Sicherheitsanforderungen sowie organisatorischen und personellen Aspekten. Die empirische Erhebung unter den Leitstellen in Deutschland ergab, dass eine breite Heterogenität hinsichtlich technischer Ausstattung, rechtlichen und finanziellen Rahmenbedingungen sowie insbesondere Vorgaben zur Informationssicherheit besteht.

Unabhängig von diesen Randbedingungen ist die hohe Bedeutung der Leitstellen für die Gefahrenabwehr hervorzuheben, da eine jederzeitige und schnelle Erreichbarkeit für Notrufe erwartet wird; Wartezeiten und Ausfälle sind weder rechtlich noch politisch hinnehmbar. Dies erfordert technische Systeme, die redundant und fehlertolerant ausgeführt sowie widerstandsfähig gegen äußere Einflussnahme ausgestaltet sind.

Die Schaffung eines grundlegenden Sicherheitsniveaus beginnend mit der Anwendungssoftware ist daher ein Ansatz zur Gewährleistung der IT-Sicherheit in Leitstellen. Ausgehend von den etablierten Software-Entwicklungsmodellen wurde ein Sicherheitsmodell entwickelt, das explizit Aspekte der IT-Sicherheit über den gesamten Entwicklungsprozess beinhaltet. Die Realisierbarkeit bei der praktischen Softwareentwicklung wurde im Rahmen einer Validierung von mehreren Herstellern bestätigt.

Unabhängig von der Anwendungssoftware sind zahlreiche weitere Aspekte zu betrachten bzw. Maßnahmen umzusetzen, um die IT-Sicherheit einer Leitstelle zu gewährleisten. Diese Maßnahmen sind als fortwährender Prozess zu verstehen, welcher mit den erforderlichen finanziellen und personellen Ressourcen ausgestattet werden muss.

# Abstract

The Public Safety Answering Points (PSAP) of the emergency services, fire departments, and police are subject to the federal states of and municipalities of Germany with regard to legal and organizational requirements and funding. Due to the federal structures, there is no consistency regarding technical equipment, security requirements, organizational and personnel aspects. The empirical survey of PSAP's in Germany revealed that there is a high heterogeneity in terms of technical equipment, legal and financial conditions, and information security requirements.

Regardless of these constraints, the high importance of PSAP's for emergency services has to be pointed out, as rapid and constant accessibility for emergency phone calls is expected. Waiting times and failures are neither legally nor politically acceptable. This requires technical systems that are redundant and fault-tolerant and designed to be resistant to external influences.

The development of a basic level of security, beginning with the application software, is therefore one approach to ensure IT security in PSAP's. Based on established software development models, a security model was developed that explicitly includes IT security aspects throughout the complete development process. Its feasibility in practical software development was confirmed by multiple companies.

Independent of the application software, numerous other aspects must be considered and measures implemented to ensure the IT security of a PSAP. These measures should be understood as an ongoing process that must be provided with the necessary financial and human resources.

# 1 Einleitung

## 1.1 Vorwort

Die durchgängige und schnelle Verfügbarkeit von Rettungsdienst, Feuerwehr und Polizei bei Notlagen ist eine Grundanforderung an ein funktionierendes Gemeinwesen. Das Bindeglied zwischen den notfallmeldenden Bürgern und den operativ tätigen Einsatzkräften bilden die Leitstellen, die für diese Aufgabe über eine umfangreiche IT-Ausstattung verfügen. Durch diese Zuständigkeit, verbunden mit jederzeitiger und schneller Reaktion auf Hilfeersuchen, werden gleichermaßen hohe Anforderungen an die IT-Ausstattung hinsichtlich Verfügbarkeit und Resilienz gestellt. Bedingt durch die Länderzuständigkeit für den Brand- und Katastrophenschutz, Notfallrettung und Polizei, gibt es keine bundesweit verbindlichen oder zumindest vereinheitlichten Vorgaben, was die IT-Sicherheit der Leitstellen betrifft. Dies spiegelt sich auch im tatsächlich vor Ort gelebten Niveau der IT-Sicherheit wider, welches sich insgesamt sehr heterogen darstellt, da mangels (detaillierter) Vorgaben auch die Finanzierung von IT-Sicherheitsmaßnahmen im bundesweiten Vergleich einer breiten Streuung unterliegt.

Im Sinne der Sicherstellung der Arbeitsfähigkeit der Leitstellen für die Notfallversorgung der Bevölkerung ist es daher unerlässlich, einen grundlegenden IT-Sicherheitsstandard zu schaffen, wobei die genutzten Softwareanwendungen neben anderen Schutzmaßnahmen den Betrachtungsschwerpunkt bilden. Die Erarbeitung eines Software-Entwicklungsmodells, welches sicherheitsrelevante Überlegungen und Realisierungsschritte durchgehend beinhaltet, ist dabei ein Baustein für die IT-Sicherheit. Die praktische Umsetzbarkeit konnte im Rahmen einer Herstellervalidierung von mehreren Unternehmen bestätigt werden.

## 1.2 Ziel der Arbeit

Zielsetzung dieser Arbeit ist es, den Stand der IT-Sicherheit in den Leitstellen zu erheben, diesen mit den aktuellen technischen und normativen Vorgaben

abzugleichen und darauf basierend ganzheitliche IT-Sicherheitsmaßnahmen für die Leitstellen zu erarbeiten. Der Fokus liegt hierbei auf der Entwicklung eines Software-Projektmodells, bei dem die Aspekte der IT-Sicherheit eine ebensolche Bedeutung genießen, wie die funktionalen Anforderungen.

## 1.3 Methodik

Um eine ganzheitliche Betrachtung der IT-Sicherheit von Leitstellen der Behörden und Organisationen mit Sicherheitsaufgaben (BOS) in Deutschland vornehmen zu können, wurde eine Umfrage unter den Leitstellen in Deutschland durchgeführt, um den IST-Stand der IT-Sicherheit zu erheben. Die Umfrage wurde als empirische Studie in Form eines Fragebogens durchgeführt, welcher überwiegend in Form von Multiple-Choice-Fragestellungen gestaltet ist und bei einigen Punkten auch Freitextantworten ermöglich. Die Auswertung erfolgte quantitativ, um statistische Häufungen zu identifizieren und hieraus Schwerpunkte an umgesetzten, geplanten und noch offenen IT-Sicherheitsmaßnahmen zu ermitteln (induktives Vorgehen).

Die Ergebnisse weisen zahlreiche Parallelen mit der Studie *Untersuchung zur Wirksamkeit der IT-Sicherheitsgesetze unter Betreibern Kritischer Infrastrukturen* auf, die im Auftrag des Bundesamtes für Sicherheit in der Informationstechnik (BSI) im Frühjahr 2023 durchgeführt worden ist:

*„Trotz der wahrgenommenen oder auch persönlich erfahrenen Gefährdungslage ist der Anteil der Unternehmen, die bereits (nahezu) alle gesetzlichen Forderungen umgesetzt haben, zum Teil noch nicht zufriedenstellend hoch.* […] *Die Defizite in ihren internen IT-Sicherheitssystemen werden vor allem mit dem hohen finanziellen und zeitlichen Aufwand begründet, denen vielerorts Personalmangel und Budgetknappheit - bei häufig wirtschaftlich mäßiger Lage des Unternehmens - gegenüberstehen. Recht häufig fehlt es auch an dem nötigen Knowhow.“* [IN23]

Parallel zur empirischen Erhebung wurde Literaturrecherche betrieben, um den aktuellen Stand der Leitstellentechnik (Hard- und Software), der rechtlichen Vorgaben (Gesetze, Verordnungen, Normen, Verwaltungsstrukturen) sowie der Arbeitsprozesse – gerade unter dem Aspekt der Kritikalität – darzustellen und deren Bedeutung für die IT-Sicherheit in Leitstellen herauszuarbeiten. Ausgehend von den

Ergebnissen der Datenerhebung und dem Literaturstand wurden die unterschiedlichen Variablen der IT-Sicherheit in Leitstellen hergeleitet, wobei der Faktor Software im Rahmen der vorliegenden Arbeit im Fokus stehen. Grundlage bilden etablierte Softwareentwicklungsmodelle, die hinsichtlich der Berücksichtigung von Sicherheitsaspekten während des Entwicklungsprozesses betrachtet werden. Darauf basierend wird die Bedeutung der IT-Sicherheit bereits während der Planungsphase über den gesamten Entwicklungsprozess von Leitstellensoftware dargestellt und entsprechende Vorgehensmodelle entwickelt und diskutiert. Zwecks Validierung der Gebrauchstauglichkeit in der Praxis wurden einschlägige Unternehmen kontaktiert, die Software für Leitstellen entwickeln und deren Votum eingeholt, so dass empirisch gewonnene Erkenntnisse und Erfahrungen der Hersteller für die Validierung herangezogen und mit den theoretischen Überlegungen abgeglichen werden konnten.

# 2 Grundlagen

## 2.1 Kritische Infrastrukturen

Das Bundesministerium des Innern hat im Jahr 2009 die Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie) herausgegeben. Hervorgerufen u.a. durch die Terroranschläge vom 11. September 2001, das Hochwasser im Sommer 2002 und den Schneefall im Münsterland mit Stromausfall (2005), wurde die Verwundbarkeit der Zivilgesellschaft in der Bundesrepublik Deutschland untersucht. Zielsetzung war hierbei, die Infrastrukturen zu identifizieren, die in der heutigen Gesellschaft unverzichtbar und damit besonders schützenswert sind. Dies wird in der Definition deutlich:

*„Kritische Infrastrukturen sind Organisationen und Einrichtungen mit wichtiger Bedeutung für das staatliche Gemeinwesen, bei deren Ausfall oder Beeinträchtigung nachhaltig wirkende Versorgungsengpässe, erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“* [BMI09]

In diesem Zusammenhang wurde auch der Begriff „Kritikalität“ gesondert definiert:

*„Kritikalität: relatives Maß für die Bedeutsamkeit einer Infrastruktur in Bezug auf die Konsequenzen, die eine Störung oder ein Funktionsausfall für die Versorgungssicherheit der Gesellschaft mit wichtigen Gütern und Dienstleistungen hat.“* [BMI09]

Die Kritischen Infrastrukturen werden in Technische Basisinfrastrukturen und Sozioökonomische Dienstleistungsinfrastrukturen unterschieden; Technische Basisinfrastrukturen sind:

- Energieversorgung
- Informations- und Kommunikationstechnologie
- Transport und Verkehr
- (Trink-)Wasserversorgung und Abwasserentsorgung

Zu den Sozioökonomischen Dienstleistungsinfrastrukturen gehören:

- Gesundheitswesen, Ernährung
- Notfall- und Rettungswesen, Katastrophenschutz
- Parlament, Regierung, öffentliche Verwaltung, Justizeinrichtungen
- Finanz- und Versicherungswesen
- Medien und Kulturgüter

Unabhängig von der Gliederung in die zwei genannten Hauptbereiche wurden die Infrastrukturen in neun Sektoren eingeteilt, wobei das Notfall- und Rettungswesen und der Katastrophenschutz keine eigenständige Infrastruktur im Sinne der Sektorenbildung mehr darstellen, sondern als Unterpunkt bei „Staat und Verwaltung“ mit eingegliedert worden sind. „Gesundheit“ (vormals „Gesundheitswesen“) und Ernährung“ hingegen bilden zwei eigenständige Sektoren. Z.T. wurden die Begrifflichkeiten verändert und/oder zusammengefasst, z.B. wurde aus „(Trink-)Wasserversorgung und Abwasserentsorgung“ der Sektor mit der Bezeichnung „Wasser“ definiert. Der Begriff „Sektor“ ist im geometrischen Sinne wörtlich zu nehmen, da die Gesamtheit der Kritischen Infrastrukturen als Kreis dargestellt ist:

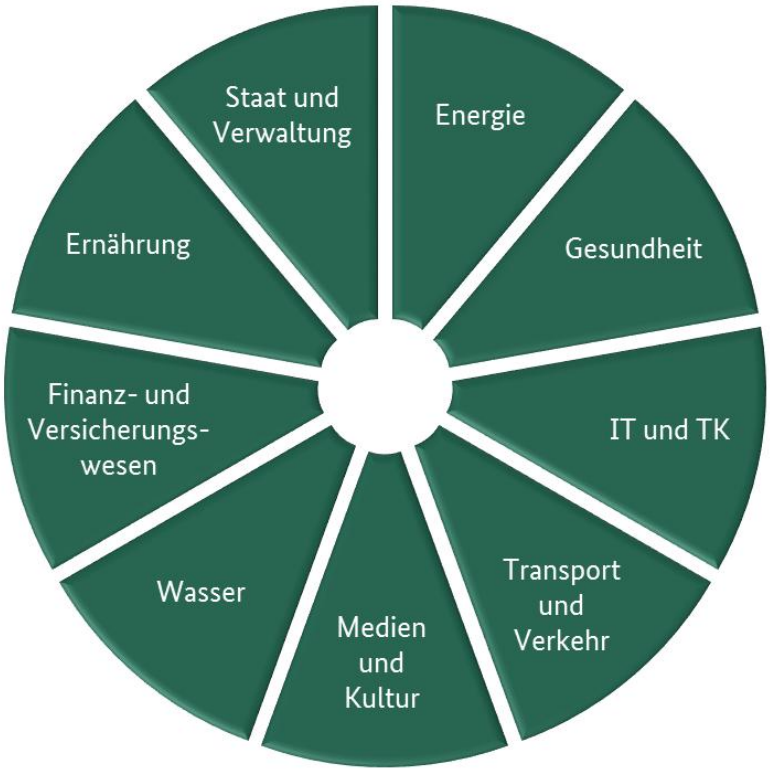



Abb. 2.1: Sicherheitsarchitektur [BMI09]

Innerhalb der Sektoren finden eine weitere Untergliederung und Erläuterung statt. Unter „Staat und Verwaltung“ sind aufgeführt:

- Regierung und Verwaltung
- Parlament
- Justiz
- Notfall- und Rettungswesen einschließlich Katastrophenschutz

Eine explizite Nennung der Leitstellen findet sich hier nicht; dies gilt ebenso für Polizei und Ordnungsbehörden, die gleichfalls keine eindeutige Erwähnung finden. Da es sich bei der KRITIS-Strategie um eine politische Absichtserklärung und nicht um ein Gesetz handelt, ist die rechtlich bindende Anwendbarkeit zu verneinen.

In der DIN 14092:2024-06 sind Feuerwehrhäuser als Bestandteil kritischer Infrastrukturen explizit genannt, so dass diese Festlegung zumindest baulich für Leitstellen gilt, die in einem Feuerwehrhaus (z.B. Feuerwache einer Berufsfeuerwehr) mit angesiedelt sind. Die DIN 14092 bezieht sich jedoch nur auf bauliche Aspekte, nicht auf IT-Ausstattung und deren Ausgestaltung und auch nicht auf betrieblich-organisatorische Prozesse.

Das Gesetz zur Erhöhung der Sicherheit in informationstechnischen Systemen (IT-Sicherheitsgesetz) [ITS15] in der Fassung vom 17. Juli 2015 verpflichtet die Betreiber Kritischer Infrastrukturen in § 8a zu organisatorischen und technischen Vorkehrungen, um die Verfügbarkeit, Integrität, Authentizität und Vertraulichkeit ihrer informationstechnischen Systeme, Komponenten und Prozesse sicherzustellen. [KB18] Zudem wird das *Bundesamt für Sicherheit in der Informationstechnik* (BSI) als zentrale Meldestelle bestimmt und den Betreibern Kritischer Infrastrukturen auferlegt, IT-Sicherheitsvorfälle dort unverzüglich zu melden (§ 8b).

Eine exakte Definition auf Bundesebene, was genau als Kritische Infrastruktur anzusehen ist, bzw. ab welcher Größenordnung, ist weder in der KRITIS-Strategie des BMI noch im IT-Sicherheitsgesetz festgelegt. Um diese Lücke zu schließen, Interpretationsspielräume zu vermeiden und damit Rechtssicherheit zu schaffen, hat der Gesetzgeber dem BSI in § 10 des BSI-Gesetzes [BSI21] die Ermächtigung erteilt, in Abstimmung mit anderen Bundesressorts eine Rechtsverordnung zu

erlassen, welche Einrichtungen, Anlagen oder Teile davon als Kritische Infrastrukturen im Sinne des BSIG anzusehen sind.

Das BSI hat dies in Form der Kritisverordnung (KritisV) [BSI16] umgesetzt; in dieser werden für alle Sektoren außer „Staat und Verwaltung“ und „Medien und Kultur“ exakt definierte Kriterien (Schwellenwerte) beschrieben, ab denen eine Einrichtung eine Kritische Infrastruktur im Sinne des BSI-Gesetzes ist. Bei der Energie- und Wasserversorgung sind dies Mindest-Leistungs- bzw. Fördermengen, so dass beispielsweise nicht jede private Photovoltaikanlage als Kritische Infrastruktur anzusehen ist.

Da der Bereich Staat und Verwaltung und damit auch das Notfall- und Rettungswesen einschließlich Katastrophenschutz mit keinem Wort – auch nicht sinngemäß – in der KritisV aufgeführt ist, ergibt sich an dieser Stelle keine Rechtsgrundlage für eine Einstufung als Kritische Infrastruktur.

Für den Sektor Gesundheit sind in der KritisV die kritischen Dienstleistungen im Gesundheitswesen benannt:

- Stationäre medizinische Versorgung
- Versorgung mit lebenswichtigen Medizinprodukten
- Versorgung mit Arzneimitteln, Blut- und Plasmaprodukten
- Labordiagnostik

In dieser abschließenden Aufzählung tauchen weder Notfallrettung und Krankentransport noch der Ärztliche Bereitschaftsdienst auf, so dass auch an dieser Stelle kein Bezug zu Leitstellen hergestellt werden kann. Wie bei den Sektoren Energie und Wasser sind auch im Gesundheitswesen bestimmte Größenordnungen der Patientenversorgung bzw. des Warenumschlages definiert, so dass nicht jede Arztpraxis bzw. jede Apotheke als Kritische Infrastruktur gilt, sondern dies erst bei größeren Einrichtungen des Gesundheitswesens und der zugehörigen Logistik entsprechender Größenordnung zum Tragen kommt.

Von den 16 Bundesländern haben bislang nur Hessen und Bayern die Leitstellen als Kritische Infrastruktur eingestuft; in beiden Fällen erfolgte dies im Herbst 2020 unter dem Einfluss der Corona-Pandemie. [HE20]

Die Bundesregierung hat in einer parlamentarischen Anfrage im Frühjahr 2021 auf die Länderzuständigkeit verwiesen und bekräftigt, dass die kommunal betriebenen Leitstellen (Berufsfeuerwehren, Kreisleitstellen) nicht unter den Regelungsumfang der des BSIG bzw. der KritisV fallen [DBT21]:

*„Frage: Wie viele kommunale Rettungsleitstellen sind nach Ansicht der Bundesregierung Teil der Kritischen Infrastruktur im Sinne des BSI-Gesetzes (BSIG)?*
*Antwort: Hierüber liegen der Bundesregierung keine Kenntnisse vor. Bei den Leitstellen handelt es sich um kommunale Einrichtungen, die nicht von der Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-KritisV) erfasst werden.“*

Im Folgejahr 2022 haben die Medizinrechtler Dittrich und Lippert auf die Beantwortung der parlamentarischen Anfrage Bezug genommen und die fehlenden Vorgaben von Bundesseite kritisiert [DL22]:

*„Integrierte Leitstellen sind zum Schutz der Bevölkerung im Bereich der Daseinsvorsorge unverzichtbar. Deshalb ist es erstaunlich, dass es keine Vorschriften zum Schutz dieser Einrichtungen gegen Angriffe von außen, vor allem im IT-Bereich, zu geben scheint. Dem Bund fehlt die Zuständigkeit zum Erlass entsprechender Vorschriften. Soweit die Länder zuständig sind, fehlen einschlägige Vorschriften überwiegend.“*

Die Thematik IT-Sicherheit im Zusammenhang mit Kritischen Infrastrukturen ist Gegenstand verschiedener Forschungsaktivitäten [Frh22], wobei hier die Energie- und Wasserversorgung, Telekommunikation, Finanzwesen, Verkehrssysteme/ ÖPNV, Logistik und öffentliche Verwaltung im Fokus stehen und die Belange des Notfall- und Rettungswesens einschließlich der Leitstellen bislang keine Beachtung finden. [RS23] [IN23] [Mag20] [KLSB22]

## 2.2 Behörden und Organisationen mit Sicherheitsaufgaben (BOS)

In Deutschland unterliegt die Gefahrenabwehr einer verfassungsmäßigen Aufteilung der Zuständigkeiten von Bund und Ländern. Nach Artikel 30 Grundgesetz (GG) obliegt den Ländern die Ausübung der staatlichen Befugnisse und die Erfüllung staatlicher Aufgaben, sofern das Grundgesetz keine anderweitigen Regelungen trifft. Artikel 70 GG ermächtigt die Länder zur Gesetzgebung, woraus sich auch die Gesetzgebungskompetenz der Länder für das Rettungswesen, den Brand- und Katastrophenschutz sowie die Sicherheits- und Ordnungsaufgaben der Polizei ableitet. Die Gesamtheit dieser Strukturen wird auch als „Innere Sicherheit“ bezeichnet.

Bedingt durch den föderalen Staatsaufbau der Bundesrepublik Deutschland ergeben sich für die verschiedenen BOS unterschiedliche rechtliche, organisatorische und finanzielle Zuständigkeiten für den Bund, die Länder und privatrechtliche (Hilfs-)Organisationen. Damit einher gehen ebenso unterschiedliche Regelungen zu Ausstattung und Betrieb der Leitstellen als kommunikationstechnische Mittelpunkte der Gefahrenabwehr. Die „Leitstellenlandschaft“ ist somit sehr heterogen, was technische Ausstattung, bauliche Struktur, organisatorische Prozesse, personelle Qualifikationen und dadurch auch Vorgaben und die tatsächliche Ausgestaltung der Informationssicherheit betrifft. [TRC22]

### 2.2.1 Polizei

Aufgrund der föderalen Struktur verfügen alle 16 Bundesländer über ein eigenes Polizeigesetz und darauf basierend eigene Polizeibehörden, wobei einerseits zentrale Aufgaben, wie z.B. Technik und Beschaffung sowie Ausbildung (Polizeischulen/-akademien) wahrgenommen werden und andererseits eine flächendeckende Polizeipräsenz durch unterschiedlich ausgeprägte Hierarchie- und Verwaltungsebenen sichergestellt wird.

Für Hilfeersuchen ist die Polizei bundesweit über die Notrufnummer 110 erreichbar, die in der örtlich zuständigen Polizei-Leitstelle aufläuft. Je nach landesrechtlicher Regelung und Struktur variiert der geografische Zuständigkeitsbereich der Leitstelle. [Bok23]

Für die länderübergreifende und internationale Kriminalitätsbekämpfung sowie den Schutz der Außengrenzen der Bundesrepublik Deutschland einschließlich der Sicherheit im Luftverkehr und auf Bahnanlagen liegt Zuständigkeit beim Bund, der hierfür gesonderte Polizeibehörden unterhält. Diese sind das Bundeskriminalamt (BKA) und die Bundespolizei (vormals Bundesgrenzschutz).
Die Polizeibehörden des Bundes besitzen die Gemeinsamkeit, dass sie nicht unmittelbar für Hilfeersuchen aus der Bevölkerung über eine Notrufnummer zu erreichen sind. Die Bundespolizei ist zwar insbesondere für Ereignisse im Bereich von Bahnanlagen telefonisch erreichbar, bezeichnet dies selbst aber als „Hotline“, nicht als Notruf bzw. Notrufnummer und verweist auch darauf, dass in dringenden Fällen der Notruf 110 (zuständige Landespolizeibehörde) zu nutzen ist.

### 2.2.2 Feuerwehr

Analog der Gesetzgebung der Länder im Polizeibereich, gibt es in jedem Land jeweils ein Feuerwehr- bzw. Brandschutzgesetz. In diesen Gesetzen bzw. den nachgelagerten Verordnungen sind für den Einsatz der Feuerwehr sog. *Hilfsfristen* festgelegt, welche die maximale Zeitspanne zwischen dem Eingang eines Notrufs in der Leitstelle und dem Eintreffen vor Ort darstellen. Die Hilfsfristen variieren je nach Bundesland, wobei auch der Zeitpunkt, ab dem die Hilfsfrist beginnt, unterschiedlich festgelegt ist (z.B. Rufsignalisierung des Anrufs, Rufannahme und Gesprächsbeginn oder auch Gesprächsende, wenn alle notwendigen Informationen vom Anrufer vorliegen). [TRC22]

Der abwehrende Brandschutz ist in allen Ländern Aufgabe der Kommunen (Städte, Gemeinden, Ämter) und wird in den Flächenländern überwiegend ehrenamtlich in Form der Freiwilligen Feuerwehren geleistet. In den Großstädten (ab 100.000 Einwohnern) bestehen Berufsfeuerwehren, dies ist in Deutschland in derzeit 114 Städten der Fall. [AGB24] Hinzu kommen Werk- und Betriebsfeuerwehren bei Liegenschaften mit besonderem Gefahrenpotenzial (z.B. Flughäfen, Chemische Industrie, große Produktionsstätten), die ausschließlich für den Brandschutz auf dem Betriebsgelände zuständig sind.

Unabhängig von der Organisationsform ist allen Feuerwehren gemein, dass sie von einer Leitstelle aus alarmiert und unterstützt werden. Die Leitstelle ist als

rückwärtige Führungseinrichtung einer der wichtigsten Ansprechpartner für die Kräfte vor Ort.

### 2.2.3 Rettungsdienst

Ebenso wie im Feuerwehrwesen ist auch der Rettungsdienst in den Rettungsdienstgesetzen der Länder geregelt. Darin werden u.a. die Träger des Rettungsdienstes definiert; dies sind i.d.R. die Kreise und kreisfreien Städte. Der Rettungsdienstträger ist für die Aufstellung und Fortschreibung des Rettungsdienst-Bereichsplans verantwortlich, in dem u.a. die örtliche Verteilung der Rettungswachen im Stadt- bzw. Kreisgebiet und die Art und Anzahl der Rettungsmittel und deren Schichtzeiten festgelegt sind.

In der Öffentlichkeit wesentlich präsenter sind die Rettungsdienst-Leistungserbringer, d.h. die Betreiber von Rettungswachen und den zugehörigen Rettungsmitteln (Fahrzeuge, z.T. auch Luft- und Wasserfahrzeuge). Leistungserbringer sind vor allem die Hilfsorganisationen Arbeiter-Samariter-Bund (ASB), Deutsches Rotes Kreuz (DRK), Johanniter-Unfall-Hilfe (JUH) und Malteser Hilfsdienst (MHD) sowie privatrechtliche Unternehmen. In größeren Städten sind die Berufsfeuerwehren ebenfalls als rettungsdienstliche Leistungserbringer tätig und halten hierfür Fahrzeuge und Personal vor.

Auch für den Einsatz des Rettungsdienstes ist die zuständige Leitstelle der zentrale Ansprechpartner, von der Notrufannahme über die Alarmierung und Einsatzlenkung bis zur Übergabe des Notfallpatienten im Krankenhaus. Ebenso wie für den Einsatz der Feuerwehr bestehen auch für den Rettungsdienst entsprechende Hilfsfristen [TRC22], die – je nach landesrechtlicher Regelung – z.T. mit den Feuerwehr-Hilfsfristen identisch sind, z.T. aber auch davon abweichen.

### 2.2.4 Katastrophenschutz

Der Katastrophenschutz fällt in Deutschland ebenfalls in die Zuständigkeit der Länder (siehe 2.2), die hierzu entsprechende Katastrophenschutzgesetze verabschiedet und ergänzende Verordnungen und Konzepte erlassen haben. Der Begriff der

*Katastrophe* bzw. wann eine Schadenslage als Katastrophe einzustufen ist, ist in den Ländern unterschiedlich definiert bzw. geregelt. Dies rührt von der unterschiedlichen Gefährdung der Länder durch Großschadensereignisse her; die Küstenregionen müssen z.B. für Sturmfluten Vorsorge treffen, während in dies in den Binnenländern nicht von Bedeutung ist. Ebenso müssen die Stadtstaaten als Metropolen aufgrund ihrer Bevölkerungsdichte andere Schwerpunkte im Katastrophenschutz setzen als die Flächenländer. Unabhängig von den länderspezifischen Ausprägungen des Katastrophenschutzes gilt: Im Katastrophenfall und auch unterhalb der Katastrophenschwelle ist die Leitstelle der Mittelpunkt der Kommunikation, was den Eingang von Hilfeersuchen, die Anforderung/Nachforderung von Einsatzmitteln und die Zusammenarbeit mit dem Führungsstab bzw. Katastrophenschutzstab betrifft.

### 2.2.5 Leitstellenarten (organisatorische Zuständigkeit)

Die DIN 13050:2021-10 „Begriffe im Rettungswesen“ definiert eine Leitstelle als *„ständig besetzte Einrichtung zur Annahme von Notrufen und Meldungen sowie zum Alarmieren, Disponieren, Koordinieren und Lenken von Einsatzkräften, sowie zur Erteilung von Hilfshinweisen an Betroffene“*. Diese Definition bezieht sich rein auf das Notfall- und Rettungswesen; da der Ausdruck „Leitstelle“ selbst nicht gesetzlich geschützt ist, findet sich dieser auch bei Verkehrsbetrieben, Energie- und Wasserversorgern, Gebäudemanagement und ähnlich gelagerten Bereichen. Letztere sind jedoch nicht Gegenstand der vorliegenden Betrachtung, sondern der Fokus liegt ausschließlich auf den Leitstellen des Notfall- und Rettungswesens.

Die DIN 13050:2021-10 beschreibt in der Begriffsdefinition die Aufgaben der Leitstellen, nicht jedoch die zur Erfüllung diese Aufgaben benötigte (technische) Ausstattung oder gar Sicherheitsanforderungen.

Im Zusammenhang mit Leitstellen im Bereich des Notfall- und Rettungswesens tauchen in der Fachliteratur und im Sprachgebrauch verschiedene Bezeichnungen auf, die sich sowohl auf die organisatorische Zugehörigkeit als auch auf regionale Zuständigkeit beziehen.

**Polizeileitstellen**

sind die Leitstellen der Polizei, die nur von dieser betrieben werden, den Notruf 110 abfragen und auch nur für die jeweilige polizeiliche Gliederung (z.B. Polizeipräsidium oder -direktion) zuständig sind. [Bok23] [Rüh10]

**Rettungsleitstellen**

bearbeiten nur die Notfallrettung und ggf. auch den Krankentransport. [Mer99] Diesen Leitstellentyp gibt es z.T. noch in Rheinland-Pfalz. Umgangssprachlich werden auch Integrierte Leitstellen (s.u.) häufig als „Rettungsleitstellen“ bezeichnet, was deren Aufgaben und Zuständigkeiten jedoch nicht vollständig abbildet, aber der Abgrenzung gegenüber den Leitstellen der Polizei oder von Verkehrsbetrieben dient.

**Integrierte Leitstellen**

sind die Zusammenführung (Integration) von Rettungs- und Feuerwehrleitstellen; dies ist der häufigste Leitstellentyp in Deutschland; bei fast allen Berufsfeuerwehren und Kreisen vorzufinden. [TRC22] Die DIN 13050:2021-10 definiert „Integrierte Leitstelle“ ergänzend zu „Leitstelle“ allgemein (s.o.) als *„ständig besetzte Einrichtung zur Annahme von Notrufen und Meldungen sowie zum Alarmieren, Koordinieren und Disponieren des Rettungsdienstes, der Feuerwehr, der technischen Hilfe und des Katastrophenschutzes, sowie zur Erteilung von Hilfshinweisen an Betroffene“.*

Für die Tätigkeit in einer Integrierten Leitstelle müssen die Disponenten eine Doppelqualifikation Rettungsdienst und Feuerwehr besitzen; Details hierzu sind jeweils landesrechtlich geregelt. [TRC22]

**Kooperative Leitstellen**

sind der Zusammenschluss aus Integrierten Leitstellen und Polizeileitstellen. Hierbei wird die Infrastruktur (Gebäude und Technik) gemeinsam genutzt. Die Betreiber Land (Polizei) und Kommune(n) für den Rettungsdienst und Brandschutz schließen eine entsprechende Vereinbarung ab, in der der gemeinsame Betrieb und die Kostenaufteilung geregelt sind. Diesen Leitstellentyp gib es derzeit in

Schleswig-Holstein und in Niedersachsen; hierbei werden meist nicht nur ein Kreis, sondern mehrere Kreise bzw. kreisfreie Städte betreut.

Trotz des gemeinsamen Gebäudes und der gemeinsam genutzten Technik sind Polizei und Feuerwehr/Rettungsdienst räumlich getrennt, dies hat vor allem datenschutzrechtliche Gründe. So muss beispielsweise ein Anrufer, der einen medizinischen Notfall in Zusammenhang mit Drogenkonsum meldet, davon ausgehen können, dass dieser Vorgang vertraulich bearbeitet wird (Ärztliche Schweigepflicht, die sich auch auf medizinische Assistenzberufe erstreckt, hier Rettungsassistenten/ Notfallsanitäter als Leitstellendisponenten). Ein Polizeibeamter wäre bei Kenntnis vom Umgang mit Betäubungsmitteln in der Pflicht, Ermittlungen einzuleiten. Ein vollständig gemeinsamer Betrieb – räumlich, technisch und betrieblich – ist aufgrund der rechtlichen Rahmenbedingen in Deutschland derzeit nicht in Sicht.

**Sonstige Leitstellen**

Neben den genannten Leitstellen, die als Notrufabfragestellen unmittelbar für hilfesuchende Bürger über die Rufnummern 110 bzw. 112 erreichbar sind, existieren bei den BOS weiteren Leitstellen, wobei „Leitstelle“ auf Bundesebene weder einheitlich definiert, ist noch einen geschützten Begriff darstellt (s.o.).

In großen Unternehmen mit Werkfeuerwehren existieren ebenfalls Leitstellen [HB23] [Schr10], Einsatzzentralen, Gefahrenabwehrzentralen oder Sicherheitszentralen (Begrifflichkeit variiert je nach Firmenphilosophie), die oftmals auch über die Rufnummer 112 der internen Telefonanlage erreichbar sind. Im Sinne der Technischen Richtlinie Notruf (TR Notruf) ist dies jedoch keine Notrufanschaltung, sondern lediglich eine entsprechend bezeichnete Nebenstelle der Telefonanlage. Neben der Werkfeuerwehr werden vielfach auch der werksinterne Rettungsdienst und/oder auch der Werkschutz von dieser Leitstelle bzw. Zentrale aus koordiniert und unterstützt.

### 2.2.6 Leitstellenarten (geografische Zuständigkeit)

Neben der organisatorischen Zuständigkeit bzw. der Trägerschaft (siehe 2.2.5) wird bei den Begrifflichkeiten z.T. auch die geografische Zuständigkeit zusammen mit dem Wort „Leitstelle“ zum Ausdruck gebracht.

**Kreisleitstellen**

sind für das Gebiet eines Kreises/Landkreises zuständig. Sie sind i.d.R. als Integrierte Leitstellen aufgestellt.

**Regionalleitstellen**

decken mehrere Kreise und/oder kreisfreie Städte ab, so dass diese Bezeichnung hier geläufig ist. [Ban23] In Thüringen ist die Bildung von Regionalleitstellen für Feuerwehr und Rettungsdienst in Planung. In Schleswig-Holstein werden mehrere Regionalleitstellen gemeinsam von der Polizei (Land) und den Kommunen/Kreisen betrieben und tragen daher die Bezeichnung „Kooperative Regionalleitstelle“ (KRLS). [BH23]

**Landesleitstellen**

decken das Gebiet eines Bundeslandes ab. Neben den Stadtstaaten Berlin und Hamburg wird auch das Saarland von nur einer Integrierten Leitstelle abgedeckt. Die Bezeichnung „Landesleitstelle“ ist aber eher theoretischer bzw. konzeptioneller Natur und wird alltäglichen Sprachgebrauch selten verwendet.

## 2.3 Schutzziele, Hilfsfrist

Der Begriff *Schutzziel* wird in verschiedentlicher Definition verwendet; zur Schutzzielbetrachtung im Sinne der Informationssicherheit siehe Abschnitt 2.5. In den landesrechtlichen Vorgaben zum Betrieb einer Leitstelle bzw. zur Aufstellung und örtlichen Abdeckung von Feuerwehrstandorten und Rettungswachen finden sich

ebenso Schutzziele, die sich vor allem in Form der Hilfsfristen darstellen. Hilfsfrist ist die Zeitspanne, die von der Notrufbearbeitung bis zum Eintreffen des Rettungsmittels an der Einsatzstelle als zeitliche Obergrenze festgelegt ist. Die Hilfsfrist unterliegt einer sehr weiten Streuung in den Ländern, wobei ebenso unterschiedlich betrachtet wird, ob die Notrufabfrage und Disposition in der Leitstelle von der Hilfsfrist mit umfasst sind, die Hilfsfrist erst mit der Alarmierung beginnt oder nur die reine Fahrzeit des (ersten) Einsatzfahrzeugs umfasst. [TRC22]

Insgesamt ergeben sich durch die föderalen Strukturen Hilfsfristen von im günstigsten Fall 8 Minuten in den städtischen Bereichen Nordrhein-Westfalens bis hin zur fast doppelt so langen Zeitdauer von 15 Minuten in Niedersachsen oder Rheinland-Pfalz. Im Stadtstaat Hamburg sind per Gesetz gar keine konkreten Fristen mit Minutenangaben festgelegt, sondern lediglich eine „bedarfs- und fachgerechte“ Abdeckung des Gebietes mit Rettungsmitteln. [TRC22]

Die Rettungsdienstgesetze und zugehörigen Verordnungen fordern keine Hilfsfristerfüllung zu 100 %, da dies bedingt durch Paralleleinsätze, weite Anfahrtswege zu abgelegenen Einzelobjekten, schwer erreichbare Einsatzstellen im Wald, Gebirge oder auf Gewässern, Verzögerungen bei der Anfahrt infolge von Baustellen, Straßensperrrungen und Verkehrsstau bis hin zu ungünstigen Witterungsverhältnissen (Starkregen, Eisglätte, Schnee, Nebel) praktisch nicht gewährleistet werden kann. Einige Länder haben eine 90- bzw. 95-prozentige Hilfsfristerfüllung vorgegeben, um den genannten widrigen Begleitumständen Rechnung tragen zu können und somit Rechtssicherheit für die Leitstelle und die Leistungserbringer bei der Nichterfüllung der Hilfsfrist in Einzelfällen zu schaffen.

Sofern die Einsatzdisposition und Alarmierung Bestandteil der Hilfsfrist sind, ist eine korrekt und verzögerungsfrei funktionierende Leitstellentechnik unabdingbarer Bestandteil zur Erfüllung der Hilfsfrist, da die Verantwortung sowohl bei der Leitstelle und den dort zügigen und fehlerfrei ablaufenden Prozessen liegt als auch bei den alarmierten Rettungsmitteln/Einheiten.

## 2.4 Besonderheiten der Kritischen Infrastruktur BOS-Leitstelle

Obwohl die BOS-Leitstellen in der KRITIS-Definition des BSIG und der KritisV keine Erwähnung finden – weder wörtlich noch sinngemäß – sind sie dennoch als Kritische Infrastrukturen anzusehen, da sie sich von anderen Elementen der Gefahrenabwehr grundlegend unterscheiden und die Definition der KRITIS-Strategie erfüllen (*„… bei deren Ausfall oder Beeinträchtigung […] erhebliche Störungen der öffentlichen Sicherheit oder andere dramatische Folgen eintreten würden.“*). [BMI09]

- Eine Leitstelle ist i.d.R. einmal pro Zuständigkeitsgebiet vorhanden. Der Ausfall einer Rettungswache, eines Feuerwehrstandortes (Feuerwache, Feuerwehrhaus) oder einer lokalen Polizeidienststelle mit Personal und Fahrzeugen ist ungünstig und störend, lässt sich aber beherrschen, indem das abzudeckende Gebiet von den Nachbarstandorten aus mitversorgt wird. Dies bringt evtl. Nachteile bei der Erfüllung der Hilfsfrist mit sich, ist aber einem totalen Versorgungsausfall vorzuziehen. Bei den Akutkrankenhäusern gehört es zum Tagesgeschäft, dass sich die Notaufnahme oder bestimmte Funktionsbereiche abmelden und der Rettungsdienst ein anderes Haus ansteuern muss, nachdem die Leitstelle zuvor freie Versorgungskapazitäten abgeklärt hat. Das Ausweichen auf Nachbarbereiche ist hier gelebte Praxis.

  Je nach landesrechtlicher Vorgabe und/oder den finanziellen Möglichkeiten der Leitstellenträger, sind in einigen Ländern Vertretungskonzepte, Leitstellenkooperationen und -vernetzungen etabliert oder im Aufbau befindlich (technisch und auch organisatorisch). Dies ist aber in Deutschland aktuell nicht flächendeckend gegeben.
- Die Leitstelle ist *die* Anlaufstelle für zeitkritische Hilfeersuchen (110/112), diese Aufgabe hebt sie hinsichtlich der Bedeutung für die Gefahrenabwehr von Callcentern und Hotlines deutlich ab. Der Anrufer erwartet eine umgehende Rufannahme und Reaktion; Warteschleifenmusik, automatische Sprachdialogsysteme und rudimentär angelernte Telefonisten stehen einer zügigen und qualifizierten Bearbeitung von Hilfeersuchen entgegen.

- Ein Totalausfall einer Leitstelle, z.B. durch ein Akutereignis (Brand, Gasaustritt, Gefahrstofffreisetzung, Bombenfund, Bedrohungslage), lässt sich oftmals schwer bis gar nicht kompensieren. Ein Umrouten der Notrufe ist über den Leitstellenservice der Deutschen Telekom AG in Meschede zwar möglich, damit kann jedoch primär nur die Notruferreichbarkeit für die Bürger sichergestellt werden. Die Nutzung von Einsatzleitsystem, Alarmplänen, Abwicklung des Funkverkehrs, Anschaltungen von Gefahrenmeldeanlagen, Einsatzdokumentation usw. bleibt damit offen. Eine Kompensation ist nur möglich, wenn die Aufgaben vollumfänglich von einer Partnerleitstelle übernommen werden und hierfür im Vorfeld die technischen, organisatorischen und personellen Voraussetzungen geschaffen worden sind und die Aufgabenübernahme eingeübt und damit jederzeit kurzfristig möglich ist.

Neben den organisatorischen Aspekten unterscheiden sich BOS-Leitstellen von anderen sicherheitsrelevanten Bereichen durch die IT-Systeme und die unterschiedlichen Schnittstellen sowie die enge Verzahnung von Datenverarbeitung und IP-basierter Telekommunikation. Eine Leitstelle kann nicht als gekapseltes System betrieben werden, da die Erreichbarkeit für Notrufe (telefonisch und per App), die Kommunikation mit Einsatzfahrzeugen und der Kontakt zu anderen Dienststellen mehrere öffentlich zugängliche Schnittstellen erfordert.

Die Onlineplattformen von Banken und Versandhändlern, die für ihre Kunden jederzeit und einfach erreichbar sein sollen, müssen sich ebenfalls gegen schädliche Einflussnahme auf ihre IT-Systeme wappnen. In diesen beiden hier beispielhaft genannten Bereichen bestehen bei einem Ausfall oder einer Störung wirtschaftliche Schäden und eine negative Außenwirkung, jedoch keine unmittelbaren Gefahren für Leib und Leben von Menschen. In der IT eines Krankenhauses, mit der Verarbeitung von Patientendaten und der Vernetzung medizintechnischer Geräte, können aus Fehlfunktionen und Ausfällen ebenfalls Gefahren für Leib und Leben von Patienten erwachsen, wenn vernetzte Medizintechnik ausfällt oder unmittelbar bevorstehende Operationen und Behandlungen aufgrund fehlenden Zugriffs auf Patientendaten, Befunde usw. nicht möglich sind. Die Krankenhaus-IT wiederum ist nicht über öffentlich bekannte und beworbene Einwahlnummern oder Apps für jedermann erreichbar, was auch hier den Unterschied zu einer Leitstelle ausmacht. Ähnlich verhält es sich mit sicherheitskritischen Anwendungen beim Militär sowie in

der Luft- und Raumfahrt; hier bestehen abgegrenzte Bereiche, die bewusst nicht für die Öffentlichkeit über Apps bzw. telefonische Einwahl erreichbar sein sollen.

*„Bei sicherheitskritischer Software sind Menschen an Leib und Leben gefährdet, wenn die Software versagen sollte. Die Palette derartiger Applikationen reicht vom Controller für das Triebwerk eines Verkehrsflugzeugs bis zum Herzschrittmacher.“* [Tha19]

Die Leitstelle ist der kommunikative Mittelpunkt für alle BOS und nimmt damit eine Schlüsselfunktion in der Notfallrettung und Gefahrenabwehr ein. Aufgrund der Bedeutung für die Notfallversorgung, die ein sofortiges Reagieren auf Hilfeersuchen erfordert und u.U. über Leben und Tod entscheiden kann, nehmen die Leitstellen mit ihren IT-Systemen organisatorisch wie technisch eine Sonderstellung gegenüber anderen sicherheitsrelevanten Bereichen ein. [Chr23]

## 2.5 Informationssicherheit

Für den Begriff *Sicherheit* gibt es unterschiedliche Definitionen, da neben der Sicherheit von technischen Systemen beispielsweise auch in den Sozialwissenschaften im Kontext von politischen, wirtschaftlichen oder gesellschaftlichen Betrachtungen der Ausdruck Sicherheit häufig Verwendung findet. Im technischen Sinn gilt gemäß DIN 0801 bzw. VDE 31000 folgende Definition:

*„Sicherheit ist eine Sachlage, bei der das Risiko nicht größer als das Grenzrisiko ist.“* [RH08]

*„Das Grenzrisiko ist das größte noch vertretbare Risiko eines bestimmten technischen Vorganges oder Zustandes.“* [GBBK09]

*„Eine absolute Sicherheit ohne jegliches Risiko gibt es weder in der Technik noch in der Natur.“* [GBBK09]

*„Risiko ist das Produkt aus Eintrittswahrscheinlichkeit und Schaden.“* [GBBK09]

Die *Informationssicherheit* bezieht sich übergreifend auf die Sicherheit von informationsverarbeitenden und -speichernden Systemen, um die Schutzziele (auch *Grundwerte* genannt)

- Vertraulichkeit
- Verfügbarkeit
- Integrität

sicherzustellen, entsprechende Risiken zu minimieren, um damit den Geschäftsbetrieb durchgängig zu gewährleisten. „Geschäftsbetrieb“ umfasst hierbei nicht nur kommerzielle Nutzer, sondern auch Regierung, Behörden, Forschungseinrichtungen, NGOs und andere nichtkommerzielle Stellen. Ein Teilbereich der Informationssicherheit ist die *IT-Sicherheit*, die sich ausschließlich auf die Inhalte fokussiert, die mittels IT gespeichert und verarbeitet werden; *Informationssicherheit* ist globaler gefasst und beinhaltet ebenso die nichttechnische Sicherheit von Information, z.B. in Form von Papierakten und dem Wissensstand der Mitarbeiter. Die Forderung nach „Informationssicherheit“ bestand bereits in der Antike, da es schon immer galt, bestimmte Informationen geheim zu halten, sicher vom Sender zum Empfänger zu transportieren und nur einem begrenzen Personenkreis zugänglich zu machen. Die IT-Sicherheit hingegen hat erst mit der Einführung der elektronischen Datenverarbeitung ab der zweiten Hälfte des 20. Jahrhunderts Bedeutung erlangt. Umgangssprachlich werden die Begriffe „Informationssicherheit“ und „IT-Sicherheit“ oftmals synonym verwendet.

Die *Vertraulichkeit* als Schutzziel bedeutet, dass Informationen nur von berechtigten Nutzern gelesen oder bearbeitet werden können. Dies betrifft sowohl Kommunikationsvorgänge (Datenaustausch) als auch den Zugriff auf gespeicherte Daten.

*Eine Information ist vertraulich, wenn sie nur von berechtigten Subjekten einsehbar ist.* [GBBK09]

Die *Verfügbarkeit* hat die Sicherstellung des technischen Betriebs mit der Datenbereitstellung zum Ziel, so dass ein jederzeitiger Zugriff gewährleistet ist und keine Ausfall- oder Wartezeiten entstehen. Bei einer BOS-Leitstelle kommt der Verfügbarkeit der technischen Systeme eine besondere Bedeutung zu.

*„Eine Information ist verfügbar, wenn sie abgerufen werden kann, wenn sie von berechtigten Objekten/Subjekten gebraucht wird.“* [GBBK09]

Hinter der Sicherstellung der *Integrität* verbirgt sich die Anforderung, dass Daten nicht manipuliert werden können bzw. dass alle Bearbeitungen nur durch berechtigte Nutzer erfolgen und eindeutig anhand einer Historie nachvollziehbar sind.

*„Eine Information ist integer, wenn sie so gelesen werden kann, wie sie zuletzt befugt gespeichert wurde.“* [GBBK09]

Neben diesen drei Hauptzielen gibt es weitere Sicherheitsziele [PP10]:

- Authentisierung
- Nichtzurückweisbarkeit
- Resilienz

Die *Authentisierung* bezieht sich auf die Echtheit und deren Überprüfbarkeit von Nutz- und/oder Zugangsdaten. [Sta20]

Die *Nichtzurückweisbarkeit* dient dazu, dass Handlungen (Dateneingaben) nicht abgestritten werden können: dies ist vor allem bei elektronisch getätigten Vertragsabschlüssen und ähnlichen Vorgängen mit rechtlicher Relevanz (z.B. Online-Shopping und -Banking) von Bedeutung. [Gor14]

Die Forderung der *Resilienz* (Belastbarkeit) wird von der Datenschutz-Grundverordnung (DSGVO) [DSG18] in Artikel 32 erhoben; IT-Systeme und -Dienste müssen widerstandsfähig gegen Ausspähungen, Störungen und Sabotagen sein. Neben einer resilienten Datenhaltung – z.B. durch Maßnahmen zur Datensicherheit (siehe 2.5.1) – muss ein resilientes System bei einer Störung selbständig in den Normalzustand zurückkehren, z.B. mittels vordefinierter Prozesse zur Aktivierung von Rückfall-Systemkomponenten, die im Regelbetrieb Stand-by betrieben werden, aber jederzeit in den Vollbetrieb gehen können und gegenüber den Benutzern keine Bedienunterschiede aufweisen. Näheres hierzu siehe Abschnitt 3.6.

In Deutschland ist das BSI die federführende Behörde, die für die IT-Sicherheit der Bundesregierung und -verwaltung zuständig ist, sowie Behörden, Wirtschaft und Bürger in Fragen der IT-Sicherheit berät. Zu den bekanntesten Publikationen gehört hierbei der IT-Grundschutz nach den BSI-Standards 200-1 bis 200-4. Des Weiteren ist das BSI im Rahmen der öffentlich-privaten Kooperation *Umsetzungsplan Kritische Infrastrukturen* (UP KRITIS) mit den besonderen Anforderungen an die IT-Sicherheit Kritischer Infrastrukturen befasst, wobei der Sektor *Staat und*

*Verwaltung* mit dem Notfall- und Rettungswesen und Katastrophenschutz nicht Bestandteil der KritisV ist und daher mangels rechtlicher Grundlage nicht die Beachtung findet, die den anderen KRITIS-Sektoren zuteilwird (siehe 2.1). Seit Jahresbeginn 2021 existiert zudem ein IT-Grundschutzprofil für BOS-Leitstellen [GSP23], dessen Grundlagen im Rahmen einer Master-Thesis gelegt worden sind. [Schm20] Die IT-Sicherheit in einer BOS-Leitstelle, dargestellt am Beispiel der Leitstelle Ostthüringen in Gera, war im Jahr 2018 Gegenstand einer Studie der Universität der Bundeswehr München:

*„Der Alarmierungsprozess vom Absetzen eines Notrufs bis zur Alarmierung der Rettungskräfte muss auch bei Ausfall von IT-Komponenten möglich sein. […] Die IT-Infrastruktur der Zentralen Leitstelle Ostthüringen muss im Spannungsfeld zwischen neuen Anforderungen, einer Diskussion der strategischen Weiterentwicklung, limitierten Ressourcen der Kommunen weiterentwickelt werden. Hochverfügbarkeit des Alarmierungsprozesses ist für die IT ein zentrales Thema.“* [GRH18]

### 2.5.1 Begriffsdefinitionen

Neben der Informationssicherheit bzw. IT-Sicherheit gibt es weitere Begriffe, die in engem Zusammenhang hierzu stehen, aber andere Ziele verfolgen bzw. auf anderen Rechtsgrundlagen beruhen:

*Datenschutz* bezieht sich auf den Schutz personenbezogener Daten vor missbräuchlicher Kenntnisnahme und Verwendung. Rechtliche Basis hierfür ist die informationelle Selbstbestimmung aller Bürger, die das Bundesverfassungsgericht im Zusammenhang mit dem sog. „Volkszählungsurteil“ im Jahr 1983 festgestellt hat. [BVG83] Damit personenbezogene Daten erhoben, gespeichert und verarbeitet werden dürfen, ist die Zustimmung des Betroffenen erforderlich; ausgenommen hiervon sind gesetzlich festgelegte Anwendungsfälle, wie z.B. Einwohnermelderegister, polizeiliche Ermittlungen und auch die automatische Anzeige und Aufzeichnung von Notrufdaten in einer BOS-Leitstelle (Details siehe 2.6.1.2 und 2.6.1.7). Der Datenschutz ist in Deutschland durch die Datenschutz-Grundverordnung (DSGVO) [DSG18], das Bundesdatenschutzgesetz (BDSG) [BDS18], und die Datenschutzgesetze der Länder geregelt und zielt sowohl auf technische als auch auf organisatorische und personelle Maßnahmen ab. Ein wichtiger Aspekt des

Datenschutzes ist die *Datensparsamkeit* (auch *Datenminimierung* oder *Datenvermeidung* genannt), d.h. es sollen nur die Daten erhoben, verarbeitet und gespeichert werden, die tatsächlich für die jeweilige Aufgabenerfüllung erforderlich sind. Die Erhebung und Verarbeitung von Daten, die keine persönlichen Informationen enthalten, unterliegt nicht den Datenschutzanforderungen, können aber aufgrund anderer Vorgaben ebenso schützenswert sein.

*Datensicherheit* ist das technisch umzusetzende Ziel, um Daten vor Verlust oder Manipulation zu schützen, d.h. die Datensicherheit zielt auf die Schutzziele „Integrität“ und „Resilienz“ ab. Eine wichtige Maßnahme zur Umsetzung der Datensicherheit ist die Anfertigung von Sicherungskopien (als physischer Datenträger zur Aufbewahrung an einem geografisch anderen Ort bzw. Cloudspeicher) [APT17]; dies wird als *Datensicherung* bezeichnet.

Der *Geheimschutz* ist der Schutz von Informationen, die im staatlichen Interesse liegen und bei Bekanntwerden eine Gefahr für die Sicherheit eines Staates oder Teilen davon darstellen. Dokumente mit vertraulichen Inhalten erhalten eine Einstufung nach der Verschlusssachen-Verordnung. Hiervon abzugrenzen sind Betriebs- und Geschäftsgeheimnisse (z.B. Geschäftsbeziehungen, laufende Projekte, Entwicklungsergebnisse usw.) der Privatwirtschaft. Betriebs- und Geschäftsgeheimnisse können zugleich den Geheimschutzanforderungen des Staates unterliegen, wenn es um die Projekte staatlicher Stellen (insbesondere Regierung, Sicherheitsbehörden, Militär) handelt, bei denen privatwirtschaftliche Unternehmen bei der Planung und Ausführung involviert sind. Der Schutz dieser vertrauenswürdigen Informationen beinhaltet sowohl technische Maßnahmen und ist damit eng mit der IT-Sicherheit verknüpft als auch personelle Maßnahmen (z.B. Tätigwerden erst nach erfolgter Sicherheitsüberprüfung).

Der *Sabotageschutz* bzw. in Langform *vorbeugender personeller Sabotageschutz* (vpS) bezieht sich auf Maßnahmen, um sicherheitskritische Bereiche von Ministerien und obersten Bundes- bzw. Landesbehörden, die als *Lebenswichtige Einrichtungen* klassifiziert sind, vor Innentätern (Saboteuren) zu schützen. Außerhalb von Regierung und Verwaltung (öffentlicher Bereich) erlangt der vpS auch im nichtöffentlichen Bereich Bedeutung bei Unternehmen und Organisationen oder Teilen davon, die ebenso als Lebenswichtige Einrichtungen klassifiziert sind. Dies sind z.B. Unternehmen, die Telekommunikationsdienstleistungen für die Regierung und bestimmte Bundesbehörden unterhalten sowie für die überregionale

Energieversorgung zuständig sind und/oder verteidigungswichtige Einrichtungen mit Material versorgen oder bei deren Instandhaltung mitwirken. Grundlage des vpS ist das *Gesetz über die Voraussetzungen und das Verfahren von Sicherheitsüberprüfungen des Bundes und den Schutz von Verschlusssachen* (Sicherheitsüberprüfungsgesetz, SÜG) [SÜG21]. Die Einstufung von Behörden und Unternehmen bzw. Teilen davon als Lebenswichtige Einrichtungen überschneidet sich in vielen Fällen mit der Einstufung als *Kritische Infrastruktur* (siehe 2.1), wobei hier unterschiedliche Rechtsgrundlagen Anwendung finden.

### 2.5.2 Verschlüsselung

Die Wissenschaft, die mit der Ver- und Entschlüsselung befasst, ist die *Kryptologie*, diese gliedert sich in die *Kryptographie* (Ver- und Entschlüsselung) und die *Kryptoanalyse* (Brechen von Verschlüsselungen). [PP10] Die Kryptographie beschäftigt sich damit, sichere Algorithmen für die Ver- und Entschlüsselung zu entwickeln und zu optimieren, während sich die Kryptoanalyse mit dem Brechen von Verschlüsselungen befasst; beide Themenfelder sind eng miteinander verknüpft, da zum Nachweis sicherer Kryptoverfahren auch die Prüfung auf Kompromittierung gehört. Zudem befassen sich Sicherheitsbehörden, Geheimdiensten und Militär und ebenso Kriminelle mit dem Brechen von Verschlüsselungen, um sich informationelle oder wirtschaftliche Vorteile zu verschaffen Die beiden Betätigungsfelder Kryptographie und Kryptoanalyse stehen in einem permanenten Wettlauf zueinander, bei dem die eine Seite versucht, sichere und dennoch praktikable Kryptoverfahren zu entwickeln (Kryptographie) und die andere Seite versucht, genau diese Verfahren zu überlisten und die chiffrierten Information als Klartext sichtbar zu machen bzw. im eigenen Sinne zu verändern (Kryptoanalyse).

Die Anforderung, bestimmte Informationen vertraulich zu behandeln und nur für den Absender und den Empfänger zugänglich zu machen, bestand bereits in der Antike. Im alten Rom fand die nach Julius Cäsar benannte *Cäsar-Chiffre* Anwendung. Hierbei werden alle Buchstaben des Alphabets um eine feste Stelle verschoben, so dass z.B. bei einer Verschiebung um vier Stellen der Buchstabe *A* auf *E* abgebildet wird, *M* auf *P* usw. Die Cäsar- bzw. Verschiebechiffre hat jedoch einen entscheidenden Nachteil: Die Häufigkeit der Buchstaben von *A* bis *Z* in einem Text

unterliegt einer bestimmten statistischen Verteilung; diese variiert je nach Sprache. So kommt z.B. der Buchstabe *E* im Deutschen wie im Englischen am häufigsten vor; die übrigen Buchstaben des Alphabets folgen entsprechend. Das *Y* steht im Englischen an 16. Stelle, im Deutschen an 25. Stelle. Wenn die Sprache des verschlüsselten Textes bekannt ist, ist es mittels einer Häufigkeitsanalyse sehr einfach, die chiffrierten Zeichen den entsprechenden Klartext-Buchstaben zuzuordnen und damit den gesamten Text in Klarschrift vorliegen zu haben. Eine Verschiebechiffre ist zur sicheren Verschlüsselung daher absolut ungeeignet. [PP10]

Die moderne Kryptographie gliedert sich in drei Gebiete:

- Symmetrische Kryptographie
- Asymmetrische Kryptographie
- Protokolle

Die *symmetrische Kryptographie* basiert darauf, dass Sender und Empfänger einer Nachricht den gleichen Schlüssel zur Ver- und Entschlüsselung verwenden. [BSW15] Symmetrische Algorithmen waren von der Antike (z.B. Cäsar-Chiffre, s.o.) bis in die 1970er Jahre Standard in der Kryptographie.
Eine grundlegende Voraussetzung für die vertrauliche Kommunikation ist ein sicherer Kanal oder eine sichere Schlüsselerzeugung, so dass der Schlüssel nur den berechtigten Kommunikationspartnern bekannt ist. Modellhaft wird die Kommunikation zwischen Sender und Empfänger wie folgt dargestellt:

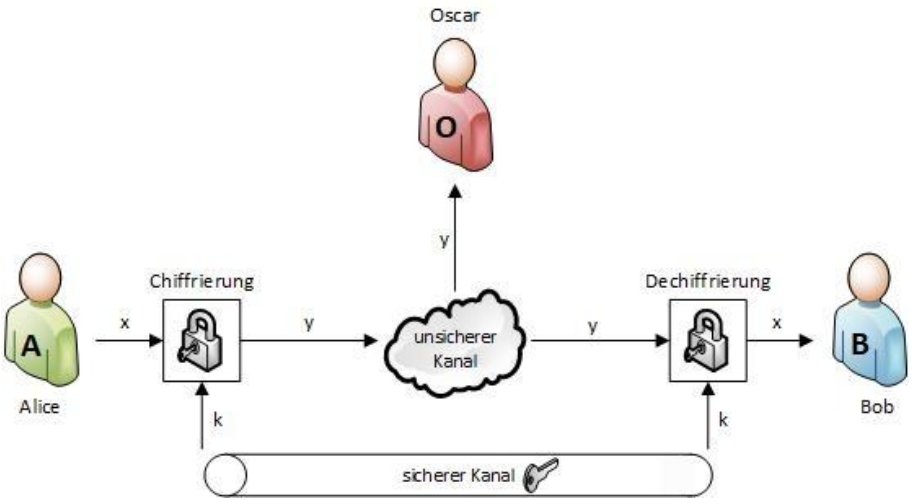



Abb. 2.2: symmetrische Kryptographie zwischen Alice und Bob

Die beiden Kommunikationspartner *A* und *B* werden namentlich als Alice und Bob bezeichnet [PP10] und entsprechen damit den in der Telekommunikation üblichen Bezeichnungen *A*- und *B-Teilnehmer*. Alice möchte eine Nachricht *x* an Bob schicken; die Nachricht *x* wird mit dem Schlüssel *k* verschlüsselt und liegt anschließend als Chiffrat *y* vor, so dass eine Übertragung über einen unsicheren Kanal möglich ist, ohne dass Fremde (hier: Oscar) vom Inhalt der Nachricht Kenntnis erlangen können. Bob benötigt den gleichen Schlüssel *k* (symmetrische Kryptographie), um das bei ihm ankommende Chiffrat *y* zu entschlüsseln und die Klartext-Nachricht *x* lesen zu können. Damit Alice den Schlüssel *k* an Bob übermitteln kann bzw. beide sich auf einen gemeinsamen Schlüssel *k* verständigen können, ist ein sicherer Kanal erforderlich, der unabhängig vom unsicheren Kanal ist. Der sichere Kanal dient allein dem Schlüsselaustausch und soll nicht den unsicheren Kanal ersetzen, der idealerweise schneller ist und über eine größere Bandbreite zur Übertragung der Nutzinformationen verfügt. Statt eines gesonderten, sicheren Kanals zum Schlüsselaustausch ist auch eine Schlüsselvereinbarung nach Diffie-Hellman (asymmetrisches Verfahren) möglich.

Mathematisch lässt die Verschlüsselung (engl. *encryption*, *e*) der Nachricht *x* mit dem Schlüssel *k* zum Chiffrat *y* folgendermaßen ausdrücken:

$$y = e_k(x)$$

Auf der Empfängerseite findet die Entschlüsselung (engl. *decryption*, *d*) statt:

$$x = d_k(y)$$

Ein fundamentaler Grundsatz der Kryptographie ist das *Kerckhoffs'sche Prinzip* (benannt nach dem niederländischen Kryptologen Auguste Kerckhoffs):

*„Eine kryptographische Lösung muss auch dann noch sicher sein, wenn der Angreifer alle Details des Kryptosystems kennt, mit der Ausnahme des Schlüssels. Insbesondere muss das Verfahren auch dann sicher sein, wenn dem Angreifer der Ver- und Entschlüsselungsalgorithmus bekannt sind."* [PP10]

D.h. für Oscar dürfen sowohl die Tatsache, dass überhaupt ein Nachrichtenaustausch zwischen Alice und Bob stattfindet als auch das Chiffrat *y* sowie das Verschlüsselungsverfahren bekannt werden, solange er nicht den Schlüssel *k* erlangt. Dieser Grundsatz ist für die Sicherheit von Kryptoalgorithmen von entscheidender

Bedeutung: Wenn der Algorithmus an sich bekannt ist und die Sicherheit nur von der Geheimhaltung des Schlüssels abhängt, kann der Algorithmus in der Fachwelt untersucht werden, ob die Verschlüsselung ohne Kenntnis des Schlüssels sicher ist und nicht gebrochen werden kann. Ähnlich verhält es sich mit einem mechanischen Türschloss: Der prinzipielle Aufbau und die Funktionsweise von Zylinderschlössern sind bekannt und z.T. sogar genormt. Die Sicherheit basiert allein auf dem Besitz des zugehörigen Schlüssels durch berechtigte Personen.

In der Kryptographie basiert die Sicherheit auf der Geheimhaltung des Schlüssels *k* und dessen sicherer Übermittlung über den sicheren Kanal. Aus dem Alltag ist diese Vorgehensweise beim Erhalt einer neuen Bank-/Kreditkarte bekannt: Unabhängig vom Postversand der neuen Karte wird die Persönliche Identifikationsnummer (PIN) separat und mit zeitlichem Versatz per Post versandt. Ein Angreifer müsste sowohl die Karte als auch die PIN abfangen, um Zahlungen tätigen zu können. D.h. der sichere Kanal ist hier der separate Versand, auch wenn die Übertragungswege (hier: Postweg) identisch sind.

Falls der als Oscar bezeichnete Angreifer in den Besitz des Schlüssels k gelangen sollte, kann er sowohl die vertrauliche Kommunikation *x* zwischen Alice und Bob mitlesen als auch verändern und chiffrierter Form *y'* über den unsicheren Kanal an Bob leiten, so dass dieser einen veränderten Klartext *x'* erhält (Abbildung 2.3).

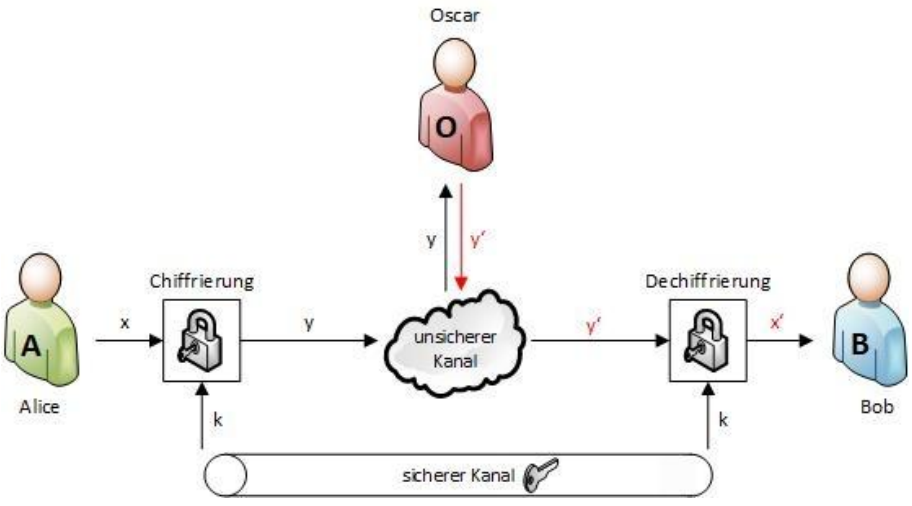



Abb. 2.3: Manipulation der Nachricht durch Oscar

In diesem Fall sind die Schutzziele der Vertraulichkeit und der Integrität untergraben; Vertraulichkeit ist nicht mehr gegeben, wenn Oscar die Nachricht

entschlüsseln und mitlesen kann, die Integrität ist hinfällig, wenn Oscar die Nachricht verändert und Bob nicht die von Alice versandte Originalnachricht zugestellt bekommt.

Bei der Verschlüsselung werden *Stromchiffren* und *Blockchiffren* unterschieden. [Buc16] Stromchiffren verschlüsseln jedes Bit einzeln, dabei ist keine Mindestlänge eines Blocks erforderlich, so dass die Verschlüsselung in Echtzeit erfolgen kann. Für die Erzeugung des Schlüsselstroms sind Zufallsgeneratoren (Random Number Generators, RNG) erforderlich. Alternativ kann ein *One Time Pad* (OTP) genutzt werden [PP10], das sich durch eine besondere kryptographische Sicherheit auszeichnet, da jedes Schlüsselstrombit nur für die Verschlüsselung eines Klartextbits verwendet wird und keine Wiederholung der Schlüsselbits stattfindet. Nachteilig hierbei ist, dass der Schlüssel genauso lang wird wie der Klartext, was ein aufwändiges Schlüsselmanagement erforderlich macht.

Bei den Blockchiffren haben sich die Verfahren *Data Encryption Standard* (DES) bzw. dessen Nachfolger *Advanced Encryption Standard* (AES) etabliert. DES ist die älteste Blockchiffre mit einer Blocklänge von 64 Bit und einer Schlüssellänge von 56 Bit, d.h. mit einer DES-Operation können 64 Klartextbits verschlüsselt werden. Grundlage von DES ist ein Feistel-Netzwerk, bei dem die Klartextblöcke in zwei Hälften aufgeteilt und in mehreren Schritten (Runden) verarbeitet werden. Mit der heutigen Rechentechnik kann DES mittels *Brute Force* („automatisiertes Ausprobieren aller Möglichkeiten“) hinsichtlich möglicher Treffer gebrochen werden. Abhilfe bietet Triple-DES (3DES), d.h. es werden nacheinander drei DES-Operationen mit drei verschiedenen Schlüsseln $k_1$, $k_2$ und $k_3$ durchgeführt.

Nachfolger von DES ist der *Advanced Encryption Standard* (AES), der mit einer Blocklänge von 128 Bit und Schlüssellängen von 128, 192 oder 256 Bit arbeitet. Im Gegensatz zu DES dient bei AES nicht ein Feistel-Netzwerk als Grundlage, sondern es kommen Rechenoperationen, die auf *Endlichen Körpern* (Galois Fields, GF) basieren, zur Anwendung. Endliche Körper als Mengenbegriff sind eine endliche Menge von Elementen, für die die vier Grundrechenarten gelten, z.B. reelle Zahlen $\mathbb{R}$ und komplexe Zahlen $\mathbb{C}$. AES kommt z.B. bei der Ende-zu-Ende-Verschlüsselung des Digitalfunks (siehe 2.6.7.1) und bei der *Transport Layer Security* (TLS) zur Anwendung.

Die *asymmetrische Kryptographie* brachte ab Mitte der 1970er Jahre gegenüber der symmetrischen Kryptographie eine wegweisende Neuerung, da hiermit das Problem der Schlüsselverteilung gelöst werden konnte. Es kommen zwei Schlüssel zum Einsatz, ein öffentlicher Schlüssel ($k_{pub}$) zur Verschlüsselung und ein geheimer Schlüssel ($k_{priv}$) zur Entschlüsselung. Mathematisch basiert die asymmetrische Kryptographie auf folgenden Ansätzen [PP10]:

- Faktorisierungsproblem: Die Multiplikation zweier großer Primzahlen $\mathbb{Z}$ ist rechnerisch einfach, aber die Faktorisierung (Primfaktorzerlegung) des Produkts ist sehr schwierig. Dies ist Grundlage des *RSA-Kryptosystems* (benannt nach den Anfangsbuchstaben der Nachnamen der drei Entwickler Ronald Rivest, Adi Shamir und Leonard Adleman). RSA ist das dominierende asymmetrische Verfahren, das z.B. für Zertifikate und Signaturen sowie den sicheren Schlüsselaustausch verwendet wird, nicht jedoch für die eigentliche Verschlüsselung. Die Verschlüsselungsanwendung *Pretty Good Privacy* (PGP), die bei der E-Mail-Kommunikation genutzt werden kann, basiert ebenfalls auf RSA.
- Diskretes Logarithmusproblem (DLP): Die diskrete Exponentialfunktion $f(x) = b^x \; mod \; p$ ist in gewissen zyklischen Gruppen eine Einwegfunktion, d.h. sie ist selbst für große Exponenten effizient berechenbar, jedoch ist umgekehrt der diskrete Logarithmus nicht durch schnellen Algorithmus zur Bestimmung des Exponenten *x* berechenbar, wenn die Basis $b$, der Modul $p$ und $f(x)$ gegeben sind. Das Prinzip des DLP kommt beim Schlüsselaustausch nach *Diffie-Hellman* bzw. *ElGamal* zur Anwendung. Der Schlüsselaustausch nach Diffie-Hellman wird z.B. bei IPSec und TLS genutzt (s.u.); die eigentliche Verschlüsselung erfolgt dann mittels AES oder 3DES.
- Elliptische Kurven (Verallgemeinerung des Diskreten Logarithmusproblems)

Gegenüber der symmetrischen Kryptographie benötigt die asymmetrische Kryptographie größere Schlüssellängen, da die Sicherheit der Kombination aus öffentlichem und geheimem Schlüssel auf mathematischen Einwegfunktionen beruht. Diese sind nur dann nicht umkehrbar (bzw. mittels Brute Force ermittelbar), wenn die Schlüssel entsprechend lang sind.

Um die Nachrichtenintegrität, -authentisierung sowie die Nichtzurückweisbarkeit von Nachrichten sicherzustellen, kommen *Signaturen* zur Anwendung. Signaturen dienen als „digitale Unterschrift“, um die Echtheit einer Nachricht verifizieren zu

können. Zur Bildung einer Signatur wird der *Hash-Wert* der Nachricht gebildet und mit dem privaten Schlüssel signiert. Die Überprüfung der Signatur ist mit Hilfe des öffentlichen Schlüssels für jedermann möglich. Durch die Bildung des Hash-Wertes ist auch die Signatur vom Nachrichteninhalt abhängig, d.h. eine Signatur allein (ohne Nachrichteninhalt) ist nutzlos.

Damit eine Signatur nicht so lang wird wie der Nachrichteninhalt, kommt der Hash-Funktion eine wichtige Bedeutung zu. Aus der Nachricht wird – unabhängig von deren Länge – ein Hash-Wert gebildet, dessen Länge vorgegeben ist. Unterschiedlich lange Nachrichten ergeben Hash-Werte stets gleicher Länge. Dabei ist die Einwegfunktion von besonderer Bedeutung; anhand des Hash-Wertes darf kein Rückschluss auf die Nachricht möglich sein, dies wird als *Urbildresistenz* bezeichnet. [Schw14] Zudem darf es zu einer gegebenen Nachricht $x_1$ nicht möglich sein, eine zweite Nachricht $x_2$ zu finden, welche den gleichen Hash-Wert besitzt, wie $x_1$. Diese Eigenschaft wird als *Zweite Urbildresistenz* bzw. *Schwache Kollisionsresistenz* bezeichnet. Hinzu kommt die *Starke Kollisionsresistenz*, d.h. es darf nicht möglich sein, zwei verschiedene Nachrichten $x_1$ und $x_2$ zu finden, die den gleichen Hash-Wert erzeugen. Hash-Funktionen spielen eine wichtige Rolle bei der Speicherung von Passwörtern auf Servern. Anhand der abgelegten Hash-Werte der Passwörter ist kein Rückschluss auf die tatsächlichen Zeichenfolgen der Passwörter möglich. Bei der Anmeldung eines Users wird aus dem eingebenden Passwort der Hash-Wert gebildet und mit dem gespeicherten Hash-Wert verglichen; das tatsächliche Passwort im Klartext wird nicht gespeichert.

Zu Modellierung dient das *Random-Oracle-Modell* (ROM) dem mathematischen Beweis der Sicherheit von kryptographischen Verfahren, da sich der Sicherheitsgewinn einer Einwegfunktion in einem Kryptosystem analytisch nur schwer abschätzen lässt. Abhilfe schafft das ROM, bei dem ein konkretes Kryptosystem (Standard-Modell) durch eine idealisierte Zufallsfunktion modelliert wird, die durch Nutzung eines Orakels (Black Box) ausgewertet wird. [Rei21] Sofern der Sicherheitsnachweis für die untersuchte Kryptofunktion im ROM erfolgreich ist, so kann daraus geschlussfolgert werden, dass dies auch im konkreten Anwendungsfall (Standard-Modell) gilt, wenn die Einwegfunktion durch eine gute pseudozufällige Funktion ersetzt wird. Sollten sich hingegen Sicherheitslücken im ROM zeigen, weist dies auf eine strukturelle Schwäche des Kryptosystem hin, so dass bei einer Realisierung im Standard-Modell keine hohe Sicherheit erwartet werden kann. [BR93]

Um User bzw. Softwareanwendungen zu authentifizieren, können auch *Zertifikate* eingesetzt werden; diese kommen häufig als Public-Key-Zertifikate zur Anwendung. Dabei wird ein öffentlicher Schlüssel zusammen mit einer Identifikation (ID) genutzt und daraus das Zertifikat gebildet. Zur Organisation der Zertifikate (Erzeugung, Verteilung) muss eine Zertifizierungsstelle (*Certificate Authority*, CA) als zentrale, vertrauenswürdige Instanz vorhanden sein. [Schw14] Um kompromittierte oder nicht mehr gültige Zertifikate erkennen zu können, muss es eine entsprechende Zertifikatssperrliste (*Certificate Revocation List*, CRL) geben. [BNS10] [PP10]

Neben der symmetrischen und der asymmetrischen Kryptographie gibt es als drittes großes Gebiet der kryptographischen Anwendungen die *Protokolle*.

Eine wichtige Sicherheitsanwendung auf Protokollebene ist *IPSec*, das auf dem Layer 3 (Vermittlungsschicht) des OSI-Modells arbeitet. Hierbei sind zwei Datenformate spezifiziert, *Authentication Header* (AH) und *Encapsulation Security Payload* (ESP). Der AH dient dem Schutz der Integrität eines IP-Paket, da er ein Verändern von Absender- und Zieladresse verhindert, so dass das Datenpaket auf dem Weg vom Absender zum Empfänger nicht zwischendurch manipuliert werden kann, beispielweise durch IP-Spoofing (siehe 2.5.3.2). D.h. mit AH wird das Schutzziel der Integrität gewährleistet. Der ESP dient der verschlüsselten Übertragung des Paketinhalts; zur Schlüsselverwaltung dient das Protokoll *Internet Key Exchange* (IKE), welches den Diffie-Hellman-Schlüsselaustausch nutzt. IPSec kann im Transport- und im Tunnelmodus betrieben werden. Im Transportmodus wird nur die Nutzlast des IP-Pakets geschützt (Nutzdaten und TCP-Header), während im Tunnelmodus das gesamte IP-Paket (incl. des IP-Headers) geschützt wird und als Nutzlast in ein übergeordnetes IP-Paket eingefügt (gekapselt bzw. „getunnelt“) wird, so dass IPSec auf das gesamte Paket angewandt wird. D.h. ESP im Tunnelmodus ist die bedeutsamste Form von IPSec. [Schw14]

Die *Transport Layer Security* (TLS, bzw. vormals *Secure Sockets Layer*, SSL) arbeitet auf der Schicht 5 (Sitzung) des OSI-Modells. Beim Verbindungsaufbau eines Clients zum Server muss sich der Server gegenüber dem Client mittels eines Zertifikats authentifizieren. Der Client überprüft die Vertrauenswürdigkeit und es erfolgt ein Schlüsselaustausch nach Diffie-Hellman. Ein abgeleiteter kryptografischer Schlüssel wird anschließend genutzt, um den Datenverkehr zwischen Server und Client symmetrisch zu verschlüsseln. Ergänzend werden die Schutzziele Integrität und Authentizität mittels *Message Authentication Code* (MAC) gewährleistet. Die

am weitesten verbreitete Anwendung von TLS ist das *Hypertext Transfer Protocol Secure* (HTTPS).

Um Angriffe auf das *Domain Name System* (DNS) zu unterbinden, wurde die Erweiterung *Domain Name System Security Extensions* (DNSSEC) entwickelt. [Schw14] Als Angriffsszenarien kommen hier z.B. Spoofing (Verfälschen der eigenen Identität), Man-in-the-Middle-Angriffe (Veränderung von Datenpakten, Anfrage abfangen und gefälschte Antwort senden) und Kompromittierung von DNS-Servern in Frage. DNSSEC sichert die Kommunikation zwischen Client und DNS-Server. Das mehrschichtige DNSSEC-Protokoll verifiziert nacheinander die Zonen „www“, die eigentliche Adresse und die Topleveldomain, um hier Sicherheit zu schaffen. DNSSEC bietet allerdings wie viele andere Verfahren keine absolute Sicherheit, da es z.B. DoS-Attacken (siehe 2.5.3.1) auf den Nameserver nicht verhindern kann.

Für die sichere Kommunikation per E-Mail kommen spezielle Verfahren zum Einsatz, am bedeutsamsten sind *Pretty Good Privacy* (PGP) und *Secure/Multipurpose Mail Extensions* (S/MIME). [Schw14] Mittels PGP können Nachrichten sowohl nur signiert, nur verschlüsselt als auch signiert und verschlüsselt werden. PGP bedient sich dabei sowohl symmetrischer als auch asymmetrischer Verschlüsselung (hybride Verschlüsselung), da der Nachrichteninhalt symmetrisch verschlüsselt wird, während der zugehörige Schlüssel selbst asymmetrisch verschlüsselt wird. MIME (*Multipurpose Mail Extensions*) erweitert die ursprünglich reine Text-E-Mail im Zeichensatz (z.B. Umlaute) und ermöglicht Dateianhänge, was der aus dem Alltag bekannten E-Mail-Kommunikation entspricht. S/MIME arbeitet in der Anwendungsschicht (Layer 7 / Application Layer des OSI-Modells), d.h. ist Bestandteil von E-Mail-Programmen bzw. kann diesen als ergänzendes Sicherheitsfunktion hinzugefügt werden. Neben einer hybriden Verschlüsselung kommen bei S/MIME auch Signaturen und Zertifikate zum Einsatz.

### 2.5.3 Bedrohungsszenarien

Bei der IT-Sicherheit in vernetzten Systemen – wozu auch die IT-Systeme in einer Leitstelle zählen – ist eine Vielzahl an Angriffsszenarien denkbar. [RL18] [GM18] Ein möglicher Weg ist das Herbeiführen einer Überlastsituation, wobei der

Angreifer versucht, das Zielsystem durch eine Vielzahl zeitgleicher Anfragen außer Kraft zu setzen, ohne dass hierfür Schadcode in das Zielsystem eingeschleust werden muss. Andere Angriffsszenarien erfordern das Einschleusen von Schadcode, was auf verschiedenen Wegen erfolgen kann und unterschiedliche Auswirkungen auf das Zielsystem haben kann, z.B. unbemerktes Abgreifen von Daten, Manipulation von Systemeinstellungen, Manipulation von Nutzdaten bis hin zur Veränderung und Unbrauchbarmachung von Daten, so dass das Zielsystem nicht mehr nutzbar ist und Dienstleistungen nicht mehr erbracht werden können.

Angriffe können zielgerichtet auf eine bestimmte Stelle (Unternehmen, Behörde, Rechenzentrum, IT-Dienstleister) erfolgen, sich rein auf die Hardware (bzw. deren Firmware) oder das Betriebssystem eines bestimmten Herstellers beziehen oder auf eine bestimmte Anwendungssoftware ausgerichtet sein. Ebenso gibt es ungerichtete (opportunistische) Angriffe, bei denen kein spezielles Ziel im Visier des Angreifers liegt. Zudem kann es bei zielgerichteten Angriffen zu „Kollateralschäden“ bei IT-Systemen kommen, die nicht im Fokus des Angreifers liegen, aber unbewusst oder sogar billigend in Kauf genommen werden.

Aktuell sind folgende Bedrohungsszenarien zu unterscheiden:

- Erzeugung von Überlast
- Identitätsmissbrauch
- Datendiebstahl und -manipulation
- Einschleusen von Malware

Vielfach ist keine klare Abgrenzung möglich bzw. es treten mehrere dieser Szenarien in Kombination auf.

Für den Bereich der Industriellen Steuerungsanlagen (*Industrial Control Services*, ICS) hat das BSI die folgenden Top-10-Bedrohungen ermittelt und mögliche Gegenmaßnahmen beschrieben [BSI22]:

1. Social Engineering und Phishing
2. Einschleusen von Schadsoftware über Wechseldatenträger und externe Hardware
3. Infektion mit Schadsoftware über Internet und Intranet
4. Einbruch in Fernwartungszugänge

5. Menschliches Fehlverhaltung und Sabotage
6. Zugriff auf Internet-verbundene Steuerungskomponenten
7. Technisches Fehlverhalten und höhere Gewalt
8. Kompromittierung von Extranet und Cloud-Komponenten
9. (D)DoS-Angriffe
10. Kompromittierung von Smartphones im Produktionsumfeld

Die erwähnten Angriffsszenarien, welche für Leitstellen von Bedeutung sind, werden nachfolgend erläutert:

#### 2.5.3.1 Erzeugung von Überlast

*Denial of Service* (DoS) ist die Verweigerung des Dienstes infolge einer Überlastung des Datennetzes oder des Servers. Hierbei werden so viele Anfragen gleichzeitig an den Server gerichtet, dass dieser aufgrund der Überlast nicht mehr reagiert und somit keine Funktion mehr erbringt. [Schw14] Diese Form des Angriffs wird häufig als *Distributed Denial of Service* (DDoS) ausgeführt, wobei der Angriff zur Lasterzeugung nicht nur von einem Rechner aus erfolgt, sondern parallel von einer Vielzahl an Rechnern. Häufig sind diese Rechner zuvor mit Schadcode infiziert worden, um einen DDoS-Angriff zu starten. Neben PCs können hierfür auch die meist schlechten gesicherten Geräte zur Hausautomation o.ä. mit Internetanbindung (*Internet of Things,* IoT) für DDoS-Angriffe infiltriert und genutzt werden. Die kompromittierten Rechner oder IoT-Geräte werden dabei oft als *Botnetz* zusammengeschaltet, um den Schadcode auf weitere erreichbare Rechner zu verteilen und somit die Anzahl der „Angriffsrechner“ stetig zu erhöhen. Mit dem Übergang von der leitungsvermittelten Telefonie hin zu IP-basierten Telefonverbindungen (VoIP) ist auch das Erzeugen von Überlast an den Telefonanschlüssen eines Angriffsziels möglich, dies wird als *Telephony Denial of Service* (TDoS) bezeichnet.

#### 2.5.3.2 Identitätsmissbrauch

Beim Identitätsmissbrauch geht es einem Angreifer darum, persönliche Daten wie Namen und Adressen, Bankverbindungen und/oder Zugangskennungen und Passwörter zu erlangen, um im Namen anderer Personen Geschäfte zu tätigen und sich zu bereichern oder in geschlossene IT-Systeme eindringen zu können. Eine Möglichkeit hierzu sind *Fake-Websites*, die den echten Internetauftritten von Online-Händlern, Kreditinstituten oder anderen Dienstleistern täuschend ähnlich nachgeahmt sind. Mittels ähnlich lautender Adressen (URL) oder gar kompromittierten DNS-Servern werden die Opfer auf die Fake-Website geleitet, mit der Hoffnung, dass diese sich dort einloggen und der Angreifer somit die Zugangsdaten erlangt. Beim *Cross-Site-Scripting* (XSS), übersetzt „webseitenüberreifendes Skripting" wird die Texteingabe auf Internetseiten genutzt [Schw14] (z.B. in Suchfeldern, Foren und Kommentarfeldern), um dort keine Textinformation, sondern Programmcode zu hinterlassen. Bei unzureichender Sicherung bzw. veralteter Forensoftware kann dieser Programmcode bei einem nachfolgenden Besucher in dessen Browser ausgeführt werden und den Nutzer beispielsweise auf eine andere Seite umgeleitet werden oder zur Eingabe von Zugangs- oder Adressdaten veranlasst werden. [Hus04] [Kof22]

Eine weitere Herangehensweise ist das *Phishing*, bei dem der Angreifer sich per gefälschter E-Mail als Kreditinstitut oder Online-Händler ausgibt, von einem angeblichen Cyberangriff berichtet und nun müsse das Zugangspasswort geändert werden. Die Ziel-URL, die minimal von der echten URL abweicht, ist als Link in den Mailtext integriert, um das Opfer auf die Fake-Website zu lotsen und dort zur Eingabe der Zugangsdaten aufzufordern. Ein weiteres Szenario ist der *CEO-Fraud*, bei dem der Angreifer sich nicht als Institution, sondern als Vorgesetzter ausgibt und das Opfer anweist, Bestellungen zu tätigen, Zahlungen zu veranlassen oder Zugangsdaten zurückzusetzen bzw. neu anzulegen; Letzteres zielt vor allem auf IT-Administratoren ab. Varianten des Phishings sind das *Smishing* (Kofferwort aus SMS und Phishing), d.h. die Kontaktaufnahme mit dem Opfer erfolgt nicht per Mail, sondern per SMS; sowie das *Vishing* (Kofferwort aus Voice und Phishing), bei dem das Opfer angerufen und zu Herausgabe von persönlichen Daten oder Passwörter veranlasst wird. Diese Art des persönlichen Kontakts und des Aufbaus von Vertrauen – auch über einen längeren Zeitraum und mehrmaligem Kontakt per

Mail, Telefon und/oder persönlich – wird als *Social Engineering* bezeichnet. [Kar20] Der hohe und professionelle Aufwand von Social Engineering wird vorrangig im Bereich von Industriespionage oder Geheimdiensttätigkeit betrieben.

Im Bereich der Telekommunikation – und damit auch für die Leitstellen von erheblicher Bedeutung – ist das *Spoofing*, d.h. Vortäuschen einer anderen Identität. [Schw14] Beim *Call-ID-Spoofing* verschleiert der Anrufer seine echte A-Teilnehmernummer und gibt sich mit einer anderen Kennung aus, die im Rahmen von CLIP bzw. CLIRO (siehe 2.6.1.2) bei der Gegenstelle angezeigt wird. Möglich wird Call-ID-Spoofing durch die Nutzung bzw. den Aufbau eines unregulierten TK-Netzes, was in Staaten mit unzureichender Aufsicht über das Telekommunikationswesen wesentlich einfacher möglich ist, als z.B. in Deutschland oder den anderen EU-Mitgliedsstaaten. Hierzu können Angreifer direkt aus dem Ausland agieren oder von Deutschland aus auf ausländische Netze zurückgreifen, so dass beispielsweise das Netz der Deutschen Telekom, welches das Zielnetz des B-Teilnehmers darstellt, die Authentizität des Anrufers und seiner Kennung nicht prüfen bzw. ausschließen kann. Parallel zur Verschleierung der Anruferkennung sind auch missbräuchliche Anrufe möglich, die stimmlich und inhaltlich mittels *Künstlicher Intelligenz* (KI) erzeugt werden, um das angerufene Ziel auf diesem Wege auszulasten und die Erkennbarkeit der missbräuchlichen Anrufe zu erschweren. [BS23]

#### 2.5.3.3 Datendiebstahl und -manipulation

Der Diebstahl persönlicher Daten fällt in den Bereich Identitätsmissbrauch (s.o.), beim Diebstahl von Nutzdaten liegt das Motiv des Angreifers häufig darin, dass Opfer zu erpressen, vor allem, wenn es sich um Geschäftsgeheimnisse handelt oder um höchstpersönliche Daten, die dem öffentlichen Ansehen des Opfers schweren Schaden zufügen können. Auch die Erlangung von Passwortlisten oder gespeicherten Zugangsdaten für andere Systeme können das Ziel von Datendiebstählen sein, wenn der Zugang zu anderen IT-Systemen das eigentliche Ziel darstellt.

### 2.5.3.4 Einschleusen von Malware

*Malware* – auch *Schadcode* genannt – ist eine Sammelbezeichnung für Software, die dem Nutzer Schaden zufügt, ohne dass der Nutzer die Aktivierung der Malware sofort bemerkt und eventuell noch verhindern kann. Hierbei gibt es mehrere Varianten:

*Computerviren* benötigen analog zu biologischen Viren einen Wirt, d.h. ein IT-System, über das sie sich auf andere IT-Systeme verbreiten können. Viren fügen sich in die Datenstruktur gewöhnlicher Anwendungs- und Systemdateien ein und werden aktiv, wenn die besagte Datei geöffnet wird. Wesentlich größere Bedeutung als Viren haben zwischenzeitlich Würmer und Trojaner erlangt. *Würmer* sind im Gegensatz zu Viren eine eigenständige Schadsoftware, die sich selbst repliziert und sich vor allem über Netzwerkverbindungen ausbreitet und über die Ausnutzung von Sicherheitslücken weitere Rechner infiziert. Allein durch die Replikation können Würmer die Bandbreite in Netzwerken erheblich beeinträchtigen und damit die Verfügbarkeit einschränken, was sich letztendlich wie ein DDoS-Angriff darstellt.

*Trojaner*, benannt nach dem Trojanischen Pferd, das – äußerlich unscheinbar – in seinem Innenraum Soldaten versteckt hielt, ist eine Form von Malware, die sich als seriöse Anwendungs- oder Systemdatei tarnt und den Schadcode als versteckte Programmzeilen enthält. Hinsichtlich der Verbreitung bzw. des Eindringens in das Zielsystem des Angreifers sind Trojaner auf die „Hilfe“ (bzw. das Fehlverhalten) des Nutzers angewiesen, indem dieser z.B. einen speziell gestalteten Link in einer E-Mail anklickt (Phishing, bzw. Drive-by-Download) oder einen präparierten Mailanhang öffnet.

Unabhängig von der Art der Verbreitung und des Einschleusens in das vom Angreifer gewünschte Zielsystem kann der Schadcode in Form von Viren, Würmern oder Trojanern unterschiedliche Auswirkungen auf das kompromittierte System haben und wird entsprechend als

- Ransomware
- Scareware
- Spyware
- Blended Malware

bezeichnet.

*Ransomware* befällt die Anwendungsdateien von IT-Systemen und verschlüsselt diese. Das Opfer wird erpresst und die Entschlüsselung erst in Aussicht gestellt, wenn Lösegeld (engl. ransom) gezahlt wurde. Die Verschlüsselung kann auch in Kombination mit Datendiebstahl auftreten, wobei die Daten vom Speicher des Opfers gelöscht werden, damit diese nicht selbst mit Hilfe von Anti-Ransom-Software entschlüsselt und wiederhergestellt werden können, was den Druck auf das Opfer, der Lösegeldforderung nachzugeben, zusätzlich verstärkt. [Loc06]

*Scareware* soll dem Opfer Angst einjagen und dazu verleiten, unter Zeitdruck einen überteuerten Kauf oder Vertragsabschluss zu tätigen, ohne die Kaufentscheidung zu überdenken oder Alternativangebote einholen zu können. Häufig ruft Scareware einen Hinweis hervor, der Rechner bzw. das IT-System sei mit Schadcode infiziert und man solle sofort eine entsprechende Schutzsoftware erwerben. Neben überteuerter Software, die entweder völlig nutzlos ist oder aber weiteren Schadcode nachlädt, geht es auch hier darum, dem Opfer wirtschaftlich zu schaden.

*Spyware* nistet sich im Hintergrund bestehender Systeme ein und spioniert – daher der Name – sämtliche Aktionen am Zielrechner aus, z.B. Tastatureingaben (*Keylogger*), Übertragung bzw. Aufzeichnung von Bild und Ton mittels angeschlossener Kameras und Mikrofone, Anfertigung von Screenshots des Bildschirminhalts und/oder Protokollierung des Netzwerkverkehrs ein- und ausgehender Daten.

*Blended Malware* stellt die Kombination verschiedener Arten von Malware in einem „Paket“ dar, wenn der Angreifer ein bestimmtes Zielsystem erreichen will und dafür mehrere Angriffswege parallel wählt; auch um mögliche Lücken in Betriebssystemen, Schutzsoftware und Firewalls auszunutzen und mindestens ein Einfallstor zu finden. Das Ausnutzen von Sicherheitslücken wird als *Exploit* bezeichnet; *Zero-Day-Exploits* sind dabei Lücken, für die noch kein Update/Patch seitens des Herstellers zur Verfügung steht.

Im Bereich der BOS-Leitstellen sind prinzipiell alle der genannten Angriffsszenarien und Schadcodetypen denkbar. Ein zielgerichteter Erpressungsversuch mittels Ransomware zur Erlangung von Geld ist jedoch eher unwahrscheinlich, da bei den zumeist behördlichen Trägern keine großen Geldbeträge zu erwarten sind; ein derartiger Angriff auf einen wirtschaftsstarken, weltweit agierenden Konzern stellt für den Angreifer ein ungleich lukrativeres Ziel dar. Denkbar ist jedoch ein Angriff auf

behördliche Einrichtungen einschließlich Leitstellen, um z.B. politischen Forderungen Nachdruck zu verleihen bzw. im Sinne einer hybriden Kriegsführung.

Ein Ausspähen von Daten (Datendiebstahl) ist im Bereich der Polizeileitstellen denkbar, wenn es dem Angreifer um das Eindringen in polizeiliche Informationssysteme geht, z.B. um polizeiliche Maßnahmen zu behindern. Ebenso kann das Einschleusen von Spyware ein Ansatz sein, um z.B. Informationen über den Stand von Ermittlungen zu erlangen, ohne das Zielsystem und dessen Datenbestand aktiv zu beeinträchtigen. Patientendaten des Rettungsdienstes und Krankentransports, die in Integrierten Leitstellen anfallen, beinhalten deutlich weniger Informationen zum Gesundheitszustand der transportierten bzw. behandelten Patienten als die Datenbestände bei niedergelassenen Ärzten, Krankenhäusern, Pflegeeinrichtungen oder Krankenversicherungen. Ein Angreifer, der es auf persönlich zuordenbare Gesundheitsdaten abgesehen hat, wird eine Leitstelle, in der Notfallrettung und Krankentransport disponiert werden, eher nicht als interessantes Ziel ansehen, sondern sich auf die genannten Ziele im Gesundheitswesen fokussieren.

Da in allen Leitstellen Standardhard- und -software eingesetzt wird – dies betrifft Netzwerkkomponenten wie Router, Switche, Speichersysteme und gleichermaßen weit verbreitete Betriebssysteme (z.B. MS Windows) oder Virtualisierungssoftware (z.B. VMware) – kann eine Leitstelle das Opfer eines opportunistischen Angriffs werden, der auf die Schwachstellen von Standardkomponenten ausgerichtet ist. Als potenzielles Einfalltor für Schadcode sind IP-basierte Dienst anzusehen, wie gemeinsame Datenbanken mehrerer Leitstellenstandort (z.B. Flottenserver) und/oder Anbindungen an Geodatendienste und Versorgungsnachweise. Spezielle Anwendungen werden meist auf autarken Rechnern betrieben, z.B. Warnsysteme oder die Abfrage von Telefonanschlüssen (AAV) über die BNetzA (siehe 2.6.1.8), wobei von den Diensteanbietern zusätzliche Schutzmaßnahmen gefordert werden, damit auf deren Dienste zugegriffen werden darf, z.B. der Einsatz SINA-Boxen als Kryptokomponente. Freies Internet zu Recherchezwecken wird im Regelfall auf separaten PCs bereitgestellt, die meist auch für die Bürokommunikation und Anbindung an das Verwaltungsnetz dienen und vom Leitstellennetz (ELS, KMS) vollständig getrennt sind.

Zielgerichtete DDoS-Angriffe sind bei BOS-Leitstellen im Bereich des IP-Notrufs möglich (TDoS), da dies der derzeit wesentliche Bereich ist, bei dem die Leitstelle für jedermann per IP erreichbar ist. Alle anderen Angriffsszenarien erfordern

Insiderwissen, sofern es sich nicht um einen opportunistischen Angriff handelt. Möglich sind auch kombinierte Angriffe, bei denen z.B. mittels TDoS eine Überlast an eingehenden Notrufen erzeugt wird und diese Hochlastsituation für einen weiteren, im Hintergrund stattfindenden Angriff ausgenutzt wird. [BS23]

Die Leitstellen erbringen ihre Dienstleistungen für die Bevölkerung überwiegend per telefonischer Erreichbarkeit; die Nutzung von Notruf-Apps gewinnt jedoch an Bedeutung. Die Internetauftritte von Leitstellen beziehen sich auf die Darstellung der Aufgaben im Rahmen der Öffentlichkeitsarbeit und bieten allenfalls ein Kontaktformular für nicht-dringende Anfragen per E-Mail; ansonsten wird auf die Notrufnummern 110 und 112 verwiesen. Die zu erwartende verstärkte Nutzung von Notruf-Apps gegen über telefonischer Kontaktaufnahme erfordert leitstellenseitig entsprechende Schutzvorkehrungen, damit über diesen Weg kein Schadcode in die Leitstellensysteme gelangen kann.

### 2.5.4 Verfügbarkeit

Der Verfügbarkeit als Schutzziel der Informationssicherheit kommt in einer Leitstelle eine besondere Bedeutung zu. Die Leitstelle muss ihre „Dienstleistung“, d.h. Entgegennahme von Notrufen und anderen Hilfeersuchen, Disposition der Einsatzmittel und deren rückwärtige Unterstützung zu jeder Zeit gewährleisten können. Dies stellt besondere Anforderungen an die eingesetzte Technik, die baulichen Gegebenheiten, organisatorische Aspekte und das Personal. Die Leitstellentechnik, d.h. die IT-Systeme des Kommunikationssystems (KMS) und des Einsatzleitsystems (ELS) müssen in sich redundant ausgeführt sein und über Rückfall- und Notebenen verfügen. Die Datensicherung muss regelmäßig und automatisch erfolgen. Ebenso muss die Stromversorgung unterbrechungsfrei zur Verfügung stehen [Kar20] und auch für sämtliche Telekommunikations- und Datendienste müssen alternative Komponenten bzw. Anbindungswege installiert sein.

### 2.5.5 Normen und Standards

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat den *IT-Grundschutz* geschaffen und schreibt diesen laufend fort. [ITG22] Zielsetzung sind die Schutzziele Vertraulichkeit, Verfügbarkeit und Integrität (siehe 2.5). Der IT-Grundschutz ist kompatibel zum internationalen Standard ISO/IEC 27001:2022-10 und spezifiziert damit die Aufstellung und Aufrechterhaltung eines *Informationssicherheits-Managementsystems* (ISMS). [DIKV19] [KKRS19] Für die Erarbeitung eines IT-Sicherheitskonzepts, bezogen auf die eigenen IT-Systeme und -Prozesse, beschreibt der IT-Grundschutz die Definition des eigenen Informationsverbundes und dessen Referenzarchitektur. Hierzu stehen eine Vielzahl an vordefinierten Beschreibungen und Bausteine zur Identifikation der IT-gestützten Arbeitsprozesse, der IT-Anwendungen, der IT-Systeme und der zugehörigen Räume zur Verfügung, um schlussendlich die Schutzbedarfe klassifizieren zu können. Für verschiedene Branchen und Anwendungsfelder bestehen eigene *Grundschutzprofile*, in denen die spezifischen IT-Anwendungen und Sicherheitsanforderungen grundlegend beschrieben sind; diese sind jedoch nicht abschließend und müssen im jeweiligen Einzelfall durch die Anwender für den eigenen Anwendungszweck angepasst und präzisiert werden. Speziell für BOS-Leitstellen besteht seit 2021 ein eigenes Grundschutzprofil [GSP23], welches gleichermaßen nicht für alle Leitstellen allgemeingültig ist, sondern den Leitstellenbetreibern als Werkzeug und Hilfestellung dient, die Informationssicherheit im eigenen Zuständigkeitsbereich zu etablieren und weiterzuentwickeln.

Für die Errichtung von Rechenzentren besteht die DIN EN 50600-1 VDE 0801-600-1:2019-08 Informationstechnik – Einrichtungen und Infrastrukturen von Rechenzentren, die z.T. auch bei Technikräumen oder Technikzentren von Leitstellen zur Anwendung kommt. Wesentlicher Bestandteile dieser Norm sind die Gewährleistung der Betriebssicherheit von Rechenzentrum durch Anforderungen an die Sicherstellung von Energieversorgung, Datenanbindung und den zugehörigen Dienstleistungen, wobei vier Verfügbarkeitsklassen definiert sind:

| **Verfügbarkeitsklasse** | **VK 1** | **VK 2** | **VK 3** | **VK 4** |
|---|---|---|---|---|
| Verfügbarkeitsgrad | gering | mittel | hoch | sehr hoch |
| Verfügbarkeit | 99,9 % | 99,99 % | 99,999 % | 99,9998 % |
| Ausfallzeit (max./Jahr) | 12 Stunden | 1 Stunde | 10 Minuten | < 1 Minute |

Tab. 2.1: Verfügbarkeitsklassen nach DIN EN 50600

Neben der Normenreihe der ISO/IEC 27001 und der DIN EN 50600, welche die grundsätzlichen Anforderungen an die IT-Sicherheit von Systemen, Anwendungen und Technikräumen beschreiben, wurde erstmals im Jahr 2014 die DIN EN 50518 verabschiedet, die sich auf *Alarmempfangsstellen* (AES) bezieht und deren Anwendbarkeit auf den BOS-Leitstellen kontrovers gesehen wurde und z.T. immer noch gesehen wird. Die Norm wurde zwischenzeitlich fortgeschrieben und liegt aktuell in der Version DIN EN 50518:2023-12 vor. Die Alarmempfangsstellen als Regelungsgegenstand werden anhand der empfangbaren Signale bzw. Anwendungen in zwei Kategorien untergliedert; Kategorie I (Sicherheitsanwendungen) und Kategorie II (nicht sicherheitsrelevante Anwendungen), wobei BOS-Leitstellen faktisch der Kategorie I zuzuordnen sind, auch wenn diese oder deren Aufgaben dort begrifflich nicht genannt sind. In den Ländern Schleswig-Holstein [SH18] und Thüringen [TH19] ist die DIN EN 50518 bei Neu- und Erweiterungsbauten anzuwenden, die anderen Länder haben sich hierzu (noch) nicht positioniert. Seitens der Bundesfachgruppe Feuerwehr und der Landesfachgruppe Feuerwehr Baden-Württemberg innerhalb der Gewerkschaft ver.di wird die Forderung erhoben, die DIN EN 50518 verpflichtend anzuwenden, um den Schutz der Mitarbeiter vor tätlichen Angriffen zu gewährleisten. [Ver15] Es bestehen zahlreiche Schnittmengen der Normen ISO/IEC 27001 und DIN EN 50518 in Bezug auf bauliche, technische und betriebliche Anforderungen. Es wird empfohlen, die beiden Normen additiv in Leitstellen umzusetzen (Maximalprinzip), so dass das jeweils höhere Schutzniveau zur Anwendung kommt. [SB23]

Für den IT-Betrieb hat sich die *Information Technology Infrastructure Library* (ITIL) als Standard etabliert, um alle Prozesse der Wertschöpfungskette abbilden zu können. [Eb21] D.h. ITIL bezieht sich auf die Planung, Einführung und den Betrieb von IT-Systemen, was u.a. das Management von Änderungen und Updates

beinhaltet sowie ein geordnetes Handeln bei Störungen und Sicherheitsvorfällen. D.h. die IT-Sicherheit ist ein Teilaspekt der ITIL-Prozesse. Hierbei sind vor allem die Practices *Problem Management* und *Incident Management* zu nennen, wobei das Problem Management sowohl reaktiv als auch proaktiv tätig wird; Letzteres, um mögliche Probleme gar nicht erst entstehen zu lassen oder zumindest zu minimieren. Das Incident Management wird eher reaktiv bei Sicherheitsvorfällen tätig, was jedoch proaktive Maßnahmen nicht ausschließt. In der Praxis ist eine eindeutige Abgrenzung zwischen Problem Management und Incident Management zwar begrifflich, aber hinsichtlich der Zuordnung der Maßnahmen zu den beiden Practices nicht immer exakt möglich. [Eb21] Beide Practices bilden einen wesentlichen Bestandteil des Notfallmanagements, welches ebenso im BSI-Standard 100-4 beschrieben ist. [BSI100-4] Hierauf baut das *Business Continuity Management* (BCM) auf, welches im BSI-Standard 200-4 festgelegt ist. Das BCM bezieht sich hierbei ausschließlich auf Störungen und Betriebsunterbrechungen, die im Zusammenhang mit dem IT-Betrieb stehen und lässt andere Aspekte, die im betriebswirtschaftlichen Sinn unter BCM verstanden werden (z.B. Ausfall von Lieferanten), außen vor. [BSI200-4]

Die Umsetzung der NIS-2-Richtlinie der Europäischen Union in nationales Recht steht bevor, wodurch sich der Geltungsbereich von verbindlichen Vorgaben zur IT-Sicherheit und der Behandlung von Sicherheitsvorfällen auf eine höhere Anzahl an Behörden, Institutionen und Unternehmen erweitert, als dies bei der KritisV der Fall ist (siehe 2.5), wobei das Notfall- und Rettungswesen einschließlich der Leitstellen auch hier nicht mit enthalten ist und auch keine sinngemäße Erwähnung findet. [NIS-2]

### 2.5.6 IT-Sicherheitsvorfälle in Kritischen Infrastrukturen

In den vergangenen Jahren gab es weltweit zahlreise Angriffe auf die IT-Systeme Kritischer Infrastrukturen. [RL18] Eine hohe internationale Bekanntheit hat der Computerwurm *Stuxnet* erlangt, der im Jahr 2010 im Zusammenhang mit dem iranischen Kernenergieprogramm entdeckt wurde. Stuxnet war auf eine industrielle Steuerung (ICS) des Herstellers Siemens ausgerichtet, die dazu diente, die Motordrehzahl von Zentrifugen zu steuern. Der Stuxnet-Angriff beeinflusste die

Rotationsgeschwindigkeit, so dass die Isotopenanreicherung und damit das iranische Kernenergieprogramm empfindlich gestört wurde. [Lan13] Nach Einschätzung des BSI dient Stuxnet als Vorlage und „Musterbeispiel“ für andere Angreifer:

*„Seit Stuxnet weiß man, dass die Sabotage von Maschinen und Einrichtungen durch Cyber-Angriffe nicht nur denkbar ist, sondern tatsächlich durchgeführt wird.“* [BSI15]

Ähnlich verhält es sich mit *Triton*, einem Trojaner, der im Jahr 2017 entdeckt wurde und ebenfalls auf industrielle Steuerungstechnik ausgerichtet war. Im Fall von Triton erfolgte der Angriff auf eine petrochemische Anlage in Saudi-Arabien; dabei war Triton auf ein Sicherheitssystem ausgerichtet, welches im Notfall die Anlage außer Betrieb nehmen soll. [Sym17]

Ein besonderes Risiko stellt der Einsatz von *Commercial-Off-The-Shelf*-Anwendungen und -Produkten (COTS) im Bereich Kritischer Infrastrukturen dar, mit denen auf individuelle IT-Lösungen verzichtet und stattdessen weit verbreitete Standardprodukte zur Anwendung kommen. COTS-Produkte erleichtern Monitoring und Wartung, es besteht eine Vielzahl an Dokumentation und Anwendungshilfen und zudem ist der Einsatz wirtschaftlich. Diese Vorteile sind gleichermaßen Nachteile im Sinne der IT-Sicherheit, da hiermit das Risiko steigt, dass Schadcode, der auf weit verbreitete IT-Anwendungen ausgerichtet ist, die Sicherheit von Kritischen Infrastrukturen bedroht. [DKV12] In Leitstellen sind COTS-Komponenten aus den erwähnten Vorteilen ebenfalls weit verbreitet, dies betrifft vor allem Hardware und Betriebssysteme.

Neben zielgerichteten Angriffen auf die IT von Kritischen Infrastrukturen stellen opportunistische Angriffe (siehe auch 2.5.3) durch die Nutzung von COTS eine Gefahr dar. Beispielhaft sind hier die Würmer *Mirai* und *WannaCry* zu nennen. Mirai zielte auf internetfähige Geräte wie z.B. Router, Smart-TVs und IP-Kameras ab, die vielfach in Privathaushalten vorhanden sind, aber auch in der Industrie genutzt werden. Mirai schaltete die kompromittierten Komponenten zu einem Botnetz zusammen, um damit DDoS-Attacken durchführen zu können. [Kre16] WannaCry wurde als Ransomware im Jahr 2017 bekannt, als es über 200.000 Windows-Betriebssysteme weltweit befiel und die Daten verschlüsselte. Hierbei zählten auch verschiedene Kritische Infrastrukturen zu den Opfern. [Bee17]

## 2.6 Leitstellentechnik

Die Kernbestandteile einer jeden BOS-Leitstelle sind das Kommunikationsmanagementsystem (KMS) und das Einsatzleitsystem (ELS), die auch die Hauptarbeitsmittel der Disponenten bilden. Das KMS dient der Zusammenführung sämtlicher ein- und ausgehender Sprachkommunikation (Notruf, allgemeine Telefonie, Sprechfunk, Elektroakustische Anlagen, Türsprechstellen) und deren Bedienung (Hören und Sprechen) von allen angebundenen Arbeitsplätzen aus. Das Einsatzleitsystem stellt eine spezielles Vorgangsbearbeitungs- und Ressourcenverwaltungssystem mit einer umfangreichen Datenbank dar, in welcher sämtliche Alarmpläne, Einsatzfahrzeuge und -einheiten, Erreichbarkeiten und Ortsdaten des Zuständigkeitsbereichs der Leitstelle abgelegt sind. Eine schematische Darstellung der in einer Leitstelle verwendeten Systeme und Komponenten zeigt Abbildung 2.4.

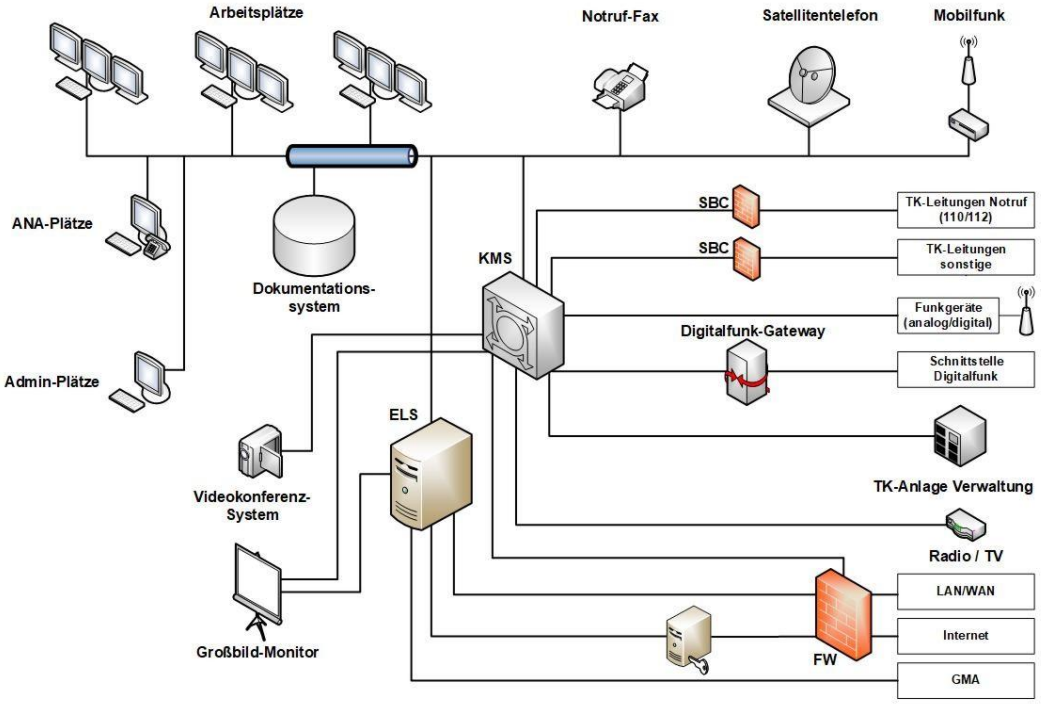



Abb. 2.4: schematische Darstellung von KMS und ELS einer Leitstelle

Auf die einzelnen Komponenten und deren Bedeutung wird in den nachfolgenden Abschnitten eingegangen.

Die Steuerung und Nutzung beider Systeme erfolgt von den Einsatzleitplätzen (ELP), diese werden auch „Leitstellenarbeitsplätze“ oder umgangssprachlich kurz

„Arbeitsplätze“ genannt aus, die mit mehreren Bildschirmen, Eingabegeräten (Tastatur, Maus), Audiotechnik (Lautsprecher, Mikrofon, Headset, Handapparat) ausgestattet sind. Optional kann insbesondere zur Bedienung des KMS ein Touchbildschirm hinzukommen, sowie ggf. weitere Geräte, die direkt am Platz bedient werden können (z.B. gesonderte Telefonapparate und/oder Funkgeräte als Rückfallebenen). Um gerade in größeren Leitstellen bzw. Leitstellenräumen einen Überblick zu haben, welche bzw. wie viele Plätze sich gerade in Telefon- oder Funkgesprächen befinden, gehören eine oder mehrere Signalleuchten an jedem Arbeitsplatz inzwischen zum Standard. Mindestens eine Leuchte zeigt an, dass am jeweiligen Platz gerade gesprochen wird (Telefonie, Funk). Weitere Signalleuchten in anderen Farben können eine längerzeitige Belegung eines ELP (z.B. durch eine Telefonreanimation), die Abwesenheit (Pause) eines Disponenten, Hilfebedarf eines Platzes bei einem schwer verständlichen Anrufer oder die Aufforderung zur Ruhe im Raum bei zu hoher Geräuschkulisse für alle anwesenden Disponenten signalisieren.

Neben den ELP mit umfangreicher technischer Ausstattung gibt es Plätze mit vereinfachter Ausstattung für gesonderte Zwecke. Hierzu gehören Ausnahme-Abfrageplätze (meist als „AAP“ oder „ANA-Plätze“ bezeichnet), die ausschließlich zur Notrufannahme bei erhöhtem Notrufaufkommen besetzt werden und lediglich die eingehenden Hilfeersuchen im Einsatzleitsystem erfassen, aber keine Fahrzeuge/Einsatzmittel disponieren und daher auch nicht über eine Funkanbindung verfügen. Typischerweise werden AAP bei Unwetterlagen in Betrieb genommen, wenn innerhalb kurzer Zeit eine Vielzahl an Unwetterschäden gemeldet wird. AAP sind üblicherweise mit einem PC des ELS sowie einem an das KMS angebundenem Systemtelefon mit Headset ausgestattet.

Des Weiteren sind die Arbeitsplätze für Administratoren und Datenpfleger ergänzend zum normalen Büro-PC mit gesonderten Clients-PCs von ELS und/oder KMS ausgestattet, um Systemeinstellungen vorzunehmen und z.T. auch zu Testzwecken auf Funktionen wie Telefonie und Funk zuzugreifen.

### 2.6.1 IT-Infrastruktur

Die Leitstellentechnik in Form von ELS und KMS ist als Client-Server-Architektur ausgeführt, wobei die Server als Virtuelle Maschinen (VM) betrieben werden. Ein

redundanter Aufbau der Server und des Netzwerkes (LAN) in baulich und brandschutzmäßig voneinander abgegrenzten Serverräumen bietet eine größtmögliche Betriebssicherheit bei Hardwareausfällen und externen Einflüssen wie z.B. Wassereintritt oder Brandereignissen. Das physikalische Netzwerk wird in logische Segmente untergliedert, die als einzelne *Virtual Local Area Networks* (VLAN) die beiden Hauptsysteme (ELS und KMS) sowie ggf. weitere Systeme voneinander abgrenzen. Hinzu kommt eine Netzwerksteuerung und -überwachung, die zumeist auf dem *Simple Network Management Protocol* (SNMP) basiert.

Bestandteil der IT-Infrastruktur sind ebenso Speichersysteme (Storage Area Network, SAN), die ebenfalls redundant ausgeführt sind. Die Absicherung gegenüber anderen Netzen (Intranet, Internet) erfolgt über Firewalls, die üblicherweise zweistufig mit *Demilitarisierter Zone* (DMZ) konzipiert werden. [Poh02] Eine Sonderform von Firewalls findet sich als *Session Border Controller* (SBC) zur Abgrenzung des internen vom externen Netz für IP-Telefonie. Ein SBC beinhaltet Firewall-Funktionen, die speziell auf die IP-Sprachdienste ausgelegt sind und ermöglicht zudem eine Medien- und Protokollumwandlung zur Anbindung von IP-Telefonanlagen bzw. KMS an den Übergabepunkt des Telekommunikationsanbieters.

#### 2.6.1.1 Kommunikationsmanagementsystem (KMS)

Das KMS dient der Bedienung aller ein- und ausgehenden Telekommunikationskanäle (Notruf, Telefonie, Sprechanlagen, Sprechfunk, Durchsagen im Haus usw.) von allen Arbeitsplätzen aus. Aus der Historie heraus werden auch die Bezeichnungen „Funk-Draht-Vermittlung“ und „Vermittlungs- und Abfragesystem“ gebraucht, ersteres weist auf die frühere Benennung „Funk“ für die hochfrequente Funkübertragung und „Draht“ für die drahtgebundene Telefonie hin; „Vermittlungs- und Abfragesystem“ (VAS) rührt von der gleichnamigen Produktbezeichnung der Fa. Siemens her und hat sich als Gattungsname etabliert. Die klassischen Zuordnungen „Draht“ und „Funk“ sind inzwischen formal hinfällig, da die Telefonie auch drahtlos erfolgen kann (Mobilfunk) und die Digitalfunkanschaltung der Leitstellen über Festnetzleitungen erfolgt (siehe 2.7.2).

Die KMS-Technik stammt ursprünglich aus der analogen Telefonvermittlung und wurde ab den 1990er Jahren im Zuge der Einführung der digitalen Telefonie (ISDN) in digitaler Sprachvermittlung realisiert. [App11] Dabei bildete die Pulscodemodulation (PCM) die technische Basis für die digitale Verarbeitung der Sprachströme. Ab den 2000er Jahren setzte sich die IP-basierte Signalverarbeitung durch, die heute Standard bei allen am Markt angebotenen KMS ist. [Cla23] Die Anschaltung von Signalquellen und –senken kann nach wie vor auch als analoge Anschlüsse, ISDN bzw. andere Modulationsverfahren, Protokolle und Codecs realisiert werden, die über entsprechende Schnittstellenbaugruppen von bzw. nach IP gewandelt werden.

Unabhängig von analoger oder digitaler Sprachvermittlung muss das KMS für alle eingehenden und ausgehenden Telekommunikationskanäle den passenden Signalpegel ausgangsseitig zur Verfügung stellen bzw. eingangsseitig verarbeiten können. Hinzu kommen unterschiedliche Bandbreiten, die ebenfalls verarbeitet werden müssen, damit eine optimale Sprachverständlichkeit eingangs- wie ausgangsseitig sichergestellt ist.

Durch die technische Ausführung moderner KMS als Client-Server-System – oftmals virtualisiert – (siehe 2.6.1) und die durchgängig IP-basierte Signalverarbeitung, hat die IT-Sicherheit enorm an Bedeutung gewonnen. In der leitungsvermittelnden Telefon-/Sprachvermittlung war das Einschleusen von Schadcode allenfalls bei genauer Kenntnis der verwendeten Technik (Hersteller, Modell, Versionsstand) möglich, z.B. über Wartungszugänge.

Ein KMS besitzt diverse Schnittstellen, um die ein- und ausgehenden Kommunikationskanäle anzubinden; dies sind im Regelfall

- Telefonie extern (VoIP, analog)
- Notruf 110/112 (VoIP)
- Telefonie intern (VoIP, QSIG, analog)
- Sprechfunk digital (Festnetzanschaltung, Funkgeräte)
- Sprechfunk analog (Gleichwellenfunk, Relaisstelle, Funkgeräte)
- Sprechstellen an Zugangstüren
- Wachalarm-/Elektroakustische Anlage (ELA)
- Faxgeräte (Ein- und Ausgang, Notruf)
- interne Rufanlage (z.B. Aufzugsnotruf)

- Rundfunk-/TV-Empfang
- Videokonferenz

Hinzu kommen weitere Schnittstellen für Sprachdaten für die Bearbeitung innerhalb der Leitstelle:

- Hör- und Sprecheinrichtungen (Mikrofon, Hör-Sprech-Garnitur, Handapparat, Lautsprecher), mit denen die o.g. Kommunikationskanäle gehört und besprochen werden können.
- Videoschnittstellen (Kameras)
- Dokumentationssystem (Sprachaufzeichnung)

Des Weiteren Steuerschnittstellen:

- IP-Schnittstelle zum Einsatzleitsystem, damit kommunikationsbegleitende Daten (Metadaten) wie Statusmeldungen der Einsatzfahrzeuge, A-Teilnehmer-Kennungen und eCall-Daten übergeben werden können bzw. Steuerbefehle aus dem Einsatzleitsystem heraus im KMS ausgeführt werden können, z.B. Anwahl einer Rufnummer aus dem Elektronischen Telefonbuch (ETB) des Einsatzleitsystems.
- Signalleuchten am Arbeitsplatz, Aktivierung z.B. bei laufendem Telefon- oder Funkgespräch; i.d.R. als potenzialfreie Kontakte ausgeführt.
- Wartungszugang (IP-basiert) für den Lieferanten oder Servicedienstleister, um Konfigurationen und Updates einspielen und Entstörungen durchführen zu können.

Die Vielzahl an externen, vor allem IP-basierten Schnittstellen birgt die Gefahr, dass Schadcode eingebracht werden kann bzw. dass zentrale Steuerfunktionen kompromittiert werden.

Um für eventuelle Störungen gerüstet zu sein, besteht ergänzend zum KMS als Hauptsystem – selbst bei vollredundantem Aufbau – eine Rückfall- oder Notebene (Begrifflichkeiten variieren), die entweder von einem anderen Hersteller stammt oder bzgl. Hersteller und Modell mit dem Hauptsystem identisch ist, aber mit einem anderen Softwarestand betrieben wird (eine oder zwei Versionsstände gegenüber dem Hauptsystem zurückliegend). Falls es durch ein Update des Hauptsystems zu

Instabilitäten kommt, kann auf das Drittsystem mit einem stabilen und erprobten Softwarestand zurückgegriffen werden.

### 2.6.1.2 Notruf

Unter „Notruf“ werden in diesem Abschnitt die über das öffentliche Telekommunikationsnetz erreichbaren Notrufnummern 110 und 112 bezeichnet. Der Ausdruck „Notruf“ ist gesetzlich nicht geschützt und taucht daher auch bei anderen Kommunikationsanlagen auf, die für Hilfeersuchen betätigt werden können, aber keine direkte Anwahl der Rufnummern 110 bzw. 112 beinhalten, z.B. Notrufsäulen an Autobahnen und Schnellstraßen, Notrufsäulen in Bahnhöfen und ÖPNV-Stationen, Aufzugsnotruf, Hausnotruf usw.

Die in Deutschland etablierte Notrufnummer 112 wurde EU-weit eingeführt und steht in allen anderen EU-Staaten sowie darüber hinaus auch in zahlreichen anderen Staaten/Kontinenten parallel zu den bestehenden nationalen Notrufnummern zur Verfügung („Euronotruf“).

Im Jahr 1973 wurden durch die damalige Deutsche Bundespost als Telefonnetzbetreiber grundlegende technische Anforderungen an Notrufverbindungen eingeführt [Mel99] [Gei03], die trotz des technischen Wandels von analoger Telefonie über ISDN und IP nach wie vor Bestand haben; hiervon rührt auch die in diesem Zusammenhang gebräuchliche Bezeichnung „Notrufsystem 73“.:

1. Notrufanschlüsse unterliegen einer priorisierten Entstörung durch die Netzbetreiber.
2. Die Notrufanschaltungen werden 24/7 auf der Transport- und Dienstebene überwacht.
3. Notrufleitungen funktionieren als „Einbahnstraße“ nur für eingehende Anrufe (Notrufe). Abgehende Gespräche sind über die Notrufanschlüsse nicht möglich, damit diese nicht unnötig belegt sind, sondern für ankommende Notrufe reserviert bleiben. Abgehende Gespräche seitens der Leitstelle werden über die herkömmlichen Telefonanschlüsse geführt.
4. Bei der Anwahl der Notrufnummer 110 oder 112 wird innerhalb des Telekommunikationsnetzes eine Notrufprozedur ausgelöst, bei der u.a. die gewählte

Notrufnummer, die keine Vorwahl enthält, in eine sog. Verkehrslenkungsnummer („1982er Nummer“) umgesetzt wird. Diese entspricht einer normalen Rufnummer, einschließlich der Ortsnetzkennzahl (ONKZ) des Leitstellenstandortes und einer Rufnummer, die mit den Ziffern 1982xxx beginnt. Dabei besteht ein sog. *Seiteneinwahlschutz*, d.h. Notrufanschlüsse können weder über eine direkte Anwahl der Verkehrslenkungsnummer 1982xxx erreicht werden, noch kann eine Notrufnummer in einer Leitstelle, die nicht für den Standort des Anrufers zuständig ist, erreicht werden. Es ist somit beispielsweise nicht möglich, von München aus durch Anwahl von 040 / 112 (Hamburger Ortsnetzkennzahl 040 und Notrufnummer 112) die Leitstelle der Feuerwehr Hamburg zu erreichen. Mit dieser technischen Beschränkung soll der Missbrauch von Notrufen und auch die gezielt herbeigeführte Überlastung von Notrufanschlüssen von einer oder mehreren entfernten Regionen aus verhindert werden.

5. Jeder Inhaber eines Telefonanschlusses (Festnetz, Mobiltelefon) kann für seinen Anschluss einstellen, ob seine Rufnummer als Anrufer (A-Teilnehmer) beim Angerufenen (B-Teilnehmer) angezeigt wird, oder nicht. Diese Leistungsmerkmale heißen *Calling Line Identification Presentation* (CLIP) zu Rufnummernanzeige beim B-Teilnehmer bzw. *Calling Line Identification Restriction* (CLIR) zur Unterdrückung der Rufnummernanzeige. Bei der Anwahl einer Notrufnummer 110 oder 112 ist die Einstellung CLIP bzw. CLIR unerheblich, da ein eventuell aktiviertes CLIR automatisch überschrieben wird (Leistungsmerkmal *Calling Line Identification Restriction Override*, CLIRO), so dass die Rufnummer des Anrufers stets bei der Leitstelle angezeigt wird; dies gilt gleichermaßen für Mobiltelefone und auch für Festnetzanschlüsse. Ein anonymer Notruf ohne jegliche Rückverfolgbarkeit des Anrufers wird damit vermieden. Einzige Ausnahme hierbei sind Mobiltelefone, die bei fehlender Verbindung („Funkloch“) zum eigenen, vertraglichen Netzbetreiber eine Notrufverbindung über ein Fremdnetz herstellen (*GSM Fallback* bzw. *Limited Service Mode*). Hierbei kann trotz CLIRO keine A-Teilnehmerkennung zur Leitstelle übermittelt werden, da der Teilnehmer in den Datenbanken des fremden Mobilfunknetzes mit seiner Mobilfunk-Teilnehmerkennung (*International Mobile Subscriber Identity*, IMSI) und der zugewiesenen Rufnummer nicht bekannt ist. Bei öffentlichen Münz-/Kartentelefonen wird eine Standortnummer übertragen, so dass anhand des Standortes der Notrufinhalt verifiziert werden kann,

wenn z.B. ein gemeldeter Notfallort weit vom Standort des Münzfernsprechers entfernt ist und dies nicht plausibel erklärt werden kann.

6. Neben der Rufnummernübermittlung (CLIRO) erfolgt zudem eine Übertragung des Standortes des Anrufers an die Leitstelle. Dies betrifft die Adresse des Anschlussinhabers bei Festnetzanschlüssen; bei Mobilfunkteilnehmern die Geoposition bzw. die Funkzelle.
7. Auch wenn sich mehrere Gemeinden (u.U. auch kreisübergreifend) eine Ortsvermittlungsstelle und damit eine ONKZ teilen, können Notrufe nach Gemeinden getrennt, zu der Leitstelle geroutet werden, die für den Standort des Anschlusses geografisch zuständig ist (sog. Trennung nach Notrufursprungsbereichen).
8. Die Notrufe 110 und 112 sind für den Anrufer kostenfrei, was aus der Zeit vor der massenhaften Verbreitung von Mobiltelefonen herrührt, als öffentliche Fernsprecher als wichtige Notrufmöglichkeit dienten, die hierfür auch ohne Münzgeld bzw. Telefonkarten genutzt werden konnten. Heutzutage, mit der weitreichenden Verbreitung von Mobiltelefonen und Flatrates als Vertragsmodell, ist die Kostenfreiheit von Notrufverbindungen von nachrangiger Bedeutung. Gleichwohl müssen die Leitstellenbetreiber für ihre Notrufanschlüsse ein monatliches Entgelt an den Telekommunikationsdienstleister entrichten.

#### 2.6.1.3 Notruffax und -app

Für Menschen mit Sprech- und/oder Hörbehinderung, die ihr Anliegen nicht verbal per Telefon äußern können, steht die Möglichkeit zur Verfügung, eine Notrufmeldung per Telefax abzusetzen. Hierfür stehen Faxvordrucke als DIN A4-Formulare zur Verfügung, auf denen die Notfallart (z.B. medizinischer Notfall, Verkehrsunfall, Brand, Straftat) anzukreuzen und der Notfallort einzutragen ist, um das Formblatt dann per Fax zur Leitstelle zu senden. [Cht23] Hierbei können sowohl die Notrufnummern 110 und 112 angewählt werden als auch gesonderte „Notruffaxnummern“, die von den jeweiligen örtlichen Leitstellen bekannt gegeben werden und nicht einheitlich sind.

Das in der Leitstelle eingehende Notruffax wird entweder automatisch vom KMS anhand der Faxkennung identifiziert und als elektronisches Dokument (PDF) dem

ELS zugeleitet und dort angezeigt. Ohne automatische Faxerkennung muss der eingehende Notruf mit dem Fax-Signalton manuell vom Disponenten auf einen internen Faxanschluss umgeleitet werden. Als Rückfallebene für die Erzeugung eines PDF-Dokuments stehen nach wie vor Telefaxgeräte als eigene Hardware zur Verfügung, auf denen das Notruffax als Papierausdruck ausgegeben wird.

Die Bedeutung von Telefaxverbindungen zum Absetzen eines Notrufs hat stark an Bedeutung verloren, da diese Notrufmöglichkeit für Menschen mit Sprach-/Hörbehinderung nur im häuslichen Umfeld von Nutzen ist, wo ein Faxgerät und die zugehörigen Notrufvordrucke zur Verfügung stehen.

Mit der Ratifizierung der UN-Behindertenrechtskonvention [UNB09] im Jahr 2009 hat sich die die Bundesrepublik Deutschland u.a. verpflichtet, für Menschen mit Sprech- und/oder Hörbehinderung einen barrierefreien Zugang zu Notrufmöglichkeiten zu schaffen, wodurch das Telefax zur Notrufmeldung zunehmend kritisch gesehen wird und praktisch an Bedeutung verliert. Durch die weite Verbreitung von Smartphones ist zudem der öffentliche Druck gestiegen, eine entsprechende App zum Absetzen eines Notrufs einzuführen und damit auch das Notruffax abzulösen, so dass auch außerhalb des häuslichen Umfeldes jederzeit Notrufmeldungen abgesetzt werden können und mittels GPS auch eine Standortbestimmung möglich ist, wenn die der Meldende nicht ortskundig ist. Die bundeseinheitliche Notruf-App *Nora* wurde zu diesem Zweck entwickelt und im Jahr 2021 vorgestellt und steht seitdem für die Betriebssysteme Android und iOS zur Verfügung. Mit der Datenübertragung von Smartphones zum Einsatzleitsystem in der Leitstelle ergeben sich auch Anforderungen in Bezug auf die IT-Sicherheit.

#### 2.6.1.4 eCall

Basierend auf dem Euronotruf 112 müssen alle PKW und leichten Nutzfahrzeuge, die ab dem 01.04.2018 eine Bauartzulassung erhalten haben, mit dem automatischen Notrufsystem „eCall“ (Langform: *Emergency Call*) ausgestattet sein. Analog der Auslösekriterien eines schweren Aufpralls für Airbags wählt das eCall-Modul automatisch den Notruf 112 an und übermittelt einen Mindest-Datensatz (*Minimum Set of Data*, MSD) und schaltet zudem eine Sprechverbindung frei. [MK23] Neben

der automatischen Auslösung bei einem schweren Unfall ist auch eine manuelle Auslösung möglich, z.B. durch Unfallzeugen, Ersthelfer oder bei Notfällen ohne Unfallereignis.

Der MSD enthält folgende Daten:

- aktuelle Position des Fahrzeugs (Koordinaten anhand GPS oder GALILEO)
- vorige drei Koordinaten, wichtig für die Fahrtrichtung auf Autobahnen und Straßen mit baulich getrennten Fahrtrichtungen
- Unfall- bzw. Auslösezeitpunkt
- Automatische oder manuelle Auslösung
- Fahrzeug-/Serviceprovider-ID

Optional können ergänzend zum MSD weitere Daten übermittelt werden:

- Anzahl der Insassen
- Sicherheitsgurte angelegt ja/nein
- Schwere des Unfalls, z.B. Überschlag

Da die eCall-Daten auf dem normalen Sprachkanal des Notrufs 112 übermittelt werden, kommt ein Inband-Modem zum Einsatz, das den MSD und ggf. ergänzende Daten per Frequenzumtastung (*Frequency Shift Keying*, FSK) in den Audiokanal moduliert. Leitstellenseitig ist zur Auswertung des MSD ein entsprechender eCall-Decoder erforderlich. Aktuell am Markt verfügbare KMS haben diese Funktion implementiert und können den MSD direkt im IP-Notruf erkennen und die Sprach- und MSD-Daten entsprechend weiterleiten bzw. verarbeiten.

Um die korrekte Signalisierung eines eCall-Notrufes in der Leitstelle zu überprüfen, sind im Fachhandel sog. „eCall-Tester“ erhältlich. Hierbei handelt es sich um modifizierte eCall-Module, die per USB von einem PC aus gesteuert werden, wobei eine freie Eingabe der Geoposition und anderer MSD-Daten möglich ist. Hiermit ist prinzipiell ein Missbrauch möglich, da Unfallszenarien mit beliebiger Position simuliert werden können. Eine Identifizierbarkeit des Anrufers ist jedoch anhand der Mobilfunkrufnummer der SIM-Karte möglich (siehe 2.6.1.2).

### 2.6.1.5 AML

Eine Möglichkeit zur automatischen Positionsbestimmung bei Anrufern mit Mobiltelefonen, die nicht ortskundig sind und daher ihren Standort nicht genau beschreiben können, ist das Verfahren *Advanced Mobile Location* (AML); diese Funktion ist bei Smartphones ab Android 2.3 bzw. iOS 13.3 implementiert. Hierbei werden beim Anwählen der Notrufnummer 112 automatisch GPS und WLAN zur Positionsbestimmung eingeschaltet, sofern diese Schnittstellen nicht ohnehin aktiv sind. Parallel zu den Sprachdaten (GSM) werden die Standortdaten per UMTS bzw. LTE übertragen. Die Standortübermittlung erfolgt in Deutschland an die beiden definierten AML-Endpunkte bei den Integrierten Leitstellen in Berlin und Freiburg. [AS22] Alle Leitstellen in Deutschland können dort die per AML übermittelten Standortdaten per https abfragen.

In Deutschland erfolgte die Einführung von AML erst nach vielen anderen Ländern, da zunächst Bedenken bezüglich des Datenschutzes ausgeräumt werden mussten.

AML stößt in zwei Fällen an seine Grenzen; zum einen wenn sich das Smartphone zum Absetzen eines Notrufs bei fehlender Mobilfunkabdeckung des eigenen Netzbetreibers in ein Fremdnetz einbucht (Limited Service Mode, siehe 2.6.1.2) und nur die Sprachverbindung, aber keine begleitende Datenübertragung möglich ist. Zum anderen, wenn ein Smartphone mit zwei SIM-Karten (Dual-SIM) genutzt wird und Telefonie und Datenübertragung getrennt über die beiden SIM-Karten erfolgen. In diesem Fall ist keine Zuordnung des Sprachnotrufs zu den Standortdaten möglich.

### 2.6.1.6 Einsatzleitsystem (ELS)

Die Begriffe *Einsatzleitsystem* (ELS) bzw. *Einsatzleitrechner* (ELR) werden umgangssprachlich oft synonym verwendet, wobei sich der Ausdruck *ELS* vorranging auf die Software und deren Funktionen bezieht und bei der Bezeichnung *ELR* die zugehörige Hardware mit umfasst ist.

Das ELS stellt die „Intelligenz“ innerhalb der Leitstellentechnik dar, da es als Datenbank, Dispositionsunterstützung und Ressourcenverwaltung neben dem KMS

das wichtigste Arbeitsmittel für die Disponenten darstellt. [Scheu23] Hierbei sind vor allem folgende Funktionen zu nennen:

- Datenbank mit allen Einsatzmitteln und -einheiten und deren Verfügbarkeiten
- Datenbank mit allen Straßen, Ortsdaten und Sonderobjekten
- Alarmpläne für alle Kommunen mit allen Ortsteilen und für alle Einsatzstichworte
- Datenerfassung und -dokumentation (beginnend mit dem Notrufeingang)
- Elektronisches Telefonbuch
- Ansteuerung der Alarmierung (Alarmgeber, Wachalarm)
- Verarbeitung von Statusmeldungen der Einsatzmittel
- Übernahme und Verarbeitung von Metadaten vom KMS (Rufnummer des Anrufers, Funkkennungen, Statusmeldungen usw.)

Das ELS unterstützt die Disponenten durch einen Alarmvorschlag, der sich aus der Einsatzart (Notfallrettung, Brand, Technische Hilfe), der Größe/Ausdehnung, Menschen bzw. Tiere in Gefahr ja/nein usw., der örtlichen Zuständigkeit der Feuerwehr(en) und Rettungswache(n) sowie ggf. aus Uhrzeit und Wochentag ergibt. Letzteres betrifft z.B. Rettungswagen, die nicht 24/7, sondern nur tagsüber unter der Woche im Dienst sind und außerhalb dieser Zeiten nicht als Ressource zur Verfügung stehen. Dies gilt gleichermaßen für Freiwillige Feuerwehren, bei denen die Alarmierung werktags tagsüber aufgrund schlechterer Verfügbarkeit von ehrenamtlichen Kräften, die im Alarmfall ihren Arbeitsplatz verlassen können, z.T. umfangreicher erfolgt als abends und an Wochenenden. Diese Randbedingungen müssen bei der Datenversorgung des ELS mit eingepflegt werden, so dass die hinterlegten Verfügbarkeiten bei jedem Alarmvorschlag berücksichtigt werden. Die Komplexität aus einer Vielzahl an Einsatzstichworten, verfügbaren Ressourcen, örtlichen Zuständigkeiten und ggf. zeitlichen Restriktionen erfordert einen hohen Aufwand bei der Datenerfassung und -pflege.

Bestandteil eines ELS – als eigenes Softwaremodul oder auch als integrierte Softwarelösung eines Drittanbieters – ist ein *Geoinformationssystem* (GIS) [Kas99], d.h. elektronisches Kartenmaterial und Luftbilder, das mehrere Funktionen erfüllt:

- Visualisierung des Standortes von Anrufern
- Anzeige des Einsatzortes und der Umgebung
- Anzeige einsatztaktisch besonders bedeutsamer Objekte
- Anzeige des aktuellen Standortes von Einsatzfahrzeugen

- Flottenmanagement mit Routingfunktion (Fahrzeug, das kürzesten Anfahrtswerg hat, wird entsandt)
- Zusammenführen von Notrufen und anderen Meldungen, die sich auf das gleiche Ereignis beziehen, aber von unterschiedlichen Standorten/Adressen aus getätigt werden.
- Abschätzung des betroffenen Gebietes bei einer Rauch- oder Schadstoffausbreitung
- Abstimmen von Maßnahmen mit Nachbarleitstellen, wenn der Einsatzort unmittelbar an der Zuständigkeitsgrenze liegt oder sich großflächig über das Grenzgebiet erstreckt

#### 2.6.1.7 Dokumentationssystem

Bestandteil einer jeden BOS-Leitstelle ist ein Dokumentationssystem, welches alle Notrufgespräche (110/112) und – je nach landesrechtlicher Regelung – auch die übrige Sprachkommunikation (Telefonie, Funk) aufzeichnet. Hierbei wird nicht nur die reine Sprache (Audio) aufgezeichnet, sondern auch die zugehörigen Metadaten (A- bzw. B-Teilnehmernummer, Funkkennungen usw.) sowie Datum und Uhrzeit. Die Speicherdauer ist ebenfalls landesrechtlich geregelt und erstreckt sich meist über 90 oder 180 Tage. Ein Löschroutine sorgt dafür, dass alle Aufzeichnungen nach Fristablauf automatisch gelöscht werden.

Die Aufzeichnung erfüllt mehrere Zwecke:

- Dokumentation des Notrufeingangs und Inhalt der Meldung, wenn im Nachgang der Vorwurf der unterlassenen Hilfeleistung erhoben wird, weil ein Rettungsmittel gar nicht oder verspätet eingetroffen ist.
- Strafrechtliche Verfolgung böswilliger Anrufer
- Nochmaliges Abhören schwer verständlicher Anrufer bzw. Funkteilnehmer durch die Disponenten
- Interne Qualitätssicherung zur Gesprächsführung, insbesondere bei Notrufgesprächen

Historisch waren Dokumentationsanlagen als Tonbandmaschinen ausgeführt und stellten bis in die 2000er Jahre eine gesonderte Hardware dar. Aktuelle Kommunikationsmanagementsysteme (KMS) haben die Dokumentationsfunktion integriert und nutzen hierfür Festplatten- oder SSD-Speichersysteme (SAN). Unterschieden

werden *Kurzzeit-* und *Langzeitdokumentation*, die auf den gleichen Datenbestand zugreifen und sich lediglich hinsichtlich der Zugriffsrechte unterscheiden.

Die Kurzzeitdokumentation dient dem Disponenten an seinem Einsatzleitplatz, schwer verständliche Telefon- und Funkgespräche nochmals anzuhören. Dabei ist der Zugriff je nach Vorgabe auf die vergangenen 30 oder 60 Minuten bzw. max. auf die eigene Schichtdauer begrenzt. Zudem besteht eine reine Abhörmöglichkeit, jedoch keine Berechtigung zum Datenexport auf einen externen Datenträger. Im Regelfall ist die Kurzzeitdokumentation so parametriert, dass bei einem Schichtwechsel der nachfolgende Disponent mit seinem Login keinen Zugriff auf die aufgezeichneten Gespräche seines Schichtvorgängers hat.

Die Langzeitdokumentation dient der Nachvollziehbarkeit von Gesprächen, wenn polizeiliche oder staatsanwaltliche Ermittlungen geführt werden bzw. zu internen Qualitätssicherungsmaßnahmen. Über Suchfunktionen (nach Datum, Uhrzeit, Einsatznummer, A-Teilnehmerkennung, Funkkennung usw.) kann das gewünschte Gespräch bzw. alle Gespräche zu einem Einsatz gefiltert werden und auf einen Datenträger exportiert werden. Hierbei werden übliche Audio-Dateiformate wie z.B. *.mp3 oder *.wav genutzt. Der Zugriff auf die Langzeitdokumentation ist nur einem eng begrenzten Personenkreis vorbehalten (Leitstellenleitung), oftmals müssen zwei Berechtigte gleichzeitig eingeloggt sein (Vier-Augen-Prinzip). Der Export und die Auswertung von Notrufen zum Zwecke der Qualitätssicherung erfordert zudem die Zustimmung des Personal- bzw. Betriebsrats.

In Bezug auf die Informationssicherheit finden folgende Schutzziele beim Dokumentationssystem Anwendung: Die *Vertraulichkeit* wird bei der Kurzzeitdokumentation dadurch erzielt, dass nur der jeweils diensthabende Disponent an seinem Einsatzleitplatz Zugriff auf seine geführten Gespräche hat. Der Zugriff auf die Langzeitdokumentation ist besonders berechtigten Personen vorbehalten. Die *Verfügbarkeit* wird herstellerseitig durch ein Speichersystem sichergestellt, bei dem die Gesprächsdaten nicht nur auf einer Festplatte/SSD liegen, sondern redundant auf zwei oder mehr Datenträgern parallel gespeichert werden. Die *Integrität* ergibt sich aus der technischen Ausführung von Hard- und Software; es findet eine fortlaufende Aufzeichnung aller Gespräche einschließlich der Metadaten statt, so dass hier keine Manipulation möglich ist. Die einzige Zugriffs- und Bedienmöglichkeit sind die Such-, Abhör- und Exportfunktion im Rahmen des Kurz- und Langzeitaufzeichnung. Sofern nach landesrechtlicher Regelung neben den Notrufen auch alle

übrigen Telefongespräche aufgezeichnet werden, besteht für die Disponenten z.T. die Möglichkeit, Telefongespräche als „privat“ zu kennzeichnen und damit die Aufzeichnung abzubrechen. Dies gilt jedoch nur für die normalen Amtsleitungen und Nebenstellen, nicht für Notrufe. Die *Nichtzurückweisbarkeit* ist ein Kernbestandteil der Sprachdokumentation, da das gesprochene Wort von Gesprächsbeginn bis Gesprächsende aufgezeichnet wird, können getätigte Aussagen beider Gesprächsteilnehmer später nicht abgestritten werden.

#### 2.6.1.8 Andere Anwendungen

Neben den beiden Hauptsystemen KMS und ELS bestehen in den Leitstellen weitere Anlagen und Anwendungen, die zumeist Internet- bzw. IP-basiert arbeiten und z.T. über Schnittstellen mit ELS und/oder KMS verbunden sind [MK23]:

- Versorgungsnachweis zur aktuellen Anzeige verfügbarer Versorgungskapazitäten in Krankenhäusern, untergliedert nach medizinischen Fachrichtungen. Hier ist beispielhaft der *Interdisziplinäre Versorgungsnachweis* (IVENA) zu nennen, der in mehreren Bundesländern genutzt wird (flächendeckend in Brandenburg, Berlin, Bremen, Hessen, Niedersachsen, Sachsen-Anhalt, Schleswig-Holstein und zu Teilen in Bayern und Sachsen). IVENA ist im Webbrowser aufrufbar, so dass freie und belegte Ressourcen der Kliniken jederzeit eingesehen werden können. Je nach landesrechtlicher Regelung sind die Krankenhäuser verpflichtet, die Angaben jederzeit auf aktuellem Stand zu halten bzw. erledigen dies aus eigenem Interesse.
- Internet und (Verwaltungs-)Intranet werden meist auf getrennten Rechnern genutzt, die unabhängig von KMS und ELS sind. Die Internetrecherche nach Namen, Telefonnummern, Fachfirmen usw. ist auch im Arbeitsalltag einer Leitstelle ein fester Bestandteil.
- Warnsysteme, die Warnung der Bevölkerung kann sowohl über Sirenen als auch über Warn-Apps (z.B. KatWarn, NINA) erfolgen. Die erforderliche Steuerungstechnik ist meist in den Leitstellen mit untergebracht, da dort eine Reaktionsfähigkeit 24/7 gegeben ist und bei größeren Schadenslagen oder sich anbahnenden Unwettern jederzeit reagiert werden kann. Technisch ist die Anbindung an die bundesweiten Warnsysteme wie KatWarn, MoWaS) durch einen

gesonderten PC sichergestellt, der hinsichtlich Hard- und Software von den übrigen Leitstellensystemen (KMS, ELS) unabhängig ist.

- Gefahrenmeldeanlagen (GMA), d.h. Brandmeldeanlagen (BMA) bzw. Einbruchmeldeanlagen (EMA) sind über IP an entsprechende Empfangsgeräte in der Leitstelle angeschaltet, welche wiederum eine direkte Schnittstelle zum ELS haben, so dass z.B. beim Eingang eines Brandmeldealarms direkt ein Einsatz mit Alarmvorschlag der zuständigen Feuerwehr/-wache eröffnet wird und die Alarmierung zeitsparend (ohne händische Eingaben) direkt erfolgen kann.
- Medientechnik ist die Verknüpfung von KMS und ELS zur Darstellung bzw. Wiedergabe in anderen Räumen (z.B. Stabs- und Führungsräumen), in denen eine Übersicht über aktuell laufende Einsätze, verfügbare Einsatzmittel und Mithören des Funkverkehrs benötigt wird. Eine digitale Kreuzschiene ermöglicht das Aufrufen und Verteilen sämtlicher Informationen (incl. Rundfunk- und TV-Empfang) auf Bildschirme, Videobeamer und Lautsprecher, die im gesamten Gebäude verteilt sein können. Ergänzt wird die Medientechnik zumeist durch Rundfunk- und TV-Empfang, Kameras und Raummikrofonen für Videokonferenzen, Abspielgeräte für Speichermedien und Anschlüsse für Notebooks. Neben der unmittelbaren Darstellung von Informationen aus dem laufenden Leitstellenbetrieb bei größeren, stabsmäßig geführten Einsätzen, dient die Medientechnik auch der Aus- und Fortbildung und für Videokonferenzen. Die Medientechnik bzw. das Medien-LAN ist vollständig vom Leitstellen-LAN getrennt; zur Einspeisung von Bildinformationen wird z.B. das Monitorsignal abgegriffen und über einen Decoder in das Medien-LAN eingespeist, so dass es keinen IP-Übergang zwischen beiden Netzen gibt.
- Wachalarm: Ständig besetzte Wachen bei Berufsfeuerwehren werden mittels Alarmgong und anschließender Durchsage alarmiert. Zusätzlich wird über die Wachalarmsteuerung die Beleuchtung in den Fluren und Fahrzeughallen eingeschaltet und Tore geöffnet. Je nach alarmierter Einheit/Fahrzeug(en) sowie Tageszeit kann sich die Alarmierung per Wachalarm auf die jeweiligen Ruheräume der Besatzungen beschränken, so dass während der Nachtstunden nicht die gesamte Belegschaft geweckt wird.
- Haustechnik bzw. Haustechniksteuerung ist z.B. die Bedienung von Beleuchtung und Sonnenschutz direkt von den Einsatzleitplätzen aus. Auch die Bedienung und Besprechung von Türsprechstellen für den Einlass in das Gebäude ist

vielfach bei der Leitstelle mit angesiedelt und wird vom KMS aus (mit)bedient. Technisch sind diese Anschaltungen derart ausgeführt, dass über IP vom ELS bzw. KMS aus eine Speicherprogrammierbare Steuerung (SPS) angesteuert wird, die entweder selbst über elektrische Schaltkontakte verfügt oder die Signalisierung auf ein Bussystem der Gebäudeautomation umsetzt.

- Vernetzung mit anderen Leitstellen und Einsatzleitwagen (ELW); zur Realisierung von Überlauf- und Redundanzszenarien sind viele Leitstellen regional oder landesweit miteinander technisch vernetzt, so dass ein Datenaustausch ermöglicht wird, der verschiedenen Zwecken dient:
  - Flottenmanagement; gemeinsamer Zugriff bzw. Einsicht in freie und gebundene Einsatzmittel,
  - Übergabe von Einsätzen an andere Leitstellen (z.B. in grenznahen Bereichen),
  - Notrufabfrage und Funkkommunikation, wenn eine Leitstelle komplett ausfüllt und die Aufgaben temporär von einer anderen Leitstelle mit übernommen werden müssen.

## 2.7 Analog- und Digitalfunk

Den BOS sind Frequenzbänder im 70 cm-, 2 m-, 4 m-, 8 m-Wellenbereich zugeteilt, wobei im Analogfunk der 8m-Bereich eine untergeordnete Rolle spielt. Wesentlich bedeutsamer waren bzw. sind der 4 m-Bereich für die Kommunikation zwischen Leitstelle und Fahrzeugen (Fahrzeugfunk) sowie der 2 m-Bereich für die Kommunikation mit Handfunkgeräten mit Handfunkgeräten an der Einsatzstelle (Einsatzstellenfunk). [Gei97] Ab den 1990er Jahren wurden Teile des 2 m-Bandes auch für die POCSAG-Alarmierung genutzt. Der TETRA-Digitalfunk nutzt ein eigenes Frequenzband innerhalb des 70 cm-Wellenbereichs.

Die 4m-Funktechnik war [Ros79] (bzw. ist stellenweise noch) das Hauptkommunikationsmedium zwischen der Leitstelle und Einsatzfahrzeugen. Neben der reinen Sprachkommunikation wurde dieser Übertragungsweg auch für Steuersignale genutzt, die als fest definierte Tonfrequenzen anstelle von Sprache übertragen wurden. Hierzu zählen die Tonrufsteuerungen [Mel99] zum Aufschalten von Relaisstellen, die 5-Ton-Alarmierung einschließlich der Sirenenansteuerung über

gesonderte Doppeltöne und das Funkmeldesystem (FMS) [Mar06] zur Kurzdaten- und Textübertragung.

Die Leitstelle als funkbetrieblicher Mittelpunkt hat die technische und betriebliche Hoheit über den eigenen Funkverkehrskreis, da sie unmittelbar an das Gleichwellenfunksystem oder eine Relaisstelle angebunden ist. Zusätzlich gibt es als Rückfallebene „normale“ Funkgeräte (wie in Fahrzeugen oder Feuerwehrhäusern), mit denen die Leitstelle am Funkverkehr von Nachbarbereichen als normaler Funkteilnehmer (ohne Sonderstellung) teilnehmen kann.

Ein wesentlicher Nachteil des analogen BOS-Funks war und ist die mangelhafte Sicherheit gegen unbefugtes Abhören. Die Übertragung erfolgt – namengebend – analog frequenzmoduliert und kann ohne besonderen technischen Aufwand mittels frei verkäuflicher Funkscanner oder den bei den Einsatzkräften ohnehin vorhandenen analogen Funkmeldeempfängern mitgehört werden. Zusätzlich zum unerlaubten Mithören des gesprochenen Wortes ist auch die Auswertung der Tonsequenzen, die bei 5-Ton-Alarmierungen und FMS-Meldungen übertragen werden, mit einfachen Mitteln möglich. Abgesehen vom passiven Abhören und Auswerten der Kommunikation des geschlossenen Nutzerkreises BOS ist auch das aktive Einwirken ohne großen Aufwand möglich. Die Erzeugung von Tonruffrequenzen, 5-Ton-Folgen und FMS-Telegrammen und deren hochfrequente Aussendung über selbst gebaute Sender bzw. aus zweifelhaften Quellen erworbene BOS-Funkgeräte, ist mit ein wenig Grundwissen im Bereich IT bzw. Funktechnik möglich. Das Internet hat sein Übriges zur Verbreitung entsprechender Anleitungen und Programme beigetragen, ebenso Verkaufsplattformen, auf denen auch BOS-Funkgeräte und Zubehör angeboten werden. D.h. die Störung des Funkbetriebes, böswillige Alarmierungen von Einsatzkräften durch Auslösung der analogen Funkmeldeempfänger und auch das Absetzen falscher FMS-Statusmeldungen ist mit einfachen Mitteln machbar, kann jedoch den Dienstbetrieb in einer Leitstelle erheblich beeinträchtigen, wenn richtige von falschen Meldungen unterschieden werden müssen und fälschlicherweise alarmierte Einsatzkräfte über Funk ihren Auftrag erfragen wollen und diesen geantwortet werden muss, dass kein Einsatzauftrag vorliegt. Da es sich bei den skizzierten Szenarien ausnahmslos um Einflussnahme auf das analoge Funksystem handelt, ist seitens der Leitstelle hier kaum eine schnelle Abhilfe möglich. Bei dauerhaften Störungen bleibt nur der Einsatz eines Peilwagens der Bundesnetzagentur, um den Störsender zu lokalisieren, ggf. auch Einheiten der Landeskriminalämter

zur Mobilfunkaufklärung, die z.T. auch über entsprechende Mess- und Ortungstechnik verfügen. Im Sinne der IT-Sicherheit sind hier die Möglichkeiten einer Leitstelle sehr begrenzt, da im Wesentlichen eine externe Abhängigkeit vom Funksystem besteht, auf das die Leitstelle nur begrenzt (technischen) Einfluss hat, aber durch gezielte Störungen und Sabotagen des Funkverkehrs unmittelbar im Dienstbetrieb beeinträchtigt wird.

Im Sinne des Datenschutzes und der Beschränkung einsatztaktischer Informationen auf berechtigte Funkteilnehmer entwickelte sich der Anspruch an ein neues Funksystem, bei dem die hochfrequente Übertragung durch Verschlüsselung geschützt ist; treibende Kraft hierfür waren vor allem die polizeilichen Nutzer. Digitale Kommunikationstechnik hatte sich im kommerziellen Bereich längst etabliert (ISDN-Telefonie, zunehmende Verbreitung von Mobiltelefonen), so dass der Wunsch nach einem neuen, digitalen Funksystem aufkam, das gegen unbefugtes Mithören geschützt ist, eine klare Verständlichkeit bietet und über mehr Funktionen und damit auch mehr einsatztaktische Möglichkeiten verfügt, als die analoge Funktechnik. Die Idee und der Wille für ein Digitalfunksystem für die BOS waren daraufhin gegeben.

Im Jahr 1996 beschloss die Innenministerkonferenz die Einführung eines gemeinsamen digitalen Funksystems für die BOS in Deutschland. Etwa zeitgleich wurde vom *European Telecommunications Standards Institute* (ETSI) der digitale Bündelfunkstandard *TETRA* verabschiedet; dieses Akronym stand ursprünglich für „Trans-European Trunked Radio“ und wurde später in „Terrestrial Trunked Radio“ umbenannt, um TETRA auch außerhalb Europas vermarkten zu können. Um die Eignung von TETRA für die Sicherheitsbehörden zu testen, wurde 1999 das „Pilotprojekt Aachen“ initiiert, bei dem aufgrund der geografischen Lage auch die funktechnische Zusammenarbeit mit den Nachbarstaaten Belgien und Niederlande erprobt wurde. Der TETRA-Standard erwies sich prinzipiell als tauglich [HM10], auch wenn beim Pilotprojekt Aachen noch keine Ende-zu-Ende-Verschlüsselung implementiert war, die im heutigen bundesweiten Wirknetz von Anfang an mit ausgerollt wurde. Die Einführung des BOS-Digitalfunks in Deutschland nahm mit der Gründung der *Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben* (BDBOS) im Jahr 2007 Fahrt auf und auch der Ebene der Länder begannen die Einführungsmaßnahmen. Von Beginn an war auch das Bundesamt für Sicherheit in der Informationstechnik (BSI) beteiligt, um in Sachen IT-Sicherheit und Kryptoverfahren zu unterstützen.

### 2.7.1 Verschlüsselung

Ein wichtiger Schutz vor unbefugtem Mithören des hochfrequenten Übertragsungsweges ist die bereits im TETRA-Standard implementierte Luftschnittstellenverschlüsselung, bei der drei Verschlüsselungsklassen (Security Classes) unterschieden werden:

- Class 1, unverschlüsselt
- Class 2, verschlüsselt mit statischem Schlüssel (Static Cipher Key, SCK)
- Class 3, verschlüsselt mit dynamischem Schlüssel (Dynamic Cipher Key, DCK)

Im BOS-Digitalfunk in Deutschland wird zur Luftschnittstellenverschlüsselung Class 3 (DCK) genutzt. Als Rückfallebene kann bei Störungen, z.B. fehlgeschlagenem Schlüsselwechsel, auf eine niedrigere Verschlüsselungsklasse gewechselt werden, d.h. in allen Funkgeräten sind zudem SCK als „Rückfallebene“ in der Firmware abgelegt. Als Schutzmaßnahme wird z.B. bei dem Funkgerät MTM800 von Motorola der SCK gelöscht, sobald das Gehäuse geöffnet wird. Hierzu befindet sich ein Kontakt an der Innenseite des Gehäusedeckels, der beim Abnehmen des Deckels die Verbindung unterbricht, was das Löschen des SCK bewirkt. Durch diese konstruktive Maßnahme wird verhindert, dass der SCK durch Öffnen des Gehäuses an den Kontakten der Bauteile bzw. der Leiterplatte ausgelesen werden kann.

Bei den Security Classes 2 und 3 kommen je nach Anwendung (industriell, behördlich; innerhalb oder außerhalb der EU) verschiedene *TETRA Encryption Algorithms* (TEA) zur Anwendung:

- TEA-1, industrielle Verschlüsselung (EU)
- TEA-2, Behördenverschlüsselung (EU)
- TEA-3, Behördenverschlüsselung (nicht EU)
- TEA-4, industrielle Verschlüsselung (nicht EU)

Beim BOS-Digitalfunk wird TEA-2 genutzt. Dieser ist in der Hardware (bzw. Firmware) der Endgeräte implementiert.

Die Luftschnittstellenverschlüsselung des TETRA-Standards schützt ausschließlich den hochfrequenten Teil des Übertragungsweges zwischen den Funkgeräten (Direktmodus) bzw. zwischen Funkgerät und Basisstation (Netzmodus). [HM10]

Die weitere Übertragung im Funknetz selbst ist nicht standardisiert. Für den BOS-Digitalfunk wurden daher zwei zusätzliche Verschlüsselungen geschaffen:

1. Ende-zu-Ende-Verschlüsselung (End-to-End-Encryption, E2EE)
   Schützt den kompletten Übertragungsweg von Endgerät zu Endgerät und ist im Fall der hochfrequenten Übertragung auch der Luftschnittstellenverschlüsselung überlagert. Der Schlüssel für die E2EE ist auf der BOS-Sicherheitskarte gespeichert und wird bei der sog. *Personalisierung* auf der Sicherheitskarte gespeichert.

2. Sandwich-Konzept (Leitstellenanbindung)
   Erläuterung und Details siehe Abschnitt 2.7.2

Für die Ende-zu-Ende-Verschlüsselung ist in den Funkgeräten der Verschlüsselungsalgorithmus Bestandteil der Firmware; da die Funkgeräte für BOS-Nutzung einer Zertifizierungspflicht unterliegen, ist sichergestellt, dass die Verschlüsselungsfunktion herstellerunabhängig bei allen zertifizierten Geräten gegeben ist. Der Schlüssel selbst ist auf der BOS-Sicherheitskarte (BOS-SiKa, siehe Abbildung 2.5) abgelegt, die unabhängig vom Erwerb des Funkgeräts über die zuständige Autorisierte Stelle (AS) bezogen werden muss. [HM10] Ähnlich wie bei einer SIM-Karte für Mobiltelefone ist auf der BOS-SiKa die Netzzugangsberechtigung hinterlegt, ebenso die zugeteilte Operativ-taktische Adresse (OPTA). Ohne BOS-SiKa ist das Einbuchen ins BOS-Digitalfunknetz und damit auch keine Teilnahme am Funkverkehr möglich. Als sicherer Kanal für die Übertragung des Schlüssels (hier: BOS-SiKa) dient der Postversand bzw. die persönliche Übergabe. Die BOS-SiKa werden von den Autorisierten Stellen in gesperrtem Zustand versendet und werden erst nach Rückmeldung des berechtigten Adressaten nach Erhalt der Karten entsperrt. Auf dem Transportweg abhanden gekommene Karten können somit nicht missbräuchlich genutzt werden.


Abb. 2.5: BOS-Sicherheitskarte (uncodierte Musterkarte)

Das kryptographische Gegenstück zur BOS-SiKa im Funkgerät ist die Mehrkanal-Kryptokomponente (MKK, siehe Abbildung 2.6), die als PCI-Einsteckkarte im Digitalfunkgateway der Leitstelle zum Einsatz kommt. [HM10] Während die BOS-SiKa nur den Schlüssel für eine Funkgruppe bereitstellt und auch das Funkgerät immer nur ein Funkgespräch ver- bzw. entschlüsseln kann, müssen in einer Leitstelle mehrere Funkgespräche parallel ver- bzw. entschlüsselt werden, daher rührt die Bezeichnung Mehrkanal-Kryptokomponente.

Die MKK-Karten sind im Auftrag des BSI von T-Systems für das BOS-Digitalfunknetz entwickelt worden. Auch die Fertigung der Karten erfolgt durch T-Systems auf Basis einer Lizenzierung durch das BSI, wobei die MKK-Karten zusätzlich zu den behördlichen Anforderungen über weitere Anwendungsfelder verfügen, um das Produkt auch außerhalb behördlicher Anwendungen vermarkten zu können (Produktbezeichnung *Telesec LineCrypt MKK BOS*). Die Abgabe der MKK-Karten erfolgt nur auf schriftliche Bestellung an Behörden bzw. berechtigte Anwender unter Führung eines Verwendungsnachweises bei T-Systems. Durch diese Verfahrensweise wird sichergestellt, dass die Schlüsselmittel bzw. die damit eng verbundene Hardware nicht in die Hände Unbefugter gelangen können.

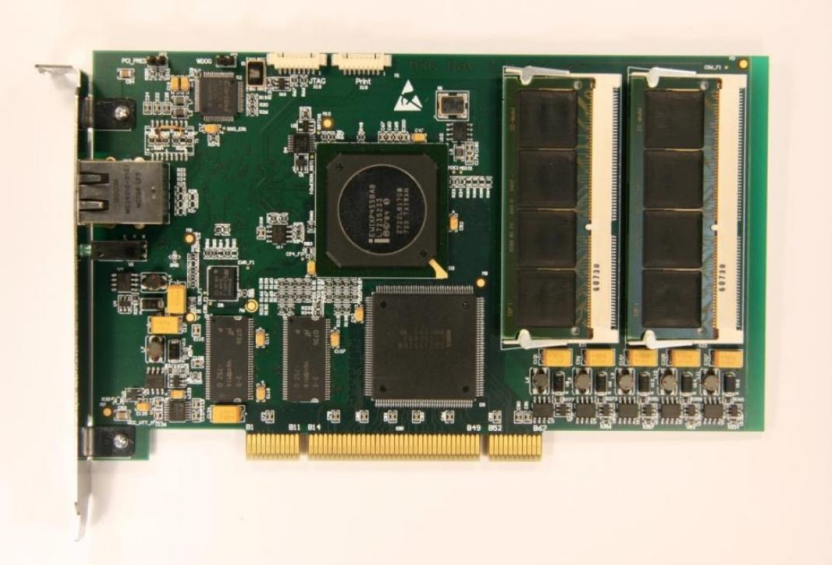


Abb. 2.6: MKK-Karte mit 64 Kanälen

Je nach Bestückung kann eine MKK-Karte 32 oder 64 Kommunikationskanäle im Duplex-Betrieb kryptieren (Bezeichnungen *MKK32* bzw. *MKK64*). Nach der Fertigung beim Hersteller T-Systems enthält die MKK-Karte lediglich die Firmware. Anschließend erfolgt die Initialisierung beim BSI, d.h. die Netzzugangsdaten und die BOS-Kryptoapplikation werden auf die Karte geladen. Nach der Initialisierung wird die MKK-Karte an T-Systems zurückgeliefert, da T-Systems dann wiederum den Vertrieb der initialisierten Karten an berechtigte Nutzer übernimmt (s.o.).

### 2.7.2 Leitstellenschnittstellen

Das BOS-Digitalfunknetz ist vom Grundaufbau her ein gesondertes Telekommunikationsnetz, das aufgrund der Vielzahl der Funkteilnehmer hauptsächlich als „Mobilfunknetz“ fungiert, wobei auch Festnetzanschlüsse existieren; zur Netz- und Teilnehmeradministration sowie zur Anbindung der Leitstellen als „Festnetzteilnehmer“.

Für die Leitstellen bestehen die Leitstellenschnittstellen LS1, LS2 und LS3, wobei LS1 zur Sprachübertragung dient, LS2 für Steuerfunktionen und LS3 für Datenübertragung und Netzmonitoring. [LC23] Die Schnittstellen sind technisch unterschiedlich ausgeführt, da LS1 als PCM-codierte Schnittstelle (G.703 / G.704) realisiert wurde, während LS2 und LS3 IP-basiert ist. Dieser Umstand hat bereits zum

Zeitpunkt der Auftragserteilung an das Unternehmen EADS z.T. für Unverständnis in der Fachwelt gesorgt, warum zur Anbindung der Leitstellen an das Digitalfunknetz verschiedene Schnittstellen und Protokolle verwendet werden und nicht durchgängig IP Verwendung findet. Die Schnittstelle LS2 wird von Seiten der Vermittlungsstelle vom *TETRA Connectivity Server* (TCS) bereitgestellt; die TCS-Clients für die Leitstellenarbeitsplätze können nach Wunsch des Nutzers im Verhältnis Sprach- zu Mithörkanälen konfiguriert werden; dabei sind die Konfigurationen 1:3, 1:7 und 1:15 möglich, so dass zu einem Sprachkanal entweder drei, sieben oder 15 Mithörkanäle zugeordnet werden können.

Die LS1 ist als E1-Datenschnittstelle ausgeführt (Übertragungsrate 2.048 kbit/s), wobei je TETRA-Gesprächskanal 8 kbit/s zur Verfügung stehen. D.h. pro LS1 sind bis zu 256 parallele TETRA-Gespräche möglich. Bei der durchschnittlichen Anzahl an Arbeitsplätzen und damit maximal parallel geführter Funkgespräche ist eine LS1/E1 pro Leitstelle mehr als ausreichend bzw. sogar überdimensioniert. Die LS1 als reine Schnittstelle für Sprachdaten ist allein nutzlos, es ist zusätzlich eine LS2 erforderlich, um die Rufsignalisierung, Sprechtaste (PTT), Gruppen- und Kanalzuordnung zu steuern. Nur das Pärchen LS1 + LS2 stellt den vollen Funktionsumfang für den Sprechfunkbetrieb und die Übermittlung der begleitenden Steuerdaten zur Verfügung. Dieses Prinzip findet sich auch bei anderen digitalen Sprachübertragungsverfahren; z.B. werden auch bei VoIP der Gesprächsaufbau und die eigentliche Gesprächsübertragung durch verschiedene Protokolle realisiert. Über das *Session Initiation Protocol* (SIP) wird der Verbindungsauf- und Abbau zwischen den beteiligten Endgeräten gesteuert, die Sprachdaten werden als Datenstrom mittels *Real Time Transport Protocol* (RTP) übertragen. Bei VoIP laufen beide Protokolle über die gleiche physikalische Schnittstelle, während es sich bei der Digitalfunkanschaltung der Leitstellen mit LS1 und LS2 um zwei physikalisch getrennte Schnittstellen handelt, welche mit PCM und IP obendrein unterschiedliche Übertragungsverfahren/Protokolle nutzen.

Zwecks Zusammenfassung der Schnittstellen LS1, LS2 und LS3 zu einer IP-Schnittstelle zwecks besserer Ressourcenverteilung und wirtschaftlichen Vorteilen bei der Leitstellenanbindung wurde von einem Arbeitskreis des Bundesverbandes Professioneller Mobilfunk e.V. (PMeV) eine entsprechende Handreichung erarbeitet („Digitalfunkstecker“). [PM16] Ungeachtet der Schnittstellenbündelung besteht

nach wie vor die Anforderung einer verschlüsselten Übertragung mittel zugelassener Verfahren.

Für Administrations- und Steuerungsaufgaben in der Netzverwaltung verfügen die Autorisierten Stellen des Bundes und der Länder eine Anbindung über eine gesonderte Schnittstelle, die Schnittstelle für Autorisierte Stellen (ASS1).

Wie bereits erwähnt, ist im TETRA-Standard lediglich die Verschlüsselung der Luftschnittstelle standardisiert. Um die Nutzinformation zu schützen, wurde daher die Ende-zu-Ende-Verschlüsselung entwickelt und implementiert. Um die Steuerinformation zu schützen, die über die Schnittstelle LS2 übertragen werden, ist eine Abschnittsverschlüsselung erforderlich, die auf der Festnetzverbindung zwischen Vermittlungsstelle und Leitstelle zur Anwendung kommt. Das „Einpacken" der beiden Endpunkte an Vermittlungsstelle und Leitstelle in einen sicheren Übertragungskanal wird als Sandwich-Konzept bezeichnet. Hierfür sind nur vom BSI zertifizierte Verschlüsselungskomponenten zulässig (z.B. SINA-Box).

### 2.7.3 POCSAG-Alarmierung

In Deutschland ist die Alarmierung von haupt- und ehrenamtlichen Einsatzkräften über tragbare Meldeempfänger mittels des POCSAG-Standards weit verbreitet; dieses Verfahren wird auch als *Digitale Alarmierung* (DA) bezeichnet, wobei hier lediglich eine begriffliche, aber keine technische Ähnlichkeit mit dem Digitalfunk (s.o.) besteht. POCSAG ist das Akronym für *Post Office Code Standard Advisory Group*, des gleichnamigen britischen Standardisierungsgremiums. Neben BOS-eigenen Netzen, die meist auf die jeweiligen Verwaltungsbereiche begrenzt sind, ist ein POCSAG-basierter Funkrufdienst auch bundesweit kommerziell im Einsatz. Bis 1999 wurde dieser unter der Produktbezeichnung *Cityruf* von der Deutschen Telekom AG betrieben und ging dann an den Betreiber e*message über und trägt seitdem den Produktnamen *e*Cityruf*.

Technisch werden Trägerfrequenzen in den Wellenlängenbereichen 2m (BOS) und 70cm (kommerziell und Amateurfunk) genutzt. Die Modulation erfolgt als 2-FSK zur Übertragung in Binärform, bei der zwischen zwei Frequenzen umgetastet wird. Zur Übertragung einer logischen „0" liegt diese 4 kHz oberhalb der Mittenfrequenz,

für eine logische „1“ liegt diese 4 kHz unterhalb der Mittenfrequenz. Da die eigentliche Trägerfrequenz keinem der beiden binären Zustände zugeordnet ist, handelt es sich um eine *Non-Return-to-Zero*-Übertragung (NRZ) und ist damit eine direkte Frequenzumtastung (*Direct Frequency Shift Keying*, DFSK). [HL93] Die Übertragungsrate beträgt 512 bzw. 1200 Baud und ist für die Alarmsignalisierung mit ergänzender Textanzeige (standardmäßig 250 alphanumerische Zeichen) ausreichend. Diese 250 Zeichen gelten bei unverschlüsselter Übertragung; wenn eine Verschlüsselung hinzukommt, reduziert sich die Anzahl der Zeichen, da einige Bits z.B. für die Initialisierungsvektoren benötigt werden. Die zugrundeliegende *Technische Richtlinie der Behörden und Organisationen mit Sicherheitsaufgaben – Geräte für die digitale Funkalarmierung* (TR-BOS) beinhaltet die technische Umsetzung des POCSAG-Verfahrens zum Zwecke der Funkalarmierung; sie enthält keine Vorgaben zur Verschlüsselung der per Funk übertragenen Daten.

Um den Anforderungen des Datenschutzes Rechnung zu tragen – dies betrifft vor allem die Bereiche Rettungsdienst und Krankentransport mit der Übermittlung von Patientendaten – hat sich seit einigen Jahren eine ergänzende Verschlüsselung zum Standard entwickelt. Hierbei haben sich im Wesentlichen zwei Verfahren am Markt etabliert, *IDEA* (International Data Encryption Algorithm) und *BOSKRYPT*.

IDEA ist eine im Jahr 1990 in der Schweiz entwickelte Blockchiffre, die eine Optimierung von DES (siehe 2.5.2) darstellt und ebenso mit Blocklängen von 64 Bit arbeitet, allerdings gegenüber DES eine Schlüssellänge von 128 Bit besitzt. Bei der Implementierung in einem POCSAG-Alarmierungssystem werden pro Netz bzw. System (i.d.R. auf eine Verwaltungseinheit begrenzt) 16 Schlüssel festgelegt, die wahlweise zur IDEA-Verschlüsselung genutzt werden können. Im Gegensatz zu BOSKRYPT besitzt IDEA weniger Overhead und auch keine feste Begrenzung übertragbarer Zeichen, während bei BOSKRYPT eine Länge von maximal 180 Zeichen fest vorgegeben ist. Kryptografisch basiert BOSKRYPT auf AES-128 mit einer Schlüssellänge von 256 Bit. Die Besonderheit bei BOSKRYPT ist die Schlüsselanzahl, da jede Rufadresse (*RIC*, Radio Identification Code) einen eigenen Schlüssel besitzt; das Schlüsselmanagement ist damit aufwändiger als bei IDEA.

Die Verschlüsselung der Alarmnachricht kann prinzipiell bereits im ELS erfolgen, das den verschlüsselten Datensatz an den *Digitalen Alarmgeber* (DAG) weitergibt oder aber dies erfolgt erst im DAG. Letzteres Verfahren hat sich am Markt etabliert,

somit bleibt die Verschlüsselung innerhalb des POCSAG-Alarmierungssystems und aus dem ELS heraus gelangt die Alarmansteuerung unverschlüsselt zum DAG.

## 2.8 Kernprozess

Bei der Betrachtung der verschiedenen Komponenten und Systeme in einer Leitstelle gilt es, die kritischen Prozesse herauszuarbeiten und diese von den nicht-kritischen abzugrenzen. Als nicht-kritisch werden hierbei Prozesse angesehen, die für die Notrufabfrage, Disposition und Alarmierung nicht relevant sind; ungeachtet möglicher rechtlicher Vorgaben.

Als Kernaufgabe der täglichen Arbeit einer Integrierten Leitstelle ist der Prozess anzusehen, der vom Eingang eines Notrufs bis zur Alarmierung der Einsatzmittel bzw. -einheiten reicht. Dieser folgt dem EVA-Prinzip der Datenverarbeitung, bestehend aus Eingabe, Verarbeitung und Ausgabe [Kas99] (Abb. 2.7).


Abb. 2.7: EVA-Prinzip

Zur Eingabe zählen der Notruf als telefonisch eingehendes Hilfeersuchen mit der begleitenden manuellen Erfassung der übermittelten Informationen während des Notrufgesprächs. Die Verarbeitung beinhaltet die Übergabe der Metadaten des Anrufers (A-Teilnehmerkennung) vom Kommunikations- an das Einsatzleitsystem; letzteres macht anhand der erfassten Informationen (Einsatzstichwort, Adresse) und den hinterlegten Vorgaben (Alarmpläne, ggf. mit tageszeitlicher Abhängigkeit) einen Alarmvorschlag für ein oder mehrere Einsatzmittel. Sowohl der Audiokanal des Notrufgesprächs als auch dessen begleiteten Daten werden gespeichert (Dokumentation), ebenso die erfassten Einsatzdaten aus dem ELS.

Beim Teilprozess Ausgabe übergibt das ELS die Ortsdaten (Adresse bzw. Geoposition) an das Geoinformationssystem zwecks Visualisierung der Einsatzstelle. Zudem wird der manuell freigegebene Alarmvorschlag an die entsprechenden Subsysteme übergeben. Im Falle einer Wachalarmierung hauptamtlicher Kräfte per Lautsprecherdurchsage ist das Audiosignal vom KMS ebenso Bestandteil der Alarmierung, sofern keine automatische Text-to-Speech-Umsetzung anhand der Einsatzdaten aus dem ELS erfolgt. Ergänzend zur Alarmierung gibt es je nach Einsatzart ggf. eine ergänzende Benachrichtigung bestimmter Personen bzw. Stellen per E-Mail, Telefax und/oder SMS. Gegenüber der Alarmierung, die ohne Zeitverzug übermittelt und im Zielsystem akustisch und optisch signalisiert werden soll, ist die Benachrichtigung nicht zeitkritisch, so dass ein eventueller Warteschlangenbetrieb bei der E-Mail-, Fax- und SMS-Übertragung vertretbar ist.

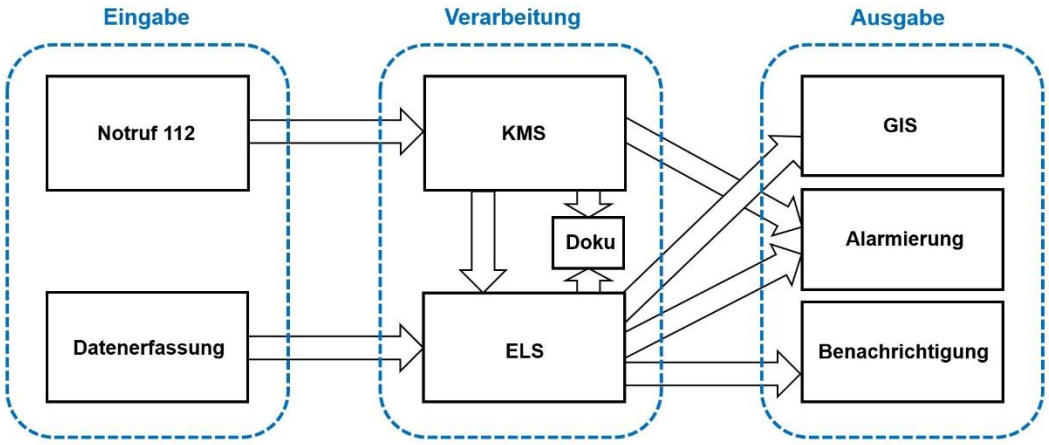



Abb. 2.8: EVA-Prinzip von Notrufannahme bis Alarmierung

Neben diesem Kernprozess sind als Varianten auch der Meldungseingang ohne den telefonischen Notruf möglich, z.B. mittels Notruf-App (siehe 2.6.1.3), durch automatischer Brandmeldeanlagen oder Nachforderungen, die von bereits vor Ort befindlichen Fahrzeugen per Funk übermittelt werden. Bei der Verarbeitung wird im letztgenannten Fall kein Einsatz neu angelegt, sondern einem bestehenden Einsatz eine Nachforderung hinzugefügt und ein geeignetes und verfügbares Einsatzmittel zugeordnet und alarmiert (Ausgabe).

Parallel hierzu gibt es eine Vielzahl weiterer Prozesse, die sich sowohl auf den akuten Einsatz beziehen als auch einsatzunabhängig getätigt werden. Während des laufenden Einsatz- bzw. Tagesgeschehens gehören beispielsweise die Erfassung

von Lagemeldungen, Abfrage freier Versorgungskapazitäten in Krankenhäusern und Patientenzuweisung, Entgegennahme von Voranmeldungen für Krankentransporte sowie Informationsbeschaffung zu Gefahrstoffen, Wetterdaten und speziellen Ansprechpartnern/Fachfirmen zu den Standardprozessen.

### 2.8.1 Kritikalität des Kernprozesses

Hinsichtlich der Sicherheitsrelevanz werden die einzelnen Teilschritte und deren Datenübergabe modellhaft gesondert betrachtet und priorisiert. Dabei liegt der Fokus auf der Notrufbearbeitung und Alarmierung, um schnellstmöglich Hilfe entsenden zu können. [GRH18] Ungeachtet der rechtlichen Vorgaben (z.B. Dokumentation) wird an dieser Stelle ausschließlich dem Kernprozess eine hohe, sicherheitskritische Relevanz eingeräumt, nicht jedoch den Nebenprozessen. Abbildung 2.9 veranschaulicht diese Festlegung, wobei die Datenübergänge mit hoher Priorität rot, mit mittlerer Priorität gelb und mit niedriger Priorität grün gekennzeichnet sind.

Als hoch priorisiert ist der Notrufeingang anzusehen und dessen Verarbeitung im KMS, d.h. optische und akustische Signalisierung („Klingeln“) an den Einsatzleitplätzen und das Herstellen der Sprachverbindung zum annehmenden Platz. An diesen Platz erfolgt die manuelle Datenerfassung anhand der Auskünfte des Anrufers. Das ELS generiert anhand der Ortsdaten und des vom Disponenten ausgewählten Einsatzstichworts einen Alarmvorschlag für die zuständigen Einsatzmittel. Die manuelle Dateneingabe ist dabei gleichermaßen von hoher Bedeutung, da ohne Grunddaten (Einsatzort, d.h. Adressangabe sowie Einsatzstichwort als Kategorisierung) kein Einsatz im ELS eröffnet und keine Einsatzmittel zur Alarmierung vorgeschlagen werden. Der Alarmvorschlag kann manuell ergänzt oder geändert werden und wird sodann vom Disponenten ausgelöst, wodurch angebundene Subsysteme (Alarmgeber, Wachalarmsystem) angesteuert werden. Diese Abläufe sind unabdingbar und daher in Abbildung 2.9 rot markiert und als hochpriorisiert eingestuft.

Die automatische Übergabe von Metadaten des Notrufs (A-Teilnehmerkennung, Ortsdaten usw.) vom KMS an das ELS ist eine wichtige Hilfe, um die Grunddaten des Einsatzes zu befüllen. Hinsichtlich der Kritikalität wird dieser Vorgang hier mit mittlerer Priorität betrachtet, da bei Wegfall dieses Automatismus‘ auch eine

manuelle Erfassung möglich ist, wobei jedoch das Risiko von Eingabefehlern nicht auszuschließen ist und zudem ein zusätzlicher Arbeitsschritt seitens des Disponenten erforderlich wird. Die Datenausgabe zum Zwecke einer alarmbegleitenden Benachrichtigung wird hier ebenfalls als mittlere Priorität klassifiziert, da die Alarmierung der Einsatzkräfte Vorrang hat (s.o.) und die begleitende Benachrichtigung über marktübliche Verfahren (E-Mail, SMS, Alarmierungs-Apps) erfolgt, wodurch eine schnellstmögliche Übermittlung ohnehin nicht gewährleistet werden kann, da hier eine vollständige Abhängigkeit von externen Telekommunikations- und IT-Dienstleistern besteht und bei hoher Netzlast ein Warteschlagenbetrieb erfolgt, auf den die Leitstelle keinen Einfluss nehmen kann. Sofern die Alarmierung hauptberuflicher Kräfte mittels Wachalarm erfolgt, schließt sich nach dem akustischen Signal (Alarmgong) eine Durchsage zu Art und Ort des Einsatzes an. Diese kann entweder direkt vom Disponenten eingesprochen werden, was in Abbildung 2.9 als Informationsübergang vom KMS zur Alarmierung dargestellt ist und hier als mittlere Priorität (gelb) angesehen wird oder es erfolgt eine automatische Durchsage mittels Text-to-Speech, die aus den Einsatzdaten des ELS generiert wird und keine Live-Durchsage erfordert.

Von nachrangiger Priorität wird an dieser Stelle die Dokumentation, d.h. die Erfassung und Aufzeichnung des gesprochenen Wortes beim Notrufgespräch, die notrufbegleitenden Metadaten sowie die manuell erfassten Daten betrachtet (grün), auch wenn es in allen Ländern rechtliche Vorgaben zur Dokumentation gibt. Die nachrangige Priorität gilt ebenso für die Darstellung des Einsatzortes im Geoinformationssystem. Letzteres wird hier beispielhaft als reines Anzeigesystem betrachtet, wobei das GIS auch dem Schritt „Verarbeitung“ zugeordnet werden kann, wenn eine ortsbasierte Disposition erfolgt, d.h. es wird das Einsatzfahrzeug entsandt, das die kürzeste Anfahrtszeit zum Einsatzort hat und nicht das, welches formal örtlich zuständig ist. Dies setzt ein GIS mit Routingfunktion sowie eine fortlaufend aktualisierte Positionsübertragung (GPS) der Einsatzmittel voraus. [Lin23]

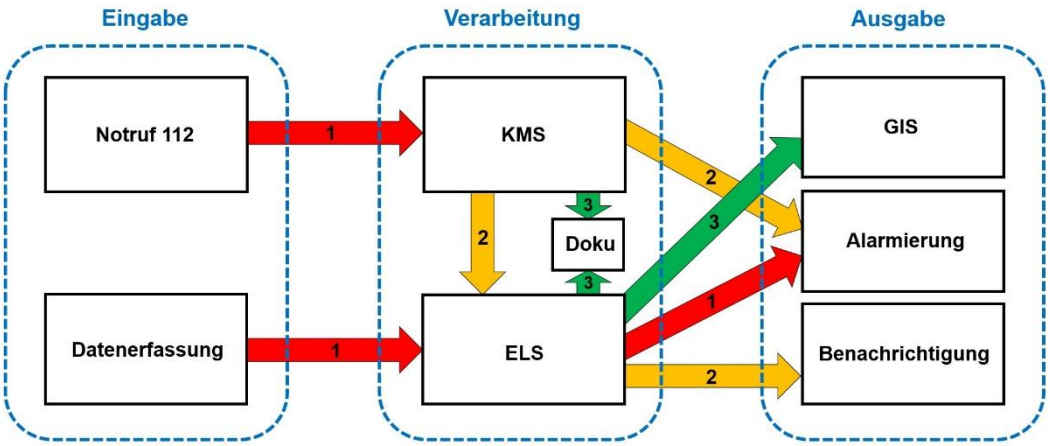



Abb. 2.9: Priorisierung der Prozesse

Im Sinne der IT-Sicherheit kommt nach der o.g. Priorisierung der Notrufannahme und der Alarmierung die höchste Bedeutung zu (kritische Pfade), da es sich einerseits um zeitkritische Prozesse handelt und andererseits eine Anbindung zu externen Systemen besteht. Die notrufbegleitende Datenerfassung ist zwar prozessual untrennbar mit dem Notrufgespräch verbunden, erfolgt allerdings innerhalb der Leitstelle und ist nicht von extern angebundenen Systemen abhängig.

Bei der vielfältigen Zusammenarbeit von Software und Softwaremodulen unterschiedlicher Hersteller ist daher stets zu hinterfragen, ob die Kombination von Modul 1 und Modul 2 – die isoliert für sich betrachtet jeweils sicher sind – ebenfalls sicher ist. D.h. hier darf nicht der Trugschluss entstehen, dass zwei (oder mehr) sichere Einzelmodule auch im Zusammenwirken ein sicheres Gesamtkonstrukt ergeben. Die UND-Bedingung der Boole'schen Algebra findet in diesem Zusammenhang keine Anwendung.

*„Im Rahmen der Weiterentwicklung der Anwendung werden die einzelnen Module oder Units zu Programmen oder Programmgruppen zusammengefügt. Die Erfahrung lehrt, dass funktionierende Einzelteile keineswegs immer ein funktionierendes Ganzes ergeben."* [Alp94]

# 3 Variablen der IT-Sicherheit

Basierend auf den organisatorischen und technischen Grundlagen in Kapitel 2 ergeben sich für Leitstellen verschiedene Variablen, welche die IT-Sicherheit direkt oder indirekt bestimmen. [FVL21]

## 3.1 Bauliche Anforderungen

Der IT-Grundschutz des BSI stellt grundlegende Anforderungen an den Baukörper, in dem IT-Systeme untergebracht und betrieben werden. Hierzu gehören ein Elementarschutz, d.h. ein Gebäude, das gegen unbefugtes Eindringen und Extremwetterereignisse widerstandsfähig ist. Dies beginnt bei der Auswahl des Grundstücks, welches nicht durch Hochwasser (Nähe zu Fließgewässern, Überflutungsbereiche) oder durch eine Hang- oder Tallage hinsichtlich Wassereintritt besonders gefährdet ist. Einbruchhemmende Fenster und Türen, Sicherung von Lichtkuppeln und Kellerschächten, Umzäunung des Geländes, Zugangskontrolle und technische Sicherheitssysteme wie z.B. elektronische Schließanlage, Kameraüberwachung, Einbruchmeldeanlage, Wasser- und Gasdetektion sind hier zu nennen. Serversysteme sollen nicht in Räumen errichtet werden, durch die Wasserleitungen verlaufen. Hinsichtlich der Resilienz gegenüber Extremwetterlagen sind auch zukünftige Entwicklungen im Rahmen des Klimawandels zu berücksichtigen. [SV20]

Dem baulichen Brandschutz, d.h. der Verwendung nicht brennbarer bzw. schwer entflammbarer Baustoffe und Materialien, brandschutztechnischer Abgrenzung wichtiger Funktionsbereiche, Brandfrüherkennung [Rau23] mittels automatischer Brandmeldeanlage sowie Entrauchungsmöglichkeiten stellen einen weiteren unabdingbaren Baustein in der materiellen Sicherheit dar.

Eine stabile und belastbare Bedachung, die widerstandsfähig gegen Starkregen, Hagel und Sturm ist und auch größere Schneelasten tragen kann, ist unabdingbar. Erd- und Untergeschoss(e) müssen gegen das Eindringen von Hochwasser gesichert sein. In jüngster Zeit gerät auch die Nutzung von Drohnen zunehmend in den Fokus von Sicherheitsbetrachtungen, da neben dem Ausspähen von vertraulichen

Informationen auch das aktive Einwirken (Sabotage) möglich ist, z.B. durch das Einbringen von Chemikalien in Lüftungsöffnungen.

## 3.2 Gebäudetechnische Anforderungen

Die Gebäudetechnik – hier ist insbesondere die Energieversorgung zu nennen – muss ebenso belastbar und in Teilen auch vollredundant ausgeführt sein. Da ein Ausfall der Stromversorgung – lokal und überregional, im Bereich von Minuten bis hin zu mehreren Tagen – niemals ausgeschlossen werden kann, ist hier eine Autarkie am Leitstellenstandort unabdingbar. Das Szenario eines mehrwöchigen Stromausfalls in weiten Teilen Europas und den Auswirkungen auf Verwaltung, Politik und Gesellschaft hat Marc Elsberg in seinem Roman „Blackout“ [Els13] skizziert; durch die Detailtiefe der fiktiven Darstellung wird das Werk vielfach als „Referenz“ im Zusammenhang mit Vorsorgemaßnahmen gegen mögliche Stromausfälle angeführt.

Eine Unterbrechungsfreie Stromversorgung (USV) sowie eine Netzersatzanlage (NEA) mit ausreichend bemessenem Kraftvorrat und der Möglichkeit zum Nachtanken bei laufendem Betrieb sind unabdingbar. Ergänzend ist ein Anschluss zur externen Einspeisung erforderlich, falls die fest verbaute NEA defekt ist oder wegen Wartungsarbeiten außer Betrieb ist und eine externe Stromversorgung durch eine mobile NEA erforderlich wird.

Heizung und Klimatechnik müssen ebenfalls redundant ausgeführt sein, da eine fehlende Kühlung von Serverräumen den IT-Betrieb erheblich beeinträchtigen kann, was einem faktischen Betriebsausfall gleichkommen kann. Die heutigen Möglichkeiten der gebäudetechnischen Ausstattung ermöglichen eine Wärmerückgewinnung aus dem Serverbetrieb, so dass sich die Aufwände für die Heizenergie mindern, was nicht nur wirtschaftlich, sondern auch nachhaltig ist.

## 3.3 Organisatorische Anforderungen

Die vorgenannten baulichen und technischen Anforderungen sind nur wirksam, wenn sie zusammen mit den organisatorischen Prozessen und personellen Maßnahmen als Sicherheitspaket zusammenwirken. Bei sämtlicher Leitstellen- und Gebäudetechnik kommen neben der Bauausführung in Installation der anschließend folgenden Instandhaltung und Wartung eine hohe Bedeutung zu. Serviceverträge zu allen Gewerken mit turnusmäßiger Wartung aller technischen Systeme sind unabdingbar. Daneben müssen für alle kritischen Systeme jederzeit verfügbare Servicetechniker mit vertraglich definierten Reaktions-, Eingriffs- und Wiederherstellungszeiten zur Verfügung stehen. Neben den Investitionen beim Bau oder der Sanierung eines Gebäudes und der technischen Ausstattung sind für den Betrieb gleichermaßen die erforderlichen Gelder in die laufende Finanzplanung mit aufzunehmen sowie Rücklagen für unerwartete Instandhaltungsmaßnahmen zu bilden.

Die Handhabung der Rückfall- und Notebenen muss regelmäßig geschult und geübt werden, damit diese Prozesse im Ernstfall beherrscht werden. Hierzu gehört auch die Sensibilisierung aller Mitarbeiter hinsichtlich Informationssicherheit und die Erstellung und Fortschreibung eines Notfallhandbuchs. Standardisierte Prozesse nach den Vorgaben von ITIL und ISO 27001; siehe hierzu auch 2.5.5. Externe Unterstützung bei Sicherheitsvorfällen kann auch durch ein *Computer Emergency Response Team* (CERT) erfolgen. Hierbei sind sowohl die Zuständigkeit des in Frage kommenden CERT (Landes- oder Kommunalebene) zu berücksichtigen als auch die Besonderheiten des BOS-Leitstellenbetriebs abzustimmen.

Ein Rechte- und Rollenmanagement, das stets auf aktuellem Stand gehalten wird, ist für den sicheren Betrieb der IT-Systeme unabdingbar.

*„Viele Anwendungen erlauben bestimmte Vorgänge nur Benutzern einer bestimmten Gruppe mit spezifischen Rechten. Ein Anwender der Standardgruppe hat beispielsweise nur das Recht, Daten einzusehen; die Anwender einer speziellen Gruppe haben hingegeben vielleicht auch die Erlaubnis, Daten zu ändern oder zu löschen; und die Anwender, die zur Gruppe der Administratoren gehören, können alle Vorgänge durchführen, einschließlich der Anwenderregistrierung und der Zuweisung von Rechten. Eine Sicherheitsbedrohung besteht immer dann, wenn Rechte auf nicht vorgesehene Art zugewiesen oder erlangt werden können – egal ob dies vorsätzlich oder aufgrund fehlerhafter Software geschieht.“* [BMK15]

Zu einer gewissenhaften Rechte- und Rollenverwaltung gehören auch die sofortige Deaktivierung und Neuvergabe von Passwörtern bei Personalwechsel oder bei Kompromittierung. Bei Prozessen, die eine hohe rechtliche Bedeutung besitzen (z.B. Abhören der Langzeitdokumentation incl. Datenexport auf Datenträger) kann durch ein Vier-Augen-Prinzip, d.h. Zustimmung per Passwort von zwei berechtigen Personen gleichzeitig, ein hohes Maß an Sicherheit hinsichtlich der Vertraulichkeit erzielt werden, so dass kein Missbrauch durch Einzelpersonen möglich ist.

Bei den Vorgaben für Passwörter ist auf eine Mindestlänge von acht Zeichen zu lassen, die beliebige Zeichen (Groß- und Kleinbuchstaben, Ziffern, Sonderzeichen, fremdsprachige Buchstaben) zulassen. Hinsichtlich der Passwortlänge sollte es keine Beschränkung geben, abgesehen von Längen, die nicht praktikabel sind. Der turnusmäßige Wechsel von Passwörtern bringt nach Ansicht des *National Institute of Standards and Technology* (NIST) keinen zusätzlichen Schutz; diese ursprüngliche Empfehlung wurde daher zurückgezogen. [Sche17]

## 3.4 Personelle Anforderungen

Die zuvor aufgeführten technischen, baulichen und organisatorischen Anforderungen können nur im Sinne der Betriebs- bzw. IT-Sicherheit wirken, wenn auch personellen Aspekte mitberücksichtigt werden. Hierzu gehört ein ausreichend bemessener Personalkörper, so dass Abwesenheiten infolge von Fortbildungsmaßnahmen, Urlaub und Krankheit mehrerer Mitarbeiter nicht zu einer Gefährdung des 24/7-Betriebs führen und die verbleibenden Mitarbeiter nicht überlastet werden. Dieser Ansatz bezieht sich sowohl auf die Disponenten und Schichtführer als auch auf die IT-Administratoren, Datenpfleger und die Leitstellenleitung, so dass alle Tätigkeits- und Verantwortungsbereiche jederzeit voll arbeitsfähig sind.

Bereits bei der Einstellung neuer Mitarbeiter ist eine Sicherheitsüberprüfung zu empfehlen, um potenzielle Innentäter erkennen und vom weiteren Stellenbesetzungsverfahren ausschließen zu können.

Die fortlaufende Schulung und Sensibilisierung hinsichtlich der Informationssicherheit ist ein ebenso wichtiger Bestandteil einer funktionierenden Sicherheitsarchitektur, um Sicherheitslücken, die auf Unachtsamkeit basieren, gar nicht erst

entstehen zu lassen. Selbiges gilt für Social Engineering und ähnlich gelagerte Versuche, Vertrauen zu Funktionsträgern aufzubauen, um diese für Sabotagezwecke auszunutzen.

Um möglichen Ausfall- und Krisensituationen zu begegnen, müssen die Mitarbeiter auch mental vorbereitet sein, hier kommt der regelmäßigen Beübung von Rückfallszenarien eine besondere Bedeutung zu. Mögliche Schwachstellen müssen fortlaufend analysiert und Gegenmaßnahmen erarbeitet und weiterentwickelt werden. Diese können im Ereignisfall aber nur dann zum Tragen kommen, wenn sie allen Mitarbeiter bekannt sind und die personelle Resilienz durch ständiges Training auf einem hohen Niveau gehalten wird. [VK20]

## 3.5 IT-Anforderungen

Da alle Komponenten und Systeme in einer Leitstelle miteinander vernetzt sind (siehe 2.6 ff.), nehmen interne und externe Schnittstellen eine besondere Bedeutung bei der Betrachtung der IT-Sicherheit ein. Durch die Zusammenarbeit der verschiedenen (Software-)Module, Betriebssysteme und Firmware müssen diese auch in Kombination sicher gegen schädliche Einflussnahme sein. Eine gehärtete und geschützte Anwendungssoftware ist – im Sinne der IT-Sicherheit – nutzlos, wenn das zugrunde liegende Betriebssystem Sicherheitslücken aufweist und hierüber eine Kompromittierung von Teilsystemen oder des Gesamtsystems möglich ist. Neben weit verbreiteten Betriebssystemen sind auch grundlegende Softwaremodule, die von Drittanbietern stammen und in Anwendungssoftware integriert werden, zu betrachten. Beispielhaft ist hier das Java-basierte Framework *Log4j* zu nennen, dessen Sicherheitslücke *Log4Shell* am 10. Dezember 2021 bekannt wurde und zu Angriffen auf globale IT-/Internetakteure wie Amazon, Apple, Twitter und Steam geführt hat. Die Verwendung von Standardmodulen als Bestandteil einer Anwendungssoftware kann daher ebenfalls ein Sicherheitsrisiko darstellen; dieses ist umso größer anzusehen, je höher der Verbreitungsgrad von Standardmodulen ist, so dass neben gezielten Angriffen auch opportunistische Beeinträchtigungen möglich, sofern der weite Verbreitungsgrad ein interessantes Ziel für einen Angreifer darstellt.

## 3.6 Resiliente Systeme

Im technischen Sinn besitzen resiliente Systeme die Eigenschaft, bei Störungen oder Teil-Ausfällen nicht vollständig zu versagen, sondern wesentliche Systemdienstleistungen aufrechtzuerhalten. [Tho14] Eine grundlegende Entwicklung hierbei war z.B. die paketweise Datenübertragung per IP, bei der keine feste Verbindung zwischen Sender und Empfänger wie bei der leitungsvermittelten Übertragung erforderlich ist, sondern die Datenpakete können beliebige Routen im Netzwerk nehmen, um das Ziel zu erreichen. Hintergrund dieses Ansatzes waren militärische Überlegungen, dass die Kommunikation zwischen verschiedenen Liegenschaften auch dann aufrechterhalten werden kann, wenn eine auf dem Kommunikationsweg liegende Zwischenstation beschädigt ist und die Daten dennoch in einem vermaschten System ihr Ziel erreichen sollen. Im weltweiten Datennetz mit seinen verschiedenen physikalischen Übertragungsmedien – leitungsgebunden (Kupfer und Lichtwellenleiter) sowie Richtfunk und Satellitenfunk – ist diese Technik als Standard gesetzt, da die Störung einer Übertragungsstrecke durch Routing über einen alternativen Weg kompensiert werden kann. In Teilnetzen kann – abhängig vom Grad der Vermaschung und der Verfügbarkeit alternativer Routen – das Gesamtsystem an seine Grenzen geraden, wenn mehr als eine Hauptübertragungsstrecke beeinträchtigt ist und Alternativen nicht (mehr) zur verfügen stehen oder überlastet sind. Hier ist beispielhaft der Anschlag auf die Deutsche Bahn AG am 08. Oktober 2022 zu nennen, bei dem an zwei Stellen (in Nordrhein-Westfalen und Berlin) Lichtwellenleiter des Zugfunk-Festnetzes durchtrennt worden waren, was zu erheblichen Einschränkungen des Bahnbetriebs in weiten Teilen Norddeutschlands geführt hat. [Mah22]

Resiliente IT-Systeme müssen zwei Grundanforderungen erfüllen:

1. Abwehr
2. Wiederherstellung

Die *Abwehr* im Sinne der Resilienz zielt auf Systeme ab, die in einer physikalisch gesicherten Umgebung betrieben werden, fehlertolerant sind, sich selbst permanent überwachen, mittels Firewall- und Intrusion-Detection-Systemen (IDS) gegen

Schadcode und unbefugtes Eindringen gesichert sind, über gesicherte Schnittstellen verfügen, welchen nur zulässige Datenformate und Adressen passieren lassen und hinsichtlich der vorgenannten Eigenschaften im Rahmen von Sicherheits- und Lasttests erfolgreich überprüft worden sind. Unter „Sicherheitstest“ sind zusammengefasst Überprüfung auf Programmierfehler hinsichtlich Sicherheitslücken (z.B. mittels Proof-Carrying-Code, SAST und DAST; Näheres siehe 6.1.4) sowie Penetrationstests zu verstehen, wobei alle Testfälle als Regressionstests zu wiederholen sind.

*„Insbesondere Penetrationstests sind ein beliebtes Mittel, um die Sicherheit von IT-Systemen im Betrieb zu testen und Schwachstellen offenzulegen.“* [Lep18]

Hinsichtlich der *Wiederherstellung* ist die Rückkehr in den normalen Betriebszustand zu verstehen, die idealerweise zügig und eigenständig erfolgt bzw. nur wenige manuelle Eingriffe erfordert. Für eine unterbrechungsfreie Bereitstellung von Systemfunktionen zentrale Komponenten (z.B. Server, Speichersysteme) mittels Virtualisierung gedoppelt vorhanden sein bzw. georedundant an verschiedenen Orten zur Verfügung stehen, so dass bei Nichterreichbarkeit einer Serverinstanz auf eine Alternativinstanz geroutet wird. Neben der Redundanz von Servern und Datenhaltung müssen auch die Übertragungsstrecken in Form eines vermaschten Systems gestaltet sein, so dass eine Störung einer Verbindung durch alternative Wegeführung kompensiert werden kann, ohne dass es zu Engpässen bei Bandbreiten, Latenzzeiten, Jitter oder Quality of Service (QoS) kommt.

In der Praxis bieten kommerzielle Dienstleister Modelle wie *Infrastructure as a Service* (IaaS) an. Hierbei muss keine eigene Server-Hardware beschafft und unterhalten werden muss, sondern diese wird als Cloud-Dienst gemietet, was vor allem in der Flexibilität bei der Lastverteilung wirtschaftlich ist; es müssen keine Kapazitäten für seltene Lastspitzen vorgehalten werden und steigende Leistungsanforderungen können durch kaskadierbare Dienste sowohl technisch als auch wirtschaftlich unkompliziert bezogen werden. Je nach Vertragsmodell können eine nahezu hundertprozentige Verfügbarkeit inklusive georedundanter Datenreplikation genutzt werden. Als marktgängiges Beispiel ist hier *Amazon Web Services* zu nennen. Unabhängig von den technischen Möglichkeiten sind für Leitstellen als behördlicher Anwenderkreis die Vorgaben des Datenschutzes zu beachten, was

zugesicherte Datenschutzmaßnahmen sowie Serverstandorte in Deutschland seitens der Anbieter erfordert.

Neben der entgeltlichen Nutzung von Serverkapazitäten bei Drittanbietern kann auch der Softwarebetrieb als Cloud-Dienst bezogen werden, so dass keine eigenen Lizenzen erworben werden müssen (On Premise), sondern der Softwarebetrieb nutzungsabhängig abgerechnet werden kann; dies wird als *Software as a Service* (SaaS) bezeichnet und kommt z.B. beim Leitstellenbetrieb im Vereinigten Königreich bereits zum Einsatz. Bei IaaS und SaaS verlagert sich die Verantwortung für einen sicheren IT-Betrieb zu großen Teilen auf den Dienstleister und dessen Systeme und es besteht eine Abhängigkeit mit begrenzten eigenen Einflussmöglichkeiten bei Störungen.

Eine weitere Möglichkeit zur Schaffung von Resilienz sind *Verteilte Systeme*. Diese werden nach Tanenbaum wie folgt definiert:

*„Ein verteiltes System basiert auf einer Menge voneinander unabhängiger Rechnersysteme und Softwarebausteine, die dem Benutzer wie ein einzelnes, kohärentes System bzw. Anwendungssystem erscheinen. Jeder Softwarebaustein einer verteilten Anwendung kann auf einem eigenen Rechner liegen. Es können aber auch mehrere Softwarebausteine aus dem gleichen Rechner installiert sein.“* [Tan08]

Hierbei werden drei Kategorien unterschieden:

1.) *Verteile Computersysteme* sind IT-Systeme für Hochleistungsaufgaben; hierzugehören Cluster- und Grid-Systeme. Cluster-Systeme bestehen aus mehreren ähnlich aufgebauten Rechnern, die per Netzwerk miteinander verbunden sind, Komponenten einer verteilten Anwendung enthalten und dadurch die Verfügbarkeit gegenüber einem Einzelrechner erhöhen. Je nach Auslegung des Clusters und der Anzahl der eingebundenen Rechner können Hochverfügbarkeitscluster (High Availability, HA) gebildet werden. Grid-Systeme hingegen werden aus IT-Systemen gebildet, die geographisch weiter verteilt sind und sich z.T. auch in unterschiedlichen Administrationsdomänen befinden und in ihrer Gesamtheit eine verteilte Anwendung

unterstützen. Cluster- und Grid-Systeme bieten eine gute Skalierbarkeit und Lastverteilung. [Man09] [BBKS15] [Gor22]

2.) Bei *Verteilten Informationssystemen* sind einzelne Funktionen, die betrieblich relevant sind, auf mehrere Rechner (mindestens zwei) verteilt. Typisch für verteilte Informationssysteme sind die große Datenorientierung (die Datenhaltung steht im Zentrum der Anwendung), die Interaktivität und die große Anzahl parallel arbeitender Benutzer. In der Praxis sind als Anwendungen z.B. die Warenwirtschaftssysteme global agierender Versand- und Logistikunternehmen zu nennen. [CDBK12]

3.) *Verteilte pervasive Systeme* sind kleine, oftmals batteriebetriebene Systeme, die in Alltagsgegenständen zur Anwendung kommen und intelligente Funktionen übernehmen. Hier sind beispielhaft medizinische Sensoren zur Überwachung von Körperfunktionen zu nennen, die per Bluetooth mit dem Smartphone des Benutzers gekoppelt sind, welches wiederum Datenkommunikation mit Web-Services betreibt. Statt verteilten pervasiven Systemen werden auch die Bezeichnungen *Ubiquitous Computing* (Ubicomp) bzw. *Internet of Things* (IoT) verwendet, wobei die exakte Abgrenzung nicht eindeutig definiert ist. [Man09] In Bezug auf die IT-Systeme in Leitstellen sind verteilte pervasive Systeme von nachrangiger Bedeutung, da es sich um externe Komponenten handelt, die aktuell (noch) nicht innerhalb von Leitstellen zur Anwendung kommen; die künftige Nutzung und die daraus resultierende sicherheitstechnische Betrachtung bleibt abzuwarten.

Um einen sicheren Betrieb Verteilter Systeme zu gewährleisten, bestehen hier besondere Anforderungen an Authentisierung der Benutzer/Clients, zudem muss die Verbreitung von Schadcode über die verteilten Systemkomponenten verhindert werden. [SS12]

Wichtige Anforderungen an Verteilte Systeme sind die Lastverteilung (*Load Balancing*) sowie die eigenständige Wiederherstellung eines stabilen Betriebszustandes (*Self-Stabilization*) bei Störungen und Ausfällen einzelner Komponenten. Das

Konzept der Self-Stabilization geht auf die Arbeit von Dijkstra zurück, der 1974 die Theorie hierzu publizierte:

*"We call the system "self-stabilizing" if and only if, regardless of the initial state and regardless of the privilege selected each time for the next move, at least one privilege will always be present and the system is guaranteed to find itself in a legitimate state after a finite number of moves."* [Dij74]

Ein Verteiltes System gilt nur dann als selbststabilisierend, wenn es aus einem beliebigen Zustand nach einer endlichen Anzahl von Schritten eigenständig in einen legitimen (stabilen) Zustand übergeht und das System zudem bis zum eventuellen Auftreten einer Störung eigenständig in einem stabilen Zustand verbleibt. Für Verteilte Systeme ist diese Funktion von maßgeblicher Bedeutung, um neben der Lastverteilung eine durchgehende Verfügbarkeit zur gewährleisten. Idealerweise bemerkt ein Anwender gar nicht, dass einzelne Komponenten (Server, Netzwerkknoten) gestört sind, da die Funktionalität durchgängig zur Verfügung steht.

Ungeachtet der rechtlichen Rahmenbedingungen bestehen vielfältige, sich stetig weiterentwickelnde technische Möglichkeiten, statt der eigenen Vorhaltung und des Betriebs von Hard- und Software am Standort der Leitstelle einzelne Dienste als Web-Services in Anspruch zu nehmen bzw. Cloud-Lösungen oder Verteilte Systeme einzurichten. Eine besondere Bedeutung kommt hierbei der Verfügbarkeit der Netzwerkanbindung zu, die hinsichtlich Bandbreite und redundanter Auslegung (idealerweise zwei unterschiedliche Wege und Provider) hohe Anforderungen stellt.

Neben der Schaffung von Resilienz durch technische Systeme kommt auch dem Faktor Mensch eine hohe Bedeutung zu; in Zusammenhang mit den technischen Gegebenheiten betrifft dies vor allem die *Mensch-Maschine-Schnittstelle* (Man-Machine-Interface, MMI). Kramser schreibt in Bezug auf das MMI für die Gestaltung der Bedienoberfläche:

*„Die Navigations- und Steuerelemente sollen einheitlich gestaltet und gruppiert sowie immer am selben Ort auf der Eingabemaske platziert werden, was auch in hektischen Situationen eine große Bediensicherheit garantiert."* [Kra23]

Gerade in Stresssituationen, wenn zu kritischen Einsätzen oder einem hohen Einsatzaufkommen noch technische Störungen hinzukommen, sind übersichtlich und intuitiv gestalteten Bedienoberflächen (GUI) in Kombination mit fehlertoleranter

Systemauslegung wichtige Voraussetzungen für ein sicheres Arbeiten. Sofern resiliente System nicht vollumfänglich selbst nach einer Störung oder einem Teilausfall in den normalen Betriebszustand zurückkehren, müssen die manuell zu verrichtenden Schritte logisch und einfach gestaltet sein. Idealerweise stehen hierfür Checklisten zur Verfügung, die jederzeit schnell zur Hand sind und die Handlungsschritte und deren Ablauf übersichtlich darstellen. Ein fehlerhaftes Nutzerverhalten darf keine Verschlechterung eines fehlerhaften Betriebszustandes nach sich ziehen, sondern muss korrigierbar sein.

*"To support security as well as to evaluate the software's behavior, it is useful to produce test cases that contain invalid inputs."* [AO16]

Zur Unterstützung der Sicherheit und zu Evaluierung des Softwareverhaltens ist es sinnvoll, Testfälle zu erzeugen, die ungültige Eingaben beinhalten. Bewusste Falscheingaben sind damit ein wichtiger Bestandteil von Softwaretests.

Sofern grundlegende Maßnahmen zur Wiederherstellung mit einer hohen Fehleranfälligkeit einhergehen, muss durch geeignete organisatorische Maßnahmen, z.B. Vier-Augen-Prinzip durch gleichzeitige Aktivität von zwei Personen (gegenseitige Kontrolle), Sicherheit geschaffen werden.

## 3.7 Zusammenfassung

Bei der IT-Sicherheit in Leitstellen spielt die *Verfügbarkeit* als Schutzziel eine große Rolle, wobei ein bedeutender Gewinn an Sicherheit durch bauliche Maßnahmen (Baukörper und Gebäudetechnik einschließlich Redundanzbildung) sowie organisatorische und personelle Maßnahmen erreicht werden kann. Beim Schutzziel *Integrität* verhält es sich ebenso; mit Zugangsbeschränkung und -überwachung sensibler Bereiche und der Übertragung sicherheitsrelevanter Aufgaben und Befugnisse auf vertrauenswürdige Personen kann hier ein hohes Maß an Sicherheit gewährleistet werden.

Technisch sind zur Sicherstellung von *Integrität* und *Vertraulichkeit* eine Reihe von Maßnahmen bzw. Voraussetzungen zu schaffen, um ein Höchstmaß an Sicherheit zu schaffen. Kritische Punkte, Komponenten und Systeme in der IT-Umgebung sind:

- Netzwerk

  Das Leitstellennetzwerk (LAN) verbindet die zentralen Systembestandteile (Server, Core-Switche) mit der Peripherie, d.h. den Arbeitsplätzen. Betrieblich und logisch ist das LAN in mehrere VLANs untergliedert, mit denen verschiedene Gewerke/Systeme voneinander getrennt betrieben werden, z.B.:
  - KMS
  - ELS
  - Verwaltung
  - Medientechnik
  - Haustechnik
  - Netzmanagement

- Standard-IT

  Es kommen überwiegend Standard-IT-Komponenten (COTS) zum Einsatz; dies hat den Vorteil guter Verfügbarkeit am Weltmarkt, Wirtschaftlichkeit und einer vergleichsweise einfachen Konfiguration und Fehlerbehebung, da die Produkte ausgereift sind, regelmäßig Updates seitens der Hersteller bereitgestellt werden, Kenntnisse über Betriebssysteme, Virtualisierung, Netzwerke usw. zur Standardausbildung von IT-Fachkräften gehören und im Fehlerfall umfangreiche Hilfestellung – auch durch Online-Recherche – genutzt werden kann. Der Vorteil der Standard-IT ist zugleich ein großer Nachteil aus Sicht der IT-Sicherheit, da Angriffsszenarien in vielen Fällen gerade auf weit verbreitete Betriebssysteme und Firmware abzielen und Leitstellen damit Opfer von opportunistischen Angriffen („Kollateralschäden“) werden können (siehe auch 2.5.6).

- Schnittstellen

  Die Vielzahl an Schnittstellen – intern wie extern – bedarf einer ausführlichen Betrachtung. Über die externen Schnittstellen muss die Erreichbarkeit jederzeit gewährleistet sein (IP-basierte Telefonie, Notruf-Apps), was gleichfalls eine Einfalltor für Schadcode darstellt. Die internen Schnittstellen zwischen den verschiedenen Komponenten und Systemen können zur Verbreitung von Schadcode beitragen, wenn ausgehend von einem kompromittierten System weitere Komponenten bzw. Systeme beeinträchtigt werden, die wiederum über

ihre Schnittstellen zur Verbreitung beitragen (Kettenreaktion bzw. Kaskadeneffekt).

- Softwarearchitektur

  Schwachstellen bei der Softwareerstellung müssen herstellerseitig mittels Last- und Sicherheitstests ermittelt und behoben werden. Hierbei müssen auch Standardprodukte wie Betriebssysteme und Firmware betrachtet werden, ebenso Softwaremodule, die Bestandteil der Anwendungssoftware werden (siehe 3.5). Tests unter Laborbedingungen können die Realität jedoch nur bedingt wiedergeben, da keine komplette Systemlandschaft einer Leitstelle mit allen Subsystemen und -schnittstellen nachgebildet werden kann. Die Abhängigkeiten zwischen den verschiedenen Komponenten unterschiedlicher Hersteller, Schnittstellen und z.T. auch „Technikgenerationen“ lassen sich nur modellieren, wobei eine Definition kritische Pfade und die Bildung von Prioritäten erforderlich sind. [Alp94] [Bur03]

- Wartung und Pflege

  Softwareupdates und -upgrades muss neben der Verbesserung funktionaler Eigenschaften auch das Schließen von Sicherheitslücken und die Beseitigung von Fehlern (Bugs) beinhalten; Wartung und Pflege müssen daher im Nachgang einer Beschaffung geregelt sein und regelmäßig erfolgen. Beim Bekanntwerden von Sicherheitslücken bzw. -vorfällen ist unverzügliches Handeln erforderlich.

# 4 Empirische Studie

Um der Stand der Informationssicherheit in deutschen Leitstellen zu erheben, wurde eine empirische Erhebung in Form eines Fragebogens durchgeführt (Fragestellungen und Rückmeldungen siehe Anlage), der über dem Fachverband Leitstellen e.V. an die Leitstellen versandt wurde. Dieser Weg wurde gewählt, um möglichst viele BOS-Leitstellen in Deutschland unmittelbar zu erreichen. Die Erhebung wurde im Zeitraum 26.07. bis 31.10.2019 durchgeführt. Zu diesem Zeitraum wurden auch Aspekte erhoben, die aktuell keine Relevanz mehr besitzen, z.B. ISDN-basierte Notrufanschaltungen (A.17) sowie turnusmäßige Passwortwechsel (A.48 und A.50).

Insgesamt liegen 28 Rückmeldungen vor, dies entspricht bei 232 Leitstellen [TRC22] einer Rückmeldequote von 12 %. Die großen Flächenländer Bayern und Niedersachsen sowie Nordrhein-Westfalen als bevölkerungsreichtes und am dichtesten besiedeltes Land sind mit jeweils mehreren Rückmeldungen vertreten, so dass die gewonnen Daten insgesamt als realistisch angesehen werden können. Das Fehlen von Rückmeldungen aus dem Stadtstaat Hamburg und aus Bremen sowie aus dem Saarland als kleinstem Flächenland sind daher vertretbar. Aus den Flächenländern Rheinland-Pfalz und Thüringen liegen leider keine Rückmeldungen vor, wobei die Antworten aus den übrigen Ländern (Baden-Württemberg, Bayern, Berlin, Brandenburg, Hessen, Mecklenburg-Vorpommern, Nordrhein-Westfalen, Niedersachsen, Sachsen, Sachsen-Anhalt, Schleswig-Holstein) eine hinreichende Datenlage bieten und sowohl Metropolregionen, groß- und mittelstädtische Bereiche als auch ländlich geprägte Gegenden beinhalten.

## 4.1 Statistische Sicherheit

Da die Rückmeldequote mit 12 % als eher gering anzusehen ist, ist eine Betrachtung der Repräsentatitivität erforderlich, damit die Aussagekraft der gewonnenen Erkenntnisse bewertet werden kann.

Hierzu wird der Stichprobenumfang ($n$ = 28) in Bezug zur Grundgesamtheit ($N$ = 232) betrachtet [HN02] [Wei08]. Da es sich bei vielen der Erhebungen um

Nominale Daten handelt, muss hierfür ein Chi-Quadrat-Test zur Anwendung kommen (Kontingenz-Tabelle).

Die hierfür benötigte Stichprobengröße für Alpha-Fehler von 0,15 und eine Teststärke (Power) von 0,8 bei vier Antwortmöglichkeiten wurde mit Hilfe der Software *G*Power* berechnet. [FELB07] Für eine Effektgröße von w = 0,55 (große Effekte) wird ein kritischer Chi-Quadrat-Parameter von 6,745 berechnet und eine minimale Stichprobengröße von 28 empfohlen.

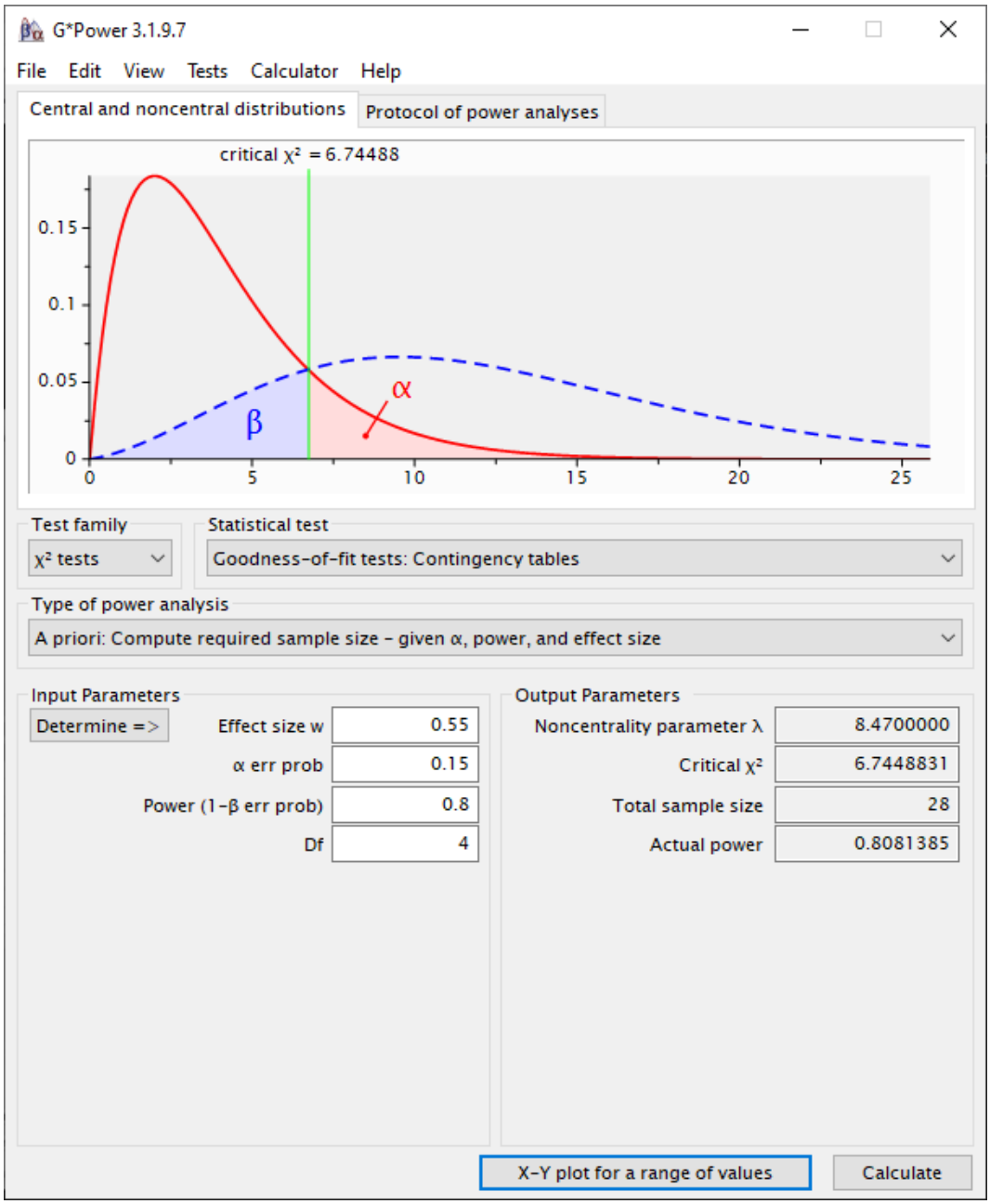



Abb. 4.1: Screenshot Statistikberechnung mit *G*Power*

Hieraus folgt, dass mit der Stichprobenanzahl die betrachteten Rückmeldungen als repräsentativ für die Grundgesamtheit angesehen werden können.

## 4.2 Auswertung

Bei der Auswertung der Rückmeldungen ergibt sich ein differenziertes Bild. Einige Sicherheitsmaßnahmen und -standards befinden sich auf einem hohen Niveau bzw. sind durchweg vorhanden. Andererseits bestehen z.T. erhebliche Sicherheitsdefizite, die zu beseitigen sind. Hierbei ergeben sich allerdings keine Häufungen nach einzelnen Regionen, Bundesländern oder Betreibern bzw. Organisationsformen. Als positiv ist die Umsetzung des Überspannungsschutzes und das Vorhandensein von Netzersatzanlagen (NEA) anzusehen, welche bei 100 % der befragten Leitstellen vorhanden sind. Ähnlich verhält es sich mit dem Blitzschutz, dessen Vorhandensein in 26 von 28 Fällen bejaht wurde (zwei der Befragten machten hierzu keine Angaben). Datensicherung wird in 24 Fällen täglich durchgeführt, in zwei Fällen sogar mehrmals täglich. Firewalls zur Sicherung des Netzwerkzugriffs kommen durchweg zur Anwendung, in vier Fällen einstufig, in 24 Fällen zweistufig. Eine DMZ mit entsprechender Server- und Netzwerkarchitektur steht in 20 Fällen zur Verfügung, ist in einem Fall geplant und in drei Fällen nicht geplant; vier Leitstellen machten hierzu keine Angaben. Passwörter der Disponenten und Administratoren werden in 26 von 28 Fällen bei Ausscheiden der Personen gelöscht, in einem weiteren Fall wird dies nicht so gehanhabt, ist aber geplant; in einem Fall erfolgten hierzu keine Angaben. Geteilt sind die Ansichten der Verantwortlichen, was die Vorgaben bzgl. IT-Sicherheit betrifft; 12 sind der Ansicht, dass die Vorgaben nicht ausreichen bzw. für Leitstellen zu unspezifisch sind; 16 erachten die Vorgaben und Standards für ausreichend und sehen keinen Handlungsbedarf. Eine Rückfallebene für den IP-basierten Notruf ist in drei Fällen vorhanden, in neun Fällen in Planung befindlich und in sieben Fällen sei dies nicht vorgesehen; neun Standorte machten keine Angaben. Hierbei ist anzumerken, dass die Migration der Notrufanschlüsse von ISDN auf IP zum Zeitpunkt der Erhebung im Gange war und sich das Vorhandensein von Rückfallebenen in lediglich drei von 28 Fällen zwischenzeitlich eine Steigerung erfahren haben dürfte.

Als kritisch sind die Rückmeldungen zu Fernwartungszugängen anzusehen, die in elf von 28 Fällen durchweg aktiv und jederzeit nutzbar sind. USB-Ports an den Arbeitsplatzrechnern sind in 20 Fällen gesperrt, in fünf jedoch nicht (davon in Fällen geplant und in einem Fall nicht geplant), drei Leitstellen machten zu dieser Frage keine Angaben. Die Schulung und Sensibilisierung der Mitarbeiter zum Thema IT-Sicherheit ist 50 % der Fälle (14 von 28 Leitstellen) Bestandteil der laufenden Fortbildung, in zehn Fällen ist dies geplant und in drei Fällen ist dies nicht geplant; ein Standort machte keine Angaben.

Mehrfachnennungen gab es bereits aufgetretenen Sicherheitsvorfällen, in Summe 81 Ereignisse), davon 51 ohne Betriebseinschränkungen, 17 mit leichten Einschränkungen des Betriebs, neun mit mittleren Einschränkungen und in vier Fällen schwere Einschränkungen, was ca. 5 % aller gemeldeten Sicherheitsvorfälle entspricht.

Zusammenfassend ist festzustellen, dass in allen Bereichen (Technik, Organisation, Personal einschließlich dessen Schulung) Nachhol- und Optimierungsbedarf besteht. Hierbei ergaben sich keine Schwerpunkte nach bestimmten Bundesländern oder Regionen; angesichts des differenzierten Gesamtbildes tragen die föderalen Strukturen in Deutschland weder zu einer Einheitlichkeit bei technischer Ausstattung, Arbeitsprozessen, personellen Anforderungen (Qualifikationen, Eingangsvoraussetzungen, Stellenansatz) oder Finanzierung bei, so dass auch hinsichtlich der Sicherheitsanforderungen derzeit keine Einheitlichkeit vorausgesetzt werden kann.

Zu zahlreichen Fragestellungen erfolgten keine Angaben, wobei dies nicht auf einzelne Rückmeldebögen beschränkt ist, sondern nahezu alle Rückmeldebögen an der einen oder anderen Stelle betrifft.

Ziel muss es daher sein, bundesweit einheitliche und verbindliche Vorgaben zu schaffen, die für alle Leitstellen als Mindestanforderung gelten und deren Einhaltung kontrolliert und nachgehalten wird. Unabhängig von organisatorischen und personellen Aspekten, stellen die Technik bzw. technische Maßnahmen einen wesentlichen Sicherheitsbaustein dar. Hier ist die eingesetzte Hard- und Software der wichtigste Ansatz, da sich deren Architektur und Ausgestaltung maßgeblich auf das Sicherheitsniveau auswirkt. Zielsetzung ist eine IT-Umgebung, die aufgrund ihrer Struktur eine inhärente Sicherheit bietet, wobei neben der Auslegung der Hardware und des Netzwerkes dem Softwaredesign eine Schlüsselstellung zukommt. Diese

Anforderungen sollen in einem speziellen Software-Entwicklungsmodell abgebildet werden, das neben den funktionalen Anforderungen die Belange der IT-Sicherheit von der Planung über die Grob- und Feinkonzeption, die programmtechnische Umsetzung, den Labortest, die Installation in der Wirkumgebung bis hin zum Probebetrieb, Abnahme, Überführung in den Echtbetrieb und nachfolgende Softwarepflege und -wartung abbildet und einfordert.

# 5 Softwaretechnik

## 5.1 Vorgehensmodelle

Der Kernarbeitsprozess in einer Leitstelle folgt dem EVA-Prinzip – Eingabe, Verarbeitung (siehe 2.7), auch wenn diese Schritte nicht streng auf die Ein- und Ausgabegeräte nur eines Rechners beschränkt sind, sondern mehrere Rechner/Systeme umfassen, z.T. auch standortübergreifend als Verteilte Systeme (siehe 3.6 ff.). Die Ergebnisse der empirischen Studie legen nahe, dass sich bei den bestehenden Leitstellensystemen die IT-Sicherheit sehr heterogen dargestellt, daher besteht die Zielsetzung darin, mittels inhärent sicherer Anwendungssoftware eine wesentliche Grundlage für einen sicheren IT-Betrieb zu schaffen. Bei der Software muss die IT-Sicherheit daher in allen Stadien des Entwicklungsprozesses eine entsprechende Gewichtung erfahren, was sich in einem eigenen Entwicklungsmodell widerspiegeln soll.

*„Eine große Cyber-Sicherheitsherausforderung ist, dass in der aktuell genutzten Software zu viele Schwachstellen vorhanden sind. Die Software-Qualität der Betriebssysteme und Anwendungen ist für die heutige Bedrohungslage nicht mehr ausreichend. Die Fehlerdichte, die Anzahl der Softwarefehler pro 1000 Zeilen Code, ist bei qualitativ hochwertiger Software heute im Schnitt 0,3.* […] *Eine qualitativ schlechte Software hat viele Softwarefehler (Schwachstellen, Bugs usw.) und ist damit grundlegende Ursache für erfolgreiche Remote-Angriffe auf IT-Systeme.“* [Poh18]

Für den Ausdruck „Fehler“ als Qualitätsmangel in einem Softwareprodukt ist in der Literatur folgende Definition zu finden:

*„Die Abweichung eines ermittelten, beobachteten oder gemessenen Wertes, Zustandes oder Verhaltens eines Softwareprodukts vom korrespondierenden spezifizierten, theoretisch richtigen oder als richtig erachteten Wertes, Zustandes oder Verhaltens.“* [PP04]

In der Softwaretechnik haben sich verschiedene Vorgehens- bzw. Entwicklungsmodelle etabliert. Ausgehend von den funktionalen Anforderungen der künftigen Nutzer gilt es, diese Erwartungen zu analysieren und in mehreren Planungs- und Realisierungsschritten („von grob zu fein“) in ein betriebsfertiges Produkt zu

überführen. Die Integration einzelner Softwarekomponenten/-module zu einem Gesamtsystem bzw. einer Anwendung im fortlaufenden Entwicklungsprozess wird auch *Kontinuierlichen Integration* (Continuous Integration, CI) bezeichnet, wobei CI nicht nur als Projektprozess (organisatorisch und zeitlich) zu verstehen ist, sondern auch mit Hilfe von CI-Tools auch softwaremäßig unterstützt wird. [Bel18]

Tests, Qualitätssicherung, Dokumentation und Softwarepflege vervollständigen den Entwicklungsprozess. In die verschiedenen bestehenden Entwicklungsmodelle fließen standardisierte Vorgehensweisen des Projekt- und Qualitätsmanagements je nach Modell unterschiedlich intensiv mit ein. [SL19] [BKP17] Als Überbegriff für die Entwicklungsmodelle hat sich auch die Bezeichnung *Software Development Life Cycle* (SDLC) etabliert.

### 5.1.1 Wasserfallmodell

Das Wasserfallmodell ist das einfachste Modell, dessen Schritte in der grafischen Darstellung als Kaskaden angeordnet sind. Dabei werden in der Fachliteratur mindestens fünf oder auch mehr Schritte beschrieben, wobei einzelne Phasen zusammengefasst oder auch getrennt betrachtet werden. Mindestens sind folgende fünf Phasen von Bedeutung [PR17], die in entsprechenden Dokumenten zu beschreiben sind:

1. Analyse der Anforderungen
2. Konzeption
3. Entwurf
4. Realisierung
5. Überprüfung/Test

Der Anforderungsanalyse kann eine Initialisierung als formaler Projektschritt vorausgehen, nach dem abschließenden Schritt der Überprüfung erfolgt die eigentliche Einführung und Installation beim Nutzer, evtl. begleitet durch Schulungen und die Weiterentwicklung kann in Form der nachfolgenden Schritte „Wartung / Softwarepflege“ ebenfalls mit abgebildet werden. [Ker15] [SW07]

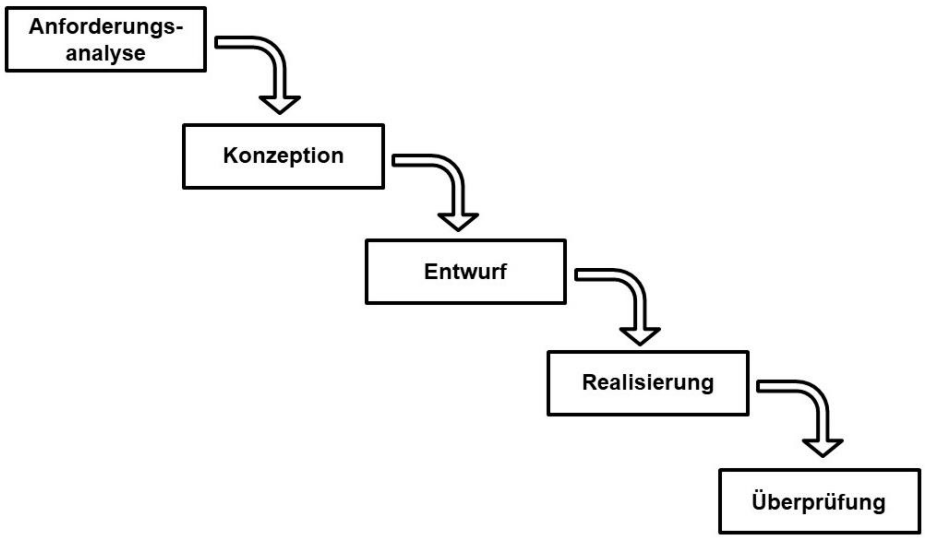



Abb. 5.1: Wasserfallmodell

Das Wasserfallmodell ist nicht-iterativ; jede Projektphase wird nur einmal durchlaufen. Das hat zur Folge, dass sich ein unzureichendes Ergebnis bei der Überprüfung mit einer erforderlichen Nachbesserung, d.h. einem nochmaligen Durchlaufen der Entwurfs- und Realisierungs- und Testphase, hiermit nicht abbilden lässt. Namengebend fließt das Wasser beim Wasserfall von oben nach unten, woraus sich eine Einbahnstraßenrichtung des Modells ergibt und die Rückkehr zu einem vorigen Schritt nicht vorgesehen ist.

Das Wasserfallmodell bietet folgende Vorteile:

- Es ist einfach verständlich
- Gut kontrollierbarer Prozessablauf durch Einführung von Meilensteinen und Dokumenten innerhalb und am Ende jeder Phase
- Gute organisatorische Beherrschbarkeit
- Wenig Managementaufwand

Nachteile des Wasserfallmodells:

- Bei dem dokumentenorientierten Vorgehen besteht die Gefahr, dass die Dokumente wichtiger werden als das eigentliche Projektziel

- Spätes Erkennen von Risiken und Fehlern im Rahmen der Realisierung und Überprüfung, d.h. ein frühes Gegensteuern sieht das Wasserfallmodell nicht vor.
- Veränderungen und Detaillierungen der Anforderungen, die im Projektverlauf zutage treten, können schlecht oder gar nicht mit dem Modell abgebildet werden.

Die praktische Anwendbarkeit dieses Modells im Vergleich zu den anderen Modellen ist daher gering, da u.a. Sicherheitsaspekte sowie Änderungen/Ergänzungen während des Projektverlaufs keine Berücksichtigung finden. Als Erweiterung für die praktische Anwendung ist in der Literatur ein iteratives Wasserfallmodell beschrieben [Ker15], das die Rückkehr zum jeweils vorangegangenen Schritt ermöglicht, so dass innerhalb der modellhaften Projektverlaufs mehrere Richtungswechsel möglich sind, bis mit dem erfolgreichen Abschluss des finalen Schrittes (Überprüfung/Test) der Prozess beendet wird. Durch die Zulässigkeit von Richtungswechseln und dem erneuten Durchlaufen voriger Schritte besteht die Gefahr, dass die genaue Bestimmung des jeweils aktuellen Projektstandes bzw. die Dokumentation hierunter leidet, was gegen eine Nutzung des Wasserfallmodells als Treppenmodell mit zulässigen Richtungswechseln spricht.

### 5.1.2 V-Modell und V-Modell XT

Das V-Modell besteht wie das Wasserfallmodell aus einzelnen, aufeinander folgenden Projektphasen (ebenfalls nicht-iterativ). Durch den höheren Detailierungsgrad erfahren Softwaretest und Qualitätssicherung deutlich mehr Gewicht, als dies beim Wasserfallmodell der Fall ist. Die V-förmige und nicht lineare oder wasserfallförmige Anordnung der einzelnen Schritte bildet zudem den zeitlichen Verlauf und den Detaillierungsgrad über der Abfolge der Entwicklungsschritte ab [FHKM09]. Ergänzend lassen sich organisatorische Zuständigkeiten auf den verschiedenen „Schichten“ (hier farblich dargestellt) mit abbilden. Mit den Achsen eines kartesischen Koordinatensystems lassen sich der zeitliche Ablauf (y-Achse) und die Detaillierungstiefe (x-Achse) zusammen mit den Projektschritten darstellen.

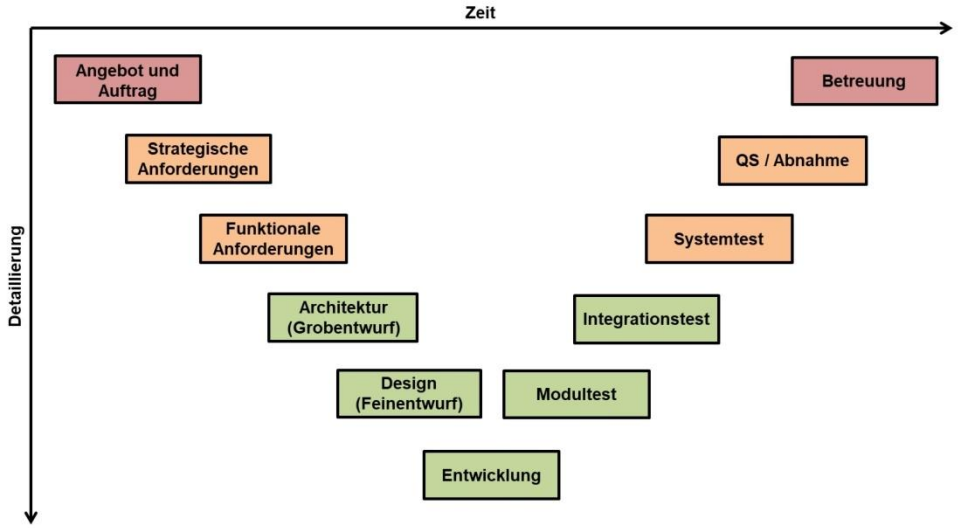



Abb. 5.2: V-Modell

Die am Beginn und am Ende des V-Modells stehenden Projektphasen betreffen vorrangig vertragliche und kaufmännische Aspekte (rot; Ebene Geschäftsführung und Vertrieb). Die Anforderungsanalyse und –definition sowie Systemtest, Qualitätssicherung und Abnahme betreffen den Aufgabenbereich der Projekt- und Produktmanager (orange). Die eigentlichen Entwurfs-, Entwicklungs- und internen Testphasen (grün) betreffen die Tätigkeit der Softwareentwickler und Programmierer.

Ebenso wie beim Wasserfallmodell ermöglicht das V-Modell nicht das nochmalige oder mehrmalige Durchlaufen einzelner Phasen, z.B. bei unzureichenden Ergebnissen interner Tests, die eine Nachbesserung und damit einen Sprung zurück zu einer vorigen Phase erfordern. Das V-Modell stößt ebenso wie das Wasserfallmodell an diesem Punkt an seine Grenzen. [Ker15]

Eine Erweiterung des V-Modells ist das *V-Modell XT*, das ursprünglich für die Bundeswehr entwickelt wurde und später für IT-Projekte aller Bundesbehörden eingeführt worden ist. Der Zusatz „XT“ steht hierbei für „Extreme Tailoring“, was mit „maßgeschneidert“ bzw. „individuell zurechtschneidbar/anpassbar“ übersetzt werden kann, d.h. es gibt keine starre Vorgabe hinsichtlich des Projektablaufs, sondern die einzelnen Schritte und Abfolgen können individuell auf das jeweilige Projekt und dessen Anforderungen angepasst werden. Gegenüber dem V-Modell ermöglicht die Weiterentwicklung V-Modell XT ein iteratives Vorgehen, d.h. ein nochmaliges Durchlaufen eines vorigen Entwicklungsschrittes; ebenso ein

inkrementelles Vorgehen, d.h. eine Aufgliederung in Einzelschritte, die zu unterschiedlichen Zeitpunkten bzw. Geschwindigkeiten erarbeitet werden (auch parallel), um anschließend zu einem Gesamtsystem zusammengeführt zu werden. Wesentlich beim V-Modell XT ist die Gliederung in einzelne *Vorgehensbausteine*, die zusammengehörige Aktivitäten, Produkte (Arbeitsergebnisse) und Rollen (Projektbeteiligte) bündeln und zudem die Abhängigkeiten von und zu anderen Vorgehensbausteinen berücksichtigen. [HHM09]

### 5.1.3 Inkrementelles Modell

Das Inkrementelle Modell untergliedert den gesamten Entwicklungsprozess in Teilschritte, die sehr feingliedrig sein können. Somit ist eine sehr gute Strukturierung der Arbeitsschritte und deren Zuteilung an die beteiligten Mitarbeiter möglich. Erst wenn ein Schritt abgearbeitet ist, beginnt der nächste. Das Inkrementelle Modell lässt sich sowohl nicht-iterativ als auch iterativ umsetzen. Neben einer feingliedrigen Abfolge der Entwicklungsschritte können voneinander unabhängige Teile der Software (Module) auch parallel entwickelt werden; das Zusammenfügen zur vollständigen Software erfolgt am Schluss, wenn alle Teilergebnisse vorliegen, siehe Abbildung 5.3.

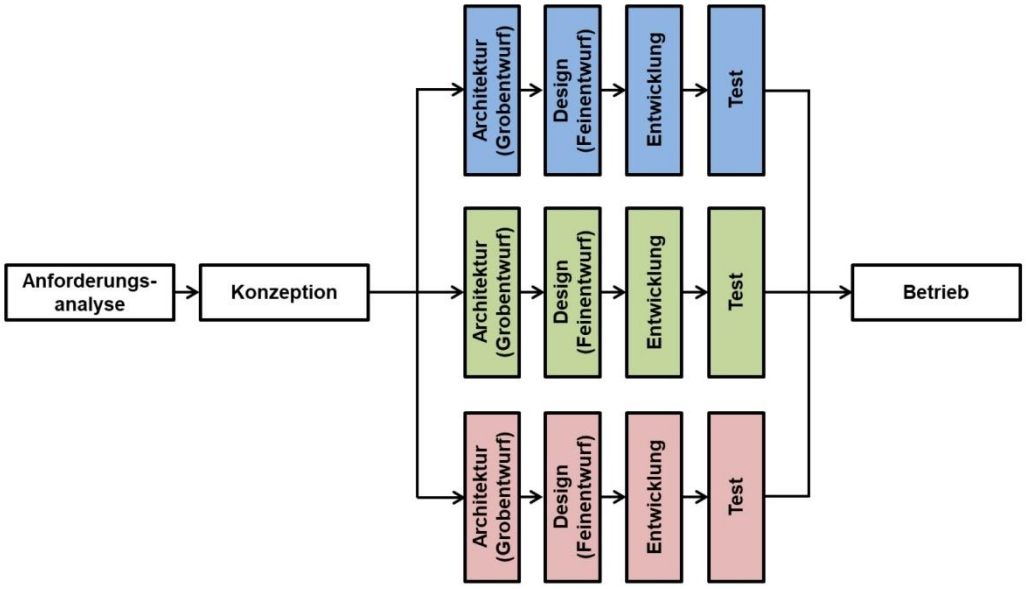



Abb. 5.3: Inkrementelles Modell

Vorteile des Inkrementellen Modells:

- Mehrere Entwicklerteams können unabhängig voneinander arbeiten. [Sie04]
- Keine zeitlichen Abhängigkeiten; wenn es bei einem Modul zu Verzögerungen kommt, können die anderen Module dennoch weiterarbeiten.

Nachteile des Inkrementellen Modells:

- Höherer Koordinierungsaufwand des Projektverantwortlichen, dass die parallel arbeitenden Entwicklerteams das Gesamtprojekt im Fokus behalten (inhaltlich und zeitlich), so dass alle parallel entwickelten Module am Schluss fehlerfrei interagieren und ein Gesamtpaket ergeben, das den Anforderungen entspricht.
- Genaue Spezifikation der Schnittstellen innerhalb des Gesamtprojekts erforderlich, damit die Entwickler die Schnittstellen der Softwareteile einhalten aber auch eine einheitliche Arbeitsplanung und Dokumentation sichergestellt sind.

Die hier beispielhaft dargestellte Untergliederung in drei Module, die unabhängig voneinander erarbeitet werden, erfordert keine einheitliche zeitliche Taktung, sondern es wird lediglich ein Endtermin seitens des Projektmanagements vorgegeben (Abb. 5.4). [Bal04] [Gol12]

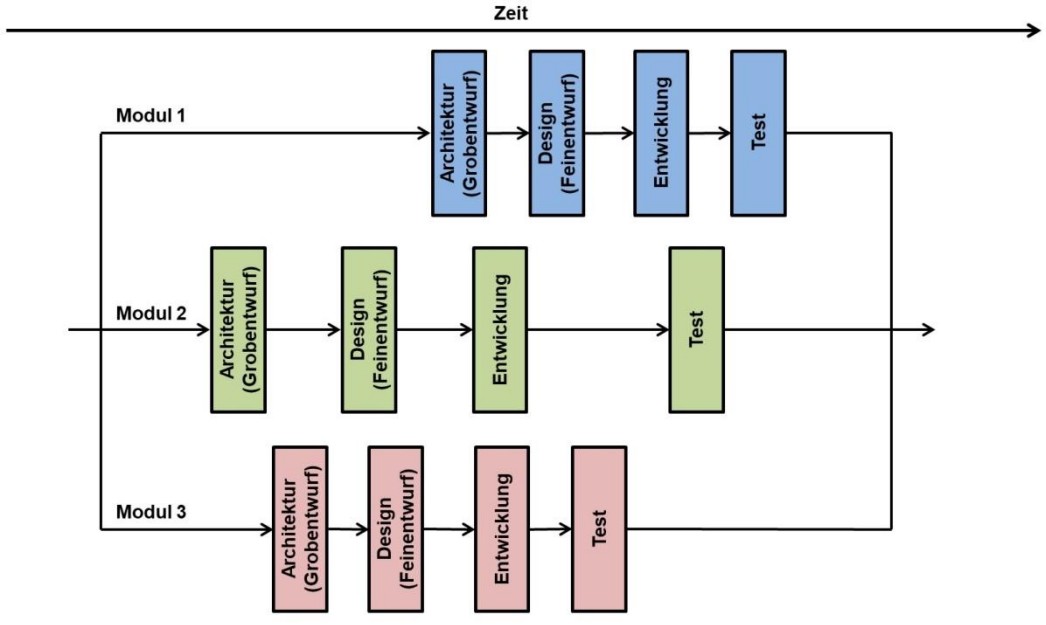



Abb. 5.4: Inkrementelles Modell mit unterschiedlichem zeitlichen Verlauf auf Modulebene

### 5.1.4 Rational Unified Process Modell

Das Rational Unified Process Modell (RUP) wurde von der Fa. Rational Software entwickelt, die im Jahr 2003 von IBM übernommen wurde. Zielsetzung der Entstehung von RUP ist die objektorientierte Softwareentwicklung mittels Unified Modeling Language (UML). Bei RUP gliedert sich die Softwareentwicklung in vier einzelne Phasen, welche wiederum mehrere Iterationen durchlaufen, so dass bei jedem Teilabschnitt innerhalb einer Phase eine Überprüfung des Ergebnisses stattfindet. Die vier Projektphasen sind *Inception* (Beginn/Konzeption), *Elaboration* (Ausarbeitung), *Construction* (Konstruktion/Programmierung) und *Transition* (Übergang zum Test und Betrieb), wobei die Phase *Transition* nicht das Ende einleitet, sondern wiederum zur *Inception* führt, so dass sich ein Kreislaufprinzip und damit insgesamt eine iterative Vorgehensweise ergibt, siehe Abb. 5.5.

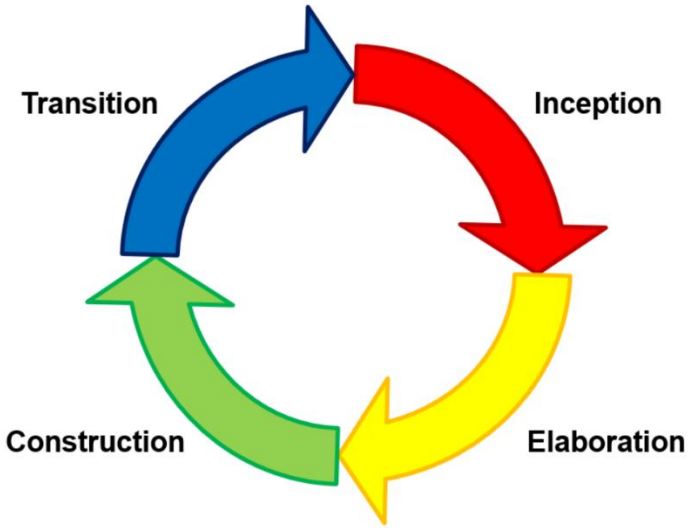



Abb. 5.5: Vier Phasen des RUP

Insgesamt besteht das RUP aus den neun Kern-Workflows:

1. Business Modelling (Geschäftsprozess, Strategie),
2. Requirements (Anforderungen, Abbildung der Geschäftsprozesse),
3. Analysis and Design (Spezifikation der Software-Architektur),
4. Implementation (Programmierung),
5. Test (Programm-, Modul- und Integrationstests),

6. Deployment (Installation, Inbetriebnahme, Schulung der Anwender),
7. Configuration Management (Konfigurations- und Änderungsmanagement),
8. Project Management (Projektmanagement, Kosten, Termine),
9. Environment (Entwicklungsumgebung, Tools, Qualitätssicherung),

die sich auf die vier Projektphasen verteilen, wobei je Phase musterhaft z.T. mehrere Iterationen durchlaufen werden, z.B. *Elaboration* zwei Iterationen, *Construction* drei und *Transition* wiederum zwei Iterationen (Abb. 5.6). [Eel14] [HHM09]

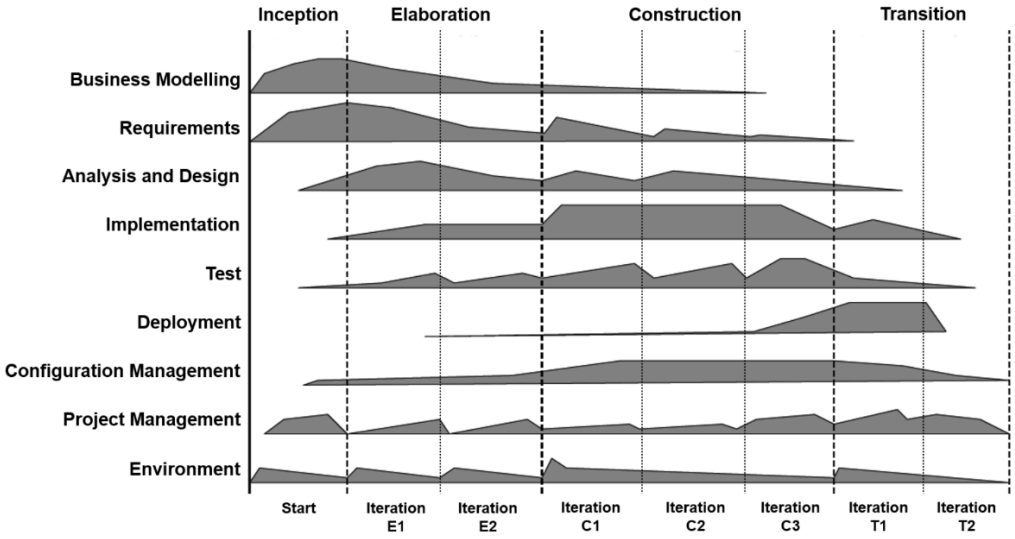



Abb. 5.6: Rational Unified Process nach [Eel14]

Vorteile von RUP:

- Flexibilität, periodische Überprüfung des Prozessablaufs
- Iteratives Vorgehen ermöglicht frühzeitiges Reagieren auf Fehler
- Gut geeignet für objektorientierte Softwareentwicklung
- Parallelität und inkrementelles Vorgehen möglich

Nachteile von RUP:

- Hoher Managementaufwand zur Entscheidungsfindung bzgl. des weiteren Prozessablaufs,
- Hohes Maß an Komplexität und Abhängigkeiten der einzelnen Workflows und Phasen,

- Hoher Aufwand für Iterationsplanung (Zeit, personelle Ressourcen)

### 5.1.5 Spiralmodell

Beim Spiralmodell, das der US-amerikanische Mathematiker Barry W. Boehm [Boe88] Mitte der 1980er Jahre entwickelt hat, werden im Gegensatz zum Wasserfall- und V-Modell alle Schritte mehrfach durchlaufen (iteratives Modell), was sich grafisch in Form der namengebenden Spirale darstellen lässt, die im Uhrzeigersinn vom Ursprung eines kartesischen Koordinatensystems aus verläuft, wobei sich der Radius stetig vergrößert. Die y-Achse bildet die Kosten ab und die x-Achse den zeitlichen Verlauf, wobei beide Größen mit jedem Spiralumlauf ansteigen (Abb. 5.7). Die vier Quadranten des Koordinatensystems bilden die vier Themenblöcke. [LL23] [PP04]

1. Festlegung der Ziele, Alternativen und Randbedingungen
2. Risikoanalyse und Bewertung von Alternativen
3. Entwicklung, Test und Implementierung
4. Planung der nächsten Iteration

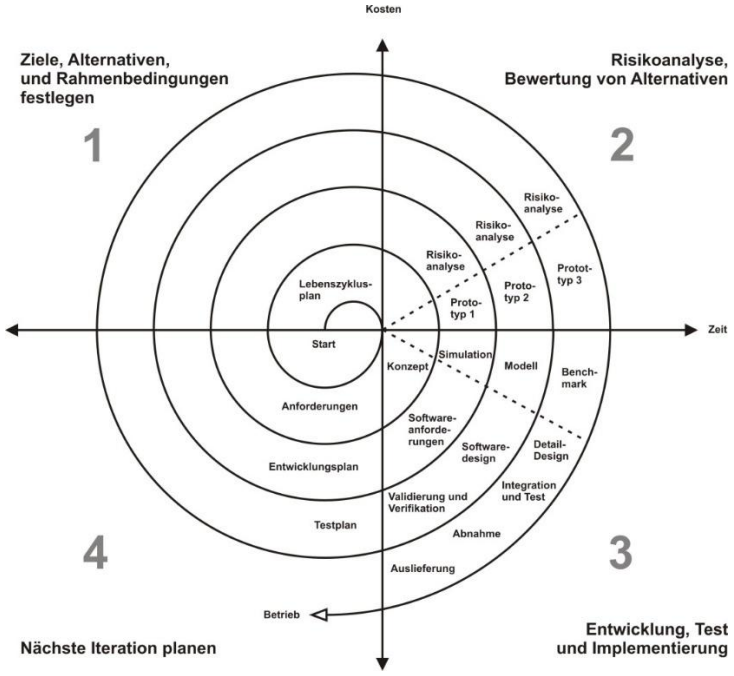



Abb. 5.7: Spiralmodell

Die Nummerierung dieser vier Themenblöcke ist nicht deckungsgleich mit der Konvention zur Benennung der vier Quadranten eines kartesischen Koordinatensystems, da sich der 1. Themenblock (Festlegung der Ziele, Alternativen und Rahmenbedingungen) im II. Quadranten befindet, d.h. es besteht eine Verschiebung um ±90° bzw. um ±1 in der Nummerierung der Themenblöcke des Spiralmodells gegenüber den Quadranten des Koordinatensystems. Dies muss allen Beteiligten bekannt sein, damit in der Projektkommunikation keine Missverständnisse über die Bezeichnung entstehen. [Bal04]

Das Spiralmodell hat keine feste Anzahl an Runden, die bis zur Fertigstellung des Softwareprodukts mindestens durchlaufen werden müssen. Der Übergang von der Entwicklung über die Inbetriebnahme bis hin zur Wartung ist fließend:

*„Es bleibt offen, wann die Spirale endet und wie die Phase der Wartung in dieses Vorgehensmodell eingebettet ist. Es wird davon ausgegangen, dass das Spiralmodell gleich gut sowohl auf die Entwicklung als auch auf die Wartung von Software-Produkten angewandt werden kann.“* [PP04]

### 5.1.6 Extreme Programming (XP)

Das *Extreme Programming* (XP) basiert auf der Lösung der Softwareanforderungen durch zeitnahe erste Ergebnisse, ohne einen formalisierten Ablauf in den Vordergrund zu stellen. Hierbei wird die Annahme vertreten, dass der Auftraggeber einer neuen Software zu Projektbeginn noch nicht alle Funktionen und Anforderungen detailliert spezifizieren kann, so dass keine vollständige Analyse und Strukturierung des weiteren Vorgehens anhand der Vorgaben möglich ist. Die Entwicklung erfolgt im engen Austausch mit dem Auftraggeber, so dass dessen Rückmeldungen unmittelbar in die nächsten Implementierungsschritte einfließen und zeit- und kostenintensive Fehlentwicklungen vermieden werden [WRL05]. Eine offene Kommunikation und Teamarbeit zwischen Auftraggeber und den Entwicklern ist dabei unerlässlich. XP als Entwicklungsmodell ist mit dem Spiralmodell vergleichbar, allerdings unter Minimierung bzw. Auslassen der formalen Schritte, sondern mit einer unmittelbaren Entwicklung eines Prototyps und dessen Verfeinerung und Optimierung in mehreren Zyklen zum Endprodukt. [BF01] [SW07]

### 5.1.7 Scrum

Bei *Scrum* (englisch: Gedränge) erfolgt namengebend eine hohe Dichte der Entwicklungsschritte in der zeitlichen Abfolge, was einer umfangreichen Koordination und einer klaren Aufgaben- und Rollenzuteilung der beteiligten Akteure bedarf. [DKS19]

Als Rollen fungieren:

Der *Product Owner* als Projektleiter ist für die Zielerfüllung hinsichtlich Funktionalität und Wirtschaftlichkeit der Software verantwortlich.

Der bzw. die *Developer* (Entwickler) ist/sind für die Umsetzung der Anforderungen in die Software (Programmierung) zuständig.

Der *Scrum Master* ist der Verantwortliche für die Organisation des Scrum-Ablaufs. Er ist moderierend und steuernd für die Abläufe zuständig, aber kein unmittelbarer fachlicher Vorgesetzter der Entwickler und nimmt die Funktion eines Controllers im Gesamtprojekt ein.

Zentraler Bestandteil von Scrum sind ein oder mehrere *Sprints*, die als geschlossene Abläufe keine Änderung des jeweils gesetzten Sprintziels erlauben (Abb. 5.8). Ein Sprint dauert max. 30 Tage, wobei alle vorgesehen Sprints die gleiche Länge haben und auch abgebrochen werden, wenn das jeweilige Sprintziel noch nicht erreicht ist. Zur arbeitstäglichen Abstimmung der anstehenden Aufgaben wird ein *Daily Sprint* abgehalten, bei dem sich alle Projektbeteiligten zu den Fortschritten und den anstehenden Aufgaben austauschen. [Pic13] [WR21]

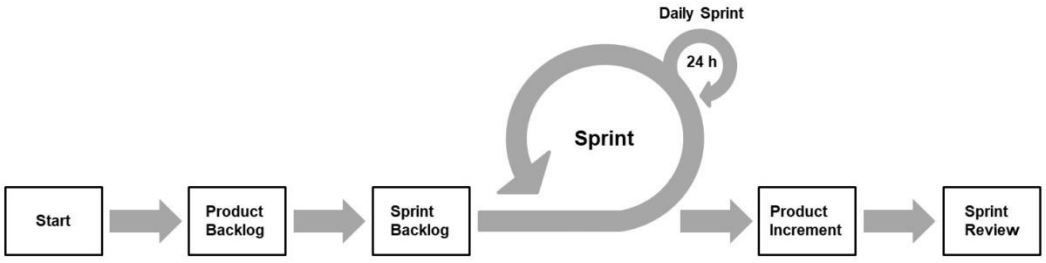



Abb. 5.8: schematischer Ablauf von Scrum

Vor dem eigentlichen Sprint stehen das *Product Backlog* und das *Sprint Backlog*. Das Product Backlog ist eine Aufstellung aller Funktionen, welche die zu entwickelnde Software haben soll. Dabei handelt es sich um eine Auflistung, die ständig

fortgeschrieben wird, d.h. abgearbeitete Punkte werden gestrichen, neue Punkte ergänzt und noch nicht bearbeitete Punkte werden detailliert oder geändert. Das Sprint Backlog ist der Plan, welche Aufgaben im bevorstehenden Sprint zu erledigen sind. Hierbei bedient sich das Sprint Backlog der Anforderungen, die im Product Backlog niedergeschrieben sind. [Glo16]

Nach einem Sprint wird ein *Product Increment* erstellt, d.h. eine Zusammenfassung aller Eintragungen aus dem Product Backlog, die bei dem Sprint relevant waren. Anschließend erfolgt das *Sprint Review*, bei dem das Product Increment mit dem Product Backlog abgeglichen wird, um letzteres bei Bedarf für den kommenden Sprint anzupassen. Des Weiteren werden die Ergebnisse des Sprints im Beisein des Auftraggebers vorgestellt und überprüft, ob das gesetzte Sprintziel erreicht worden ist sowie die nächsten Schritte bzw. der nächste Sprint geplant. [WR21]

### 5.1.8 Kruchten-Modell

Der französische Informatiker Philippe Kruchten entwickelte ein Architekturmodell, das nach ihm benannt ist oder auch als 4+1 Sichtenmodell (4+1 Architecture View Model) bezeichnet wird. Die vier Ansichten sind die logische, die Entwicklungs-, die Prozess- und die physische Sicht. Im Mittelpunkt stehen die Szenarien (Anwendungsfälle) als fünfte Ansicht („+1“). [Kru95]

Das Kruchten-Architekturmodell soll die Sichtweisen der verschiedenen Stakeholder (Anwender, Entwickler, Systemingenieur, Projektmanager) auf eine zu entwickelnde Software abbilden und gleichzeitig die Abhängigkeiten der Sichtweisen (Pfeile in Abb. 5.9) untereinander aufzeigen. Laut Kruchten ist sein Modell generisch ausgerichtet und nicht auf ein Entwurfsmodell oder Tool begrenzt. Im Gegensatz zu den zuvor beschriebenen Entwicklungsmodellen wie Wasserfall-, V-, Inkrementelles-, Spiral-Modell, XP oder Scrum wird beim Kruchten-Modell kein zeitlicher Verlauf einzelner Projektphasen zugrunde gelegt, sondern die Anforderungen an die Funktionalität aus verschiedenen Sichtweisen betrachtet, die sich im finalen Produkt wiederfinden sollen. Als eigenständiges Vorgehensmodell eignet sich das Modell von Kruchten nicht, da es keine zeitliche Abfolge einzelner Entwicklungsschritte als „roten Faden“ beinhaltet. Es veranschaulicht aber die unterschiedlichen

Perspektiven und Bedürfnisse der Stakeholder und stellt eine Gleichberechtigung der unterschiedlichen Sichtweisen her (zumindest theoretisch), da keine der 4+1 Ansichten dominiert bzw. nachrangig behandelt wird.

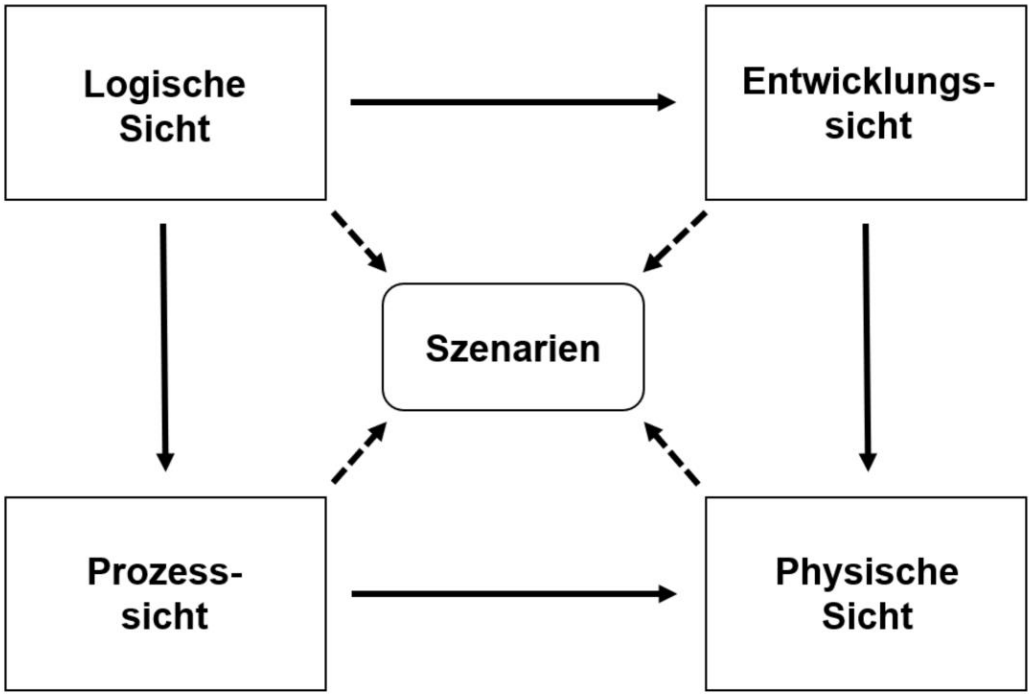



Abb. 5.9: Kruchten 4 + 1 Architekturmodell

**Logische Sicht**

Die logische Sicht beinhaltet die Funktionalität, die dem Anwender geboten werden soll. Zur Darstellung der logischen Sichtweise wird UML mit Klassen- und Zustandsdiagrammen genutzt.

**Entwicklungssicht**

Mit der Entwicklungssicht wird die Software aus dem Blickwinkel des Programmierers (Entwicklers) dargestellt und auch als Implementierungsansicht bezeichnet. Zur Beschreibung dieser Sicht kommen das Komponenten- und das Paketdiagramm der UML zur Anwendung.

### Prozesssicht

Bei der Prozesssicht liegt der Fokus auf den dynamischen Aspekten der Software, d.h. die internen Prozesse, deren Kommunikation und das Laufzeitverhalten. Wichtige Parameter der Prozesssicht sind Parallelität, Leistung, Verteilung und Skalierbarkeit. Als UML-Bestandteile dienen das Aktivitäts-, Kommunikations- und das Sequenzdiagramm.

### Physische Sicht

Mit der physischen Sicht wird die Software aus dem Blickwinkel des Systemingenieurs dargestellt. Hierbei ist die Topologie der Software und ihrer Komponenten auf der physikalischen Ebene (Hardware) und den Verknüpfungen zwischen den Komponenten. Als UML-Diagramm kommt hier das Bereitstellungsdiagramm zur Anwendung. In der Telekommunikation bzw. Netzwerktechnik entspricht die physische Sicht der Schicht 1 (Layer 1) des OSI-Modells.

### Szenarien

Die fünfte Sicht sind die Szenarien (Anwendungsfälle); diese beschreiben die Iteration zwischen Objekten und Prozessen. Die Szenarien dienen dazu, die Architektur bzw. deren Entwurfsansätze zu veranschaulichen und zu validieren. Ebenso dienen die Szenarien als Grundlage für Tests im deren Entwicklungsprozesses.

## 5.2 Zusammenfassung

Die einschlägigen Vorgehensmodelle zur Softwareentwicklung haben allesamt ihre Daseinsberechtigung, da je nach Komplexität der Anforderungen, der zeitlichen Dringlichkeit zur Fertigstellung eines betriebsfertigen Produkts und der möglichen Außenwirkung bei verzögerter Umsetzung und/oder Softwarefehlern unterschiedliche Ansprüche dominieren können. Die Einhaltung und Dokumentation aller formalen Prozesse kann im Widerspruch dazu stehen, möglichst schnell eine Lösung zu entwickeln und die Aufwände für Formalien des Projektmanagements möglichst

gering zu halten. Aspekte der IT-Sicherheit finden bei den genannten Modellen keine oder nur am Rande Erwähnung, da im Sinne des Projektmanagements die zielgenaue Erfüllung der funktionalen Anforderungen dominiert.

# 6 Entwicklungsmodell für Leitstellensoftware

Für BOS-Leitstellen, deren Hard- und Software – abgesehen von Standard-IT-Komponenten – einen Nischenmarkt darstellt, werden hohe Anforderungen an die Betriebssicherheit gestellt, was für das Inkrementelle Entwicklungsmodell und Scrum spricht. Um neue Anforderungen in betriebsfertiges Produkt zu überführen, ist ein iteratives Modell erforderlich, da regelmäßigen Tests eine wichtige Bedeutung im Entwicklungsprozess zukommt. [Alp94]

### 6.1.1 Ansatz mit bestehenden Entwicklungsmodellen

Verfahren wie das Wasserfallmodell oder das V-Modell sind aufgrund der fehlenden Iteration eher ungeeignet, da ein Zurückkehren an einen früheren Punkt des Entwicklungsablaufs bei Auftreten von Fehlern nicht vorgesehen ist. Namengebend verlaufen die Schritte des Wasserfallmodells „von oben nach unten“ und sind für die Rückkehr zu einem vorigen Schritt daher nicht geeignet. Zudem müsste die namengebende Bezeichnung von „Wasserfallmodell“ beispielsweise in „Treppenmodell“ geändert werden, da eine Treppe in beiden Richtungen begangen werden kann und ein Richtungswechsel jederzeit möglich ist; dieser Ansatz wird von Kersken beschrieben.

*„In einer reinen Form ist das Wasserfallmodell nicht einsetzbar, da in der Praxis Überarbeitungen von vorherigen Phasenergebnissen erforderlich werden. Wasserfallmodelle werden daher mit Rückkopplungsschleifen (sog. iterative Modelle) in der Praxis eingesetzt.“* [Ker15]

Alternativ ist eine Verkettung mehrerer Wasserfallmodelle denkbar, so dass die Iteration durch eine Kaskadierung mehrerer einzelner Wasserfall-Abläufe hergestellt wird. Ein aufgetretener Fehler am Ende der ersten Wasserfall-Sequenz kann in der

nachfolgenden Sequenz behoben werden. Dieses Variante ist in Abbildung 6.1 dargestellt; nach der ersten Wasserfall-Sequenz (blau) folgt die zweite (rot) und dann die dritte (grün). Die modellhafte Darstellung wird jedoch mit zunehmender Anzahl an Einzel-Wasserfällen unübersichtlich und damit schlecht handhabbar.

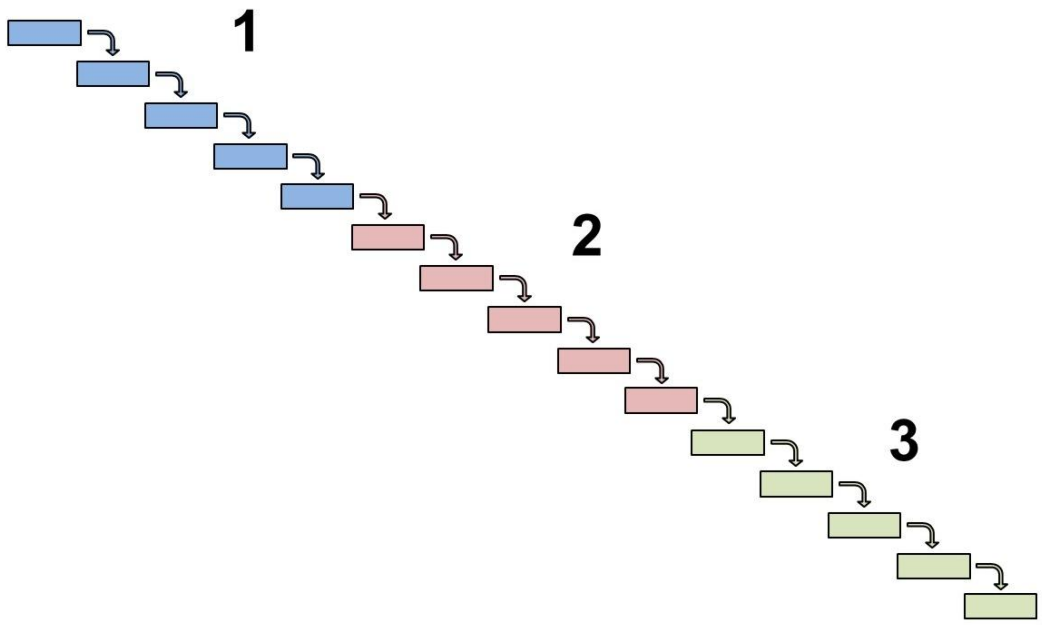



Abb. 6.1: Kaskadiertes Wasserfallmodell

Eine weitere Option ist die Überführung des nicht-iterativen V-Modells in ein iteratives Modell durch die Verkettung mehrerer V-Modelle, was in der grafischen Darstellung die Bezeichnungen „Wellenmodell“ oder „Zackenmodell“ nahelegt, siehe Abbildung 6.2.

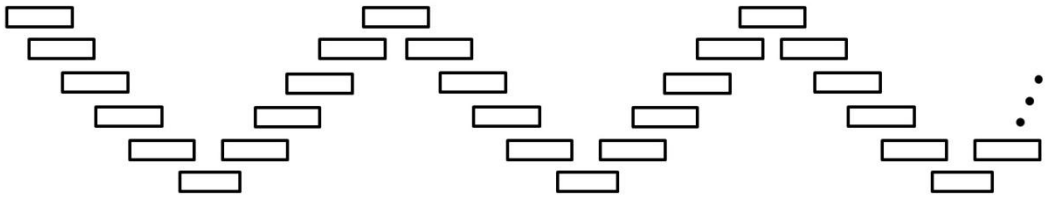


Abb. 6.2: Verkettete V-Modelle

Ebenso wie bei der Kaskadierung mehrerer Wasserfall-Sequenzen zu einem Gesamt-Wasserfall (Abbildung 5.8) ist eine Verkettung mehrerer V-Modelle (Abbildung 5.9) aufgrund der mit steigender Anzahl an Sequenzen zunehmender Unübersichtlichkeit für die praktische Projektabwicklung wenig geeignet.

Um den wiederkehrenden Testschritten im Entwicklungsprozess Rechnung zu tragen, sind daher das Spiralmodell und Scrum eher geeignet; für die parallele Entwicklungsarbeit an verschiedenen Modulen bieten sich Aspekte des Inkrementelle Modells an.

Bei sicherheitskritischen Anforderungen kommt den Schutzzielen *Verfügbarkeit*, *Integrität* und *Resilienz* (vgl. 2.5.1) eine sehr hohe Bedeutung zu. Der Erfüllung der Schutzziele im Planungs- und Entwicklungsprozess muss daher mindestens die gleiche Bedeutung eingeräumt werden, wie der Erfüllung der inhaltlich-funktionalen Anforderungen. [TKR07]

### 6.1.2 Definition der Anforderungen

Eine ausschließlich auf IT-Sicherheit ausgelegte Software, die aber in Bezug auf Bedienkomfort und Funktionsumfang mangelhaft ist, wird keine Akzeptanz finden. Ebenso muss das Bewusstsein bei allen Beteiligten – angefangen bei den Softwareentwicklern über die Verantwortlichen für Vertrieb bzw. Einkauf bis hin zu den Anwendern – geschaffen werden, dass von einer intuitiv gestalteten, benutzerfreundlichen und mit einem breiten Funktionsumfang ausgestatteten Software Abstand zu nehmen ist, wenn die Anforderungen an die IT-Sicherheit nachrangig betrachtet wurden. Hier gilt es die Balance zwischen den Anforderungen an die Usability und der IT-Sicherheit herzustellen (Abbildung 6.3).

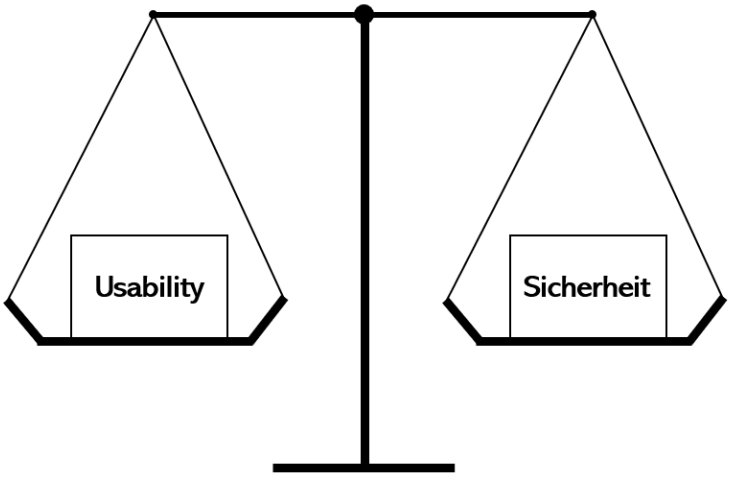



Abb. 6.3: Balance zwischen Usability und Sicherheit

D.h. es sind folgende Randbedingungen beim Softwaredesign zu berücksichtigen und zu priorisieren:

1. Sicherheit
2. Funktionalität
3. Usability

In Bezug auf die Anforderungen an die IT-Sicherheit sind im Vorfeld und auch während des laufenden Entwicklungsprozesses folgende Aspekte von Relevanz:

- An welchen Stellen bzw. in welchen Situationen sind bislang Störungen und Ausfälle aufgetreten, die beim neuen System unbedingt vermieden werden sollen? – exakte Analyse der Fehlerquellen
- Risikoanalyse; welche Risiken bestehen, welche Möglichkeiten zur Abhilfe bestehen? Welche Restrisiken müssen akzeptiert werden?
- Forderung nach aktueller Softwarearchitektur einschließlich agiler (Weiter-)Entwicklung oder klassische, bewährte Architekturen? [Mey14]
- Welche Abhängigkeiten bestehen von Hardware, Betriebssystemen, Virtualisierungsanwendungen, Datenbanken, Schnittstellen usw.? Bis zu welchem Punkt besteht – zumindest teilweise – Fremdbestimmtheit bei der IT-Sicherheit durch Standardsoft- und -hardware? [Gru03]
- Wer hat Zugriff auf welche Bestandteile des Systems (exakte Definition der Rollen/Tätigkeiten und der zugehörigen Rechte)?
- Datensparsamkeit – nur die Daten erheben und verarbeiten, die tatsächlich zur Aufgabenerfüllung (unter Berücksichtigung der rechtlichen Vorgaben) benötigt werden. Im Falle einer Kompromittierung ist der Datenverlust geringer und ein Angriffsziel wird umso uninteressanter, je weniger Daten zu erlangen sind.
- Automatische Anonymisierung der Daten und deren Speicherung, so dass die Zusammenführung personenbezogener Daten erschwert und der Rückschluss auf einzelne Personen weitgehend verhindert wird. Dies ermöglicht auch eine direkte Nutzung für statistische Auswertung und für Forschungszwecke (bei der Anonymisierung sind die rechtlichen Vorgaben zu Dokumentations- und Aufbewahrungspflichten zu beachten).

- Zusammensetzung des Technologiestacks, d.h. ausgereifte, qualitätsgesicherte Software, Technologien und Programmiersprachen, die sowohl für die Realisierung des Backends als auch des Frontends zum Einsatz kommen.
- Beobachtungen in der Fachwelt der IT-Sicherheit; welche Angriffsszenarien hat es in der Vergangenheit gegeben, welche gibt es aktuell, welche Trends bestehen? Des Weiteren: Welche Schutzmaßnahmen sind aktuell Stand der Technik und welche Trends zeichnen sich hier ab?
- Wie soll sich das System unter Last verhalten (Antwort-Zeit-Verhalten)? Betrachtung von Normallast über hohe Last bis hin zur maximal möglichen Last verhalten; auch im Hinblick auf mögliche DDos-Angriffe. Die Kriterien für Lasttests müssen passend gewählt werden:
  *„Last und Performance ist auf den ersten Blich relativ leicht zu testen, solange man einen geeigneten Lasttreiber und ein paar passende Lastmonitore hat. Leider ist das meist dann doch eine kompliziertere Sache, weil man schnell unrealistische Situationen testet oder die passenden Datenzustände und -massen nicht zusammenbekommt (beispielsweise indem man die Hintergrundlast auf den Maschinen vergisst oder falsch simuliert).“* [BKP17]
- Durchführung von Sicherheitstests am Ende der Softwareentwicklung oder auch zwischendurch, z.B. für einzelne Module? [Ker95]
- Können vorhandene Softwaremodule integriert und weitergenutzt werden, die sich im praktischen Betrieb bewährt haben und ausgereift sind (stabiler Betrieb, Bugs durch bisherige Patches und Updates bereinigt)? – Konsequenter Ausschluss von Modulen mit bekannten Sicherheitslücken wie z.B. Log4shell (siehe 3.5).
- Reputation und Referenzen des Lieferanten; hat dieser hinreichend Erfahrung mit sicherheitsrelevanter Software und verfügt über entsprechende Expertise im eigenen Haus? Referenzanforderungen mit dieser Schwerpunktsetzung sind bereits in der Phase der Vergabe und Auftragserteilung von hoher Bedeutung, damit nur ein Lieferant mit der Entwicklung betraut wird, der entsprechende, durch Referenzen nachgewiesene, Erfahrungen in der Entwicklung sicherheitsrelevanter Software nachweisen besitzt. [Har18]
- Implementierung von Sicherheitsverfahren für den späteren Betrieb (siehe 6.1.5); was muss bereits bei der Planung frühzeitig berücksichtigt werden?

Bei der Festlegung der funktionalen Anforderungen ist das gleiche Verständnis aller Beteiligten (Nutzer, Auftraggeber, Projektleitung, Programmierer usw.) von besonderer Bedeutung. Die unterschiedlichen Sichtweisen und Erfahrungswelten der Beteiligten erfordern eine interdisziplinäre Zusammenarbeit sowie einen einheitlichen und fest definierten Sprachgebrauch. [FK04] [Gei16]
Hinsichtlich der Funktionalität sind folgende Aspekte zur berücksichtigen:

- Anforderungen, die betrieblich und funktional vom Anwender/Auftraggeber gefordert werden
- Anforderungen, die sich aus technischen und rechtlichen Vorgaben, Normen und Standards ergeben (z.B. Telekommunikation, Digitalfunk, Technische Richtlinien, Dokumentationspflichten usw.)
- Einbettung von Fremdsystemen bzw. -modulen
- Schnittstellen zu Bestandssystemen und zu künftig geplanten Systemen
- Vergabe von Rollen und Rechten mit beliebigem Zuschnitt
- Einspielen von Updates und Patches bei laufendem Betrieb, ohne dass es zu Betriebseinschränkungen kommt
- Möglichkeit zu Fernwartung über gesonderten und gesicherten Zugang
- Erweiterbarkeit/Kaskadierbarkeit um weitere Arbeitsplätze, Lizenzen, Softwaremodule, Schnittstellen (Zukunftsfähigkeit, Investitionssicherheit).
- Customizing vs. auftraggeberspezifische Entwicklung

Bei der Usability

- Intuitive Bedienung, Informationen zu Funktionen/Schaltflächen z.B. per Mouseover
- Eingabefunktion, die sich z.B. bei der Einsatzerfassung mit der Notrufannahme an den gängigen Abfrageschemata orientiert und die Informationen in der Reihenfolge eingegeben werden, die Ablauf des Notrufgesprächs entsprechen. Strukturierte bzw. Standardisierte Notrufabfragesysteme [TRC22] bieten sich hier zur Implementierung bzw. Einbettung von Fremdsystemen an.
- Fehlertoleranz, einfache und schnelle Korrektur bzw. Rückgängigmachen falscher Eingaben
- Eingabehilfen, Autovervollständigen bei der Eingabe von Personen-, Straßen- und Ortsnamen

- Automatische Suche im Hintergrund bei der Erfassung von Personen-, Straßen- und Ortsnamen zwecks alternativer Schreibweisen einschließlich phonetischer Suche
- Ergonomische und ermüdungsfreie Gestaltung der Bedienoberfläche (Mensch-Maschine-Schnittstelle, Schriftgrößen, Farben, Kontrast) [Her18] [Kra23]
- Einfaches Anpassen der Bedienoberfläche durch den Administrator
- Single Sign On (SSO) bei der Anmeldung zu Schichtbeginn

### 6.1.3 Grundlegendes Vorgehen

Die zuvor aufgeführten Punkte bzw. Erkenntnisse müssen sich in der Projekt- bzw. Anforderungsbeschreibung wiederfinden und somit – ohne Details – auch in einem Entwicklungsmodell Berücksichtigung finden. Übertragen auf das Spiralmodell bedeutet das, dass sich der erste Zyklus ausschließlich auf die Sicherheitsanforderungen bezieht, während die funktionalen Anforderungen erst im zweiten Zyklus Einzug in den Gesamtprozess erhalten. Der dritte Schritt dient der Erfüllung der Benutzerfreundlichkeit (Usability), was sich vor allem durch die Gestaltung der Bedienoberfläche (Frontend), Eingabehilfen (z.B. Autovervollständigen), intuitive Bedienbarkeit und Fehlertoleranz auszeichnet. Dieser theoretisch-planerische Ansatz mit den drei aufeinander folgenden Zyklen bedeutet in der Praxis jedoch, dass eine Rückkehr zu einem früheren Schritt – beispielsweise, wenn im Rahmen eines Tests ein sicherheitsrelevanter Fehler auftritt – formal keine Rückkehr zum ersten Zyklus (Sicherheit) mehr möglich ist. Ebenso können Mängel bei der Umsetzung der funktionalen Anforderungen nicht mehr behoben werden, wenn sich bereits der dritte Zyklus (Usability) in Bearbeitung befindet. Die formale Einhaltung des Spiralmodells stößt daher in der Praxis an ihre Grenzen, da erfahrungsgemäß eine Rückkehr zu einem früheren, bereits abgeschlossenen Programmierschritt nötig ist, um Fehler zu beheben, die erst in einer späteren Phase zutage treten. Selbiges gilt für das Wasserfallmodell, das auch in einer kaskadierten Variante (Abb. 6.1) keine Rückkehr zu einem früheren Entwicklungsschritt vorsieht, um Korrekturen vorzunehmen. D.h. es ist ein Entwicklungsmodell erforderlich, das einerseits die Sicherheitsanforderungen hochpriorisiert beinhaltet und andererseits ein mehrfaches

Durchlaufen der Projektphasen ermöglicht, um Fehler zu bereinigen oder zwischenzeitliche Änderungen und Ergänzungen der funktionalen Anforderungen berücksichtigen zu können.
Gerade den Änderungen, die sich im Verlauf des Softwareprojekts ergeben, kommt auch nicht zur funktional, sondern auch im Hinblick auf die IT-Sicherheit eine hohe Bedeutung zu, damit Abhängigkeiten zu den anderen Funktionen, Modulen, Schnittstellen usw. nicht zu Sicherheitslücken führen. [LKM12]

Als Grundsätze einer ordnungsgemäßen Modellierung sind nach [BRS95] die *Richtigkeit*, die *Relevanz*, die *Wirtschaftlichkeit*, die *Klarheit*, die *Vergleichbarkeit* und der *systematische Aufbau* zu berücksichtigen. Die *Richtigkeit* betrachtet die korrekte syntaktische (vollständige, konsistente) und semantische (Orientierung am Soll-/Idealmodell, keine Widersprüche zu anderen Modellen) Korrektheit; die *Relevanz* bezieht sich auf die enthaltenen Elemente eines Modells, die allesamt von Bedeutung sein müssen und das Fehlen eines oder mehrerer Elemente würde die Nutzbarkeit des Gesamtmodells verringern. Der Grundsatz der *Wirtschaftlichkeit* betrachtet die Aufwände einer Modellbildung, die in einem vertretbaren Verhältnis zur Zielsetzung stehen müssen, d.h. keine zu hohe Modellierungsintensität, die Zeit (Kosten) erfordert, aber wenig Nutzen erbringt. Die *Klarheit* fordert für ein Modell eine Übersichtlichkeit in der Ausgestaltet, um die Nachvollziehbarkeit zu gewährleisten, hierbei nimmt auch die grafische Darstellung einen hohen Stellenwert ein. Zudem sollen Erweiterungen und Anpassungen möglich sein und die Differenz vom Ursprungsmodell eindeutig erkennbar sein. Mit der *Vergleichbarkeit* soll der Abgleich mit anderen Methoden und Modellen ermöglicht werden, wobei analog zur *Richtigkeit* (s.o.) syntaktische und semantische Aspekte gesondert betrachtet werden. Der *systematische Aufbau* bezieht sich auf die Integration einzelner Sichten (vgl. Kruchten-Modell, 5.1.8) zu einem Gesamtmodell, wobei sichtenorientierte Betrachtungen stets im Kontext zu den anderen Sichten zu berücksichtigen sind.

Die unterschiedlichen Aspekte von Softwareentwicklungsmodellen und deren Ausgestaltung und Weiterentwicklung steht auch im Zusammenhang mit der Qualitätssicherung, welche sich auch – aber nicht nur – auf IT bzw. Software bezieht. Hierbei ist der PDCA-Zyklus ein wichtiger Grundsatz. Ausgehend von der Planung und Konzeption (*Plan*) folgt die Umsetzung (*Do*), anschließend eine Analyse und

Überprüfung (*Check*) und mit dem vierten Schritt (*Act*) ein Review und – sofern erforderlich – eine Anpassung der Zielsetzung, bevor mit der erneuten Planung (*Plan*) der Zyklus erneut durchlaufen wird (siehe Abb. 6.4. D.h. die Iteration muss grundlegender Bestandteil des Entwicklungsmodells besitzen, damit bei Mängeln der Abgleich mit den Anforderungen sowie die Mängelbeseitigung erfolgt, bevor abermals die Überprüfung hinsichtlich Funktion und Sicherheit erfolgt. [CW07] Mit dem RUP-Modell (siehe 5.1.4) findet sich eine vierphasige Schrittfolge, die analog zu PDCA sich zyklisch wiederholend abläuft.

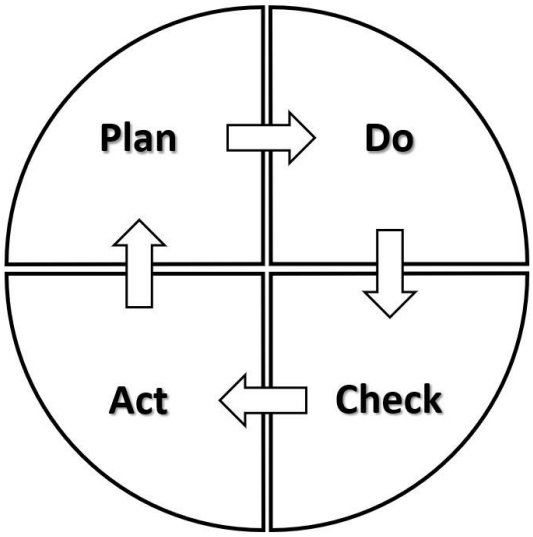



Abb. 6.4: PDCA-Zyklus

Es gilt daher, aus den etablierten, unter 5.1 ff. beschriebenen Vorgehensmodellen die Vorteile zu extrahieren und zu einem neuen Modell zusammen zu fügen. Hierbei ist gleichermaßen der Parallelität der Entwicklung verschiedener Softwaremodule Rechnung zu tragen, welche nach individueller Fertigstellung zu einem Gesamtpaket zusammengefügt werden. D.h. das Inkrementelle Modell mit der parallelen Arbeit an verschiedenen Modulen bildet eine gute Grundlage. Die erforderliche Iteration muss hierbei ebenso berücksichtigt werden. [AO16]

### 6.1.4 Sicherheitstests

Um Software auf Schwachstellen zu testen, bestehen verschiedene Testverfahren bzw. -ansätze, die sowohl während des Entwicklungsprozesses als auch bei bereits vermarkteter Software zur Anwendung kommen können [Jan21]:

1.) Beim **Static Application Security Testing (SAST)** wird der Quellcode der Software auf Schwachstellen überprüft. Hierfür muss sich die Software nicht aktiv im Betrieb befinden, sondern es genügt das Durcharbeiten des Quellcodes in Textform durch einen fachkundigen Programmierer oder auch automatisiert mittels spezieller Testprogramme
2.) Beim **Dynamic Application Security Testing (DAST)** erfolgt im Gegensatz zum SAST der Betrieb der zu testenden Software, um Sicherheitslücken erkennen zu können. Dies kann ebenfalls manuell oder automatisiert mittels Testprogrammen erfolgen. Gerade bei Webanwendungen können DAST-Testprogramme über das Frontend mit der zu überprüfenden Anwendungssoftware interagieren, um Schwachstellen zu erkennen. Hierbei besteht kein Zugriff auf den Quellcode wie beim SAST, sondern mögliche Schwachstellen werden durch tatsächlich gelungene Angriffsversuche identifiziert. DAST-Prozeduren gehören damit zu den Penetrationstests.
Automatisierte ablaufende Tests schaffen identische Testabläufe, so dass Änderungen im Quellcode bei Korrekturen oder Weiterentwicklungen stets nach den gleichen Kriterien und Abläufen getestet werden:

*„Ein äußerst wichtiges Mittel zur Steigerung der Effizienz und Effektivität von Tests ist die Testautomation. Erst reproduzierbare, automatisierte Test bilden das Sicherheitsnetz, durch das Software änderbar bleibt.“* [SVEH07]

3.) Das **Interactive Application Security Testing (IAST)** ist eine Kombination aus SAST und DAST, d.h. Schwachstellen sollen gleichermaßen durch Beobachtung (SAST) und Interaktion (DAST) mit der zu prüfenden Software erkannt werden. Dieses Verfahren wird von mehreren Unternehmen, die sich auf Anwendungssicherheit spezialisiert haben, eingesetzt. [Jan21]

4.) Der **Proof Carrying Code (PCC)** ist ein Algorithmus, der auf Basis eines Axiomensystems den Quellcode sowie begleitende Metadaten analysiert. Hierbei können neben Sicherheitslücken auch andere (funktionale) Mängel erkannt werden. PCC bietet sich auch an, um mittels Webzugriff von einem Client aus die Vertrauenswürdigkeit eines Hosts zu überprüfen, indem abgerufene Metadaten auf dem Client mittels PCC dort überprüft werden. [NL98]
5.) **Lasttests** dienen dem Nachweis, dass die Soft- und Hardware auch unter hoher Auslastung zuverlässig funktioniert bzw. Vorkehrungen gegen DoS-Angriffe (siehe 2.5.3.1) getroffen worden sind. Damit werden Anforderungen hinsichtlich der Resilienz (siehe 3.6) nachgewiesen und auch die Erfüllung des Schutzziels der Verfügbarkeit (siehe 2.5.4) überprüft.

Insgesamt stellen Software-Sicherheitstests hohe Anforderungen sowohl an die Softwareentwickler als auch an die Tester:

*"Designing and testing software systems to insure that they are safe and secure is a big issue facing software developers and test specialists."* [Bur03]

### 6.1.5 Sicherheitsmodell – Ansatz 1

Wie bei allen Vorgehensmodellen steht am Beginn die Erfassung der Anforderungen hinsichtlich Sicherheit, Funktion und Usability (Details siehe 6.1.2) und deren Zielsetzung, wodurch sich eindeutige und unmissverständliche Vorgaben für die nachfolgenden Entwicklungsschritte ergeben müssen. Die Anforderungen fließen in eine schriftlich zu fixierende Konzeption ein, in welcher die Zuständigkeiten und Abgrenzungen für die nachfolgende Aufteilung (gemäß Inkrementellem Modell) eindeutig beschrieben sind, so dass weder Doppelzuständigkeiten noch Lücken entstehen. Modulweise – in Abbildung 6.5 beispielhaft für drei parallele Module dargestellt – wird für jedes Modul ein Grob- und Feinentwurf erstellt, die eigentliche Programmierung erfolgt auf Basis des Feinentwurfs. Wie unter 5.1.3 dargestellt, kann die zeitliche Abfolge der Schritte innerhalb eines Moduls unterschiedlich verlaufen. Nach Abschluss der Programmerstellung erfolgen nacheinander Funktions-, Last- und Sicherheitstests auf Modulebene. Sofern alle modularen Testfälle ohne

Beanstandungen durchlaufen wurden, hat das Modul einen finalen Stand. Bei Unzulänglichkeiten werden die Modulschritte erneut durchlaufen, Wiederbeginn beim Grobentwurf des jeweiligen Moduls; Abbildung 6.5 zeigt den Ablauf.

Für alle vorgesehenen Module werden diese Schritte durchlaufen und erst nach erfolgreichen Tests aller Module erfolgt das Zusammenfügen und eine erneute Testprozedur des Gesamtsystems hinsichtlich Funktion, Last und Sicherheit. Erst wenn diese abschließenden Tests ebenfalls ohne Beanstandungen verlaufen sind, ist das System reif für Auslieferung und Betrieb. Ergeben sich bei den Testfällen des Gesamtsystems Mängel, erfolgt eine Fehleranalyse und dann ein Rücksprung (Iteration) auf die Phase vor der modularen Aufteilung in die einzelnen Module (A) oder direkt in das entsprechende Modul (B); in Abb. 6.5 beispielhaft für das untere, rot gekennzeichnete Modul dargestellt.

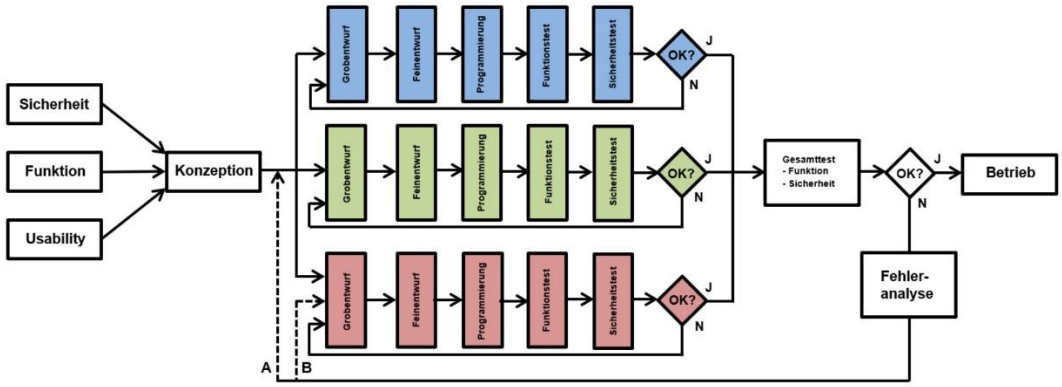



Abb. 6.5: Erweiterung des Inkrementellen Modells zum Sicherheitsmodell

Sofern ein bereits vorhandenes, in der Praxis erprobtes und ausgereiftes Modul zur Verfügung steht, können die Entwicklungsschritte für dieses Modul entfallen (in Abbildung 6.6 beispielhaft für das blau gekennzeichnete Modul dargestellt). Tests hinsichtlich Funktion, Verhalten unter Last sowie Penetration müssen nach den gleichen Maßstäben erfolgen, wie bei neu zu entwickelnden Modulen. Der erneute Funktionstest ist hierbei in Zusammenhang mit den anderen Modulen und der Funktionalität des Gesamtsystems zu sehen, ebenso die erneuten Last- und Sicherheitstests. Sollten in diesem Modul Unzulänglichkeiten auftreten, muss auch hier eine Nachbesserung erfolgen.

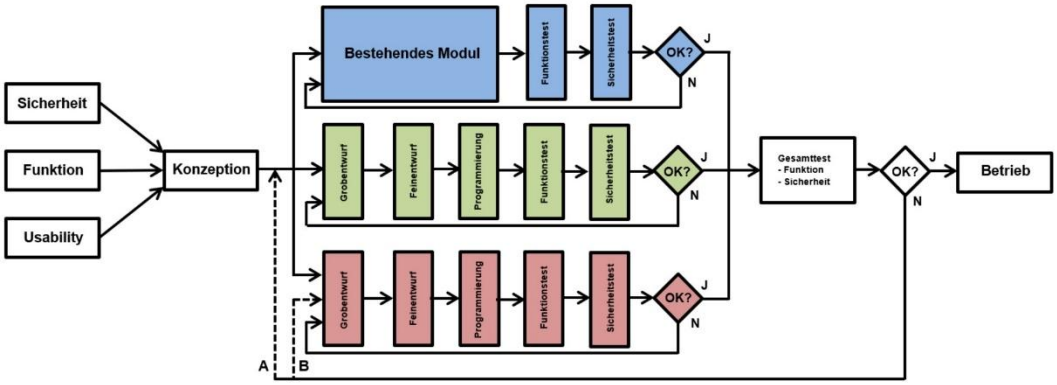



Abb. 6.6: Sicherheitsmodell mit Integration eines bestehenden Softwaremoduls

Das eigentliche Vorgehen bei der Softwareerstellung von der Konzeption bis zur Umsetzung kann auf verschiedene Arten erfolgen, z.B. als XP (Extreme Programming) oder Scrum. Letzteres ist für das blau gekennzeichnete Modul in Abbildung 6.7 dargestellt; nach den Product- und Sprint-Backlog folgen die Sprints – einschließlich Daily Sprints – und anschließend das Product Increment und Sprint Review, bevor im nächsten Schritt die Tests anstehen. Innerhalb dieses Zweiges können mehrere Sprint-Schleifen und -Reviews durchlaufen werden (einschließlich Funktions- und Sicherheitstests), auch wenn aus Darstellungsgründen nur eine Sprint-Schleife eingezeichnet ist.

Extreme Programming ist aufgrund der fehlenden Formalitäten hinsichtlich der Abarbeitung eher ungeeignet, da mangels einer exakten Zieldefinition und formaler Projektabläufe ein hohes Risiko besteht, dass Sicherheitsaspekte zugunsten einer zügigen Umsetzung der funktionalen Anforderungen wenig oder gar keine Berücksichtigung finden.

Je nach Anforderung und Komplexität der Module können auch unterschiedliche Vorgehensweisen Anwendung finden. Wichtig ist eine einheitliche Vorgehensweise und einheitliche Maßstäbe bei den Testszenarien. Die eigentliche Softwareerstellung nach verschiedenen Vorgehensmodellen kann z.B. bei der Beteiligung verschiedener Abteilungen, Niederlassungen oder Auftragserteilung an verschiedene Subunternehmer zur Anwendung kommen, falls den Beteiligten diese Freiheit zugestanden wird und ein bevorzugtes Entwicklungsmodell zur jeweiligen Unternehmens- oder Abteilungskultur gehört.

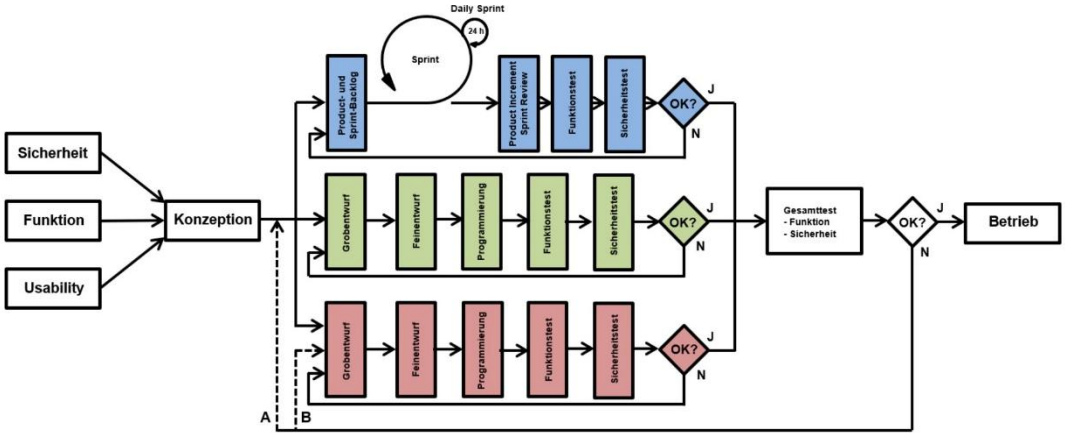



Abb. 6.7: Sicherheitsmodell mit einem inkrementellen Zweig als Scrum

### 6.1.6 Sicherheitsmodell – Ansatz 2

Ausgehend vom Kruchten-Modell (siehe 5.1.8), welches die verschiedenen Blickwinkel (Ansichten) der Beteiligten eines Softwareprojekts darstellt, lässt sich auch auf dieser Grundlage ein Sicherheitsmodell entwickeln. Da die Darstellung der 4+1 Ansichten keinen zeitlichen Ablauf im Sinne eine Projektplans beinhaltet, lässt sich die IT-Sicherheit als weiterer Stakeholder (fünfte Sicht) in das bestehende Modell integrieren, so dass sich ein „5+1 Modell“ ergibt (Abb. 6.8).

Hierbei nimmt die IT-Sicherheit einen gleichberechtigten Stellenwert mit den anderen vier Ansichten ein.

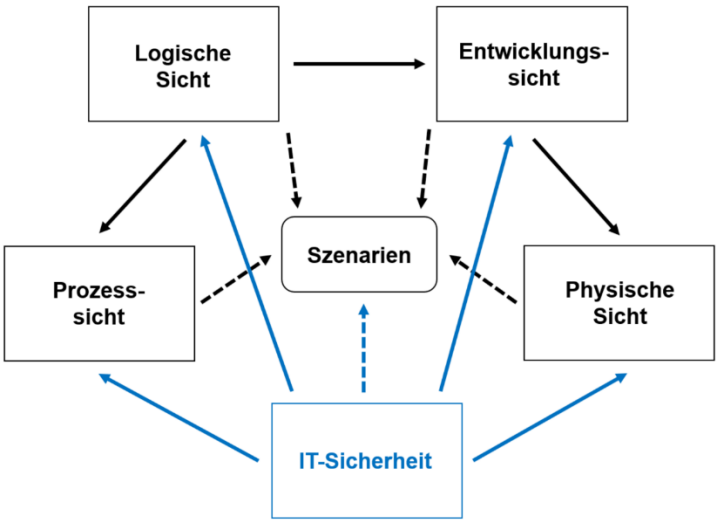



Abb. 6.8: Erweiterung des 4+1-Modell nach Kruchten zum 5+1-Modell

Da das 4+1 Modell nach Kruchten bzw. die Weiterentwicklung zu einem 5+1 Modell zwar die verschiedenen Sichtweisen veranschaulicht, aber keinen zeitlichen Verlauf einzelner Entwicklungsschritte beinhaltet, ist es nicht als eigenständiges Softwareentwicklungsmodell anwendbar (siehe auch 5.1.8), sondern kann nur in Kombination mit einem Modell angewendet werden, welches auch den zeitlichen Verlauf des Entwicklungsprozesses beinhaltet. Das 5+1 Modell hat dennoch seine Berechtigung, um den Stellenwert der IT-Sicherheit gegenüber den vier anderen Sichten zu betonen.

### 6.1.7 Validierung durch Hersteller

Zwecks Validierung des Entwicklungsmodells unter 6.1.5 ist der Verfasser an sechs Unternehmen herangetreten, die in Deutschland auf dem Leitstellenmarkt aktiv sind und entsprechende Anwendungssoftware entwickeln und vertreiben. Vier der angefragten Unternehmen (CKS Systeme, Eurofunk Kappacher, Sinus Nachrichtentechnik sowie Vomatec Innovations) haben Rückmeldungen hinsichtlich der praktischen Umsetzbarkeit gegeben. Anmerkungen hinsichtlich missverständlicher Ausführungen oder nicht eindeutiger Verwendung von Begrifflichkeiten sind bereits in die vorgenannten Abschnitte mit eingeflossen. Um Rückschlüsse auf Betriebsinterna der genannten Unternehmen zu vermeiden, sind die nachfolgenden Stellungnahmen anonymisiert und die Unternehmen nach der Reihenfolge des Eingangs der Rückmeldungen mit A, B, C und D bezeichnet.

**Unternehmen A**

1. Das Sicherheitsmodell mit einem inkrementellen Zweig als Scrum (Abb. 6.7) besitzt eine starke Überschneidung zum Softwareentwicklungsprozess Scaled Agile Framework (SAFe), der seit einigen Jahren genutzt wird.
2. Bereits während der iterativen Sprint-Schleifen sollten Maßnahmen und Tests zur Gewährleistung der Sicherheit stattfinden.
3. Die sich daran anschließende Phase des Produkt-Inkrements und die darauf angewendeten Funktions-, Usability- und Sicherheitstest stellen nochmal eine Prüfung vor der Integration in das Gesamtsystem dar.

4. Beginnend mit den Ausschreibungen werden Entscheidungen zum künftigen System-Setup getroffen. Diese, oft weitreichenden Entscheidungen, besitzen schon Einfluss auf die Sicherheit des Systems, beispielsweise Rückfallebenen, Anzahl und geografische Lage der Rechenzentren oder eingebundene Software Dritter. Abgesehen von diesen Spezifika werden allgemein umzusetzende Anforderungen im Bereich Cybersicherheit und Datenschutz durch Institutionen wie beispielsweise dem BSI in die grundlegende Konzeption übernommen. Dies ermöglicht, den unterschiedlichen Entwicklungsabteilungen einen Rahmen vorzugeben. Dadurch können einzelne Anforderungen durch technische Basisframeworks schon frühzeitig in der Entwicklung geprüft und damit sichergestellt werden.
5. Eine Art Test-Driven-Development, durch Testframework und Static Application Security Testing (SAST), für einige wiederkehrende sicherheitsrelevante Implementierungen. Ebenso, nur automatisiert effizient auffind- bzw. lösbare Softwareschwachstellen sind jene der verwendeten Open-Source-Software (OSS), dazu wird im Buildprozess des jeweiligen Moduls importierte OSS durch Scanner mit Schwachstellendatenbanken abgeglichen, um auch dort Sicherheit zu gewährleisten.
6. Im Bereich Usability wird zwar nicht viel automatisiert während der Entwicklung getestet, es ist jedoch zum/zur vereinfachten Erscheinungsbild bzw. Produktnutzung ein Designkatalog für Standard-User-Interfaces in Verwendung. Dieser Katalog setzt unsere allgemeine Best Practice im Bereich User Experience um.
7. Allgemein gilt anzumerken, dass Penetrationstest nicht die einzige Möglichkeit zur Überprüfung sicherheitsrelevanter Aspekte sind. Darüber hinaus sind – insbesondere in den iterativen Phasen der Entwicklung – bereits oben erwähnte andere Mittel sinnvoll und notwendig. Daher sollte im Modell nicht ausschließlich der Begriff „Penetrationstest“ verwendet werden.
8. Die dargelegten Abläufe zeigen, dass schon während der Entwicklung vieles im Bereich Sicherheit und Usability voraus- und umgesetzt wird. Dies spiegelt sich auch in den unterschiedlichen Stadien unserer *Definitionen of Done* (DoD) wider. Darin sind konkret *Non-Functional Requirements* (NFR) bezüglich der Themen Performance, Sicherheit und Usability verankert. Somit finden Tests, welche die Sicherheit des Produkts gewährleisten, schon

während den Entwicklungsiterationen statt. Eine Gegenüberstellung mit Abb. 6.7 zeigt, die Teststadien finden sich auch bei uns wieder, aber sind zu wenig. In der Praxis zeigt sich deutlich, dass schon während der Entwicklung der unterschiedlichen Software-Komponenten Tests angebracht sind. Dort werden sicherheitsrelevante Tests durchgeführt und negative Ergebnisse können dann effizienter gelöst werden. Das Teststadium vor „Betrieb“ (Test – Funktion, Last, Penetration) in Abb. 6.7, der sich auf die Verifikation des Gesamtsystems bezieht, ist umfangreich und wirtschaftlich betrachtet das teuerste Stadium, um negative Ergebnisse lösen zu können.

9. Durch die vermehrte Nutzung von OSS ist es weiterhin notwendig, die im Betrieb befindlichen Software-Versionen stetigen Tests zu unterziehen (funktional durch SW-Regression sowie nicht funktional durch eventuelle Schwachstellen). Was zu einem allgemeinen Exkurs zum SDLC führt, der hier in einem stärkeren Ausmaß Beachtung finden sollte. Der Betrieb einer Leitstelle findet, zumindest in unserem derzeitigen Kontext, in einem abgegrenzten System statt, sowohl hardware- als auch netzwerktechnisch. Es rückt der Betrieb aber immer näher ins Zentrum der Betrachtung im Produktentwicklungszyklus (Cloudlösung – *Infrastructure as Code* (IaC), *Software as a Service* (Saas), …), auch bei der Erfüllung der *Certified Internal Auditor*-Anforderungen (CIA), doch durch restriktive Sicherheitspolitik (Sicherheitsfreigabe, System-Setup etc.) können wir kein allgemein gültiges Entwicklungs- bzw. SDLC-Modell anwenden. Diese Betrachtung fehlt, zumindest in den übermittelten Abschnitten, dazu zählt beispielsweise sichere Ausrollung von (neuen) Releases, *Principle of Least Priviledge* (PoLP) und personenbezogene Nachweisbarkeit (Auditierung) in der Software-Infrastruktur.
10. Sicherheit, Funktionalität und Bedienbarkeit sind sehr große, zusammenfassende Begriffe – welche NFR müssen im Kontext von Leitstellen noch näher betrachtet werden?
11. Definition von „Modul“ – wird oftmals unterschiedlich verstanden. Ist ein Modul eine eigene Applikation oder ein Stück Code in einer Applikation?
12. Risikobewertung und Risikomanagement ist ein weiterer Aspekt, der in der Cybersecurityabhandlung zu finden sein sollte.

**Unternehmen B**

1. Die reine Lehre der Methoden hat sich bei uns in der Praxis nicht bewährt. In der Vergangenheit waren im Projektmanagement alle Funktionen vereint: Funktion, Usability, Umsetzungskonzept.

   Hier haben wir Anpassungen vorgenommen, so dass wir zwischen einem funktionalen und technischen Produktmanagement unterscheiden. Das Thema IT-Sicherheit fällt hier in den Bereich des technischen Produktmanagements.
2. Die Herausforderung besteht hier immer wieder, produkt- und projektspezifische Anforderungen wartungsarm zu vereinen. In den Prozess der technischen Umsetzungen binden wir hier frühzeitig die entsprechenden Softwareentwickler mit ein. Wichtig für uns ist auch die frühzeitige Definition der Testcases für die QS sowie das Thema Schulung und Weiterbildung, gerade im Hinblick auf die Verwendung der IT-Konzepte für den Bereich IT-Sicherheit.
3. In regelmäßigen, kurzen Zyklen erfolgen Meetings zur Klärung von Fragen und zur Definition des Entwicklungsstandes. Ein Schwerpunkt während der Implementierung ist auch die Vervollständigung der Testcases durch den Softwareentwickler.
4. Unterstützt wird der komplette Softwareentwicklungsprozess durch moderne Tools. Dies umfasst nicht nur das Ticketmanagement, sondern auch die Automatisierung von Releasenotes, Softwaregenerierung und Testing.
5. Durch das automatische Testing erfahren wir einen hohen Grad an Unterstützung für die Durchführung von Lasttests. In unregelmäßigen Abständen führen wir entsprechende Penetrationstests an unseren Systemen durch.
6. Erfreulicherweise erfahren wir im Bereich der Schnittstellen mittlerweile einen hohen Standardisierungsgrad, da sich dieser Bereich immer mehr auf das Web-Umfeld bezieht. Dies macht das Testing vor der Softwarelieferung wesentlich einfacher.
7. Generell kann ich sagen, dass für mich der Softwareentwicklungsprozess ein Schwerpunktthema in der täglichen Arbeit ist. Hier steckt viel Potenzial für Effizienz und Kundenzufriedenheit.

**Unternehmen C**

Ich habe mir das alles durchgelesen und empfinde es als sehr passende Abhandlung. Was mir jedoch fehlt, ist die Kombination aus den Entwicklungsmodellen mit dem Projekt. Also eine Art Mix als z.B. V-Modell eingebettet in ein Projektmanagement. Dies wird meines Erachtens immer aus dem Auge gelassen. Wir haben ja alle Zeit- und Kostendruck.

**Unternehmen D**

Praktische Umsetzbarkeit und Vorteile:

- geregelte, in das Vorgehensmodell integrierte Betrachtung des Sicherheitsaspektes
- gewisse Unabhängigkeit vom Entwicklungsmodell
- zeitliche Unabhängigkeit bei der Umsetzung der Inkremente
- Unabhängigkeit vom Entwickler/vom Entwicklungsteam
- Abbildbarkeit des Vorgehens in Testautomation-Pipelines bzw. CI-Systemen

Praktisch schwieriger umzusetzen / Verbesserungsvorschläge:

- Die Anforderungen zum Aspekt „Sicherheit“ sind häufig unvollständig und somit in Teilen unbekannt. Ursache hier ist häufig die Abhängigkeit von den Zielsystemen und deren extreme Vielfalt (Hardware, Betriebssystem, Virtualisierungslösung, unterschiedliche Versionsstände der angebundenen Anlagen/Geräte/Fremdsoftwaren etc., entsprechend Ihrer Anmerkungen im Kapitel 6.1.8 Betrieb). Unbekannte Anforderungen können während des gesamten Vorgehensmodells nicht berücksichtigt werden. Sie fließen somit weder in die Konzepte noch in die Entwicklung oder Tests mit ein. Der vollständige (formale) Nachweis der Sicherheit ist extrem schwierig.

  Die bekannten Anforderungen zum Aspekt „Sicherheit“ fließen natürlich in die Konzepte mit ein, aber auf einem hohen Abstraktionsniveau („Konzeptionelle Sicherheit“). So wird beispielsweise bezüglich des Datenschutzes eine Anonymisierung vorgesehen. Durch Programmierfehler verursachte Sicherheitslücken können dadurch aber nicht oder nur mit einer gewissen Wahrscheinlichkeit (durch die Tests) vermieden werden. Hierzu wäre eine

bindende Richtlinie/Vorgehensweise für die Entwickler sinnvoll, deren Einhaltung bei allgemeinen Sicherheits-Reviews überprüft wird.

- Bei der Verbindung des Sicherheitsmodells mit Scrum sehe ich keine Notwendigkeit, die Funktions- oder Sicherheitstests im jeweiligen Modul/der Story außen vor zu lassen. Die im Scrum-Framework verwendete DoD (Definition of Done) kann gerade wichtige QS-Aspekte enthalten, die erfüllt sein müssen, damit ein Inkrement als fertig betrachtet werden kann (Tests vorhanden und bestanden, Security Checkliste erfüllt, keine „gefährlichen" Fremdkomponenten verwendet etc.).
- Auch sind andere Ansätze wie TDD (Test Driven Development, üblicherweise auch ein Teil von XP), bei denen die Tests vor dem eigentlichen Programmcode geschrieben werden, so nicht abgedeckt. Diese erlaub Ihr Modell aber ja durchaus, wenn die Reihenfolge innerhalb eines Modells flexibel sein darf. Der positive Effekt von Pair Programming auf die Software-Qualität ist in verschiedenen Studien belegt.

Sonstiges / Hinweise:

- Die frühzeitige Erkennung von Sicherheitslücken könnte im Zuge der Tests mit Hilfe von Fuzzy-Tests und/oder auf künstlicher Intelligenz basierenden Penetrationstests verbessert werden.
- Einbeziehung des (Bediener-)Personals ist entscheidend für die spätere Akzeptanz
- Intuitive Bedienbarkeit ist aus unserer Sicht nicht im Widerspruch zur IT-Sicherheit, eher im Gegenteil (beispielsweise sollten sicherheitsrelevante Einstellungen in einer Software klar und eindeutig in Beschreibung, Bedienung und Funktion umgesetzt sein).
- SSO bietet zwar einen hohen Komfort / Usability für den Anwender, der Mehrwert ist aber weitaus höher
- Beim Thema Testing auf die „Testpyramide" oder den „Testpokal" achten. Tests sollen prinzipiell auch bei Änderungen verhindern, dass Fehler eingebaut werden. Diese Tests sollen im Idealfall in schneller Folge ausführbar sein. Tests auf Systemebene sind hingegen langwierig (und teuer) und komplex, gerade wenn auch Hardware involviert ist.

Fazit der Hersteller-Validierung:

1. Das Sicherheitsmodell mit einem inkrementellen Zweig als Scrum (Abb. 6.7) besitzt eine starke Überschneidung zum Softwareentwicklungsprozess Scaled Agile Framework (SAFe), der bei einem Unternehmen genutzt wird.
2. Neben dem reinen Prozess zur Softwareentwicklung mit durchgehender Gewährleistung der Sicherheitsaspekte sind im praktischen Betrieb auch Hardwarearchitekturen, Verteilte Systeme, (Geo-)Redundanzen, Betriebssysteme, Firmware, Schnittstellen sowie organisatorische und personelle Aspekte zu berücksichtigen, so dass sich insgesamt eine hohe Komplexität ergibt. IT-Sicherheit kann nicht allein durch eine Anwendungssoftware erzielt werden, die während des Entwicklungsprozesses mehrfach hinsichtlich Sicherheit getestet worden ist.
3. Vielfach bestehen in der praktischen Umsetzung Konflikte bei Softwareprojekten, ob der Fokus auf Funktion, Usability, Sicherheit, Wirtschaftlichkeit oder Schnelligkeit der Projektumsetzung gelegt wird.
4. Ein Entwicklungs-/Projektmodell kommt in der Praxis nicht exakt „nach Lehrbuch“ zum Einsatz, vielfach erfolgen Anpassungen und Abweichungen.
5. Softwaretests erfolgen vielfach automatisiert, künftig bietet sich durch den Einsatz von KI hier zusätzliches Potenzial.

### 6.1.8 Betrieb

Der auf der rechten Seite in den Abbildungen 6.5 bis 6.7 dargestellte Betrieb kann sowohl der Echtbetrieb als auch der Probebetrieb in der Echtanwendung sein, so dass Mängel, die in den vorigen Tests nicht zutage getreten sind, erst im Echtbetrieb auffallen. Mit Funktions- und Lasttests in der Entwicklungsumgebung lassen sich die realen Bedingungen nicht hundertprozentig nachstellen, da die Eigenschaften tatsächlicher Schnittstellen zu externen Systemen mit ggf. verschiedenen Versionsständen und Datenformaten sowie Bedienfehler der Anwender sich in ihrer Vielfalt kaum vorab spezifizieren lassen. [DRP13] Dem Probebetrieb in der realen Anwendung kommt daher eine besondere Bedeutung zu, um die Funktionalität und Stabilität beobachten zu können, aber auch um sicherheitsrelevante Aspekte zu prüfen; z.B. erneuter Sicherheitstest in der Echtinstallation. Sollten hierbei Mängel

auftreten, ist anhand des Schweregrades und der möglichen Auswirkungen abzuwägen und zu entscheiden, ob das System weiterhin im Echtbetrieb benutzt werden kann, oder ob eine frühere Version bzw. das Vorgängersystem wieder zur Anwendung kommt.

Nicht betrachtet in den beschriebenen Abläufen ist der Bereich Schulung, da für neu entwickelte Software sowohl Anwender als auch Administratoren geschult werden müssen. Dieser Schritt kann zwischen das fertiggestellte Produkt und die Installation für den Echtbetrieb erfolgen, so dass Erkenntnisse aus den Schulungen – dies betrifft vor allem die Usability – noch angepasst werden können, bevor der Echtbetrieb beginnt.

Im Echtbetrieb sind Sicherheitsverfahren ebenso unerlässlich, wie die Berücksichtigung der Sicherheitsaspekte im Rahmen der Softwareentwicklung. Zum sicheren IT-Betrieb gehören technische Maßnahmen wie

- Passwortschutz incl. Neuvergabe von Passwörtern bei Personalwechsel oder möglicher Kompromittierung
- Zertifikate
- Verschlüsselte Datenübertragung und -speicherung
- Datensicherung
- Mehrfaktor-Authentifizierung
- Kontinuierliche Risikoanalyse und Risikomanagement
- Notfallmanagement / Business Continuity Management (BCM)
  *„Abschließend lässt sich festhalten, dass ein angepasstes Notfall- und Krisenmanagement einen unverzichtbaren Bestandteil des Leitstellenbetriebs darstellt, um die Resilienz und Kontinuität auch in widrigen Situationen sicherzustellen. Im Zukunftsausblick ist die Koordination mit Partner- sowie Nachbarleitstellen und bundeslandübergreifende Abstimmung zur Kompatibilität der Lösungsoptionen und Ansätze von entscheidender Bedeutung, um eine effektive Zusammenarbeit zu ermöglichen und somit Sicherheit für die Bevölkerung zu gewährleisten.“* [Io24]

# 7 Praktische Umsetzung

Ein Software-Entwicklungsmodell ist zunächst ein theoretisch-ideales Konstrukt, welches das Vorgehen in einzelnen Schritten beschreibt und als „roter Faden“ für die Abarbeitung dient, so dass für alle Beteiligten (Projektleitung, Controlling, Programmierer) jederzeit erkennbar ist, in welcher Phase man sich aktuell befindet und welche als nächstes ansteht. Die tatsächliche praktische Umsetzung ist von zahlreichen Randbedingungen geprägt, die sich nicht vollumfänglich durch ein theoretisches Modell abbilden lassen. Hierzu gehören z.B. Änderungen des Funktionsumfangs (Change Requests, CR), die erst während der Softwareerstellung auftreten oder ein Mehrbedarf an Schnittstellen, Mehrbedarf an zu integrierenden Subsystemen oder Anpassungen an zwischenzeitlich geänderte Normen, Standards und Rechtsvorschriften. Um die möglicherweise entstehende „Eigendynamik“ bei der Implementierung der Änderungen während der laufenden Softwareerstellung zu Lasten der Sicherheitsaspekte so gering wie möglich zu halten, gilt es daher, mögliche Schwachstellen vorab zu identifizieren sowie Lösungsansätze und Vorgehensweisen zu festzulegen.

## 7.1 Mögliche Schwachstellen

In der Praxis sind Neuentwicklungen erfahrungsgemäß stets von einzuhaltenden Zeit- und Kostenvorgaben und damit einem gewissen zeitlichen Druck geprägt, da entweder kundenspezifische Arbeiten innerhalb des vorgesehenen, vertraglich fixierten Projektplans zu realisieren sind oder aber die Wettbewerbssituation ein zügiges Vorgehen bzw. die Fertigstellung zu einem definierten Zeitpunkt (z.B. feststehender und bereits kommunizierter Termin zur Präsentation eines neuen Produkts) erwartet. Ein eng gesteckter zeitlicher Rahmen steht damit im Spannungsfeld zur schrittweisen Umsetzung gemäß Vorgehensmodell und der exakten Einhaltung der Sicherheitsvorgaben, wenn die zügige Finalisierung eines neuen Produkts Priorität gegenüber der Erfüllung formaler und sicherheitstechnischer Vorgaben gewinnt.

Auch zwischenzeitliche Änderungen hinsichtlich funktionaler Anforderungen oder geänderten Normen, Standards und Rechtsvorschriften bergen die Gefahr, dass sich

die Fokussierung auf das formale Vorgehen und die Beachtung der IT-Sicherheitsvorgaben und gewissenhafte Durchführung der Testfälle in Richtung einer zügigen Fertigstellung verschiebt. Letztendlich ist die Gewissenhaftigkeit des Projektleiters der Schlüssel zur Einhaltung der Sicherheitsaspekte im Entwicklungsprozess, damit nicht allein die zügige Fertigstellung nach den funktionalen Vorgaben dominiert und die IT-Sicherheit vernachlässigt wird.

Auch mit sehr hohem Testaufwand, der entsprechend zeit- und kostenintensiv ist, lässt sich keine absolute Sicherheit nachweisen:

*„Testen kann Fehlerfreiheit nicht nachweisen. Um dies zu tun, müsste das Programm in allen möglichen Situationen, mit allen möglichen Eingaben und unter Berücksichtigung aller unterschiedlichen Randbedingungen getestet werden. Ein solcher vollständiger Test ist praktisch nicht durchführbar. Durch die Vielzahl kombinatorischer Möglichkeiten ergibt sich eine nahezu unbegrenzte Anzahl an Tests, die durchzuführen wären. Ein solches „Austesten" aller Kombinationen ist nicht möglich."* [SL19]

Hinzu kommt bei der Vielfalt an möglichen Testszenarien die Randbedingung, dass zwei oder mehr voneinander unabhängige Softwaremodule für sich betrachtet als sicher erachtet werden, dies jedoch nicht für das Zusammenwirken mehrerer Module gelten muss (siehe 2.8.1). Durch diese Komplexität wird deutlich, dass die Durchführung von Softwaretests für alle möglichen Kombinationen aus Einzelbestandteilen (Module, Schnittstellen) in der Praxis nicht durchführbar ist.

## 7.2 Lösungsansätze und Diskussion

Um der IT-Sicherheit im Rahmen der Softwareentwicklung das erforderliche Gewicht zu geben, sind eine Reihe von Randbedingen zu beachten; diese sind in der einschlägigen Literatur zu finden:

1. Ein Software-Entwicklungsmodell ist erforderlich, um die Anforderungen eines Softwareprojekts strukturiert bearbeiten zu können und damit auch der Qualitätssicherung Rechnung zu tragen. Dies gilt umso mehr, je größer der Personenkreis der Projektbeteiligten ist. Ein unstrukturiertes Erstellen von Programmcode sowie der Verzicht auf eine kontinuierliche Dokumentation

widerspricht einer qualitativ hochwertigen Softwareentwicklung. [SL19] [BKP17]

2. Jedes (Software-)Projekt hat einen Zeitrahmen, den es seitens aller Projektbeteiligten einzuhalten gilt. Zeitdruck bei der Softwareentwicklung hat erhebliche Auswirkungen auf die Ergebnisqualität [PBG11]; hier nicht nur auf die Umsetzung des erwünschten Funktionsumfangs, sondern auch auf die Einhaltung der IT-Sicherheitsvorgaben. Die zeitliche Planung des gesamten Softwareprojekts muss daher ausreichend bemessen sein, auf funktionale Änderungen während der bereits laufenden Softwareerstellung und auf zu Tage getretene Unzulänglichkeiten während der Tests reagieren und nachbessern zu können. Entsprechende Zeitpuffer sind hierbei für jeden Teilschritt vorzusehen. [Gol12]
3. Im Sinne eines geordneten Vorgehens, welches entsprechend protokolliert bzw. dokumentiert wird, muss jede nachträgliche Änderung der Anforderungen – auch wenn diese unbedeutend scheint – als Change Request betrachtet und entsprechend formal gehandhabt werden. Nicht schriftlich dokumentierte Änderungen „auf Zuruf“ müssen sowohl seitens der Projektleitung als auch von den ausführenden Programmierern konsequent abgelehnt und in ein dokumentiertes Änderungsmanagement überführt werden. Hier bietet sich z.B. die Orientierung am ITIL-Standard an. [Eb21]
4. Neben der rein funktionalen Softwareentwicklung im Sinne der Erstellung des Programmcodes müssen sicherheitsrelevante Verfahren des späteren Betriebs implementiert werden, z.B. Verschlüsselungsverfahren für Datenübertragung und -speicherung sowie die Nutzung von Zertifikaten, welche wiederum turnusmäßig zu aktualisieren sind. [Schw14]
5. Das komplette IT-System (Server, Speicher, Netzwerk) muss gegen Kompromittierung geschützt werden. Als Schutzmaßnahmen zählen vor allem Firewall-Systeme, Session Border Controller, Redundanzbildung, Datensicherung, Intrusion Detection sowie organisatorische Maßnahmen wie z.B. Passwortregeln, Mehrfaktor-Authentifizierung sowie Schulung und Sensibilisierung der Mitarbeiter zur Informationssicherheit. [GM18]
6. Eine absolute Sicherheit und Fehlerfreiheit lässt sich durch Softwaretests nicht erreichen, auch wenn diese umfangreich und mehrfach durchgeführt

werden, da es praktisch nicht möglich ist, alle denkbaren Szenarien und Testfälle durchzuführen. [SL19] Es verbleibt somit immer ein Restrisiko.

Um den o.g. Punkten Rechnung zu tragen und diese hinsichtlich der Anforderungen an sicherheitskritische Software zu präzisieren und in der Praxis umzusetzen, ergeben sich ergänzend folgende bedeutende Aspekte:

7. Die Aufwendungen für die gewissenhafte Umsetzung der IT-Sicherheit bei der Softwareentwicklung erfordern personelle und auch materielle Ressourcen und schlagen sich damit in den Projektkosten nieder. Neben der vollständigen Erfüllung der inhaltlichen Anforderungen ist die Wirtschaftlichkeit von Softwareprojekten ein ebenso bedeutsamer Aspekt. Dies gilt vor allem dann, wenn die öffentliche Hand als Leitstellenbetreiber und Auftraggeber hier mit Steuergeldern agiert; die Wirtschaftlichkeit ist ein wesentliches Kriterium bei der Vergabe öffentlicher Aufträge. Das Kostenargument darf jedoch kein Grund sein, die IT-Sicherheit lediglich als Randthema zu betrachten – vielmehr muss hier mindestens eine Gleichrangigkeit der IT-Sicherheit mit den funktionalen Anforderungen gelten. Gerade im Hinblick auf die Rolle der Leitstellen als Bestandteil der Kritischen Infrastruktur (siehe 2.2 ff.) müssen die Aufwände für Invest und Betrieb nicht nur bezogen auf das Gebäude, die Gebäudetechnik einschließlich Energieversorgung, Zugangskontrolle und Sicherheits-/Überwachungstechnik sowie redundant ausgeführte IT-Hardware betrachtet werden, sondern gleichermaßen auf unter IT-Sicherheitsaspekten entwickelte und gehärtete Software.
8. Im Sinne der IT-Sicherheit ist seitens der Beteiligten (Projektleitung, Programmierer, ggf. Modul-Verantwortliche) dafür Sorge zu tragen, dass die Schritte und Meilensteine, die sich auf die Sicherheitsaspekte beziehen, den gleichen Stellenwert einnehmen, wie die funktionalen Anforderungen. Ein möglicher Ansatz ist hierbei die Benennung eines Verantwortlichen für die IT-Sicherheit des Softwareprojekts, der auf der gleichen Hierarchieebene angesiedelt ist, wie der Projektleiter. Alternativ ist im Sinne eines Organigramms diese Zuständigkeit für die IT-Sicherheit von Softwareprojekten als Stabsstelle bei der Projektanleitung anzusiedeln, nicht jedoch im Bereich der Teilprojekte, damit die übergeordnete Bedeutung der IT-Sicherheit

sowohl organisatorisch hervorgehoben wird und auch praktisch gelebt werden kann.

In Abgrenzung zum IT-Sicherheitsbeauftragten des Unternehmens und dessen regulären Aufgaben, die vorranging im Bereich der internen IT angesiedelt sind, ist daher ein gesonderter IT-Sicherheitsbeauftragter für die Projektabwicklung zu benennen, der die Einhaltung der IT-Sicherheitsstandards über den gesamten Verlauf des Softwareprojekts steuert und überwacht. Um Verwechslungen mit dem IT-Sicherheitsbeauftragten des Unternehmens zu vermeiden und die besondere Rolle bei der Projektabwicklung zu betonen, ist hierfür eine gesonderte und eindeutige Tätigkeitsbezeichnung erforderlich, z.B. *IT Security Controller (IT-SC)*.

9. Neben der internen Umsetzung bei einem Softwarehersteller muss der IT-Sicherheit bereits bei der Definition der Anforderungen Gewicht eingeräumt werden. Da die Leitstellen größtenteils durch die öffentliche Hand betrieben werden (siehe 2.2.5), ist bei Beschaffungen stets das Vergaberecht zu beachten, d.h. oberhalb festgelegter Schwellenwerte muss die Leistung öffentlich ausgeschrieben werden. Der Auftraggeber hat hierbei das sog. *Leistungsbestimmungsrecht*, d.h. er kann im Rahmen des Bedarfs Kriterien festlegen, wie die Leistung zu erbringen ist. Hierzu gehören vor allem der Leistungsumfang, Abgrenzung von Nachbargewerken, Formalien zum Projektabwicklung (Projektmanagement) [SW07], einzuhaltende Normen/Standards/Zertifizierungen und auch Vorgaben zur IT-Sicherheit. Hierbei können auch Last- und Sicherheitstests zu verschiedenen Phasen des Entwicklungsprojekts mit festgelegt werden bzw. auch das Beisein des Auftraggebers bei den Tests vertraglich mit vereinbart werden; bis hin zur Freigabe von Zwischenschritten durch den Auftraggeber im Rahmen von vor-Ort-Terminen beim Auftragnehmer (nächster Entwicklungsschritt darf erst begonnen werden, wenn die Tests zuvor ohne Beanstandungen verlaufen sind usw.).
10. Die Einbindung fachkundiger Dritter, die die Umsetzung der IT-Sicherheitsvorgaben bei der Softwareentwicklung von externer Seite aus mit überwachen und begleiten, ist ein weiterer Ansatz. Durch die Einbindung externer Expertise ist der Softwarehersteller ständig gefordert, seine Arbeitsweise, Dokumentation, Testergebnisse und IT-Sicherheits-

maßnahmen gegenüber einer Kontrollinstanz offenzulegen. Eine strikte Einhaltung der formalen Vorgaben hinsichtlich Projektabwicklung, Vorgehensmodell, Softwaretests und IT-Sicherheit wird hierdurch besser erzielt, als durch rein interne Controllingmechanismen.

Die Erfüllung der Anforderungen hinsichtlich der Nutzung eines Softwareentwicklungsmodells zur strukturierten Bearbeitung (1.), einem ausreichend bemessenen Zeitansatz (2.) und der Berücksichtigung von sicherheitsrelevanten IT-Verfahren für den späteren Betrieb (4.) sollten bei einer Neu- oder Weiterentwicklung von sicherheitsrelevanter Software als selbstverständlich erachtet und auch eingehalten werden. In der Praxis besteht erfahrungsgemäß ein Spannungsfeld bei der Projektlaufzeit und den Kosten. Eine neue Software bzw. ein Softwareupdate soll zeitnah zur Verfügung stehen, um stets auf dem aktuellen Stand der Technik zu sein. Eine Entwicklungszeit von beispielsweise sechs Monaten und mit einer intensiven Testphase, die sich über mehr als weitere sechs Monate erstreckt, wird wenig Akzeptanz beim Auftraggeber finden. Für den Kostenaufwand gilt dies sinngemäß; wenn die Aufwände für (Sicherheits-)Tests höher liegen als für die eigentliche Erstellung des Programmcodes, ist auch hier nur eine geringe Akzeptanz auf Auftraggeberseite zu erwarten. Ungeachtet hoher Sicherheitsanforderungen für Software in der Kritischen Infrastruktur BOS-Leitstelle muss in der Praxis stets die Balance zwischen funktionalen und sicherheitskritischen Aspekten einerseits und dem zur Verfügung stehenden Zeit- und Kostenrahmen andererseits gefunden werden. Lang andauernde Testverfahren hinsichtlich Last und Penetration stehen einer zeitnahen Umsetzung neuer Funktionen entgegen. Im konkreten Fall muss daher abgewogen werden, wie sicherheitskritisch eine künftige Anwendung ist (z.B. unmittelbare externe Schnittstelle vorhanden, ja oder nein) und welcher Aufwand für Sicherheitsmaßnahmen gerechtfertigt und auch praktisch umsetzbar ist. Hinsichtlich eines pragmatischen Vorgehens sind Interpretationsspielräume durch eine exakte Definition der funktionalen und formalen Vorgaben seitens des Auftraggebers zu vermeiden.
Im Strahlenschutz findet sich das sog. *ALARA*-Prinzip (*As Low As Reasonably Achievable*), d.h. alle Maßnahmen zur Minimierung der Strahlenexposition sollen „vernünftig“ bzw. „so gut wie nötig“ eingehalten werden, da unrealistische Maximalforderungen weder pragmatisch noch wirtschaftlich sind. Im Strahlenschutz besteht ein ähnliches Spannungsfeld *Sicherheit – Kosten – Zeit*, wie in der IT-

Sicherheit, wobei die ALARA-Regel als Richtschnur für einen pragmatischen Ansatz dient. Übertragen auf die IT-Sicherheit und deren Umsetzung im Rahmen der Softwareentwicklung ist vor allem die Auftraggeberseite gefordert, entsprechende Mindestanforderungen bzgl. geordnetem Vorgehen (Projektmodell), Dokumentation, realistischem Zeitansatz incl. Zeitpuffer sowie der Benennung eines IT-Sicherheitsverantwortlichen für das Softwareprojekt vorzugeben. Aus den Rückmeldungen der Hersteller ist ersichtlich, dass unterschiedliche Ansätze hierzu existieren, jedoch durchweg eine strukturierte Herangehensweise besteht (siehe 6.1.7). Die Einbindung externer Expertise als zusätzliche Kontrollinstanz bildet einen weiteren wichtigen Baustein in der Umsetzung der IT-Sicherheit von der Erstellung der Anforderungsbeschreibung bis hin zum Echtbetrieb.

Für die Hersteller von Leitstellensoftware kann das Einräumen einer hohen Priorität von Sicherheitsaspekten während der Entwicklungsphase ein wichtiges Kriterium zur Abgrenzung gegenüber den Wettbewerbern darstellen und damit auch mögliche Haftungsfragen bei Sicherheitsvorfällen entkräften, wenn die IT-Sicherheit bestmöglich nach dem jeweils aktuellen Stand der Technik umgesetzt worden ist und dies auch projektbegleitend lückenlos dokumentiert ist.

# 8 Zusammenfassung und Ausblick

Die Integration der IT-Sicherheit in den Softwareentwicklungsprozess ist unabdingbar, um Software für sicherheitskritische Anwendungen wie z.B. BOS-Leitstellen zu entwickeln. Hierfür bietet sich das vorgeschlagene Sicherheitsmodell an, das in ähnlicher Form von zumindest einem Hersteller bereits praktiziert wird. IT-Sicherheit ist keine „Einzelmaßnahme“, sondern ist als Prozess zu verstehen, welcher mit den Überlegungen zur Beschaffung einer neuen Software beginnt, sich über die schriftlich niedergelegte Definition der Anforderungen und der programmtechnischen Umsetzung bis hin zum Produktivbetrieb erstreckt. Der Fokus auf sicherheitsrelevante Aspekte bereits in der Projektierung sowie kontinuierliche Funktions-, Last- und Penetrationstests während der Entwicklung bilden eine grundlegende Voraussetzung für eine hochverfügbare und fehlertolerante Anwendung. In Kombination mit der Realisierung als Verteiltes System incl. Self-Stabilization kann ein Höchstmaß an Redundanz und Verfügbarkeit erzielt werden. Abgerundet wird ein derart ausgestaltetes System durch einen standardisierten IT-Betrieb (z.B. nach ITIL) und unter fortwährender Anwendung des IT-Grundschutzes nach BSI. Der Weiterentwicklung von Hard- und Software ist ein stetiger Prozess, so dass eine fortlaufende Anpassung an die IT-Sicherheit erfolgen muss.

Alle diese Maßnahmen erfordern finanzielle Aufwände, sind jedoch für einen hochverfügbaren IT-Betrieb, der in einer BOS-Leitstelle unmittelbaren Einfluss auf Leib und Leben hat, unerlässlich. Alle Betreiber von BOS-Leitstellen sind daher in der Pflicht, die notwendigen Investitionen zu tätigen sowie den laufenden Betrieb finanziell und personell zu gewährleisten.

Aktuell findet die Thematik *Künstliche Intelligenz* (KI) reichhaltig mediale Beachtung. In Bezug auf Leitstellen werden in der Fachwelt vor allem der Nutzen hinsichtlich besserer Abgrenzung von dringenden Ereignissen gegenüber Bagatellen bei der Notrufannahme diskutiert, des Weiteren automatische Übersetzungsfunktion für das Gespräch mit Anrufern, die weder Deutsch noch Englisch sprechen sowie eine Unterstützung der Fahrzeugdisposition und das Erkennen von Trends beim Anruf- und Einsatzaufkommen zwecks zukünftiger Planungen. [GMD23]

KI-gestützte Systeme können ebenso einen wichtigen Beitrag zur IT-Sicherheit leisten, um z.B. ungewöhnliche Aktivitäten im Netzwerk zu erkennen (hohes

Lastaufkommen trotz wenig Betrieb, Häufung bestimmter Dateiformate usw.). Andererseits bestehen auch Risiken, dass KI-basiert Angriffe ausgeführt werden, die sich unauffällig in den bestehenden Datenverkehr einfügen und durch herkömmliche Antivirensoftware, Firewalls und Session Border Controller nur schwer erkannt werden können. Bei der Anwendung von KI liegen somit gleichermaßen Chancen und auch Risiken. Diese zu untersuchen, bietet ein breites Feld für Forschungsvorhaben, sowohl allgemein als auch in Bezug auf Kritische Infrastrukturen bzw. BOS-Anwendungen.

# Abkürzungs- und Symbolverzeichnis

Im Folgenden werden die verwendeten Abkürzungen erläutert.

| | |
|---|---|
| AAP | Ausnahme-Abfrageplatz |
| AAV | Automatisiertes Auskunftsverfahren |
| Abb. | Abbildung |
| Abk. | Abkürzung |
| AEG | Allgemeine Eletricitäts-Gesellschaft |
| AES | Advanced Encryption Standard |
| AI | Air Interface |
| AML | Advanced Mobile Location |
| ANA | Ausnahme-Abfrageplatz |
| AP | Arbeitsplatz |
| AS | Autorisierte Stelle |
| ASB | Arbeiter-Samariter-Bund |
| ASS | Schnittstelle für Autorisierte Stellen |
| BBK | Bundesamt für Bevölkerungsschutz und Katastrophenhilfe |
| BCM | Business Continuity Management |
| BDBOS | Bundesanstalt für den Digitalfunk der Behörden und Organisationen mit Sicherheitsaufgaben |
| BHKW | Blockheizkraftwerk |
| BKA | Bundeskriminalamt |
| BMA | Brandmeldeanlage |
| BMI | Bundesministerium des Innern |
| BNetzA | Bundesnetzagentur |
| BOS | Behörden und Organisationen mit Sicherheitsaufgaben |
| BPol | Bundespolizei |
| BRD | Bundesrepublik Deutschland |
| BS | Basisstation |
| BSI | Bundesamt für Sicherheit in der Informationstechnik |
| BSIG | Gesetz über das Bundesamt für Sicherheit in der Informationstechnik |

| | |
|---|---|
| CA | Certificate Authority |
| CEO | Chief Executive Officer |
| CERT | Computer Emergency Response Team |
| CI | Continuous Integration |
| CIA | Certified Internal Auditor |
| CIO | Chief Information Officer |
| CISO | Chief Information Security Officer |
| CLIP | Calling Line Identification Presentation |
| CLIR | Calling Line Identification Restriction |
| CLIRO | Calling Line Identification Restriction Override |
| COTS | Commercial-Off-The-Shelf |
| CR | Change Request |
| CRL | Certificate Revocation List |
| | |
| *d* | Decryption (Entschlüsselung) |
| DAG | Digitaler Alarmgeber |
| DAST | Dynamic Application Security Testing |
| DCK | Dynamic Cipher Key |
| DDoS | Distributed Denial of Service |
| DES | Data Encryption Standard |
| DIN | Deutsches Institut für Normung e.V. |
| DLP | Diskretes Logarithmusproblem |
| DNS | Domain Name Server |
| DoD | Definition of Done |
| DoS | Denial of Service |
| DRK | Deutsches Rotes Kreuz |
| DSGVO | Datenschutz-Grundverordnung |
| | |
| *e* | Encryption (Verschlüsselung) |
| EADS | European Aeronautic Defence and Space Company |
| EENA | European Emergency Numbering Association |
| ELA | Elektroakustische Anlage |
| ELS | Einsatzleitsystem |
| ELW | Einsatzleitwagen |
| EMA | Einbruchmeldeanlage |
| EN | Europäische Norm |

| | |
|---|---|
| ETB | Elektronisches Telefonbuch |
| ETSI | European Telecommunications Standards Institute |
| EU | Europäische Union |
| e.V. | eingetragener Verein |
| E2EE | End-to-End-Encryption |
| FMS | Funkmeldesystem |
| FRT | Fixed Radio Terminal |
| FSK | Frequency Shift Keying (Frequenzumtastung) |
| FW | Firewall |
| GG | Grundgesetz |
| GF | Galois Fields (Endliche Körper) |
| GMA | Gefahrenmeldeanlage |
| GPS | Global Positioning System |
| GSM | Global System für Mobile communication |
| HF | Hochfrequenz |
| IaC | Infrastructure as Code |
| IAST | Interactive Application Security Testing |
| IBM | International Business Machines |
| ID | Identifikation |
| IDEA | International Data Encryption Algorithm |
| IDS | Intrusion Detection System |
| IEC | International Electrotechnical Commission |
| IMSI | International Mobile Subscriber Identity |
| IP | Internet Protocol |
| ISDN | Integrated Services Digital Network |
| ISI | Inter-System Interface |
| ISO | International Organization for Standardization |
| ISSI | International Short Subscriber Identity |
| IT | Informationstechnik |
| ITIL | Information Technology Infrastructure Library |
| IT-SC | IT Security Controller |
| ITU | International Telecommunication Union |

| | |
|---|---|
| JUH | Johanniter-Unfall-Hilfe |
| *k* | key (Schlüssel) |
| KI | Künstliche Intelligenz |
| KMS | Kommunikationsmanagementsystem |
| KRITIS | Kritische Infrastruktur |
| KritisV | Verordnung zur Bestimmung Kritischer Infrastrukturen |
| KRLS | Kooperative Regionalleitstelle |
| LAN | Local Area Network |
| LS | Leitstellen-Schnittstelle |
| MHD | Malteser Hilfsdienst |
| MKK | Mehrkanal-Kryptokomponente |
| MMI | Man-Machine-Interface |
| MoWaS | Modulares Warnsystem |
| NATO | North Atlantic Treaty Organization (Nordatlantikpakt-Organisation) |
| NFR | Non-Functional Requirements |
| NGO | Non-Government Organization (Nichtregierungsorganisation) |
| NIST | National Institute of Standards and Technology |
| OPTA | Operativ-Taktische Adresse |
| ONKZ | Ortsnetzkennzahl |
| ÖPNV | Öffentlicher Personennahverkehr |
| OSS | Open-Source-Software |
| OTP | One Time Pad |
| PCC | Proof Carrying Code |
| PCI | Peripheral Component Interconnect |
| PCM | Pulscodemodulation |
| PDF | Portable Document File |
| PGP | Pretty Good Privacy |
| PIN | Persönliche Identifikationsnummer |
| PKW | Personenkraftwagen |
| PMeV | Bundesverband Professioneller Mobilfunk e.V. |

| | |
|---|---|
| POCSAG | Post Office Code Standard Advisory Group |
| PoLP | Principle of Least Priviledge |
| QM | Qualitätsmanagement |
| QSIG | Q-Interface Signalling Protocol |
| RAS | Rauchansaugsystem |
| RSA | Rivest – Shamir – Adleman |
| RTP | Real Time Protocol |
| RUP | Rational Unified Process |
| SAFe | Scaled Agile Framework |
| SAN | Storage Area Network |
| SAST | Static Application Security Testing |
| SBC | Session Border Controller |
| SCK | Static Cipher Key |
| SDLC | Software Development Life Cycle |
| SEL | Standard Elektrik Lorenz |
| SiKa | Sicherheitskarte |
| SIM | Subscriber Identity Module |
| SIP | Session Initiation Protocol |
| SPS | Speicherprogrammierbare Steuerung |
| SSL | Secure Sockets Layer |
| SÜG | Sicherheitsüberprüfungsgesetz |
| TCP | Transmission Control Protocol |
| TCS | TETRA Connectivity Server |
| TDD | Test Driven Development |
| TEA | TETRA Encryption Algorithm |
| TETRA | Terrestrial Trunked Radio |
| THW | Bundesanstalt Technisches Hilfswerk |
| TK | Telekommunikation |
| TLS | Transport Layer Security |
| TR | Technische Richtlinie |
| TV | Television (Fernsehen) |

| | |
|---|---|
| UDP | User Datagram Protocol |
| UGM | Universelles Gefahrenmeldesystem |
| UN | United Nations (Vereinte Nationen) |
| URL | Uniform Resource Locator |
| US | United States (Vereinigte Staaten) |
| VAS | Vermittlungs- und Abfragesystem |
| VDE | Verband der Elektrotechnik, Elektronik und Informationstechnik |
| VoIP | Voice over IP |
| vpS | vorbeugender personeller Sabotageschutz |
| WAN | Wide Area Network |
| *x* | Klartext-Nachricht (Original) |
| *x‘* | Klartext-Nachricht (verändert) |
| XSS | Cross-Site-Scripting |
| *y* | verschlüsselte Nachricht (Original) |
| *y‘* | verschlüsselte Nachricht (verändert) |
| 3DES | Triple Data Encryption Standard |

# Abbildungsverzeichnis

# Tabellenverzeichnis

# Literaturverzeichnis

**[AGB24]**
Arbeitsgemeinschaft der Leiter der Berufsfeuerwehren (AGBF), 2024
www.agbf.de, abgerufen am 18.05.2024

**[APT17]**
Adelmeyer, M., Petrick, C., Teuteberg, F., 2017
IT-Risikomanagement von Cloud-Services in Kritischen Infrastrukturen,
1. Auflage, Springer-Verlag, Berlin, Heidelberg, New York

**[AS22]**
Ahrens, S., Schmidtpott, H., 2022
Mit dem Notruf wird der Standort des Anrufers an uns übermittelt
www.spiegel.de/panorama/notrufe-wie-handys-automatisch-geortet-werden-und-warum-man-trotzdem-sagen-soll-wo-man-ist-a-887f18db
(abgerufen am 28.03.2022)

**[Alp94]**
Alper, M., 1994
Professionelle Softwaretests – Praxis der Qualitätsoptimierung kommerzieller Software, 1. Auflage, Vieweg-Verlag, Wiesbaden

**[AO16]**
Ammann, P., Offutt, J., 2016
Introduction to Software Testing, 2. Auflage, Cambridge University Press, Cambridge

**[App11]**
Appel, B., 2011
Grundlagen der Leitstellenplanung, 1. Auflage, Steinbeis-Edition, Stuttgart

**[Bal04]**
Balzert, H., 2004
Lehrbuch Grundlagen der Informatik, 1. Auflage, Springer-Verlag, Berlin, Heidelberg, New York

**[Ban23]**
Bandlow, S., 2023
Integrierte Regionalleitstelle
in: Hackstein, A., Sudowe, H. (Hrsg.): Handbuch Leitstelle – Strukturen, Prozesse, Innovationen, 3. Auflage, SK-Verlag, Edewecht, pp. 39 – 42

**[Bau17]**
Baumgartl, B., 2017
Upgrade ISO 9001:2015 im Rettungsdienst – Handlungsanleitung für Führungskräfte und QM-Verantwortliche, 1. Auflage SK-Verlag, Edewecht

**[BBKS15]**
Bengel, B., Baun, C. Kunze, M., Stucky, K.-U., 2015
Masterkurs Parallele und Verteilte Systeme - Grundlagen und Programmierung von Multicore-Prozessoren, Multiprozessoren, Cluster, Grid und Cloud,
2. Auflage, Springer-Verlag, Berlin, Heidelberg, New York

**[BMK15]**
Bath, G., McKay, J., 2015
Praxiswissen Softwaretest - Test Analyst und Technical Test Analyst, 1. Auflage,
Dpunkt-Verlag, Heidelberg

**[Bee17]**
Beer, K., 2017
Nach WannaCry-Attacke: Dobrindt für schärferes IT-Sicherheitsgesetz
www.heise.de/newsticker/meldung/Nach-WannaCry-Attacke-Dobrindt-fuer-schaerferes-IT-Sicherheitsgesetz-3713755.html
(abgerufen am 06.11.2023)

**[Bel18]**
Belmont, J.-M., 2018
Hands-On Continuous Integration and Delivery, 1. Auflage,
Packt Verlag, Birmingham

**[BF01]**
Beck, K., Fowler, M., 2001
Extreme Programming planen, 1. Auflage, Addison Wesley Verlag, Bonn

**[BH23]**
Bandlow, S., Hackstein, A., 2023
Kooperative Regionalleitstelle
in: Hackstein, A., Sudowe, H. (Hrsg.): Handbuch Leitstelle – Strukturen, Prozesse, Innovationen, 3. Auflage, SK-Verlag, Edewecht, pp. 43 – 45

**[BKP17]**
Baumgartner, M., Klonk, M., Pichler, H., Seidl, R., Tanczos, S., 2017
Agile Testing – Der agile Weg zur Qualität, 2. Auflage, Carl Hanser Verlag,
Leipzig

**[BMI09]**
Bundesministerium des Innern, 2009
Nationale Strategie zum Schutz Kritischer Infrastrukturen (KRITIS-Strategie), Berlin

**[BNA18]**
Bundesnetzagentur für Elektrizität, Gas, Telekommunikation, Post (BNetzA), 2018, Technische Richtlinie Notrufverbindungen, Ausgabe 2.0, Mainz

**[BNS10]**
Beutelspacher, A., Neumann, H., Schwarzpaul, T., 2010
Kryptografie in Theorie und Praxis – Mathematische Grundlagen für Internetsicherheit, Mobilfunk und elektronisches Geld, 2. Auflage, Springer-Verlag, Berlin, Heidelberg, New York

**[Boe88]**
Boehm, B.W., 1988
A Spiral Model of Software Development and Enhancement,
in: Computer, May 1988, IEEE Computer Society, Washington D.C, pp. 61 – 72

**[Bok23]**
Bokelmann, J., 2023
Leitstellen der Polizei
in: Hackstein, A., Sudowe, H. (Hrsg.): Handbuch Leitstelle – Strukturen, Prozesse, Innovationen, 3. Auflage, SK-Verlag, Edewecht, pp. 54 – 64

**[BR93]**
Bellare, M., Rogaway, P., 1993
Rand Oracles are practical - A paradigm for designing efficient protocols
in: ACM Conference on computer and communication Security, pp. 62 – 73

**[BRS95]**
Becker, J., Rosemann, M., Schütte, R., 1995
Grundsätze ordnungsgemäßer Modellierung
in: Wirtschaftsinformatik Nr. 37/1995, Springer-Verlag, Berlin, Heidelberg, New York, pp. 435 – 445

**[BS23]**
Buchmann, R., Sinnwell, T., 2023
Leitstelle down – KI-Angriff auf die Lebensretter
Vortrag beim Leitstellen-Summit, Messe PMRexpo Köln, 30.11.2023

**[BSI15]**
Bundesamt für Sicherheit in der Informationstechnik (BSI), 2015
Die Lage der IT-Sicherheit in Deutschland 2015. Bonn

**[BSI16]**
Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz (BSI-Kritisverordnung - KritisV) vom 6. September 2021 (BGBl. I S. 4163)

**[BSI21]**
Gesetz über das Bundesamt für Sicherheit in der Informationstechnik (BSI-Gesetz) vom 23. Juni 2021 (BGBl. I S. 1982)

**[BSI100-4]**
BSI-Standard 100-4 Notfallmanagement, Bundesamt für Sicherheit in der Informationstechnik (BSI), Version 1.0, 2008, Bonn

**[BSI200-4]**
BSI-Standard 200-4 Business Continuity Management, Bundesamt für Sicherheit in der Informationstechnik (BSI), 2023, Bonn

**[BSW15]**
Beutelspacher, A., Schwenk, J., Wolfenstetter, K.-D., 2015
Moderne Verfahren der Kryptographie – Von RSA zu Zero-Knowledge, 1. Auflage, Springer-Verlag, Berlin, Heidelberg, New York

**[Buc16]**
Buchmann, J., 2016
Einführung in die Kryptographie, 6. Auflage, Springer-Verlag, Berlin, Heidelberg, New York

**[Bur03]**
Burnstein, I., 2003
Practical Software Testing, 1. Auflage, Springer-Verlag, Berlin, Heidelberg, New York

**[CDKB12]**
Coulouris, G., Dollimore, J., Kindberg, T., Blair, G., 2012
Distributed Systems - Concepts and Design, 3. Auflage, Pearson Verlag, Harlow/UK

**[Chr20]**
Christiansen, J., 2020
Leitstellen als Bestandteil der KRITIS – Eine Betrachtung in Hinblick auf die Corona-Pandemie, in: BOS Leitstelle aktuell, August 2020, SK-Verlag, Edewecht, pp. 11 – 15

**[Chr23]**
Christiansen, J., 2023
Leitstelle als Bestandteil der kritischen Infrastruktur
in: Hackstein, A., Sudowe, H. (Hrsg.): Handbuch Leitstelle – Strukturen, Prozesse, Innovationen, 3. Auflage, SK-Verlag, Edewecht, pp. 491 – 497

**[Cht23]**
Christophersen, L., 2023
Notrufsysteme für Hör-, Sprach- und/oder Sehbehinderte – Der barrierefreie Notruf mit Barrieren?
in: Hackstein, A., Sudowe, H. (Hrsg.): Handbuch Leitstelle – Strukturen, Prozesse, Innovationen, 3. Auflage, SK-Verlag, Edewecht, pp. 515 – 519

**[Cla23]**
Clausen, V., 2023
Notrufabfragesysteme
in: Hackstein, A., Sudowe, H. (Hrsg.): Handbuch Leitstelle – Strukturen, Prozesse, Innovationen, 3. Auflage, SK-Verlag, Edewecht, pp. 511 – 514

**[CW07]**
Chess, B., West, J., 2007
Secure Programming with Static Analysis, 1. Auflage, Addison Wesley Verlag, Boston

**[DBT21]**
Deutscher Bundestag, 19. Wahlperiode, Drucksache 19/27556 vom 15.03.2021
Antwort der Bundesregierung auf die Kleine Anfrage mehrerer Abgeordneter der FDP-Fraktion betreffend „Bundesweite Standards für kommunale Einsatzleitstellen als Teil der Kritischen Infrastruktur“

**[Dij74]**
Dijkstra, W.E., 1974
Self-stabilizing systems in Spite of Distrubted Control,
Communications of the Association für Computer Machinery,
Nr. 11/1974, pp. 643 – 645

**[DIKV19]**
Dotsenko, S., Illiashenko, O., Kamenskyi, S., Kharchenki, V., 2019
Integrated Security Management System for Enterprises in Industry 4.0
in: Information &Security, Nr. 3/2019, Verlag Procon Ltd., pp. 294 – 304

**[DKS19]**
Dräther, R., Koschek, H., Sahling, C., 2019
Scrum kurz und gut, 2. Auflage, O'Reilly Verlag, Heidelberg, pp. 17, 24 – 25

**[DKV12]**
Dacier, M., Kargl, F., Valdes, A., 2012
Securing Critical Infrastructures from Targeted Attacks
Dagstugl Reports, Schloss Dagstuhl, Leibniz-Zentrum für Informatik, pp. 49 – 62

**[DL22]**
Dittrich, T., Lippert, H.-D., 2022
Die Integrierte Leitstelle – ein einheitlicher und vor allem sicherer Meldekopf für Einrichtungen der Daseinsfürsorge
in: Medizinrecht, Juli 2022, pp. 565 – 568

**[DRP13]**
Dustin, E., Rashka, J., Paul, J., 2013
Software automatisch testen, 1. Auflage, Springer-Verlag, Berlin, Heidelberg, New York

**[DSG18]**
Datenschutz-Grundverordnung (DS-GVO), 2018
vom 23.5.2018, S. 2 (Amtsblatt L 127)

**[DT19]**
Deutsche Telekom AG (DTAG), 2019
Infotag Leitstellentechnik, Präsentation; 06.11.2019, Frankfurt am Main

**[Eb21]**
Ebel, N., 2021
Basiswissen ITIL 4
1. Auflage, Dpunkt Verlag, Heidelberg

**[Eel14]**
Eeles, P., 2014
in: Barbar, M.A., Brown, A.W., Mistrik, I.: Agile Software Architecture,
1. Auflage, Elsevier Verlag

**[Els13]**
Elsberg, M., 2013
Blackout – Morgen ist es zu spät, 7. Auflage, Blanvalet Verlag, München

**[FELB07]**
Faul, F., Erdfelder, E., Lang, A.G., Buchner, A., 2007
G*Power 3: A flexible statistical power analysis program for the social, behavioral and biomedical sciences.
in: Bevavior Research Methods, 39/2007, pp. 175 – 191

**[FHKM09]**
Friedrich, J., Hammerschall, U., Kuhrmann, M., Sihling, M., 2009
Das V-Modell XT - Für Projektleiter und QS-Verantwortliche kompakt und übersichtlich, 2. Auflage, Springer-Verlag, Berlin, Heidelberg, New York

**[FK04]**
Forbrig, P., Kerner, I., 2004
Lehr- und Übungsbuch Softwareentwicklung, 1. Auflage, Carl Hanser Verlag, Leipzig

**[FVL23]**
Fachverband Leitstellen e.V. (FVLST), 2023
Die Leitstellen der Behörden und Organisation mit Sicherheitsaufgaben als Bestandteil der Kritischen Infrastruktur, Version 3.6, Lemgo

**[Frh22]**
Fraunhofer-Gesellschaft, 2022
Forschung für den Schutz Kritischer Infrastrukturen
https://www.fraunhofer.de/de/forschung/aktuelles-aus-der-forschung/archiv/forschung-fuer-den-schutz-kritischer-infrastrukturen.html
(abgerufen am 28.11.2022)

**[GBBK09]**
Grechenig., T., Bernhart, M., Breiteneder, R., Kappel, K., 2009
Softwaretechnik – Mit Fallbeispielen aus realen Entwicklungsprojekten, 1. Auflage, Pearson Verlag, München

**[GM18]**
Gutierrez Astilleros, P., Mertka, W., 2018
Cybersecurity – Guidelines and Best Practices for Emergency Services
European Emergency Number Association (EENA), Brüssel

**[Gei97]**
Geisel, H.-O., 1997
Feuerwehr-Sprechfunk, 6. Auflage, W. Kohlhammer Verlag, Stuttgart

**[Gei03]**
Geisel, H.-O., 2003
Fernmeldetechnik
in: Rönnfeldt, J. (Hrsg.): Feuerwehr-Handbuch der Organisation, Technik und Ausbildung, 1. Auflage, W. Kohlhammer Verlag, Stuttgart, pp. 412 – 429

**[Gei16]**
Geirhos., M., 2016
IT-Projektmanagement – Was wirklich funktioniert und was nicht, 2. Auflage, Rheinwerk Computing Verlag, Bonn

**[Gol12]**
Goll, J., 2012
Methoden des Software Engineering – Funktions-, daten-, objekt- und aspektorientiert entwickeln, 1. Auflage, Springer Verlag, Berlin, Heidelberg, New York

**[Gor14]**
Gorton, I., 2014
Essential Software Architecture, 2. Auflage, Springer Verlag, Berlin, Heidelberg, New York

**[Gor22]**
Gorton, I., 2022
Foundations of Scalable Systems – Designing Distributed Architecture, 1. Auflage, O'Reilly Verlag, Sebastopol/CA

**[Glo16]**
Gloger, B., 2016
Scrum – Produkte schnell und zuverlässig entwickeln, 5. Auflage, Carl Hanser Verlag, Leipzig

**[GMD23]**
Groß, H., Marikar, A., Dohmeier, F., 2023
KI in der Leitstelle: Herausforderungen, Innovationen und Anwendung
Vortrag beim Leitstellen-Summit, Messe PMRexpo Köln, 30.11.2023

**[GRH18]**
Gurschler, T., Rieb, A., Hofmeier, M., 2018
Zentrale Leitstelle Ostthüringen: IT-Sicherheit in einer Leitstelle
in: Lechner, U., Dännart, S., Rieb, A., Rudel, S. (Hrsg.): Case Kritis – Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen, 1. Auflage, Logos Verlag, Berlin, pp. 151 – 167

**[Gru03]**
Grupp, B., 2003
Das IT-Pflichtenheft zur optimalen Softwarebeschaffung, 2. Auflage,
mitp Verlag, Frechen

**[GSP23]**
IT-Grundschutzprofil für Leitstellen, Version 2.0, 2023, herausgegeben vom Bundesamt für Sicherheit in der Informationstechnik mit Patenschaft des Fachverbandes Leitstellen e.V.

**[Har18]**
Harich, T., 2018
IT-Sicherheitsmanagement – Praxiswissen für IT Security Manager, 2. Auflage,
mitp Verlag, Frechen

**[HB23]**
Hurst, J., Benz, A., 2023
Leitstelle der Werksicherheit „Mercedes-Benz-Werk Rastatt“
in: Hackstein, A., Sudowe, H. (Hrsg.): Handbuch Leitstelle – Strukturen, Prozesse, Innovationen, 3. Auflage, SK-Verlag, Edewecht, pp. 73 – 75

**[HE20]**
Land Hessen, 19.10.2020, zuletzt aktualisiert am 21.03.2024
Bereiche Kritischer Infrastrukturen (KRITIS) - Hessische Übersicht über Sektoren, Branchen, kritische Dienstleistungen, kritische Prozesse und Beispiele für Anlagen / Einrichtungen sowie Zuständigkeiten in der Landesverwaltung

**[Her18]**
Herczeg, M., 2018
Software-Ergonomie – Theorien, Modelle und Kriterien für gebrauchstaugliche interaktive Computersysteme, 4. Auflage, De Gruyter Verlag, Oldenburg

**[HHM09]**
Hindel, B., Hörmann, K., Müller, M., Schmied, J., 2009
Basiswissen Software-Projektmanagement – Aus- und Weiterbildung zum Certified Professional for Project Management nach iSQI-Standard, 3. Auflage,
Dpunkt Verlag, Heidelberg

**[HM10]**
Hartl, P., Merzbach, G., 2010
Digitalfunk, 2. Auflage, W. Kohlhammer Verlag, Stuttgart

**[HN02]**
Hudec, M., Neumann, C., 2002
Stichproben & Umfragen – Grundlagen der Stichprobenziehung
Institut für Statistik, Universität Wien, pp. 23 - 32

**[HL93]**
Hügle, T., Lehmann, R., 1993
Digitale Alarmierung für den BOS-Bereich, 2. Auflage, Swissphone GmbH, Gundelfingen

**[Hus04]**
Huseby, S., 2004
Sicherheitsrisiko Web-Anwendung – Wie Web-Programmierer Sicherheitslücken erkennen und vermeiden, 1. Auflage, Dpunkt Verlag, Heidelberg

**[Jan21]**
Janca, T., 2021
Alice & Bob learn Application Security, 1. Auflage Wiley Verlag, Hoboken, pp. 121 – 151

**[IN23]**
Info GmbH Markt- und Meinungsforschung, 2023
Untersuchung zur Wirksamkeit der IT-Sicherheitsgesetze unter Betreibern Kritischer Infrastrukturen, im Auftrag des BSI, Berlin

**[Io24]**
Ioannidis, P., 2024
BCMS-Umsetzungsleitfaden zur Stärkung der Resilienz und zum Aufbau eines Notfallmanagements für integrierte Leitstellen
Bachelorarbeit, TH Köln

**[ITS15]**
Gesetz zur Erhöhung der Sicherheit in informationstechnischen Systemen (IT-Sicherheitsgesetz) vom 17. Juli 2015 (BGBl. I S. 1324)

**[KGM16]**
Karutz, H., Geier, W., Mitschke, T., 2016
Bevölkerungsschutz – Notfallvorsorge und Krisenmanagement in Theorie und Praxis, 1. Auflage, Springer-Verlag, Berlin, Heidelberg, New York

**[Kas99]**
Kasperczyk, S., 1999
Einsatzleitsysteme
in: Vergeiner, G. (Hrsg.): Leitstellen im Rettungsdienst – Aufgaben, Organisation, Technik, 1. Auflage, SK-Verlag, Edewecht, pp. 169 – 172

**[KB18]**
Kipker, D.-J., Buchner, B., 2018
Gesetzliche Anforderungen an die IT-Sicherheit in Deutschland und Europa
in: Lechner, U., Dännart, S., Rieb, A., Rudel, S. (Hrsg.): Case Kritis – Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen. 1. Auflage, Logos Verlag, Berlin, pp. 22 – 26

**[Ker15]**
Kersken, S., 2015
IT-Handbuch für Fachinformatiker, 7. Auflage, Rheinwerk Computing Verlag, Bonn

**[Ker95]**
Kersten, H., 1995
Sicherheit in der Informationstechnik, 2. Auflage Oldenbourg Verlag, München

**[KKB18]**
Kastens, U., Kleine-Büning, H., 2018
Modellierung – Grundlagen und formale Methoden, 4. Auflage, Carl Hanser Verlag, Leipzig

**[KKRS19]**
Kersten, H., Klett, G., Reuter, J., Schröder, K.-W., 2019
IT-Sicherheitsmanagement nach der neuen ISO 27001, 2. Auflage, Springer-Verlag, Berlin, Heidelberg, New York

**[KLSB22]**
Kerger, S., Löwen, D., Stecken, R., Boos, B., 2022
IT-Sicherheitsniveau kritischer Infrastruktur unterhalb der KritisV
in: WasserWirtschaft, 11/2022, pp. 42 – 46

**[Kof22]**
Kofler, M. et. al., 2022
Hacking & Security – Das umfassende Handbuch, 3. Auflage, Rheinwerk Computing Verlag, Bonn

**[Kra23]**
Kramser, T., 2023
Ergonomie in Leitstellen
in: Hackstein, A., Sudowe, H. (Hrsg.): Handbuch Leitstelle – Strukturen, Prozesse, Innovationen, 3. Auflage, SK-Verlag, Edewecht, pp. 97 – 106

**[Kre16]**
Kremp, M., 2016
Telekom-Hack hätte viel schlimmer kommen können
www.spiegel.de/netzwelt/web/deutsche-telekom-stoerung-war-misslungener-bot-net-angriff-a-1123544.html
(abgerufen am 28.12.2021)

**[Kru95]**
Kruchten, P., 1995
Architectural Blueprints – The „4+1“ View Model of Software Architecture
in: IEEE Software, No. 12 (6), November 1995, pp. 42 – 50

**[Lan13]**
Langner, R., 2013
To Kill a Centrifuge - A technical analysis of What Stuxnet’s Creators Tried to Achieve. Arlington, Hamburg, München, pp. 7 – 12

**[Lan24]**
Lange, C., 2024
Beurteilungswerte im ABC-Einsatz
in: Das Feuerwehr-Lehrbuch – Grundlagen, Technik, Einsatz, 8. Auflage, W. Kohlhammer Verlag, Stuttgart, pp. 1063 – 1064

**[LC23]**
Lang, V., Christiansen, J., 2023
Digitalfunk und Leitstelle
in: Hackstein, A., Sudowe, H. (Hrsg.): Handbuch Leitstelle – Strukturen, Prozesse, Innovationen, 3. Auflage, SK-Verlag, Edewecht, pp. 503 – 510

**[Lep18]**
Leps, O., 2018
Hybride Testumgebungen für Kritische Infrastrukturen, 1. Auflage, Springer-Verlag, Berlin, Heidelberg, New York

**[Lin08]**
Linde, C., 2008
Aufbau und Technik des digitalen BOS-Funks, 1. Auflage, Franzis Verlag, Poing

**[Lin23]**
Lindner, K., 2023
GPS-gestützte Rettungsmitteldisposition
in: Hackstein, A., Sudowe, H. (Hrsg.): Handbuch Leitstelle – Strukturen, Prozesse, Innovationen, 3. Auflage, SK-Verlag, Edewecht, pp. 571 – 575

**[LKM12]**
Lang, M., Kammerer, S., Amberg, M., 2012
Perfektes IT-Projektmanagement – Best Practices für Ihren Projekterfolg, 1. Auflage, Symposion Publishing, Düsseldorf

**[LL23]**
Ludewig, J., Lichter, H., 2023
Software Engineering – Grundlagen, Menschen, Prozesse, Techniken, 4. Auflage, Dpunkt Verlag, Heidelberg

**[Loc06]**
Lockhart, A., 2006
Network Security Hacks – 100 Industrial-Strength Tips & Tools, 1. Auflage, O'Reilly Verlag, Sebastopol/CA

**[Mag20]**
Maggale, St. A., 2020
IT-Sicherheit für Kritische Infrastrukturen
Masterarbeit, Campus 02 Fachhochschule der Wirtschaft, Graz

**[Mah22]**
Mahn, J., 2022
Sabotage bei der Bahn: Viele vertrauliche Infos sind offen zugänglich
https://www.heise.de/news/Sabotage-bei-der-Bahn-Viele-vertrauliche-Infos-sind-offen-zugaenglich-7307277.html
(abgerufen am 18.10.2023)

**[Man09]**
Mandl, P., 2009
Masterkurs Verteilte betriebliche Informationssysteme – Prinzipien, Architekturen und Technologien, 1. Auflage, Vieweg + Teubner Fachverlage, Wiesbaden

**[Mar06]**
Marten, M., 2006
BOS-Funk, Band 1 – Grundlagen, Geräte, Betriebstechnik, 5. Auflage, Siebel-Verlag, Baden-Baden

**[Mel99]**
Melioumis, M., 1999
Kommunikationstechnik
in: Vergeiner, G. (Hrsg.): Leitstellen im Rettungsdienst – Aufgaben, Organisation, Technik, 1. Auflage, SK-Verlag, Edewecht, pp. 235 – 259

**[Mey14]**
Meyer, B., 2014
Agile! – The Good, the Hype and the Ugly, 1. Auflage, Springer-Verlag, Berlin, Heidelberg, New York

**[Mer99]**
Meron, G., 1999
Die Leitstelle – ein medizinischer Dienstleistungsbetrieb
in: Vergeiner, G. (Hrsg.): Leitstellen im Rettungsdienst – Aufgaben, Organisation, Technik
1. Auflage, SK-Verlag, Edewecht, pp. 17 – 36

**[MK23]**
Mommsen, B., Kahl, T., 2023
Integration in die Leitstellenumgebung (Schnittstellen)
in: Hackstein, A., Sudowe, H. (Hrsg.): Handbuch Leitstelle – Strukturen, Prozesse, Innovationen, 3. Auflage, SK-Verlag, Edewecht, pp. 554 – 558

**[NIS-2]**
Richtline über Maßnahmen für ein gemeinsames Cybersicherheitsniveau in der gesamten Union (NIS2-Richtlinie)
https://digital-strategy.ec.europa.eu/de/faqs/directive-measures-high-common-level-cybersecurity-across-union-nis2-directive-faqs
(abgerufen am 10.06.2024)

**[NL98]**
Necula, G.C., Lee, P., 1998
Safe, untrusted agents using Proof-Carrying-Code
in: Vigna, G. (Hrsg.): Lecture Notes in Computer Science, Vol. 1419, Springer-Verlag, Berlin, Heidelberg, New York

**[PBG11]**
Posch, T., Birken, K., Gerdom, M., 2011
Basiswissen Softwarearchitektur – Verstehen, entwerfen, wiederverwenden, 3. Auflage, Dpunkt Verlag, Heidelberg

**[PP04]**
Pomberger, G., Pree, W., 2004
Software Engineering – Architektur-Design und Prozessoptimierung, 3. Auflage, Carl Hanser Verlag, Leipzig

**[PP10]**
Paar, C., Pelzl, J., 2010
Understanding Cryptography, 1. Auflage, Springer-Verlag, Berlin, Heidelberg, New York

**[PR17]**
Pfetzing, K., Rohde, A., 2017
Ganzheitliches Projektmanagement, Schriftenreihe ibo, Verlag Dr. Götz, Gießen

**[Pic13]**
Pichler, R., 2013
Agiles Projektmanagement mit Scrum – Erfolgreich als Product Owner arbeiten, 1. Auflage 2013, Dpunkt Verlag, Heidelberg

**[PM16]**
Bundesverband Professioneller Mobilfunk e.V. (PMeV), 2016
Hinweise und Handreichungen zur Schnittstelle „Digitalfunkstecker“ (DF-Stecker) und ihrer Verwendung, Version 1.0.1, Berlin

**[Poh02]**
Pohlmann, N., 2002
Firewall-Systeme, 5. Auflage, mitp Verlag, Frechen

**[Poh18]**
Pohlmann, N., 2018
Cyber-Sicherheit – Das Lehrbuch für Konzepte, Prinzipien, Mechanismen, Architekturen und Eigenschaften von Cyber-Sicherheitssystemen in der Digitalisierung, 1. Auflage, Springer-Verlag, Berlin, Heidelberg, New York

**[Rau23]**
Raudszus, F., 2023
Anforderungen an einen Technikraum
in: Hackstein, A., Sudowe, H. (Hrsg.): Handbuch Leitstelle – Strukturen, Prozesse, Innovationen, 3. Auflage, SK-Verlag, Edewecht, pp. 542 - 548

**[Rei21]**
Reischuk, R., 2021
Kommunikations-Sicherheit / Communication Security
Vorlesungsskript zum Modul CS4701, Universität zu Lübeck, pp. 23 – 26

**[RH08]**
Reussner, R., Hasselbring, W. (Hrsg.), 2008
Handbuch der Software-Architektur, 2. Auflage, Dpunkt Verlag, Heidelberg

**[RL18]**
Rieb, A., Lechner, U., 2018
Bedrohungen der IT-Sicherheit Kritischer Infrastrukturen
in: Lechner, U., Dännart, S., Rieb, A., Rudel, S. (Hrsg.): Case Kritis – Fallstudien zur IT-Sicherheit in Kritischen Infrastrukturen. 1. Auflage, Logos Verlag, Berlin, pp. 31 – 35

**[Ros79]**
Rosemeier, F.-W., 1979
Handbuch über den UKW-Sprechfunk bei den Sicherheitsdiensten, 2. Auflage, Carl Heymanns Verlag, Köln, Berlin, Bonn, München

**[RS23]**
Rehbohm, T., Sandkuhl, L., 2023
Referenzarchitektur Cybersicherheit im Föderalsystem Deutschlands
in: HMD Praxis der Wirtschaftsinformatik
https://link.springer.com/article/10.1365/s40702-023-01014-7
(abgerufen am 09.01.2024)

**[Rüh10]**
Rühl, U., 2010
Leitstellen der Polizei
in: Hackstein, A., Sudowe, H. (Hrsg.): Handbuch Leitstelle – Strukturen, Prozesse, Innovationen, 1. Auflage, SK-Verlag, Edewecht, pp. 29 – 31

**[Sche17]**
Scherschel, F.A., 2017
Sichere Passwörter: Viele der herkömmlichen Sicherheitsregeln bringen nichts
https://www.heise.de/news/Sichere-Passwoerter-Viele-der-herkoemmlichen-Sicherheitsregeln-bringen-nichts-3797935.html
(abgerufen am 24.06.2024)

**[Scheu23]**
Scheuschner, D., 2023
Anforderungen an die Software
in: Hackstein, A., Sudowe, H. (Hrsg.): Handbuch Leitstelle – Strukturen, Prozesse, Innovationen, 3. Auflage, SK-Verlag, Edewecht, pp. 523 – 533

**[Schm20]**
Schmidtpott, H., 2020
Erstellung eines IT-Grundschutzprofils für Rettungsleitstellen
Masterarbeit, Fernuni Hagen

**[Schr10]**
Schreiber, J., 2010
Leitstellen der Werkfeuerwehr
in: Hackstein, A., Sudowe, H. (Hrsg.): Handbuch Leitstelle – Strukturen, Prozesse, Innovationen, 1. Auflage, SK-Verlag, Edewecht, pp. 31 – 33

**[Schw14]**
Schwenk, J., 2014
Sicherheit und Kryptographie im Internet – Theorie und Praxis, 4. Auflage, Springer-Verlag, Berlin, Heidelberg, New York

**[SH18]**
Landesverordnung zur Durchführung des Schleswig-Holsteinischen Rettungsdienstgesetzes (SHRDG-DVO) vom 4. Dezember 2018, Kiel

**[Sie04]**
Siedersleben, J., 2004
Moderne Softwarearchitektur – Umsichtig planen, robust bauen mit Quasar, 1. Auflage, Dpunkt Verlag, Heidelberg

**[SL19]**
Spillner, A., Linz, T., 2019
Basiswissen Softwaretest – Aus- und Weiterbildung zum Certified Tester, 6. Auflage, Dpunkt Verlag, Heidelberg

**[SV20]**
Steenhoek, S., Voßschmidt, S., 2020
Klimawandel
in: Voßschmidt, S., Karsten, A. (Hrsg.): Resilienz und Kritische Infrastrukturen – Aufrechterhaltung von Versorgungsstrukturen im Krisenfall, 1. Auflage, W. Kohlhammer Verlag, Stuttgart, pp. 84 – 99

**[SVEH07]**
Stahl, T., Völter, M, Efftinge, S., Haase, A., 2007
Modellgetriebene Softwareentwicklung – Techniken, Engineering, Management, 2. Auflage, Dpunkt Verlag, Heidelberg

**[SB23]**
Strohbach, U.A., Behrens, S., 2023
IT-Sicherheit
in: Hackstein, A., Sudowe, H. (Hrsg.): Handbuch Leitstelle – Strukturen, Prozesse, Innovationen, 3. Auflage, SK-Verlag, Edewecht, pp. 549 – 553

**[SS12]**
Schill, A., Springer, Th., 2012
Verteilte Systeme, 2. Auflage, Springer-Verlag, Berlin, Heidelberg, New York

**[Sta20]**
Starke, G., 2020
Effektive Softwarearchitekturen – Ein praktischer Leitfaden, 9. Auflage, Carl Hanser Verlag, Leipzig

**[SW07]**
Schneider, U., Werner, D., 2007
Taschenbuch der Informatik, 6. Auflage, Carl Hanser Verlag, Leipzig

**[Sym17]**
Symantec, 2017
Triton – New Malware Threatens Industrial Safety Systems
www.symantec.com/blogs/threat-intelligence/triton-malware-ics
(abgerufen am 22.03.2023)

**[Tan08]**
Tanenbaum, A., van Stehen, M., 2008
Verteilte Systeme – Prinzipien und Paradigmen, 2. Auflage, Verlag Pearson Studium, München

**[TH19]**
Richtlinie zur Gewährung von Zuwendungen des Freistaats Thüringen für die Förderung von Investitionen der kommunalen Gebietskörperschaften zur Strukturoptimierung und Anpassung der Zentralen Leitstellen an den Stand der Technik (FörderRL Leitstellen), 2019, Erfurt

**[Tha19]**
Thaller, G.E., 2019
Software-Test, Verifikation und Validation, 3. Auflage, Heise Verlag, Hannover

**[Tho14]**
Thomas, K., 2014
Resilien-Tech – „Resilience-by-Design“: Strategie für die technologischen Zukunftsthemen, 1. Auflage, Utz-Verlag, München

**[TKR07]**
Teich, I., Kolbenschlag, W., Reiners, W., 2007
Der richtige Weg zur Softwareauswahl – Lastenheft, Pflichtenheft, Compliance, Kontrolle, 1. Auflage, Springer-Verlag, Berlin, Heidelberg, New York

**[TRC22]**
Trautmann, R., Reuter-Oppermann, M., Christiansen J., 2022
PSAP-G-ONE, Eine explorativ-deskriptive Studie über Leitstellen der nichtpolizeilichen Gefahrenabwehr in der Bundesrepublik Deutschland. Deutsche Gesellschaft für Rettungswissenschaften, Aachen

**[UNB06]**
Übereinkommen über die Rechte von Menschen mit Behinderungen (UN-Behindertenrechtskonvention), 2006, New York

**[Ver15]**
Unsere Anforderungen und Thesen zur Arbeit in Leitstellen, 2015
Vereinigte Dienstleistungsgewerkschaft (ver.di), Bundesfachgruppe Feuerwehr, Berlin

**[Wei08]**
Weiß, C., 2008
Basiswissen Medizinische Statistik, 4. Auflage, Springer-Verlag, Berlin, Heidelberg, New York

**[WR21]**
Wolf, H., Roock, S., 2021
Scrum verstehen und erfolgreich einsetzen, 3. Auflage, Dpunkt Verlag, Heidelberg

**[WRL05]**
Wolf, H., Roock, S., Lippert, M., 2005
eXtreme Programming – Eine Einführung mit Empfehlungen und Erfahrungen aus der Praxis, 2. Auflage, Dpunkt Verlag, Heidelberg

# Anhang - Datenerhebung

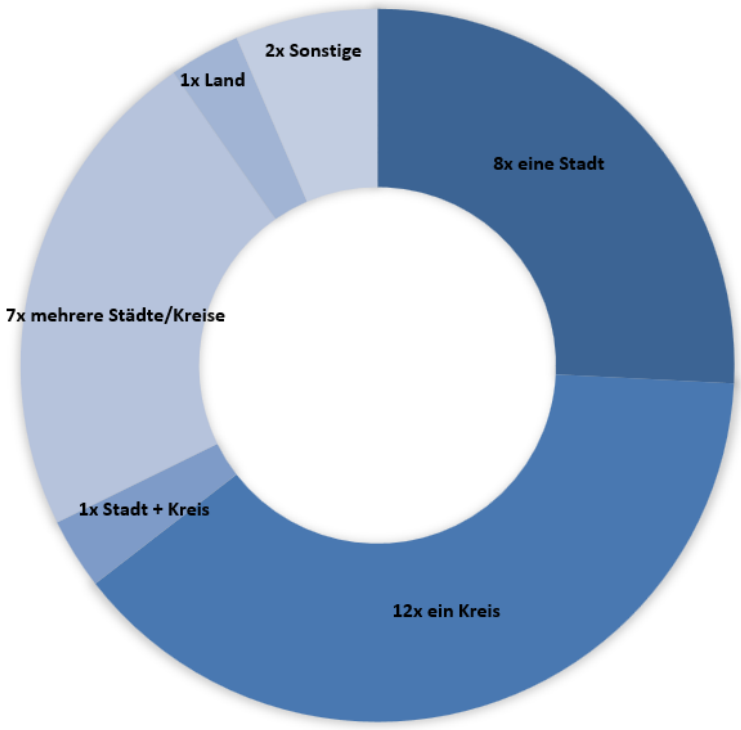
Die Fragestellungen des Erhebungsbogens sind jeweils nach der Überschrift aufgeführt. Der überwiegende Teil der Antwortmöglichkeiten bestand aus Ankreuzfeldern (Multiple-Choice), in einigen Fällen aus Freitextfeldern.

## A.1 Organisation

Frage: *Wie heißt Ihre Leitstelle (Kreis-, Stadt- bzw. Behördenbezeichnung)?*
Diese Angabe (Freitextantwort) diente rein der Erfassung der eingehenden Rückmeldungen. Rückmeldende Organisationen waren 15 kreisangehörige Leitstellen, neun Leitstellen von Berufsfeuerwehren sowie vier Kooperative Leitstellen (Integrierte Leitstellen für Brandschutz, Katastrophenschutz, Rettungsdienst und Polizei).

## A.2 Örtliche Zuständigkeit

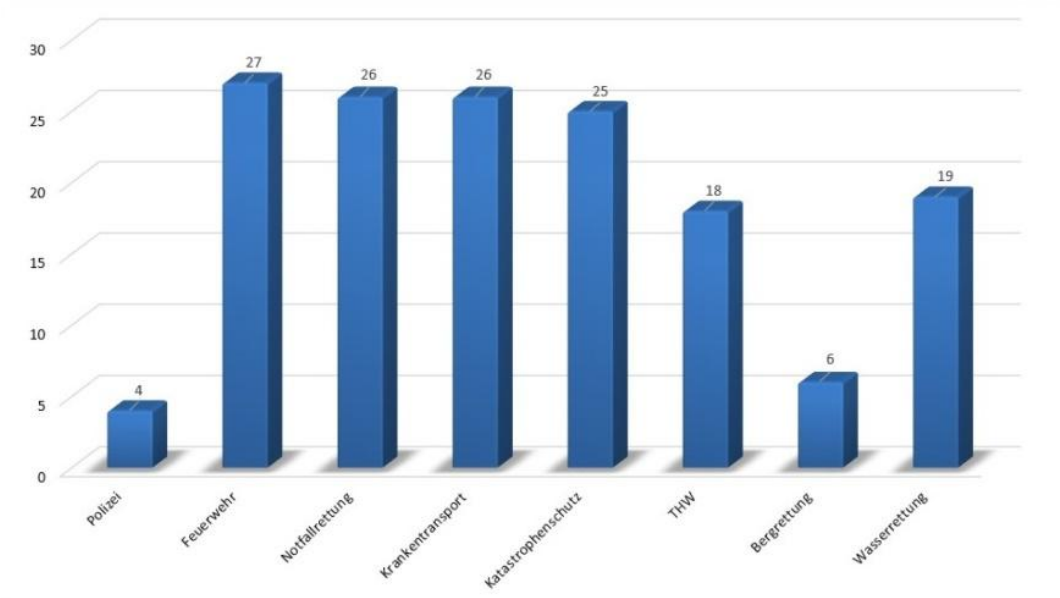
Frage: *Für welches Gebiet (geographisch / politisch) ist Ihre Leitstelle zuständig?*



Fast die Hälfte der Rückmeldungen (*n* = 12, entspricht 42,8 %) stammt aus Kreisleitstellen, die für einen Landkreis zuständig sind, hinzu kommen 7 Rückmeldungen (25 %) aus Regionalleitstellen, die für mehrere Landkreise zuständig sind. Aus kreisfreien Städten liegen acht Rückmeldungen (28,5 %) vor. Dies ergibt in Summe 67,8 % an kreiszuständigen Leitstellen.

## A.3 Organisatorische Zuständigkeit

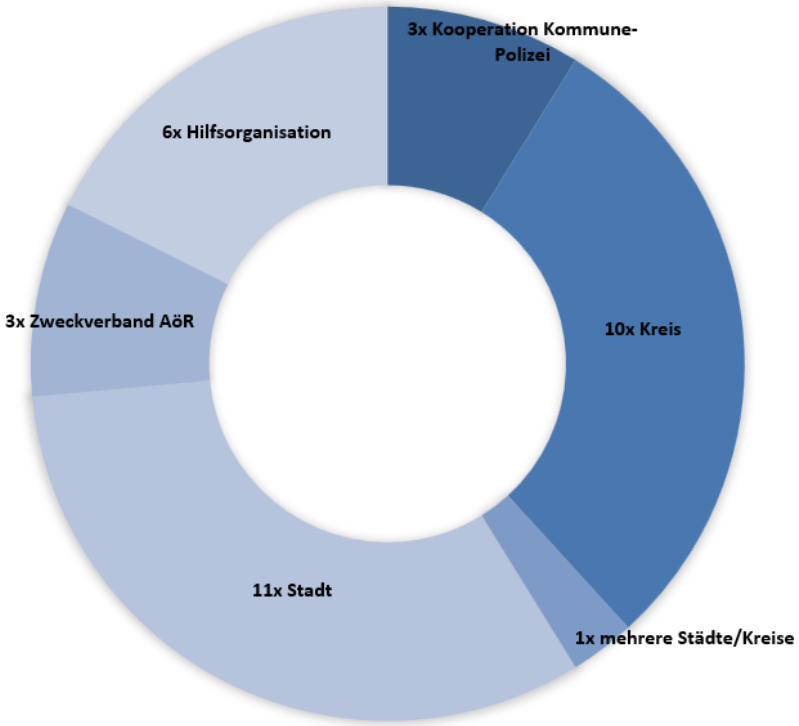
Frage: *Welche Behörden, Organisationen und Dienststellen werden von Ihrer Leitstelle geführt?* (Mehrfachantworten möglich)




Die Mehrzahl der Leitstellen deckt gleichermaßen die Bereiche Feuerwehr, Rettungsdienst, Krankentransport und Katastrophenschutz ab, hinzu kommen THW, Berg- und Wasserrettung, was dem Aufgabenspektrum Integrierter Leitstellen entspricht. Polizeiliche Zuständigkeit ist in vier Fällen gegeben (z.B. Kooperative Leitstellen), wobei hinsichtlich der Sicherheitsanforderungen an Leitstellen keine Unterscheidung erfolgt.

## A.4 Betreiber

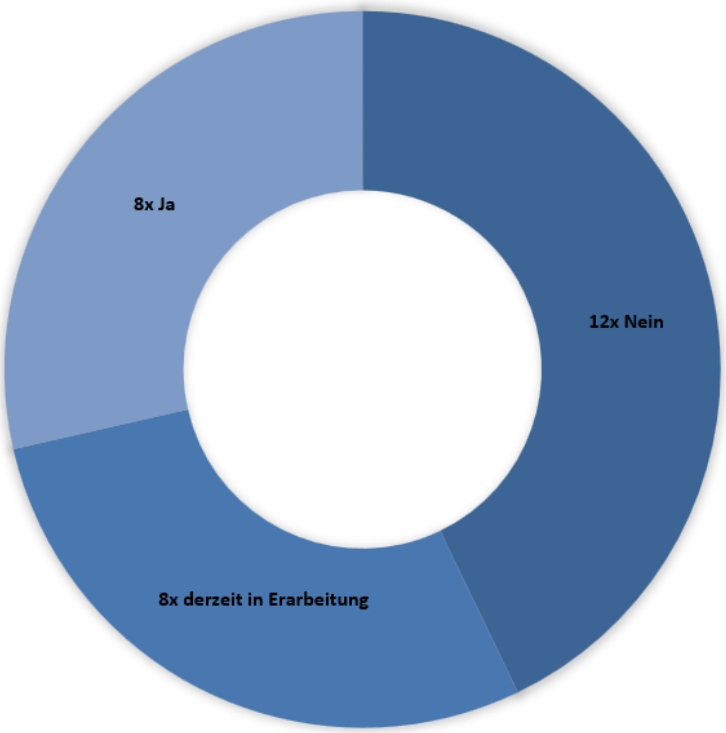
Frage: *Wer ist Betreiber der Leitstelle?*




Bei der Betreiberschaft stellt sich die Situation anders dar als bei der örtlichen Zuständigkeit (siehe A.2). Da als Betreiber nicht nur die kommunalen Gebietskörperschaften (Städte, Landkreise) in Frage kommen, sondern auch Hilfsorganisationen oder Kooperationen bzw. Zweckverbände mehrerer Beteiligter als Betreiberkonsortium existieren, verschieben sich an dieser Stelle die Verhältnisse aus Abschnitt A.2.

## A.5 Rechtliche Vorgaben

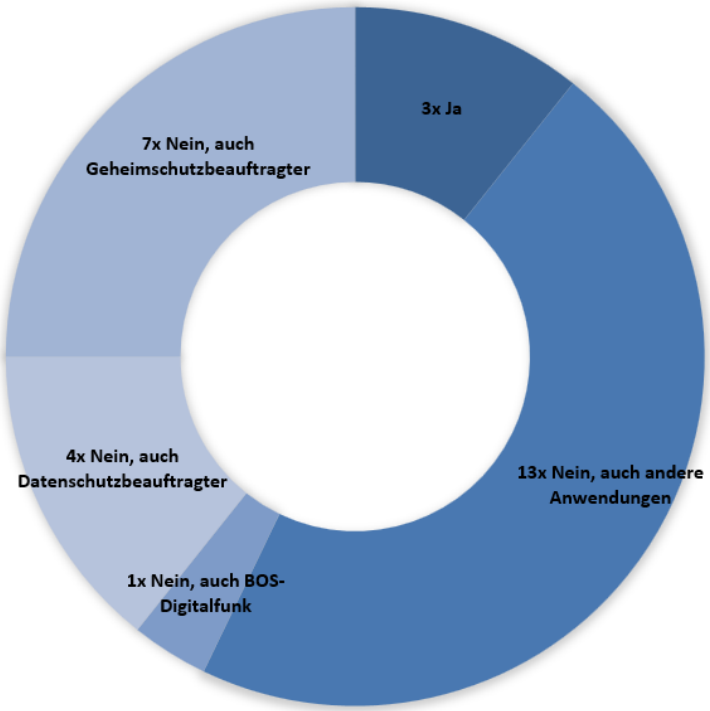
Frage: *Gibt es eine Vorgabe hinsichtlich Sicherheitsanforderungen, die für Ihre Leitstelle gilt?*




Mehrheitlich existierten zum Zeitpunkt der Erhebung keine Vorgaben zu Sicherheitsanforderungen in Form von Gesetzen oder Rechtsverordnungen, die explizit auf BOS-Leitstellen Bezug nehmen (organisations- bzw. behördeninterne Vorgaben siehe 3.8). Lediglich 28,5 % der befragten Leitstellen bestätigten die Existenz von Sicherheitsanforderungen in Form von Rechtsvorgaben. Bei mehr als zwei Dritteln der Leitstellen hingegen existieren keine entsprechenden Anforderungen (und stehen auch nicht unmittelbar vor der Einführung) bzw. werden gerade erarbeitet.

## A.6 Sicherheitsbeauftragter – Zuständigkeit

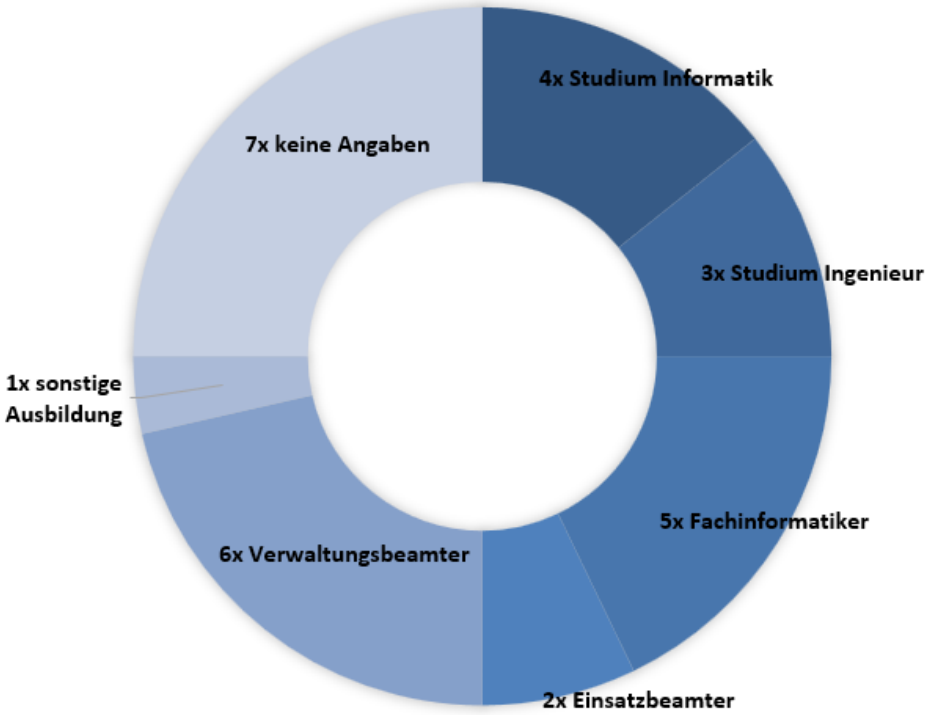
Frage: *Gibt es in Ihrer Leitstelle einen Beauftragten für IT-Sicherheit, der ausschließlich für die BOS-Leitstelle zuständig ist?*




Hintergrund dieser Frage ist, ob sich der die IT-Sicherheit zuständige Mitarbeiter der Leitstelle ausschließlich dieser Aufgabe widmen kann, oder ob dieser auch für andere Sicherheitsanwendung zuständig ist bzw. weitere Beauftragungen innehat. Lediglich drei Leitstellen (10,7 %) bestätigten die ausschließliche Zuständigkeit des IT-Sicherheitsbeauftragten für die Leitstelle; die Mehrzahl der Rückmeldungen lässt erkennen, dass die IT-Sicherheitsbeauftragten auch andere Anwendungen betreuen bzw. weitere Zuständigkeiten in verwandten Bereichen (z.B. Datenschutz, Geheimschutz) besitzen.

## A.7 Sicherheitsbeauftragter – Qualifikation

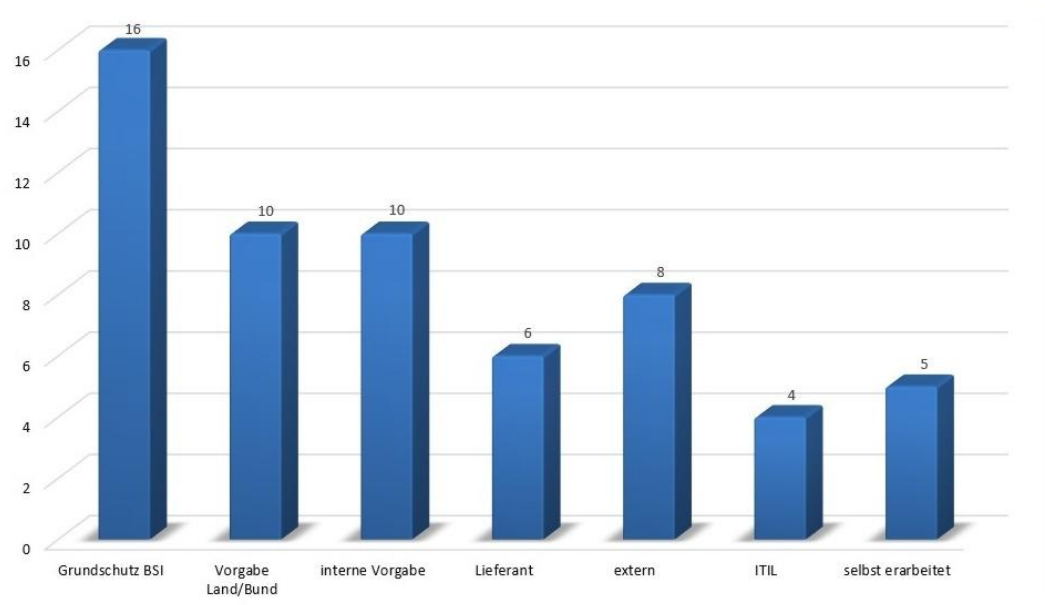
Frage: *Welche Qualifikation hat der IT-Sicherheitsbeauftragte der Leitstelle?*




Bei der Qualifikation des IT-Sicherheitsbeauftragten ergeben sich in 12 von 28 Rückmeldungen (42,7 %), dass eine grundständige Fachausbildung in Form eines Ingenieurstudiums (Elektrotechnik/Nachrichtentechnik/IT), eines Informatikstudiums oder einer abgeschlossenen Ausbildung zum Fachinformatiker vorliegt. In 28,5 % der rückmeldenden Leitstellen wird das Aufgabenfeld der IT-Sicherheit von Einsatzbeamten (Feuerwehrtechnischer Dienst), Polizeivollzugsbeamten oder Verwaltungsbeamten wahrgenommen, die neben ihrer Laufbahnausbildung entsprechende Weiterbildungen absolviert haben. In einem Fall (3,5 %) liegt eine anderweitige Ausbildung vor (ohne nähere Benennung); sieben Leitstellen (25 %) machten keine Angaben zur Qualifikation.

## A.8 Grundlage der Sicherheitsvorgaben

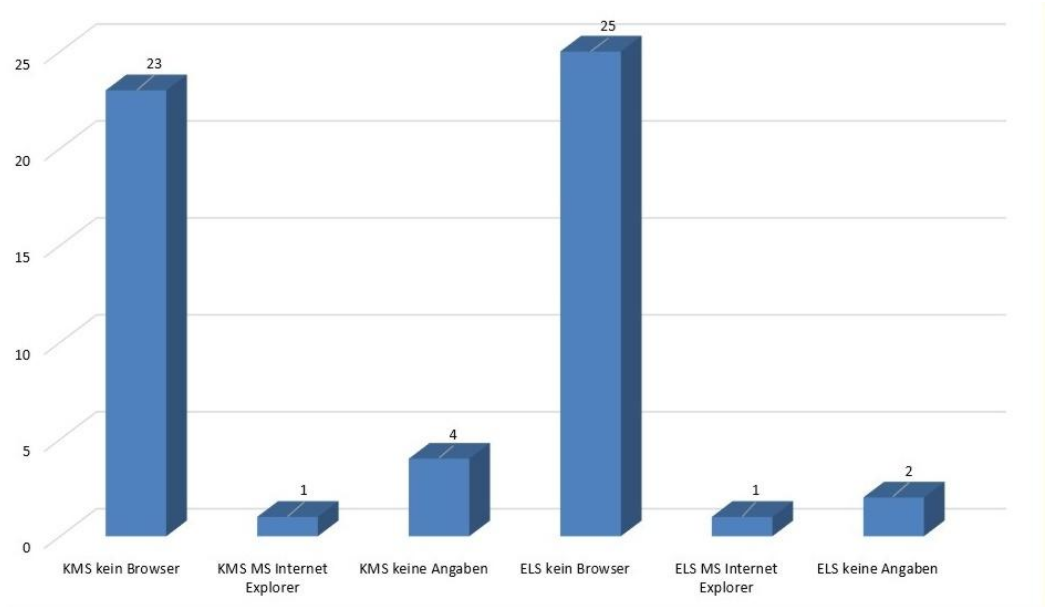
Frage: *Auf welchen Vorgaben/Konzepten basiert die IT-Sicherheit in Ihrer Leitstelle?* (Mehrfachantworten möglich)




In 16 von 28 Leitstellen (57,1 %) bildet der IT-Grundschutz des BSI die Basis für die IT-Sicherheit. In zehn Fällen liegen zudem Vorgaben des Landes oder Bundes zugrunde; dies deckt sich mit den Antworten unter 3.5. Behörden- oder betreiberinterne Vorgaben finden in ebenfalls zehn Fällen Anwendung, während sechs Fällen die Lieferanten Sicherheitskonzeptionen vorgelegt haben bzw. externe Dienstleister hinzugezogen wurden (acht Fälle). Selbst erarbeitete Konzepte liegen in fünf Leitstellen zugrunde.

## A.9 KMS im Browser

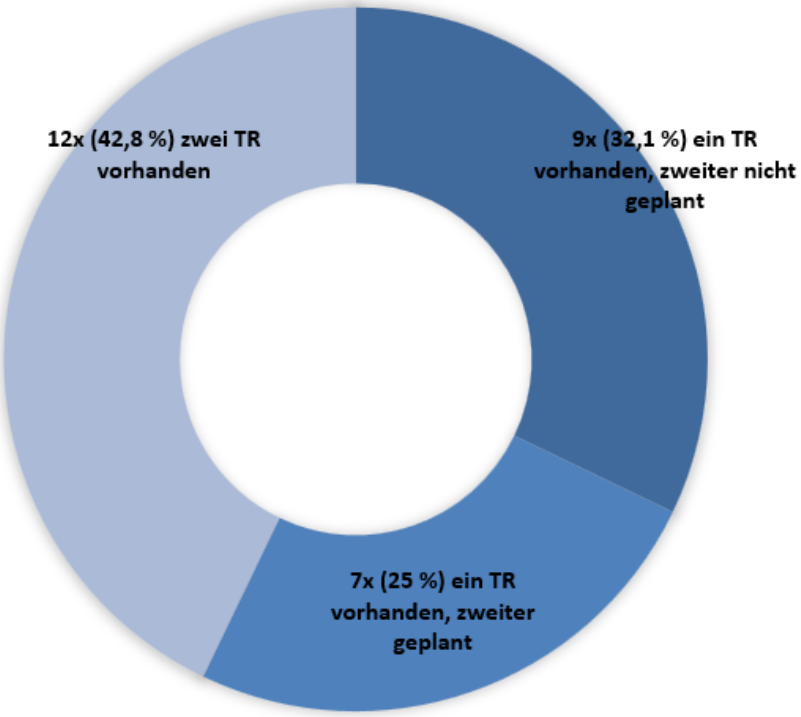
Fragen: *Wird für das Kommunikationssystem bzw. das Einsatzleitsystem eine Bedienoberfläche auf einem Webbrowser genutzt? Wenn ja, welcher?*
(Mehrfachantworten möglich)




Bei der überwiegenden Mehrzahl kommen keine Webbrowser als Grundlage für das Frontend als Bedienoberfläche zur Anwendung; dies betrifft 23 Leitstellen (82,1 %) beim KMS und 25 Leitstellen beim ELS (89,2 %). Nur in jeweils einem Fall beim KMS und ELS kommt der Microsoft Internet Explorer zum Einsatz; in vier bzw. zwei Fällen erfolgten keine Angaben zur Browsernutzung.

## A.10 Redundanz Technikraum

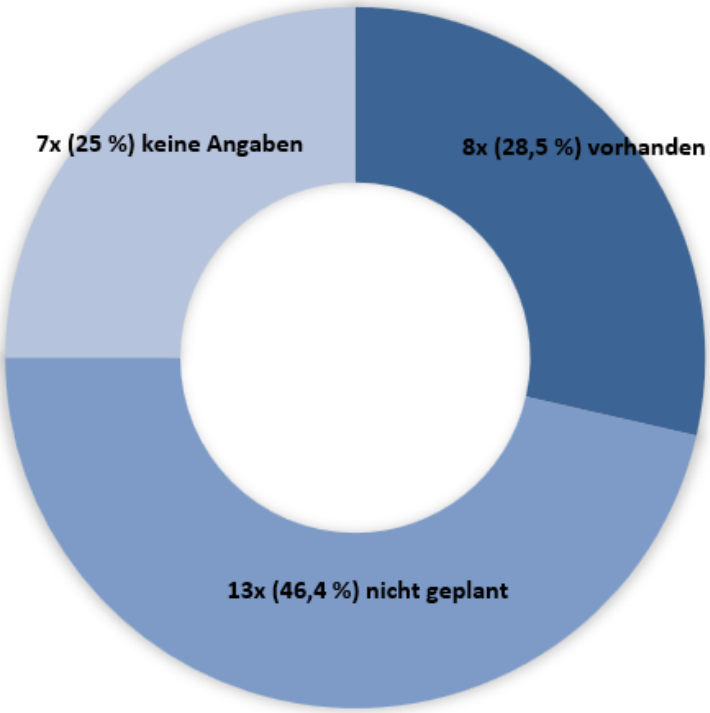
Frage: *Einer oder zwei Technikräume vorhanden bzw. in Planung?*




In 42,8 % der Fälle sind zwei baulich getrennte Technikräume vorhanden, in denen redundante Systeme betrieben werden. Ein Viertel verfügt derzeit nur über einen Technikraum, es ist jedoch ein zweiter Technikraum geplant. In etwa einem Drittel der Leitstellen (32,1 %) ist nur ein Technikraum vorhanden, woran zunächst auch nichts geändert werden soll. Die Schaffung zweier baulich getrennter Technikräume ist bei Bestandsgebäuden meist schwierig und wird daher vor allem bei Neubauten oder grundlegenden Gebäudesanierungen mit eingeplant.

## A.11 Hochwasserschutz

Frage: *Wurden Vorkehrungen zum Hochwasserschutz getroffen bzw. befinden sich in Planung?*



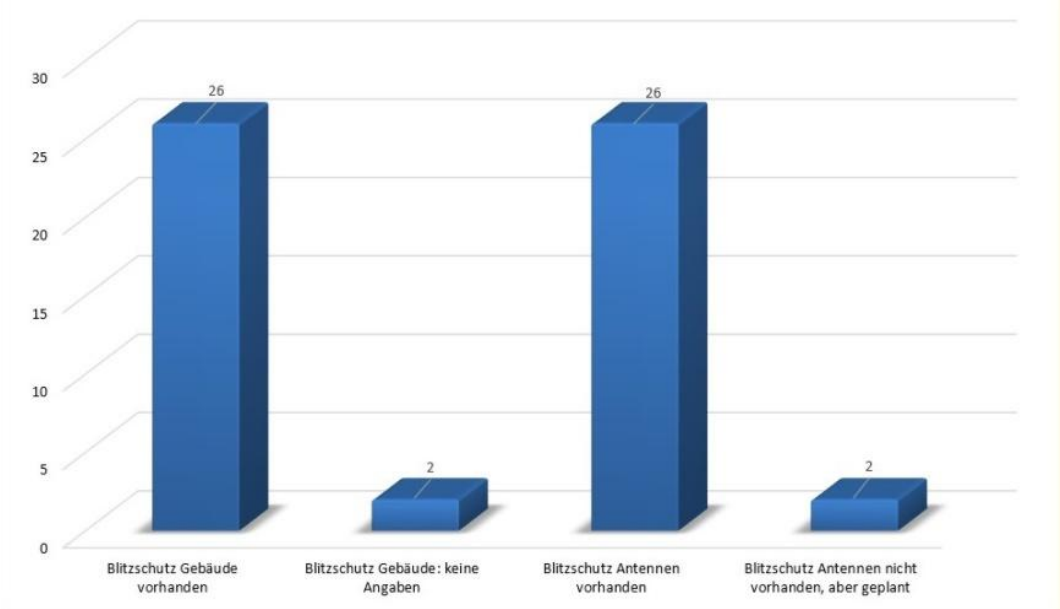

Maßnahmen zum Hochwasserschutz beziehen sich vor auf den Schutz vor von außen eindringendem Wasser in das Erd- bzw. Untergeschoss, nicht auf Vorkehrungen bzgl. eines Wasserrohrbruchs innerhalb des Gebäudes. Da sich die Hauseinführungen der Elektrizitäts- und Telekommunikationsanschlüsse im Regelfall im Untergeschoss befinden, sind diese bei einem Wassereintritt gefährdet. Auch haustechnische Anlagen wie z.B. die Heizung oder Netzersatzanlage (NEA) befinden sich meist im Untergeschoss. Andere technische Systeme, die für den Leitstellenbetrieb unentbehrlich sind, können auch in den höherliegenden Geschossen untergebracht sein, z.B. Serverschränke mit der Systemtechnik, USV, Lüftung und Klimatisierung. Durch die erdverlegten Versorgungsleitungen (Elektrizität, Telekommunikation) und deren Hauseinführungen, sind tiefergelegene Geschosse bei einer Hochwasserlage besonders gefährdet, wenn es um die Aufrechterhaltung des Leitstellenbetriebs geht.

Acht Leitstellen (28,5 %) haben geantwortet, dass Maßnahmen zum Hochwasserschutz ergriffen wurden, dies mag in Anbetracht der Gesamtzahl an Rückmeldungen gering erscheinen, jedoch ist bzgl. Hochwasserschutz die geographische Lage

des Leitstellengebäudes, d.h. die Nähe zu Fließgewässern und das Höhenniveau in Bezug auf den regulären Wasserpegel zu berücksichtigen. Leitstellengebäude, die sich auf einer Anhöhe befinden und weit genug von Gewässern entfernt liegen, unterliegen keiner besonderen Gefährdung durch Hochwasser, so dass keine entsprechenden Vorkehrungen erforderlich sind. Dies spiegelt sich auch in den Rückmeldungen wider, da in 46,4 % der Fälle erklärt wurde, dass Hochwaserschutzmaßnahmen nicht geplant sind. In sieben Fällen (25 %) wurden keine Angaben gemacht.

## A.12 Blitzschutz Gebäude

Frage: *Wurden Vorkehrungen zum Blitzschutz getroffen bzw. befinden sich in Planung?* (Mehrfachantworten möglich)




Blitzschutzmaßnahmen am Gebäude und an den Antennen wurden in 26 von 28 Fällen bejaht (92,8 %), in zwei Fällen erfolgten keine Angaben zum Blitzschutz des Gebäudes bzw. der Blitzschutz der Antennen wurde in ebenfalls zwei Fällen als nicht vorhanden, aber in Planung befindlich beschrieben.

D.h. bzgl. Blitzschutz bestehen keine Defizite, sondern der Blitzschutz wird als Standardmaßnahme angesehen, insbesondere bei Antennenanlagen.

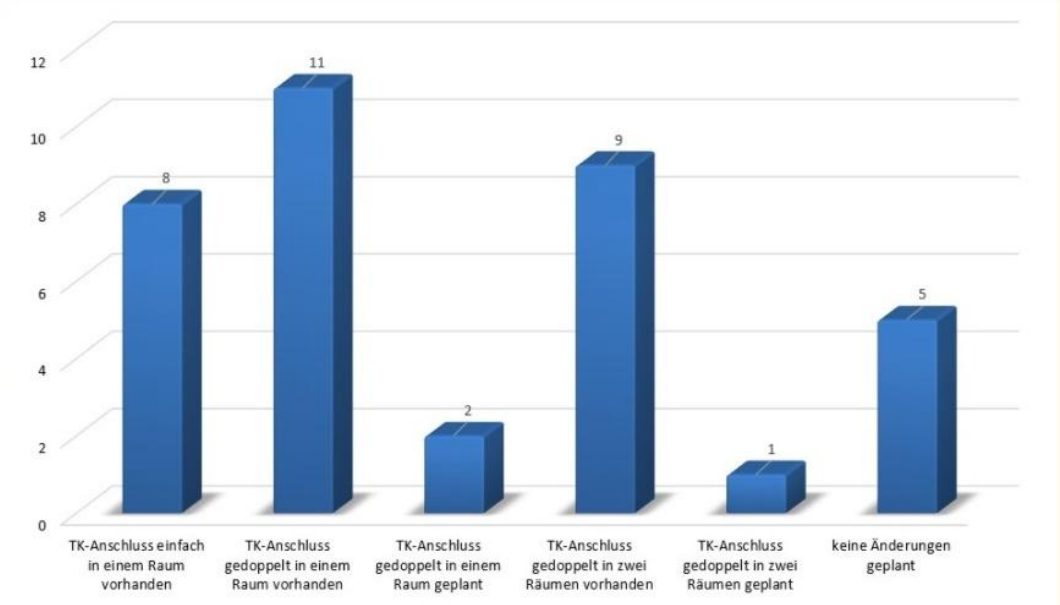
## A.13 Überspannungsschutz

Frage: *Wurden Vorkehrungen zum Überspannungsschutz getroffen bzw. befinden sich in Planung?* (Mehrfachantworten möglich)

Antwort: Überspannungsschutz ist zu 100 % bei den rückgemeldeten Leitstellen erfüllt.

## A.14 Redundanz TK-Anbindung

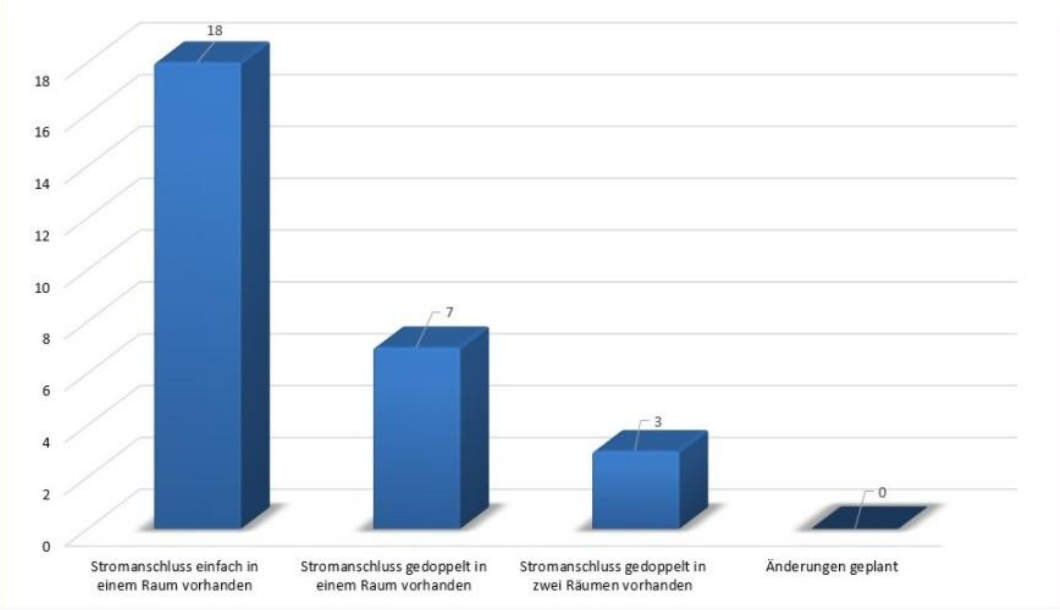
Frage: *Redundanter Hausanschluss der TK-Leitungen vorhanden bzw. in Planung?* (Mehrfachantworten möglich)




Ein einfach vorhandener TK-Anschluss wurde in acht Fällen bejaht, davon ist in zwei Fällen eine Dopplung vorgesehen, die im gleichen Raum terminiert; in einem Fall ist im Zuge eines Um-/Neubaus die Dopplung mit der Schaffung von Abschlusspunkten in zwei getrennten Räumen geplant. In elf Fällen sind gedoppelte Anschlüsse in einem Raum vorhanden, bei neun Leitstellen sind gedoppelte Leitungen vorhanden, die in zwei getrennten Räumen enden. Eine gedoppelte Leitungszuführung minimiert das Risiko eines Ausfalls der drahtgebundenen Telekommunikation und Datenanbindung, wenn eine Leitung z.B. durch einen Baggerschaden beeinträchtigt wird.

## A.15 Redundanz Stromversorgung

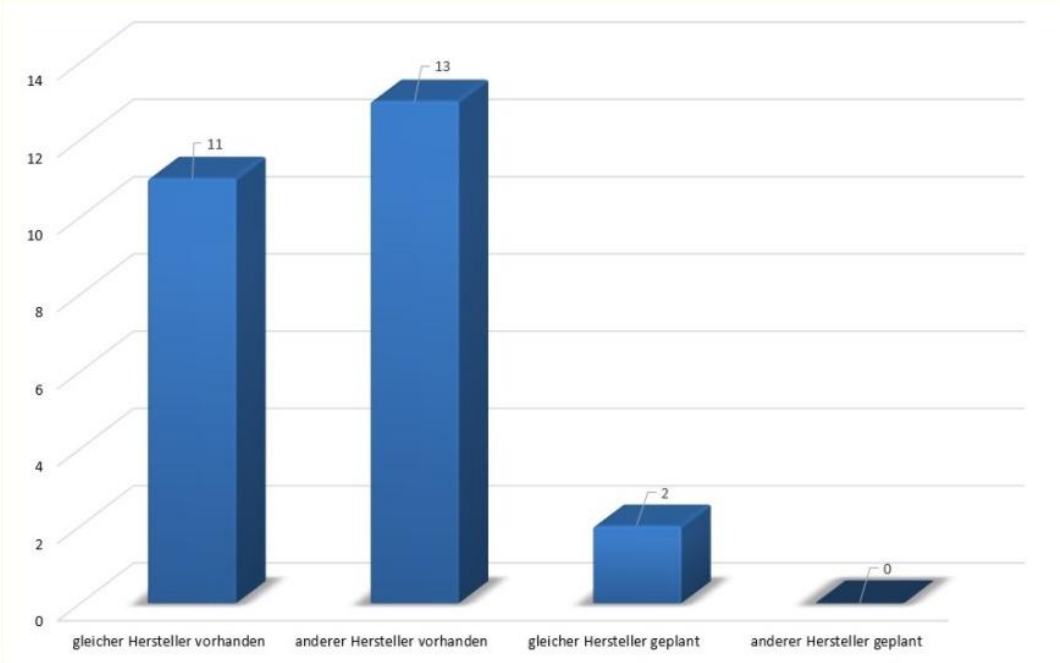
Frage: *Redundanter Hausanschluss der Stromversorgungsleitungen vorhanden bzw. in Planung?* (Mehrfachantworten möglich)




Im Gegensatz zu redundanten Zugangswegen bei den TK-Leitungen (3.14) bzw. der Planung, diese redundant auszuführen, ergibt sich bei der Stromversorgung ein anderes Bild: 18 von 28 Leitstellen (64,2 %) verfügen über einen Hausanschluss zur Stromversorgung, der in einem Anschlussraum terminiert. In sieben Fällen ist eine gedoppelte Anbindung vorhanden, die im gleichen Raum endet. In lediglich drei Fällen sind getrennte Hauseinführungen in getrennten Räumen vorhanden. Änderungen an den Hausanschlüssen der Stromversorgung sind in keinem Fall vorgesehen.

## A.16 Rückfallebene Kommunikationssystem

Frage: *Rückfallebene des KMS vorhanden oder in Planung? Sofern vorhanden bzw. in Planung; identischer Hersteller wie das Hauptsystem oder anderer Hersteller?* (Mehrfachantworten möglich)




Kommunikationsmanagementsysteme (KMS) werden i.d.R. redundant ausgelegt, so dass ein unterbrechungsfreier Betrieb gewährleistet werden kann. Je nach Ausprägung der Redundanz (zentrale Komponenten, Virtualisierung der Serverumgebung, Schnittstellen, Client-PCs, separate Funkgeräte usw.) ist zusätzlich eine Rückfallebene erforderlich, mit der die Grundfunktionen – Telefonie und Funkverkehr – weiterhin möglich sind, wenn auch mit reduziertem Bedienkomfort. Es ist eine Frage der Philosophie, ob als Rückfallebene dasselbe System vorgehalten wird, wie das Hauptsystem oder aus Gründen der Fehlervermeidung auf ein Alternativprodukt gesetzt wird. Für dasselbe System spricht die identische Bedienung, d.h. bei einer Störung des Hauptsystems ergeben sich keine geänderten Abläufe, so dass auch Fehlerquellen, die bei der Nutzung selten genutzter Anwendungen aufgrund fehlender Routine entstehen können, nicht zum Tragen kommen. Nachteilhaft kann bei diesem Ansatz sein, dass Schwachstellen in der Hard- und/oder Software gleichermaßen das Haupt- und das Rückfallsystem betreffen und Schadcode

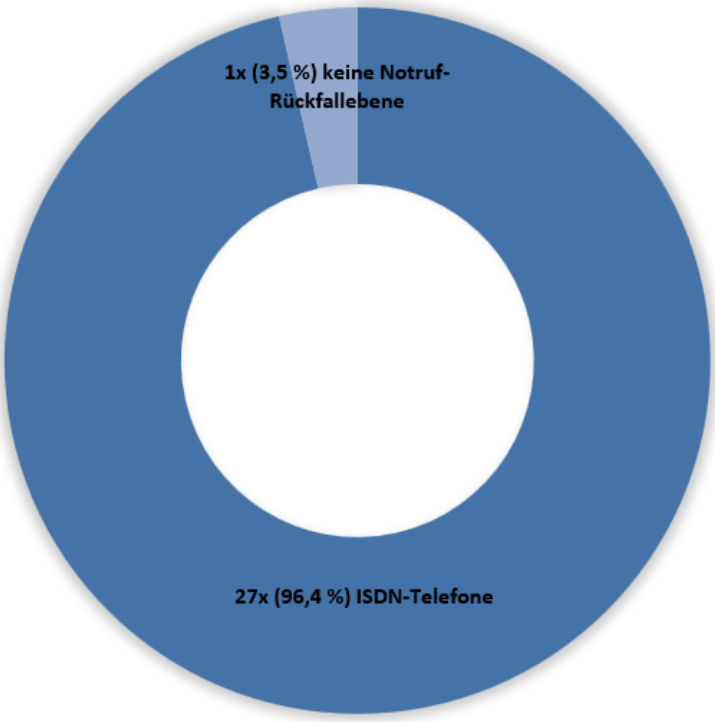
beide Systeme gleichzeitig beeinträchtigen kann. D.h. Sicherheitslücken ziehen sich nach dem „Käsescheibenmodell“ über beide Systeme.

Die Nutzung einer Rückfallebene eines anderen Herstellers vermeidet den „Käsescheibeneffekt“, bringt aber evtl. Unsicherheiten bei der Benutzung des Rückfallsystems mit sich, wenn dessen Bedienung selten erforderlich wird und nicht regelmäßig trainiert wird.

Diese beiden Ansätze spiegeln sich in den Zahlen der Rückmeldungen wider; 11 Leitstellen nutzen ein typgleiches System als Rückfallebene, wie das Hauptsystem. Bei 13 Leitstellen kommt ein anderes System als Rückfallebene zur Anwendung. Bei Erneuerungsplanung sehen zwei Leitstellen den Einsatz eines typgleichen Systems vor; die Beschaffung eines anderen Herstellers ist derzeit in keinem der rückgemeldeten Fälle vorgesehen. In vier Fällen erfolgten keine Angaben.

## A.17 Rückfallebene Notruf (ISDN)

Frage: *Rückfallebene für die ISDN-basierte Notrufabfrage vorhanden? Wenn ja, als ISDN-Einzeltelefonapparate?*

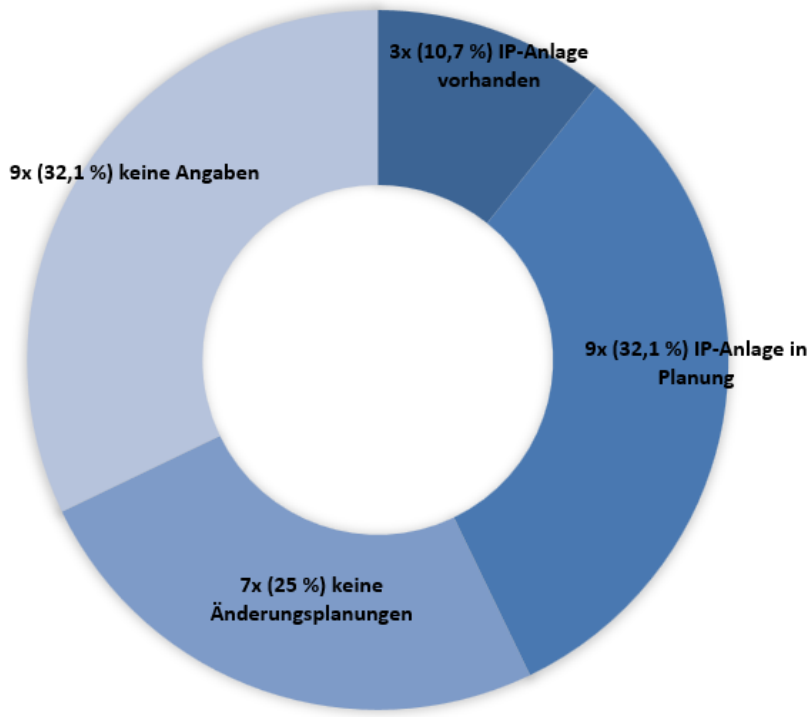



Die Umstellung der öffentlichen Fernsprechnetze von ISDN-basierter Vermittlungs- und Anschlusstechnik auf IP ist inzwischen abgeschlossen. Von den 28

Leitstellen, die eine Rückmeldung gegeben hatten, wurden bei 27 Standorten einzelne ISDN-Telefonapparate für jeden Anschluss ($S_0$) vorgehalten. Für den Ausfall von KMS bzw. deren Schnittstellenbaugruppen, wurden die ISDN-Telefonapparate direkt an die $S_0$-Schnittstellen der NTBA gesteckt. Z.T. bestanden auch relaisbasierte Umschalteinrichtungen, die das Umstecken der Patchkabel ersparten und direkt auf die bereitgehaltenen ISDN-Apparate umgeschaltet haben. Dies sparte Zeit und vermied das Verwechseln von Patchkabeln und Steckbuchsen, erfüllte aber technisch den gleichen Zweck, nämlich die direkte Kontaktierung der ISDN-Rückfalltelefone an die $S_0$-Schnittstellen.

## A.18 Rückfallebene Notruf (IP)

Frage: *Rückfallebene für die IP-basierte Notrufabfrage vorhanden? Wenn ja, als IP-Einzeltelefonapparate?*

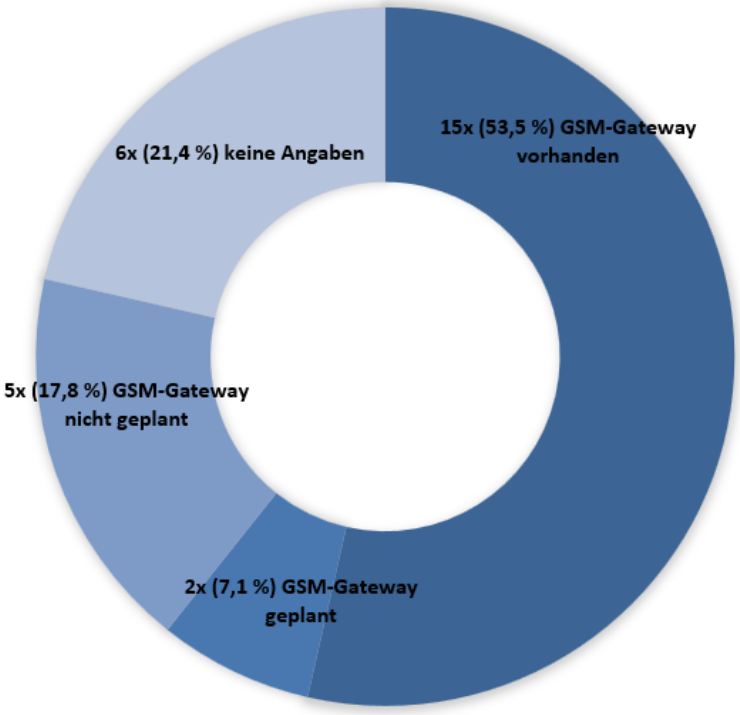



Da die Umstellung von ISDN- auf IP-basierten Notruf sich zum Zeitpunkt der Erhebung gerade in der Umstellung befand, hatte erst ein Teil der Leitstellen (3 von 28) für die Notrufabfrage eine Rückallebene in Form einer gesonderten IP-

Telefonanlage nebst Telefonapparaten beschafft. Bei neun Leitstellen war eine entsprechende IP-Telefonanlage in Planung; sieben Standorte hatten zurückgemeldet, dass keine Änderungsplanungen bestehen, da der exakte Zeitpunkt der Umstellung noch nicht greifbar war. In neun Fällen erfolgten keine Angaben hierzu.

## A.19 GSM-Gateway als Rückfallebene für die Telefonie

Frage: *Rückfallebene in Form eines GSM-Gateways für die Anbindung an das Telefon-Festnetz vorhanden?*



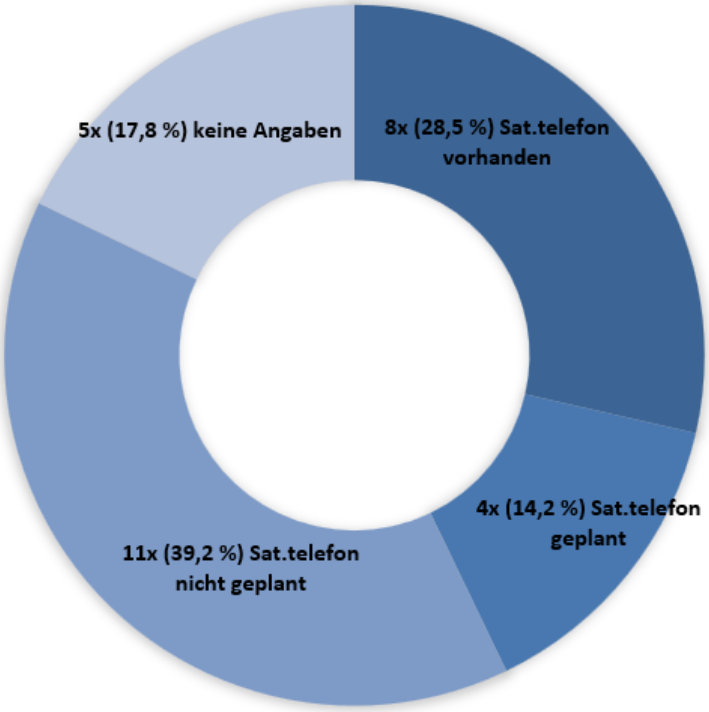

Im Fall eines Leitungsschadens (z.B. durch Baggerarbeiten), bei dem die Festnetztelefonie gestört ist, muss die Leitstelle in der Lage sein, mit externen Stellen zu kommunizieren, d.h. im ersten Schritt, den Leitungsschaden dem TK-Dienstleister zu melden. Für derartige Störungen im leitungsgebundenen Telefonnetz wird der Mobilfunk als Ausweichmöglichkeit genutzt. GSM-Gateways stellen als stationäre Mobiltelefone die Verbindung zum Telefonnetz her und ermöglichen damit – zumindest eingeschränkt – die telefonische Erreichbarkeit der Leitstelle. Dies stellt allerdings keine Alternative für Notrufanschaltungen dar, da Notrufverbindungen

aufgrund rechtlicher Vorgaben nicht auf Mobiltelefonteilnehmer geroutet werden dürfen.

In der Mehrzahl der Leitstellen (15 von 28) sind GSM-Gateways vorhanden, bei weiteren zwei Leitstellen sind diese in Planung. Fünf Leitstellen halten kein GSM-Gateway vor bzw. haben das auch nicht geplant. In sechs Fällen wurden keine Angaben gemacht.

## A.20 Satellitentelefon als Rückfallebene für die Telefonie

Frage: *Rückfallebene in Form eines Satellitentelefons für die Anbindung an das Telefon-Festnetz vorhanden?*

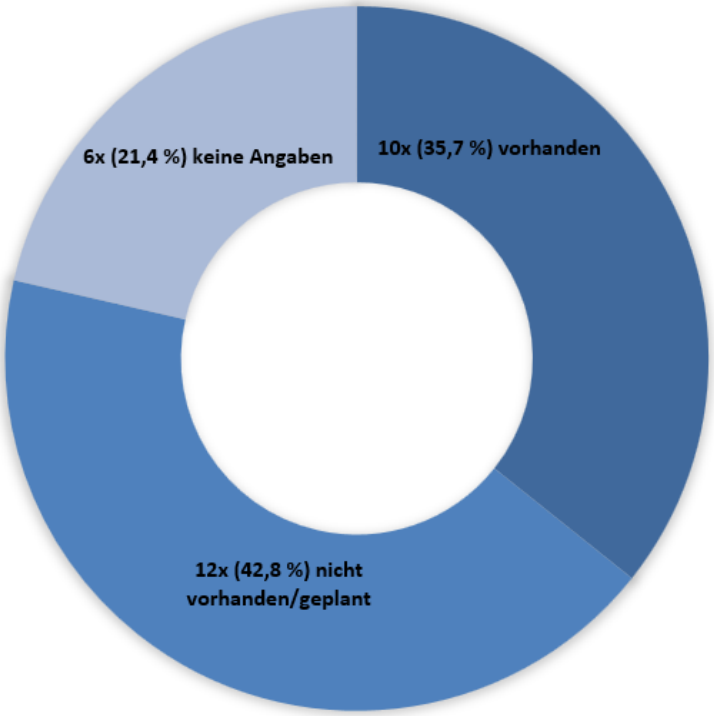



Ebenso wie ein GSM-Gateway werden teilweise auch Satellitentelefone vorgehalten, mit denen bei einer lokalen Störung im Telefonnetz (Festnetz, Mobilfunknetz) eine Kommunikation möglich ist. Dies ist vor allem für Katastrophenlagen vorgesehen, bei denen aufgrund länger andauernder Störungen bei der Stromversorgung bzw. Telekommunikation die Leitstellen Kontakt zu den Nachbarkreisen oder zu übergeordneten Stellen (Landesregierung o.ä.) halten können.

Satellitentelefone sind bei acht der befragten Leitstellen vorhanden, bei weiteren vier in Planung befindlich. Weitere elf Leitstellen sehen kein Satellitentelefon vor; fünf Standorte machten keine Angaben.

## A.21 Eigenes TK-Netz

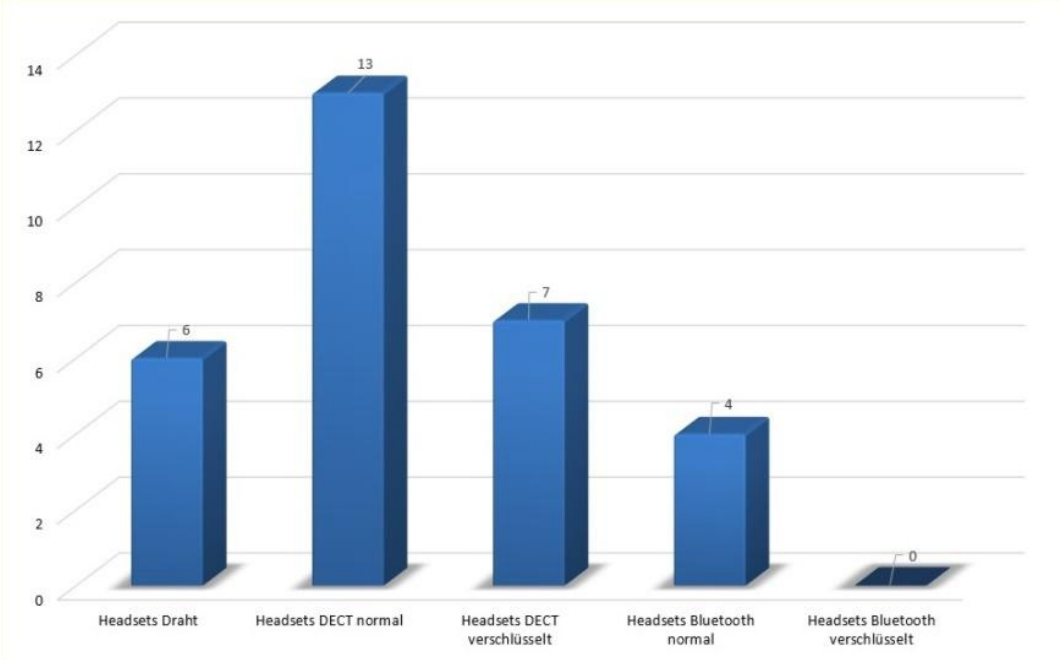
Frage: *Ist ein eigenes TK-Netz vorhanden, das als Rückfallebene bei einer Störung des öffentlichen TK-Netzes genutzt werden kann?*




Zehn der befragten Leitstellen haben das Vorhandensein eines behördeneigenen TK-Netzes bestätigt (bei den Polizeileitstellen ohnehin Standard; Polizeisondernetz). In 12 Fällen ist ein eigenes TK-Netz weder vorhanden noch geplant; von sechs Leitstellen liegen keine Angaben vor.

## A.22 Headsets

Frage: *Werden drahtlose oder drahtgebundene Headsets an den Leitstellenarbeitsplätzen genutzt? Sofern drahtlos, welcher Standard und mit oder ohne Verschlüsselung?* (Mehrfachantworten möglich)

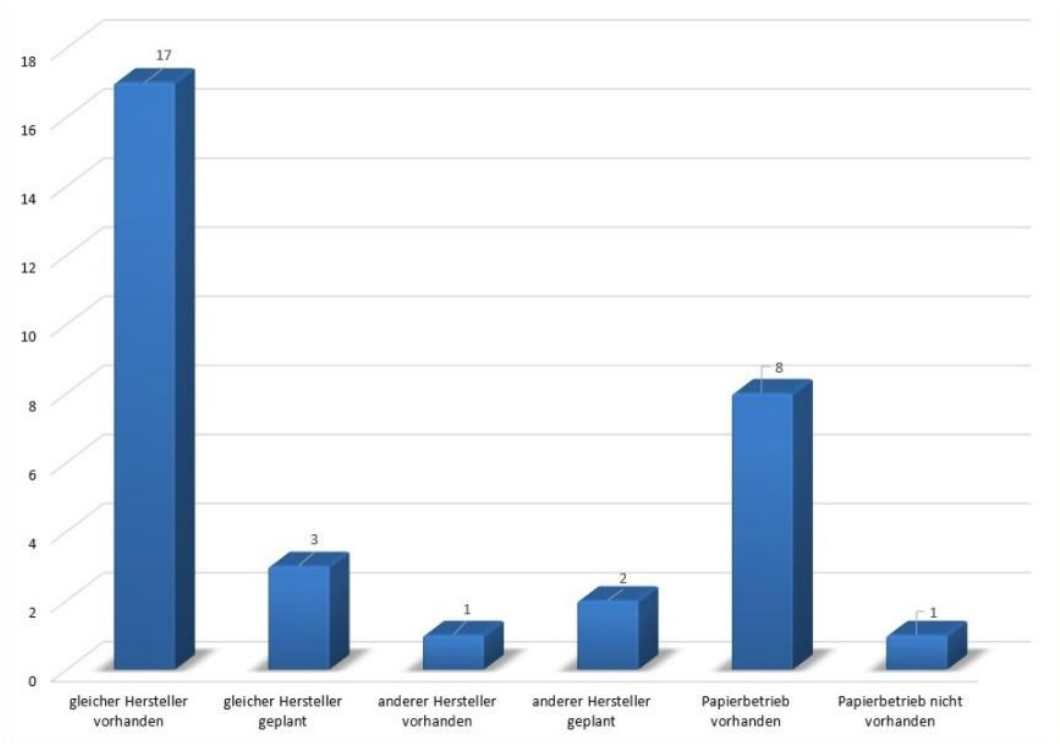



Die Frage nach den Headsets ergibt sich aus dem Sicherheitsgedanken heraus, da sich bei sämtlichen drahtlosen Anwendungen die Ausbreitung der hochfrequenten Wellen nach physikalischen Gesetzmäßigkeiten erfolgt und nicht an der Gebäudewand oder der Grundstückgrenze Halt macht. Ein Abhören der Gespräche oder ein Stören der Headsetnutzung durch einen leistungsstarken Störsender sind denkbar.

In sechs der 28 Leitstellen kommen drahtgebundene Headsets zum Einsatz, in 13 Fällen drahtlose Headsets auf DECT-Basis (unverschlüsselt), in weiteren sieben Fällen ebenfalls DECT, aber verschlüsselt. Auch Bluetooth wird genutzt, allerdings nur bei vier Leitstellen und allesamt im normalen Übertragungsmodus (unverschlüsselt). Bluetooth-Headsets mit Verschlüsselung sind bei den befragten Leitstellen nicht vorhanden. Insgesamt liegt die Anzahl der Rückmeldungen hier höher als 28, da Mehrfachantworten möglich waren. Dies ist auf den „Mischbetrieb“ drahtgebundener und drahtloser Headsets an zwei Leitstellenstandorten zurückzuführen.

## A.23 Rückfallebene Einsatzleitsystem

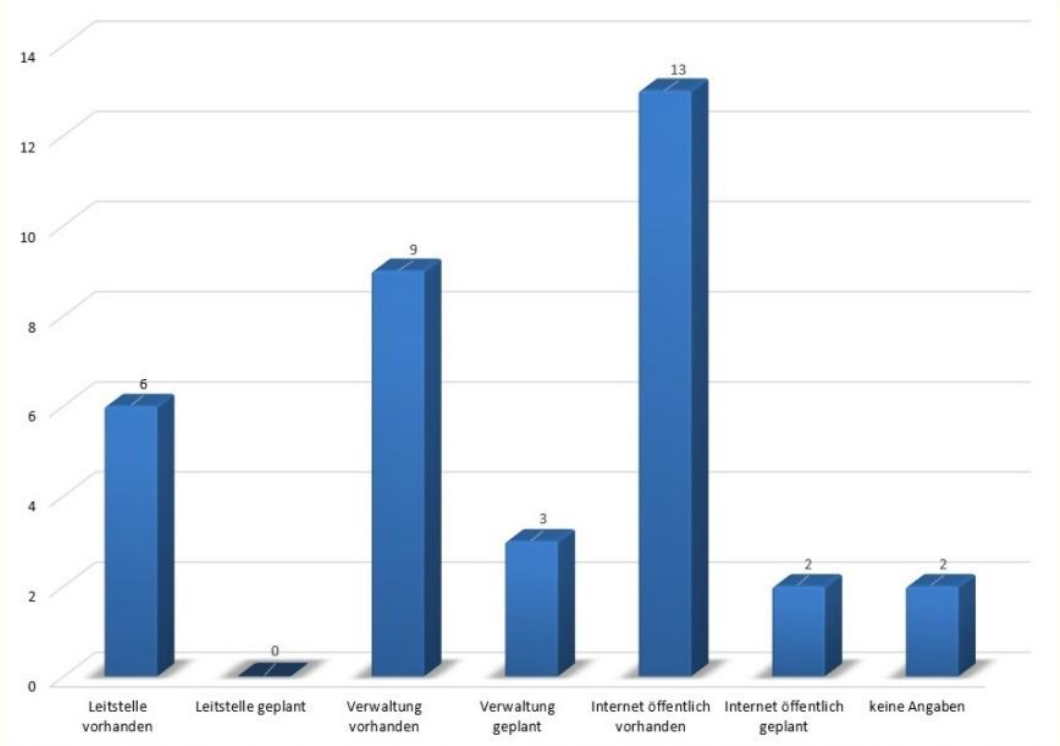
Frage: *Rückfallebene des ELS vorhanden oder in Planung? Sofern vorhanden bzw. in Planung; identischer Hersteller wie das Hauptsystem oder anderer Hersteller?* (Mehrfachantworten möglich)




Analog zum Punkt A.16 (Rückfallebene KMS) wird hier der Frage nach dem gleichen oder einem alternativen Anbieter für ein Rückfallsystem zum (Haupt-)Einsatzleitsystem nachgegangen. In 17 der Fälle existiert ein Rückfallsystem des gleichen Herstellers; in drei Fällen ist dies geplant. Ein Rückfall-ELS eines anderen Herstellers ist nur in einem Fall vorhanden und in zwei Fällen in Planung befindlich. Dem „Papierbetrieb“ kommt eine deutlich höhere Bedeutung zu, da acht Leitstellen bei einem Ausfall des ELS auf handschriftliche Einsatzerfassung und Hand-Alarmpläne setzen. In einem Fall wurde der Papierbetrieb verneint.

## A.24 WLAN

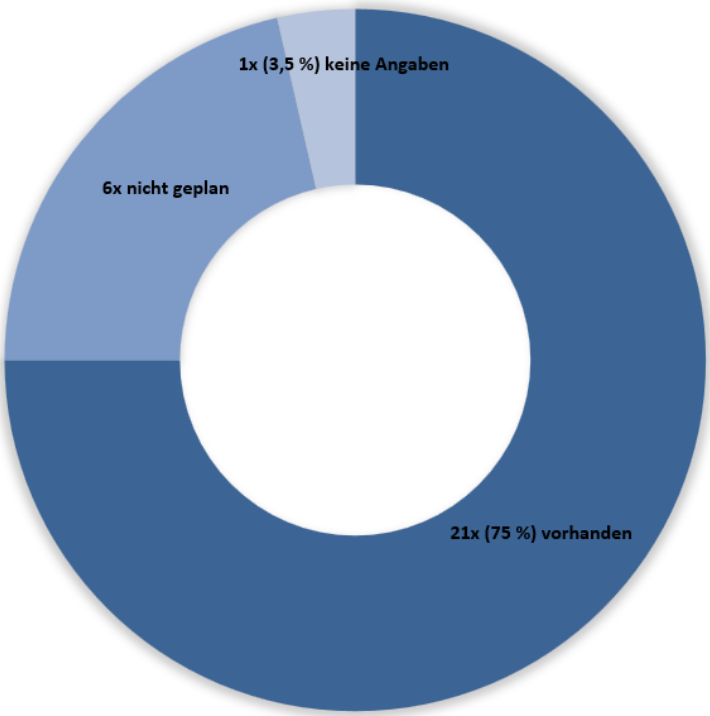
Frage: *WLAN in der Leitstelle bzw. den zugehörigen Bereichen im Gebäude vorhanden? Wenn ja, für welche Funktionen bzw. für welche Anwender?*
(Mehrfachantworten möglich)




In sechs Fällen besteht ein leitstelleninternes WLAN, das hauptsächlich für administrative Zecke oder zur Steuerung der Medientechnik über drahtlos betriebene Endgeräte genutzt wird. An neun Standorten steht das Verwaltungsnetz auch als WLAN zur Verfügung, bzw. ist bei drei Standorten geplant. An 13 Standorten existiert WLAN für öffentlich zugängliches Internet; dies betrifft ausschließlich Kreisverwaltungen, bei denen Publikumsverkehr herrscht und gleichermaßen die Leitstelle untergebracht ist. An zwei weiteren Standorten von Kreisleitstellen ist der öffentliche Internetzugang per WLAN geplant. In zwei Fällen wurden keine Angaben zu WLAN gemacht.

## A.25 DECT

Frage: *Wird in der Leitstelle drahtlose Telefonie auf DECT-Basis genutzt?*

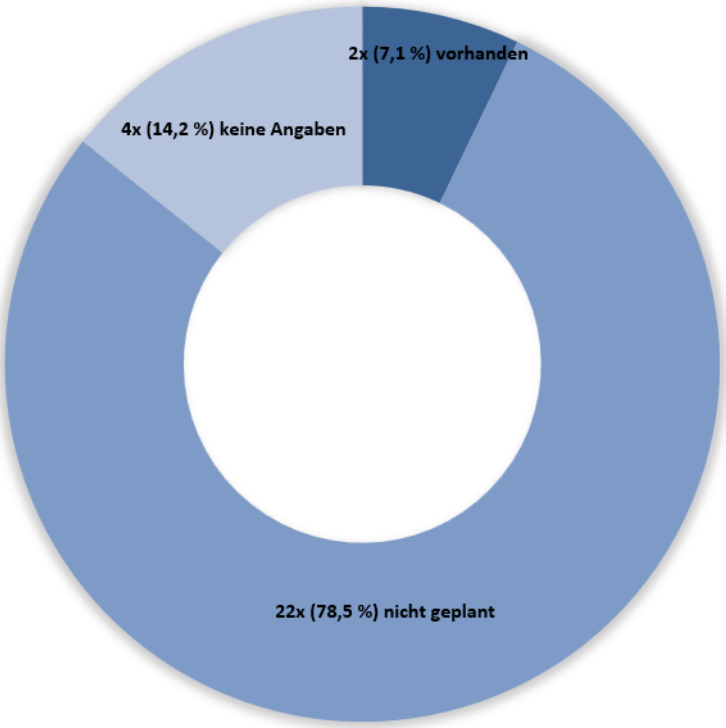



Die schnurlose Telefonie auf Basis des DECT-Standards betrifft weniger die Leitstellenarbeitsplätze (dort kommt DECT nur bei drahtlosen Headsets in Betracht, siehe 3.22), sondern den Leitstellenbereich mit den zugehörigen Nebenräumen, sofern dort eine DECT-Versorgung für die mobile Erreichbarkeit der Administratoren, der Leitstellenleitung oder im Stabsbereich gewünscht ist. Mit der drahtlosen Telefonie wird auch für Störer eine Möglichkeit eröffnet, auf die TK-Anlage bzw. auf das KMS einzuwirken, sofern insbesondere das KMS als TK-Knoten für die DECT-Versorgung des Leitstellenbereichs fungiert.

Mit großer Mehrheit der Rückmeldungen (21 von 28, d.h. 75 %) wird DECT-Telefonie genutzt, an sechs Standorten hingegen ist DECT-Telefonie weder vorhanden noch vorgesehen. Ein Leitstellenstandort machte keine Angaben zur Nutzung von DECT-Telefonie.

## A.26 Bluetooth

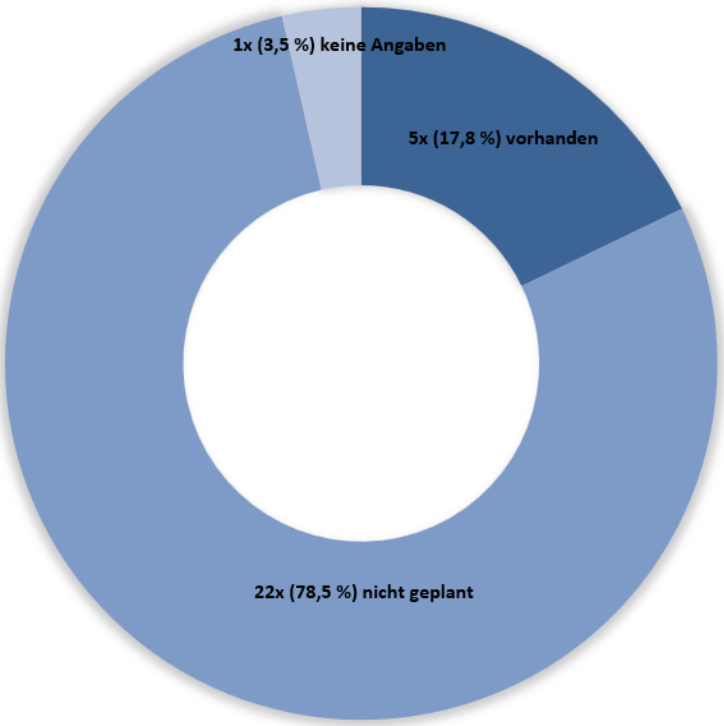
Frage: *Werden in der Leitstelle drahtlose Anwendungen auf Bluetooth-Basis genutzt?*




Analog zu den prinzipiellen Möglichkeiten der Einflussnahme über Drahtlosverbindungen bei DECT (siehe 3.25) wurde auch die vorhandene und künftig geplante Nutzung von Bluetooth erfragt (ausgenommen drahtlose Headsets, siehe hierzu A.22). Hier ergibt sich ein deutlich anderes Bild als bei DECT, da nur in zwei Fällen die Nutzung von Bluetooth bestätigt wurde. In der Mehrzahl der Rückmeldungen (22 von 28) ist Bluetooth weder vorhanden noch angedacht. Von vier Standorten liegen keine Rückmeldungen vor.

## A.27 drahtlose Eingabegeräte

Frage: *Werden in der Leitstelle drahtlose Eingabegeräte (Tastatur, Maus) genutzt?*

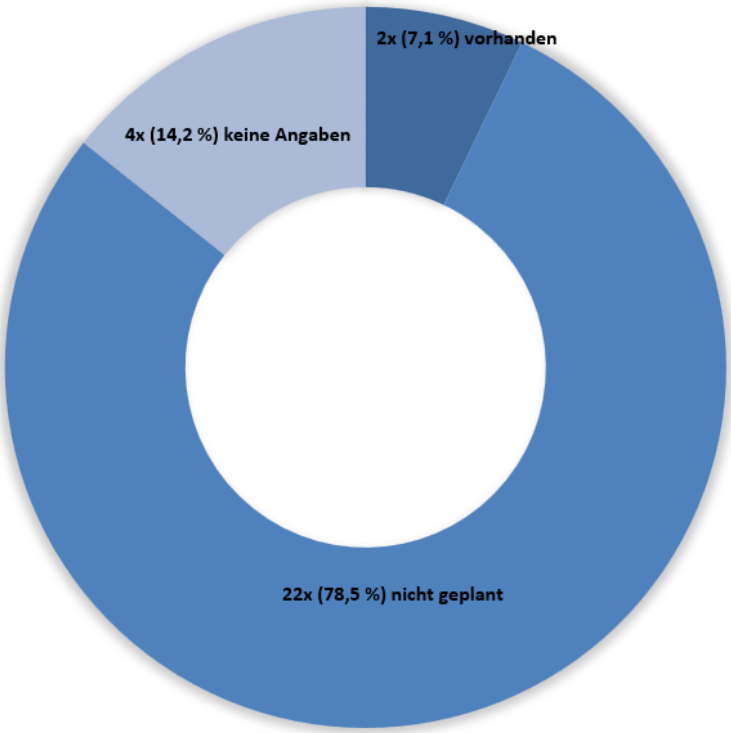



Eine weitere Drahtlosanwendung sind Eingabegeräte wie Tastaturen und Mäuse. Diese nutzen – abgesehen von Bluetooth – keinen international einheitlichen Standard, sondern proprietäre Formate. Gerade bei drahtlosen Tastaturen besteht prinzipiell die Möglichkeit, das drahtlose Signal abzufangen (Schutzziel der Vertraulichkeit gefährdet) und damit Eingaben – sowohl Einsatz- und Personendaten als auch Passwörter beim Login – abzufangen.

Drahtlose Eingabegeräte werden bei fünf von 28 Leitstellen verwendet; die Mehrzahl (22 von 28) nutzt drahtgebundene Eingabegeräte. In einem Fall erfolgten keine Angaben.

## A.28 drahtlose Anwendungen Haustechnik

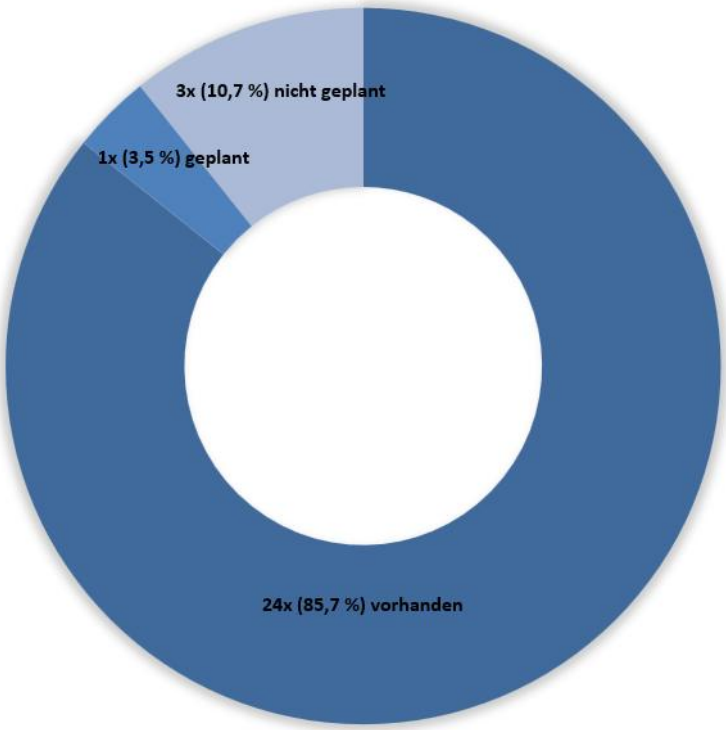
Frage: *Werden in der Leitstelle drahtlose Geräte zur Steuerung der Haustechnik genutzt?*




Drahtlose Geräte zur Steuerung der Haustechnik – ohne nähere Benennung des Funkstandards – werden in zwei Leitstellen genutzt; eine künftige Nutzung ist in der Mehrzahl der Leitstellen (22 von 28) nicht vorgesehen. Von vier Leitstellenstandorten liegen keine Angaben vor.

## A.29 Netztrennung (physikalisch)

Frage: *Ist das Netzwerk (LAN) der Leitstelle von anderen Netzen (Verwaltung) physikalisch getrennt?*

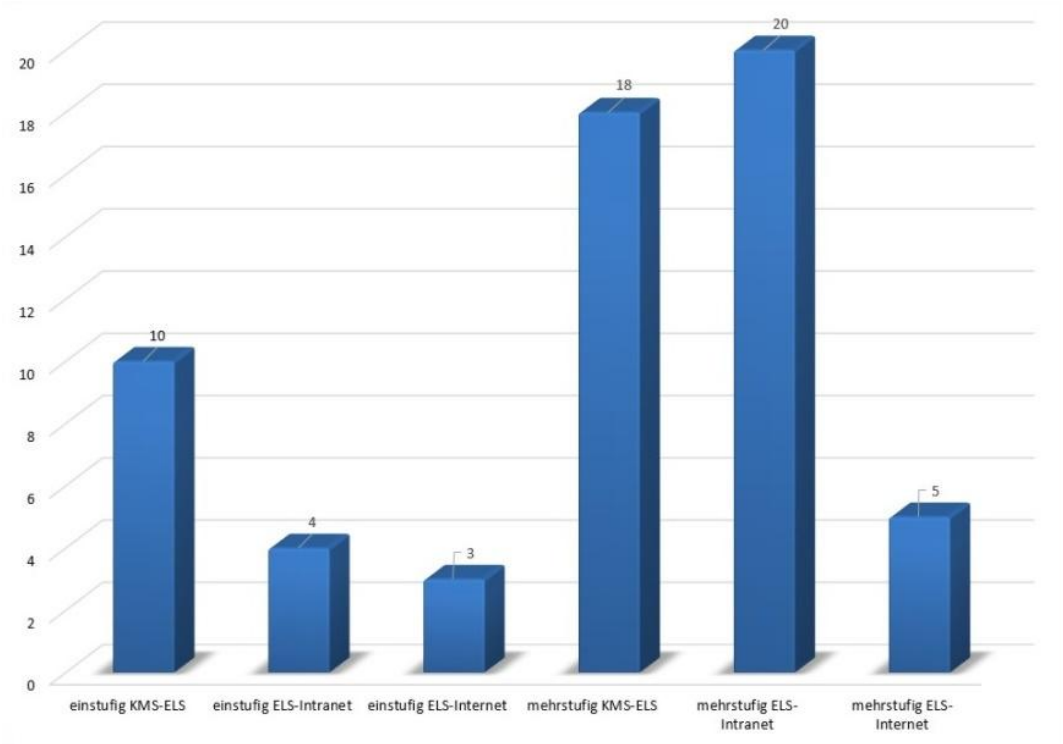



In der Mehrzahl der Rückmeldungen (24 von 28 Leitstellenstandorten) ist das Leitstellen-LAN physikalisch von anderen Netzen, z.B. Verwaltungs-LAN/ Intranet getrennt. An einem Standort werden die Leitstellensysteme noch in einem gemeinsamen Netz betrieben, die Trennung der Netze ist jedoch in Planung. Von drei Leitstellen liegen hierzu keine Angaben vor.

## A.30 Firewalls

Frage: *Werden aktuell einstufige oder mehrstufige Firewalls zur Abgrenzung von KMS und ELS bzw. des Leitstellen-LANs gegenüber dem Verwaltungsnetz und dem öffentlichen Internet eingesetzt bzw. was ist künftig geplant)?*

(Mehrfachantworten möglich)

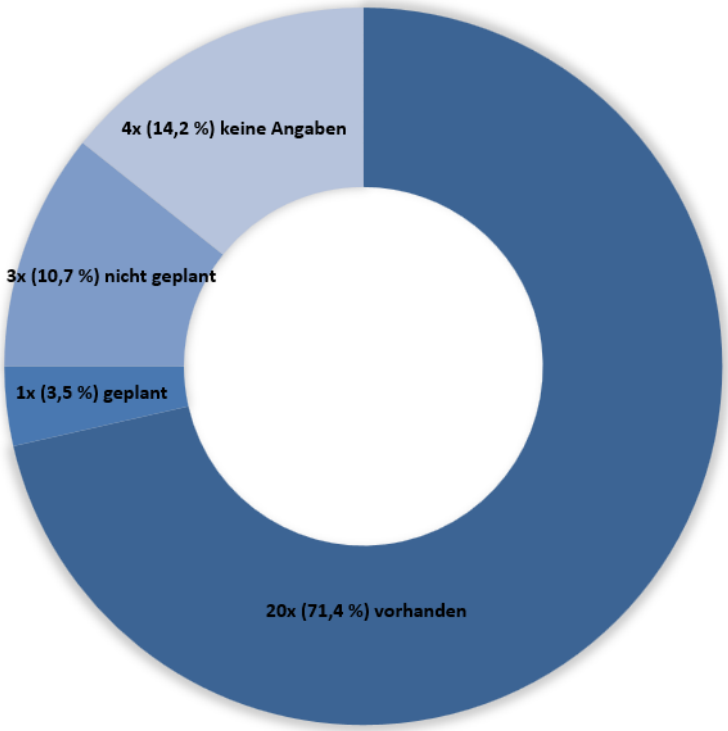



Eine einstufige Firewall zwischen KMS und ELS ist bei zehn Leitstellen im Einsatz, an 18 Standorten eine mehrstufige Firewall. Zwischen ELS und Verwaltungsnetz/Intranet kommt in vier Fällen eine einstufige Firewall zur Anwendung; in 20 Fällen mehrstufig. Gegenüber dem öffentlichen Internet wird in drei Fällen eine einstufige Firewall genutzt, in fünf Fällen eine mehrstufige. Nach allen vorliegenden Rückmeldungen sind keine Änderungen an diesem Status Quo vorgesehen.

Auffällig an diesen Zahlen ist, dass der Abgrenzung des Leitstellennetzes gegenüber dem Verwaltungsnetz in Form einer mehrstufigen Firewall eine größere Bedeutung zugemessen wird (in 20 von 28 Fällen) als der Abgrenzung gegenüber dem öffentlichen Internet, wo eine mehrstufige Firewall in lediglich fünf von 28 Fällen zur Anwendung kommt.

## A.31 DMZ

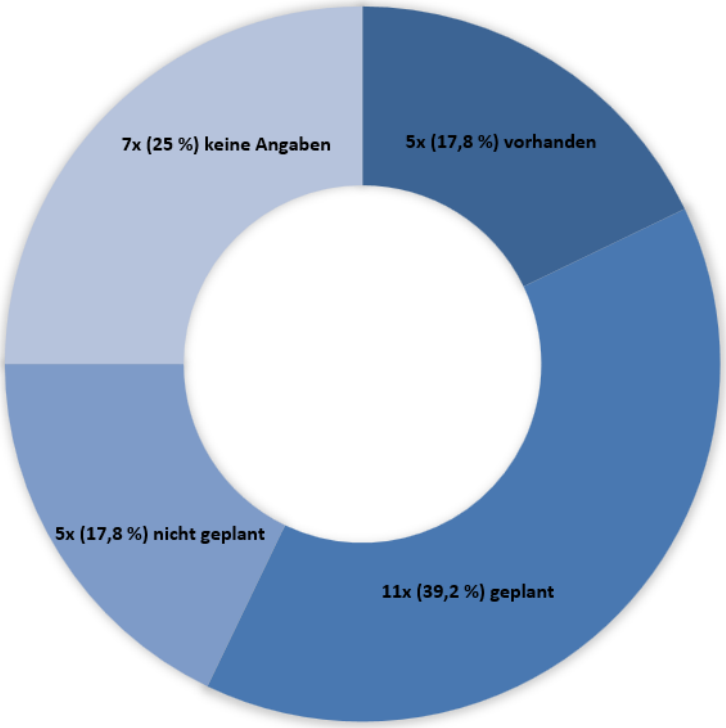
Frage: *Ist eine Demilitarisierte Zone (DMZ) im Netzwerk bzw. eingerichtet?*




In Ergänzung zum vorigen Punkt (3.30) antworteten 20 von 28 Leitstellenstandorten, dass eine DMZ eingerichtet ist. In einem Fall ist keine DMZ vorhanden, aber in Planung befindlich. Drei Leitstellen meldeten, dass eine DMZ nicht vorgesehen ist; in vier Fällen liegen keine Angaben zur DMZ-Nutzung bzw. -Planung vor.

## A.32 Session Border Controller für IP-Notruf

Frage: *Werden Session Border Controller (SBC) für die Abgrenzung des internen, IP-basierten TK-Netzes gegenüber dem öffentlichen TK-Netz eingesetzt bzw. was ist künftig geplant?*

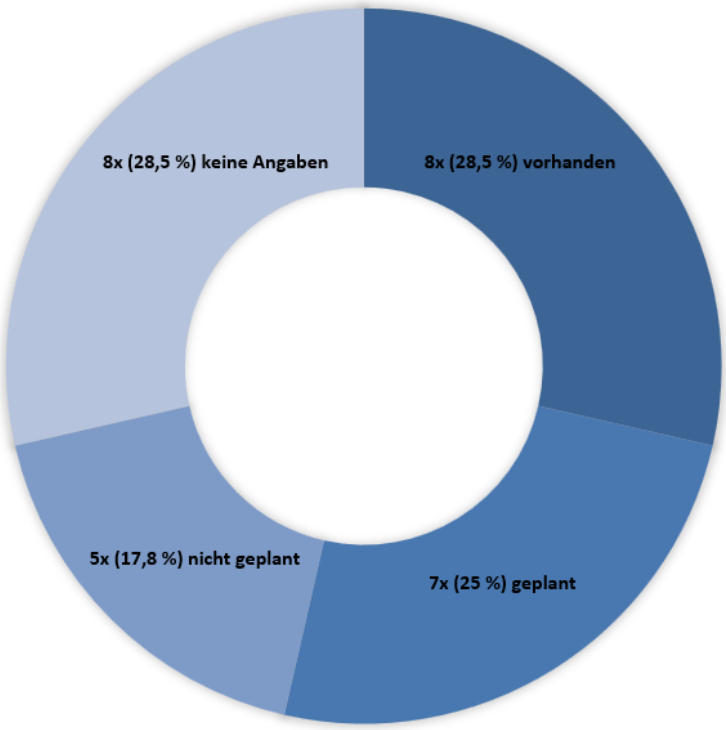



SBC sind in fünf von 28 Standorten im Einsatz, bei elf Standorten ist dies in Planung. Weitere fünf Leitstellen sehen derzeit keine SBC vor; von sieben Leitstellen liegen keine Angaben vor.

Diese Zahlen spiegeln den Stand im Herbst 2019 wider und dürften sich zwischenzeitlich verändert haben, da die Umstellung der Notrufanschlüsse auf IP in vollem Gange ist. Mit dem Abschluss der Migrationsmaßnahmen dürfte die Quote der SBC für Notrufanschlüsse (IP-basiert) künftig bei 100 % liegen.

## A.33 Session Border Controller für IP-Telefonie

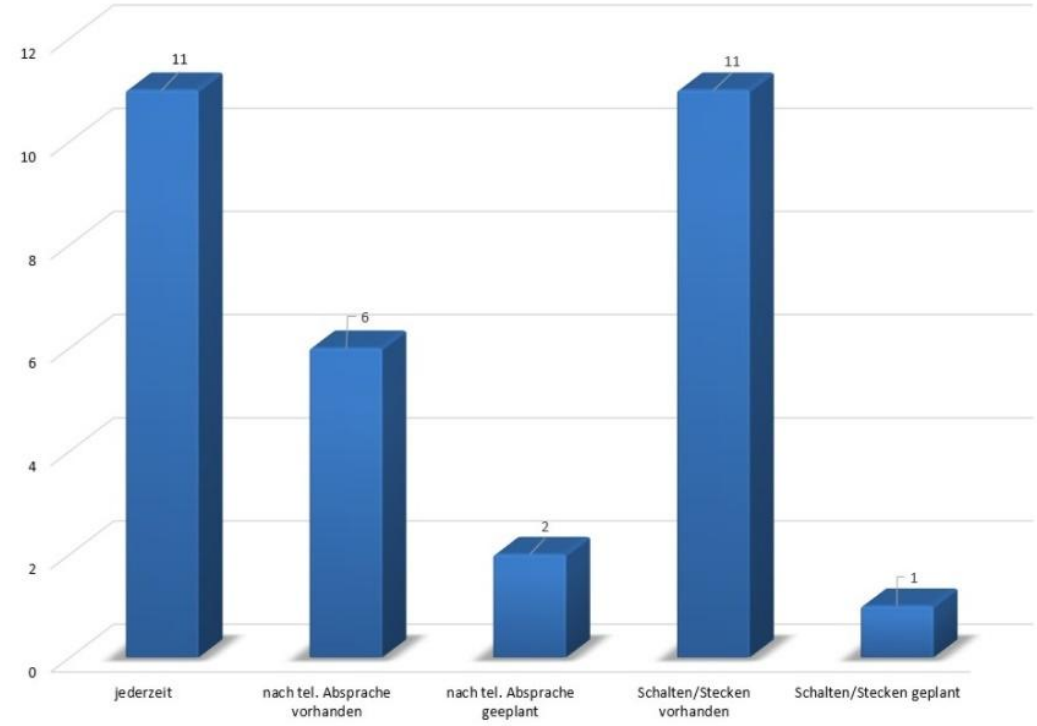
Frage: *Werden Session Border Controller (SBC) für die Abgrenzung des internen, IP-basierten TK-Netzes gegenüber dem öffentlichen TK-Netz eingesetzt bzw. was ist künftig geplant?*




Bei den Standard-Telefonanschlüssen (in Abgrenzung zum IP-Notruf, siehe A.32) ist an acht von 28 Standorten ein SBC in Betrieb, sieben weitere Leitstellenstandorte planen den Einsatz eines SBC. Fünf Standorte sehen keinen SBC vor; von acht Leitstellen liegen hierzu keine Angaben vor.

## A.34 Fernwartung

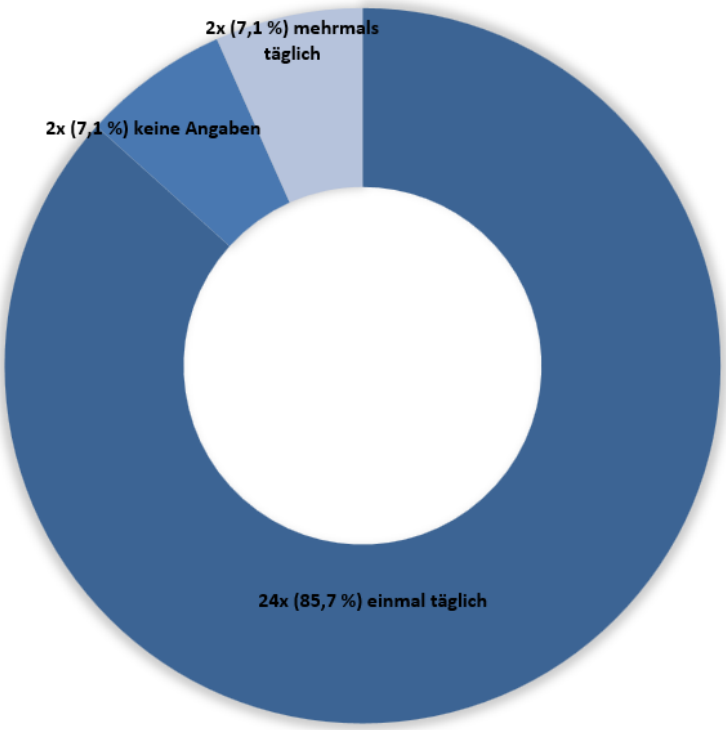
Frage: *Ist der Fernwartungszugang für die Lieferanten jederzeit nutzbar oder ist eine vorherige Absprache und/das die manuelle Aktivierung des Fernwartungszugangs erforderlich bzw. was ist künftig geplant?* (Mehrfachantworten möglich)




An elf der 28 Standorte ist ein jederzeitiger Zugriff mittels Fernwartung möglich, bei sechs Standorten ist eine vorherige telefonische Abstimmung erforderlich, bi zwei Leitstellen ist die vorherige telefonische Abstimmung geplant. An weiteren elf Standorten ist neben der telefonischen Absprache ein aktives Stecken bzw. Schalten der Verbindung erforderlich. I.d.R. ist hierbei auch vereinbart, dass der Lieferant sich nach Beendigung des Fernzugriffs abermals telefonisch meldet, so dass die Verbindung wieder deaktiviert werden kann. Dies stellt eine wichtige Schutzmaßnahme gegen unbefugte Systemzugriffe über den Fernwartungszugang dar. Z.T. sind für die telefonische Absprache bestimmte Kennwörter vereinbart oder der Anruf muss von einer bestimmten Rufnummer (bekannte A-Teilnehmerkennung) aus erfolgen, damit eine Authentisierung des Anrufers möglich ist.

## A.35 Datensicherung

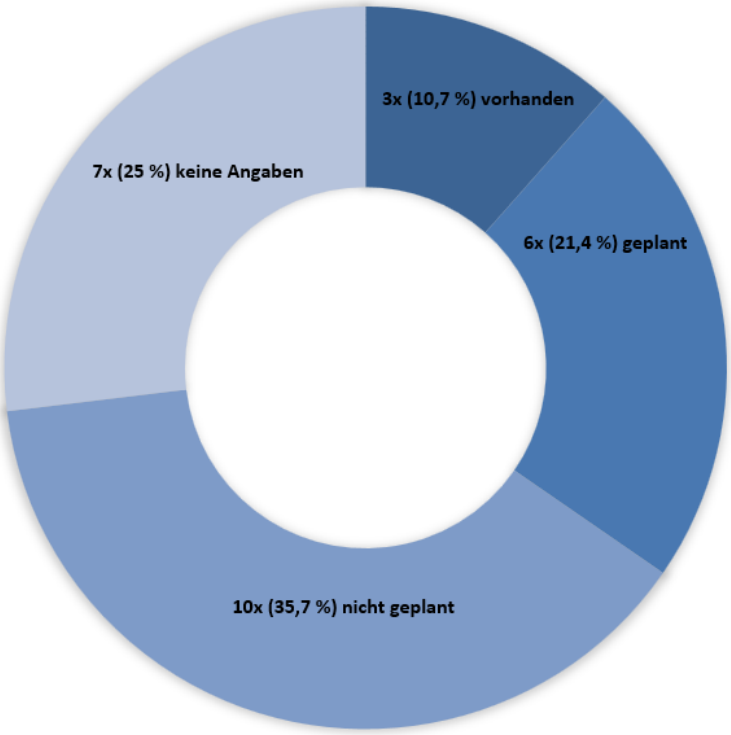
Frage: *In welchem Turnus findet die Datensicherung statt?*




Die Mehrzahl der Leitstellen (24 von 28) führt eine tägliche Datensicherung durch, bei zwei Standorten sogar mehrmals täglich. Von zwei Leitstellen liegen keine Angaben zur Häufigkeit der Datensicherung vor.

## A.36 Verschlüsselung KMS

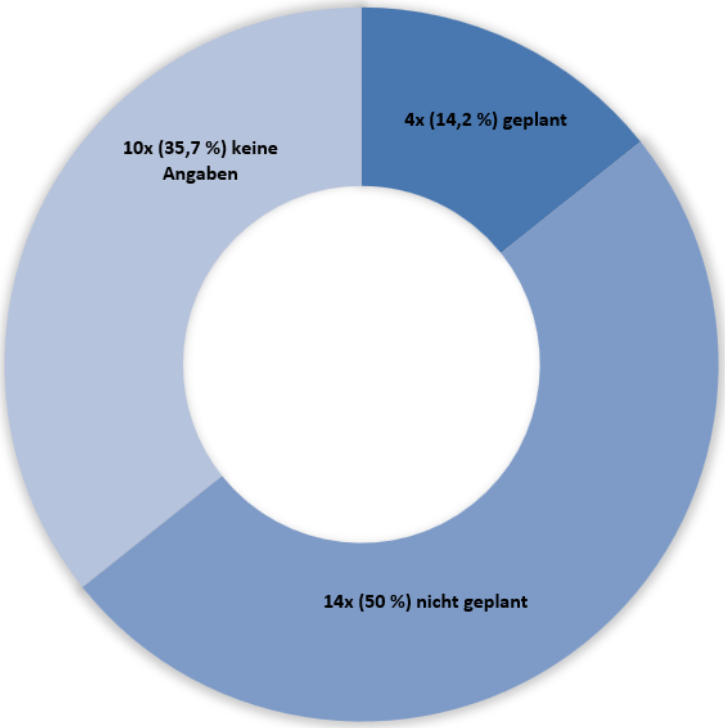
Frage: *Werden die Daten des KMS verschlüsselt gespeichert?*




Lediglich bei drei von 28 Standorten findet eine verschlüsselte Datenspeicherung statt, bei sechs Leitstellen ist dies geplant. Bei zehn Leitstellen ist keine verschlüsselte Speicherung der KMS-Daten geplant, von sieben Leitstellenstandorten liegen keine Angaben vor. Die damit verbundene Frage nach dem vorhandenen bzw. geplanten Verschlüsselungsverfahren wurde in keinem Fall beantwortet, so dass hierzu keine Informationen vorliegen.

## A.37 Verschlüsselung ELS

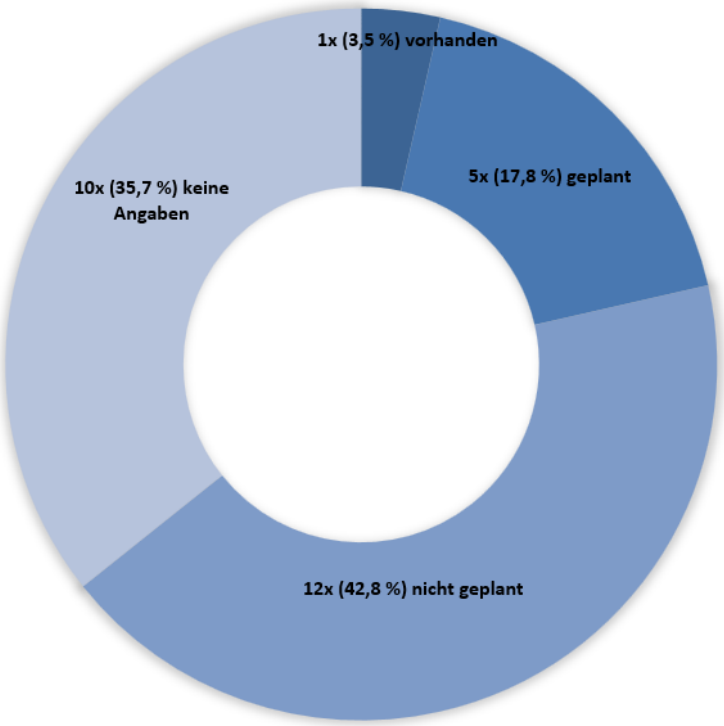
Frage: *Werden die Daten des ELS verschlüsselt gespeichert?*




Die Daten des Einsatzleitsystems werden derzeit in keiner Leitstelle verschlüsselt gespeichert; 4 Standorte haben rückgemeldet, dass dies geplant ist. Bei 14 Leitstellen ist dies nicht geplant, von 10 Standorten wurde keine Angaben gemacht.

## A.38 Verschlüsselung Doku

Frage: *Werden die Daten des Dokumentationssystems verschlüsselt gespeichert?*

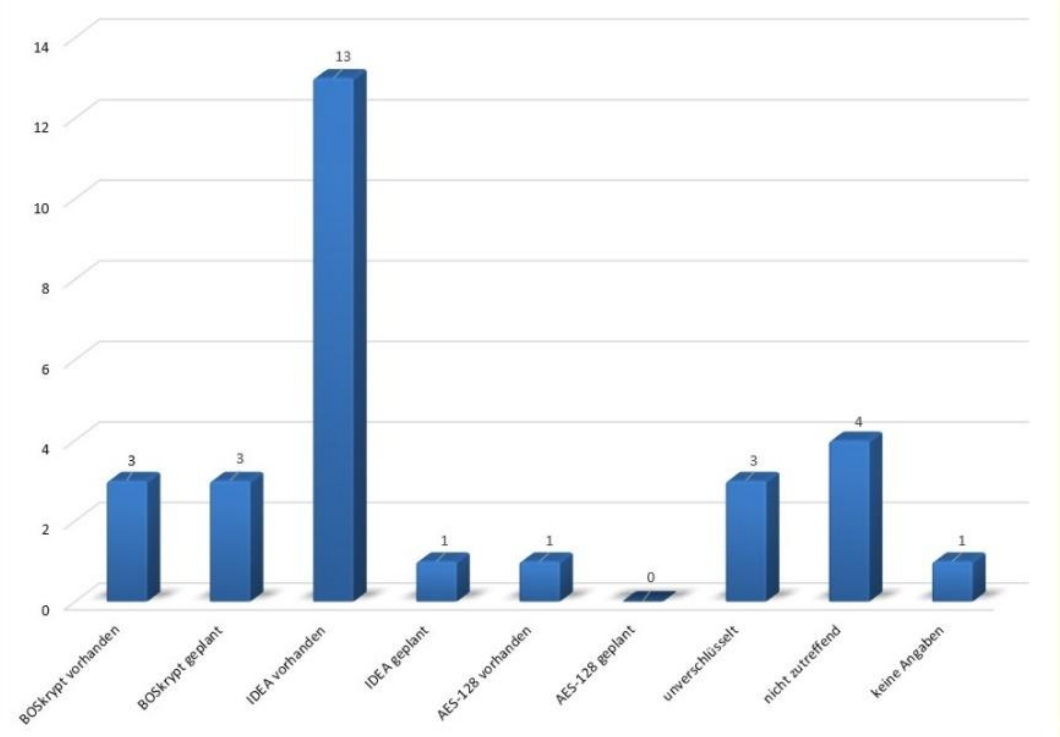



Die Daten des Dokumentationssystems werden in einem Fall verschlüsselt gespeichert, bei fünf Standorten ist dies geplant; 12 Leitstellen haben mitgeteilt, dass dies nicht geplant sei. Von zehn Standorten liegen keine Rückmeldungen vor. Das Dokumentationssystem als Ablage der aufgezeichneten Sprachdaten der Notrufe und des Funkverkehrs (z.T. auch der gesamten Telefonie, je nach landesrechtlicher Regelung) ist hinsichtlich des Datenschutzes einer der sensibelsten Bereiche einer Leitstelle, da es als Archiv das gesprochene Wort sämtlicher Anrufer des Notrufs enthält, einschließlich der begleitenden Metadaten. Zusammen mit den Einsatzdaten und dem zugehörigen Zeitstempel (z.B. Zeitpunkt des Ausrückens und der Ankunft an der Einsatzstelle) sind hier Informationen abgelegt, die ein hohes Potenzial für missbräuchliche Verwendung bieten. Der Zugang zu den Daten des Dokumentationssystems ist daher auf einen begrenzten Personenkreis reduziert; Auszüge für staatsanwaltschaftliche Ermittlungen können oftmals nur nach dem 4-Augen-Prinzip mit zwei berechtigten Nutzern (Leitstellenleitung, Administrator) erstellt werden. Hinsichtlich der Vertraulichkeit von Notrufgesprächen hat es in Deutschland

bereits mehrere Vorfälle gegeben, bei denen Notrufe als Videoclip aufbereitet auf der Plattform „Youtube“ gelandet sind.

## A.39 Verschlüsselung Digitalalarm

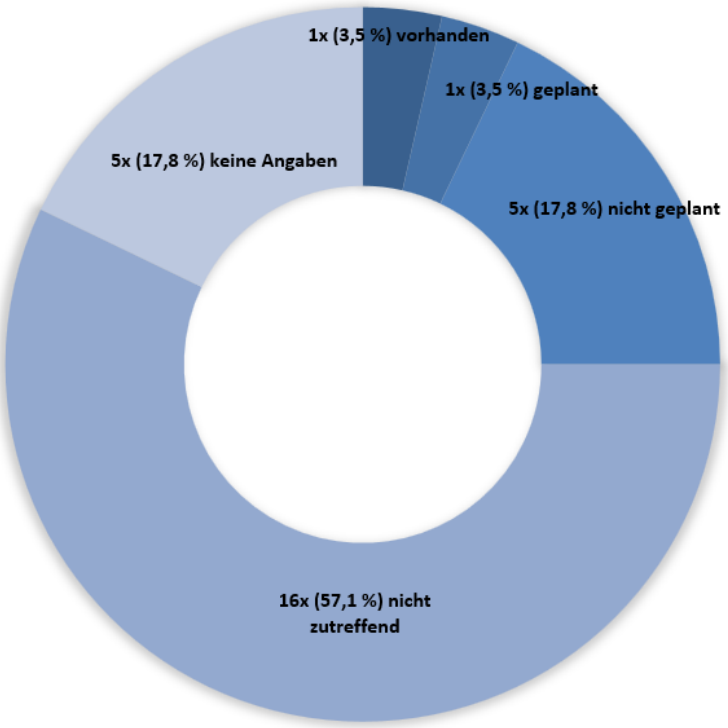
Frage: *Wird die Datenübertragung bei der Digitalen Alarmierung verschlüsselt? Wenn ja, mit welchem Verfahren?* (Mehrfachantworten möglich)




Von den 28 rückmeldenden Leitstellen haben 13 geantwortet, dass IDEA zur Verschlüsselung des Digitalalarm eingesetzt wird, bei drei Standorten wird BOSkrypt verwendet, ein weiterer Standort verwendet eine AES-Verschlüsselung mit 128 Bit. An drei Standorten erfolgt eine unverschlüsselte Übertragung. Wechsel sind geplant; in drei Fällen der Wechsel zu BOSkrypt und in einem Fall zu IDEA. Von vier Leitstellen erfolgte die Rückmeldung, dass diese Anforderung nicht zutrifft (anderes Alarmierungsverfahren oder gar keine Alarmierung, z.B. reine Polizeileitstelle). In einem Fall wurden keine Angaben gemacht.

## A.40 Verschlüsselung Wachalarm

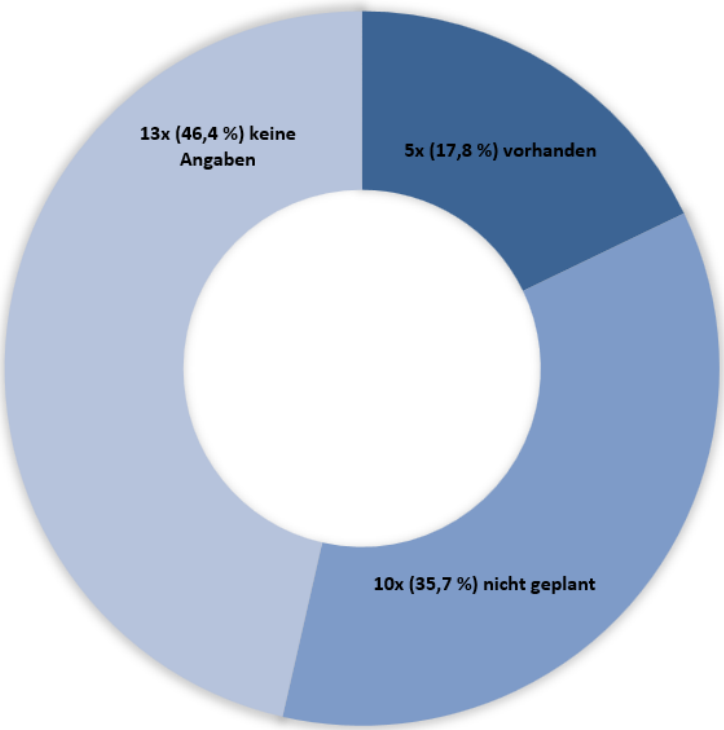
Frage: *Wird die Datenübertragung beim Wachalarm verschlüsselt?*




Die Verschlüsselung bei der Übertragung des Wachalarms trifft ausschließlich Berufsfeuerwehren bzw. Feuerwehr- und Rettungsdienststandorte, bei denen die Alarmierung nicht nur mittels Meldeempfängern, sondern durch ein Wachalarmsystem erfolgt, sowie die zugehörigen Leitstellen. Dies spiegelt sich in den Rückmeldungen wider; 16 Standorte gaben an, dass das Thema für sie nicht zutrifft, an sieben Leitstellenstandorten gehört auch die Ansteuerung von Wachalarmtechnik zu dem Alarmierungsmöglichkeiten. Von diesen sieben Leitstellen wird bei einer die Wachalarmsteuerung verschlüsselt übertragen, bei einer weiteren ist dies in Planung, bei weiteren fünf Leitstellen ist derzeit nicht geplant. In fünf Fällen erfolgten keine Angaben.

## A.41 Verschlüsselung abgesetzte Arbeitsplätze

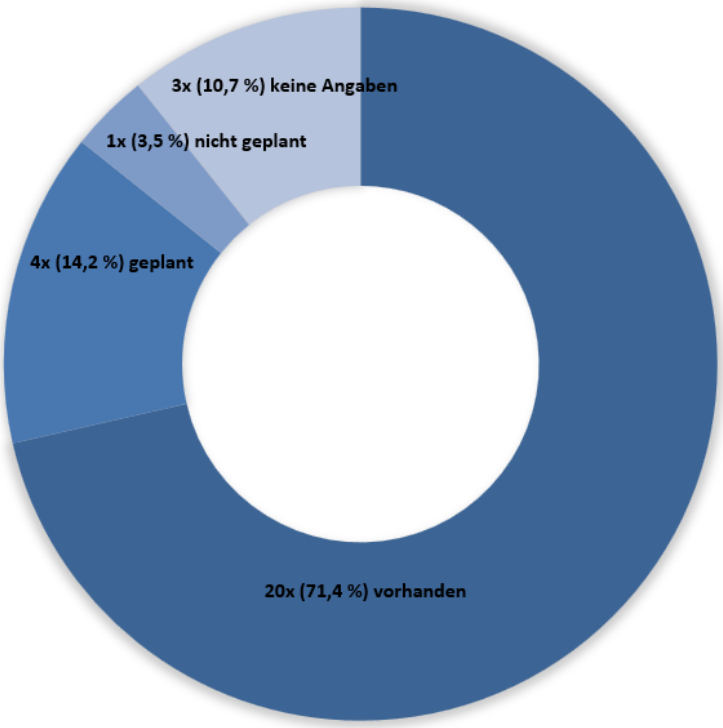
Frage: *Wird die Anbindung abgesetzter Arbeitsplätze verschlüsselt?*




Abgesetzte Leitstellenarbeitsplätze befinden sich räumlich getrennt von der eigentlichen Leitstelle und müssen daher über eine Datenverbindung an die Leitstelle angebunden werden. Die Einbindung externer Plätze erfordert entsprechende Sicherheitsmaßnahmen, damit über die Schnittstellen des Hauptsystem keine Kompromittierung möglich ist. Eine Verschlüsslung kommt allerdings nicht durchgängig zur Anwendung, diese ist in lediglich fünf Fällen vorhanden. Zehn Leitstellen haben keine Verschlüsselung bei der Anbindung abgesetzter Arbeitsplätze geplant und 13 Standorte machten hierzu keine Angaben.

## A.42 Sperren USB-Ports

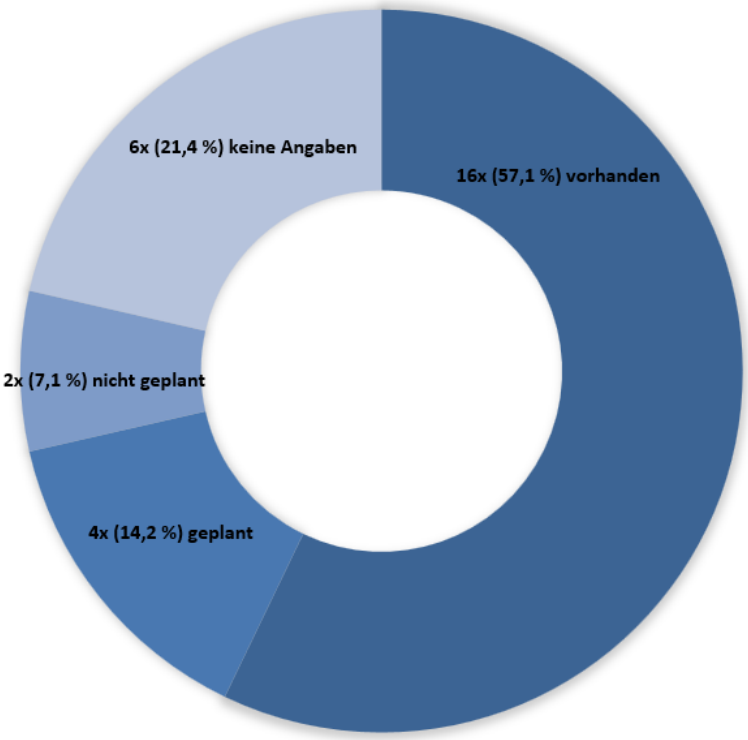
Frage: *Sind die USB-Ports an den Arbeitsplatzrechnern und den Servern gesperrt?*




Das Sperren der USB-Ports an den Arbeitsplatz-PCs ist bei 20 Leitstellen (71,4 %) gelebte Praxis; bei 4 Standorten (14,2 %) ist dies geplant und in einem Fall wurde geantwortet, dass dies nicht geplant ist (3,5 %). In drei Fällen (10,7 %) erfolgte hierzu keine Antwort.

## A.43 Port-Security

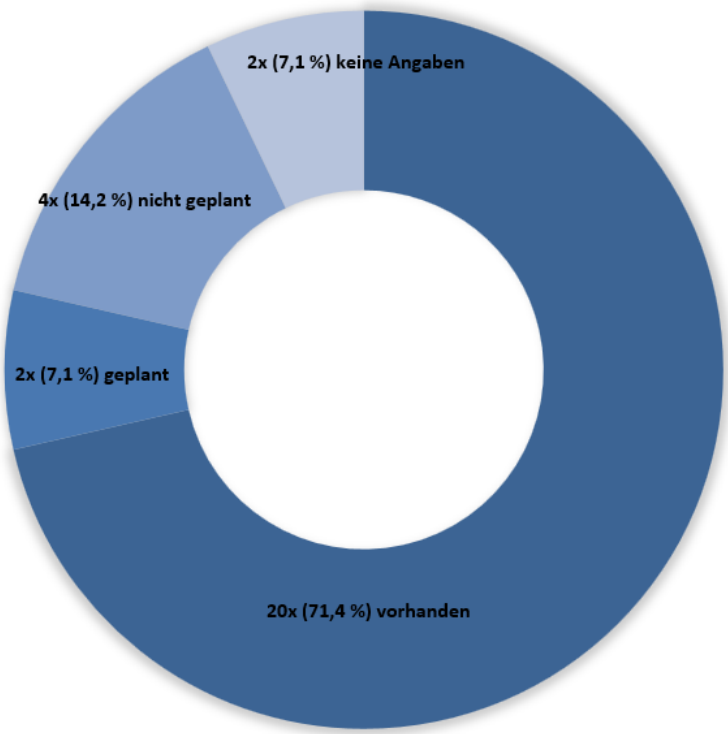
Frage: *Wird Port-Security in den Netzwerkswitchen eingesetzt?*




Port-Security, d.h. die feste Zuordnung der Switch-Schnittstellen mit einer oder mehrerer MAC-Adressen als Whitelist, ist in der Mehrzahl der Leitstellen (16 von 28) vorhanden. Bei vier Standorten ist dies geplant; bei zwei Leitstellen ist keine Port-Security vorgehen. Sechs Leitstellenstandorte machten keine Angaben.

## A.44 Kiosk-Modus

Frage: *Werden die Arbeitsplatz-PCs im Kiosk-Modus betrieben?*

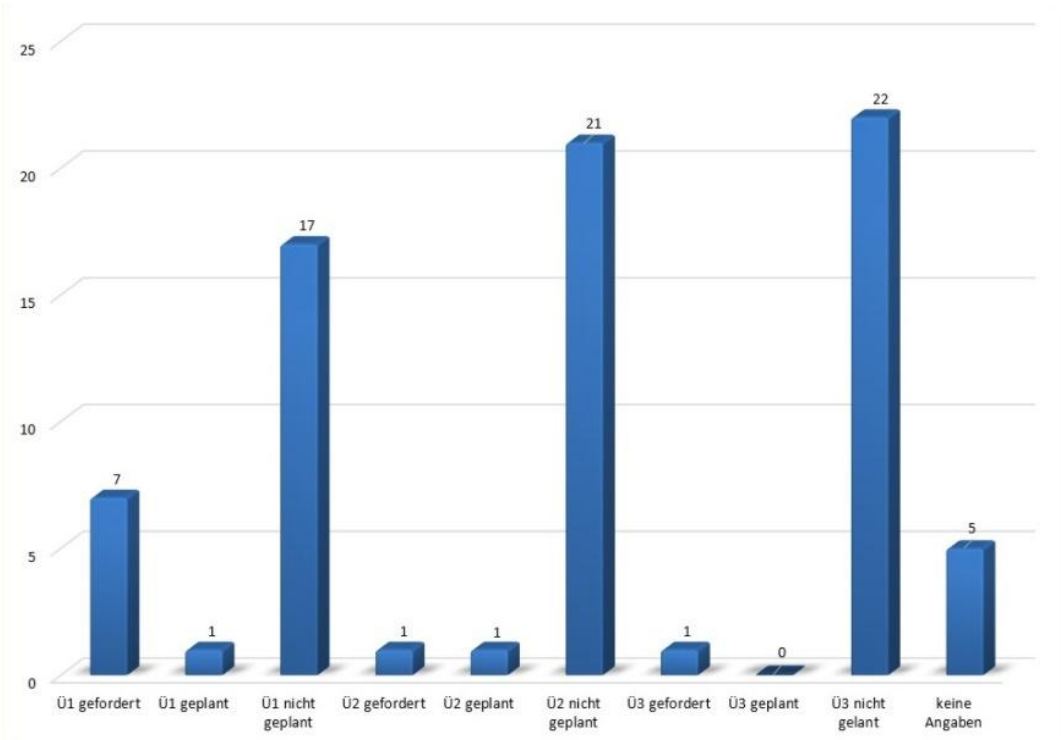



Der Kiosk-Modus ist ein Betriebsmodus zur öffentlichen Nutzung von PCs, z.B. in Internet-Cafés, wobei nur die Anwendungen (Browser, Office) für den Nutzer zugänglich sind, jedoch kein Zugriff auf die Systemsteuerung oder gar Administrationsrechte für Systemeinstellungen, Installation neuer Software möglich sind. Damit lassen sich bewusste Manipulationen und auch unbewusste Veränderungen vermeiden. Für die Arbeitsplatzrechner einer Leitstelle kommt dieser Betriebsart ebenfalls eine wichtige Bedeutung zu, damit sich die Anwender (Disponenten) nur innerhalb der Anwendungssoftware bewegen können, jedoch keinen Zugriff auf die Betriebssystemebene haben. Dies ist unabhängig vom Rollen- und Rechtemanagement, da es sich beim Kiosk-Modus um eine Zugangsbeschränkung zur Systemsteuerung des lokalen Arbeitsplatzrechners handelt, nicht um die Rechte (Schreiben, Lesen) der Anwendungssoftware.

In der Mehrzahl der Leitstellen (20 von 28) findet der Kiosk-Modus Anwendung, bei zwei weiteren ist der Einsatz geplant. An vier Standorten wird kein Kiosk-Modus eingesetzt und ist auch nicht geplant; zwei Standorte machten keine Angaben.

## A.45 Sicherheitsüberprüfung Disponenten

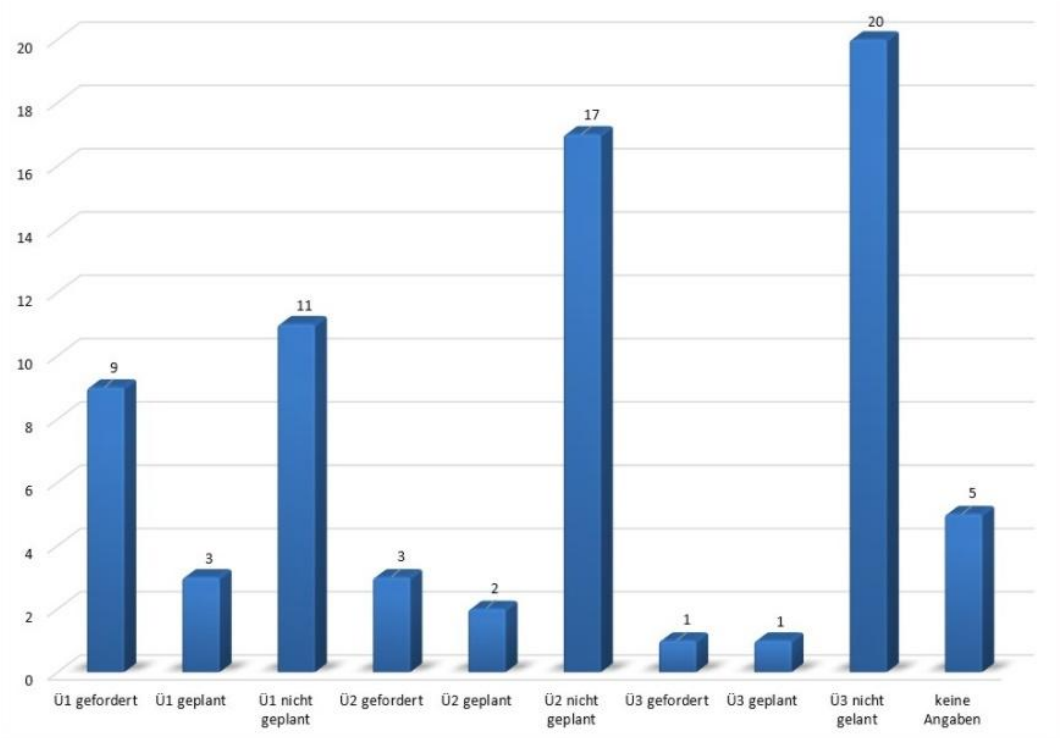
Frage: *Müssen sich die Disponenten einer Sicherheitsüberprüfung (SÜ) unterziehen? Wenn ja, welche Stufe?* (Mehrfachantworten möglich)




Die *einfache Sicherheitsüberprüfung* (Ü1) wird bei sieben von 28 Leitstellen gefordert (25 %). Die höheren Stufen *erweiterte Sicherheitsüberprüfung* (Ü2) bzw. *erweiterte Sicherheitsüberprüfung mit Sicherheitsermittlungen* (Ü3) werden in jeweils einem Fall verlangt. Mehrheitlich sind keine Sicherheitsüberprüfungen geplant; Planungen bzgl. Ü1 wurden in 17 Fällen, Ü2 in 21 Fällen und Ü3 in 22 Fällen verneint. Fünf Leitstellen machten keine Angaben zur Sicherheitsüberprüfung für Disponenten.

## A.46 Sicherheitsüberprüfung Administratoren

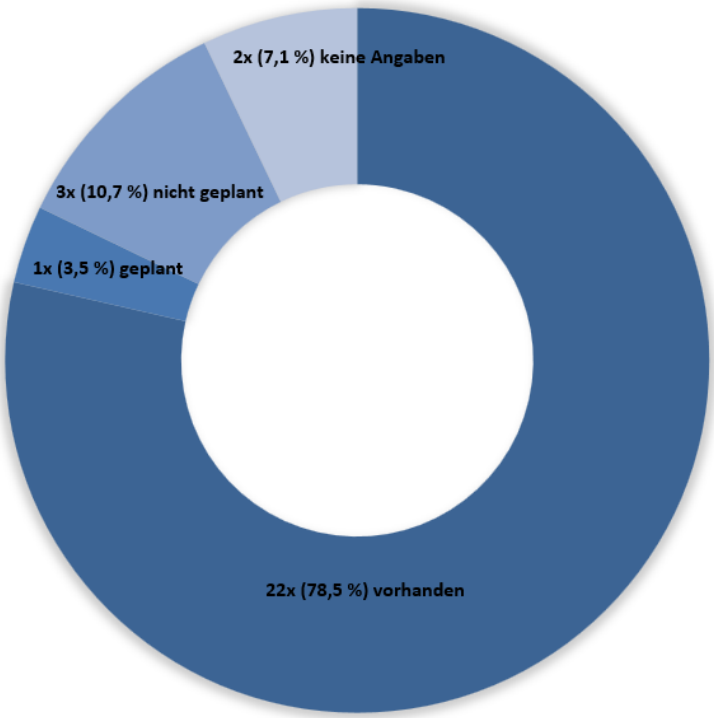
Frage: *Müssen sich die Administratoren einer Sicherheitsüberprüfung (SÜ) unterziehen? Wenn ja, welche Stufe?* (Mehrfachantworten möglich)




Bei der Sicherheitsüberprüfung für Administratoren ergibt sich ein geringfügig anderes Bild, als bei den Disponenten, auch wenn der Trend identisch ist: Ü1 wird derzeit in neun Fällen von den Administratoren verlangt, Ü2 in drei Fällen und Ü3 in einem Fall. Geplant ist die Einführung von Ü1 in drei Fällen, Ü2 bei zwei Leitstellen und Ü3 bei einer Leitstelle. Nicht geplant sind Ü1 in elf Fällen, Ü2 in 17 Fällen und Ü3 in 20 von 28 Fällen. Fünf Standorte machten keine Angaben zur Sicherheitsüberprüfung für Administratoren.

## A.47 Rollen- und Rechte-Konzepte

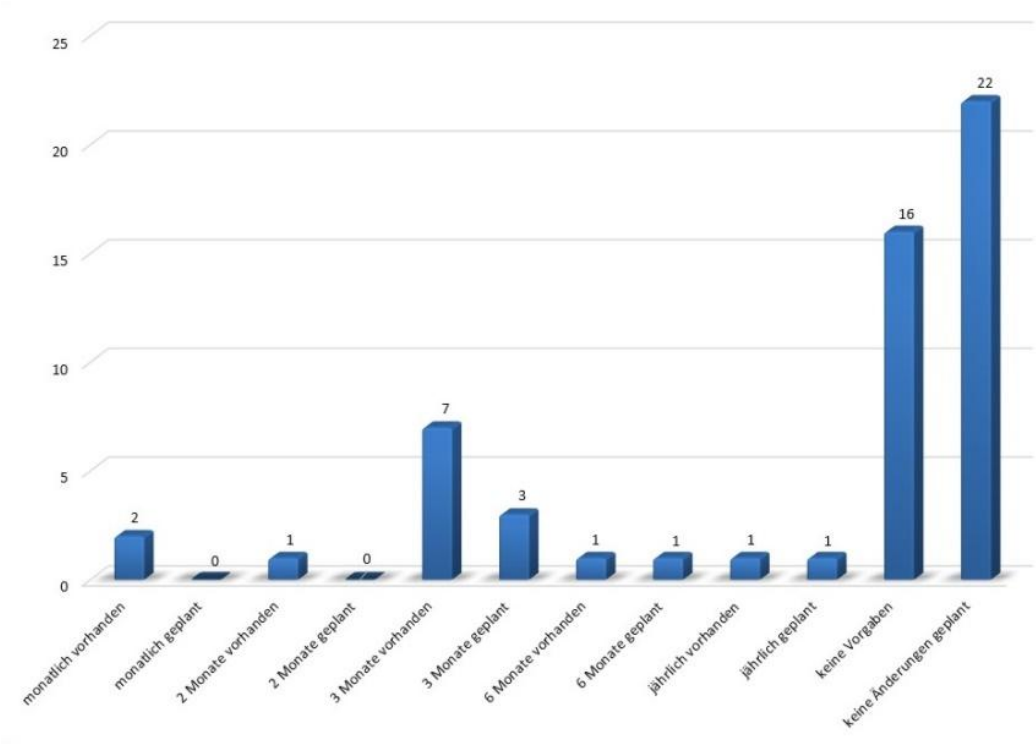
Frage: *Existieren getrennte Rollen- und Rechte-Konzepte für die unterschiedlichen Nutzer (Disponenten, Schichtleiter, Datenpfleger, Administratoren, ...)?*




In der Mehrzahl der Fälle (22 von 28) sind Rollen und Rechte je nach Aufgabe zugeteilt; in einem Fall ist dies geplant. Drei Leitstellen haben und planen kein Rollen- und Rechte-Konzept, zwei Standorte machten keine Angaben hierzu.

## A.48 Passwörter der Disponenten – Wechsel turnusmäßig

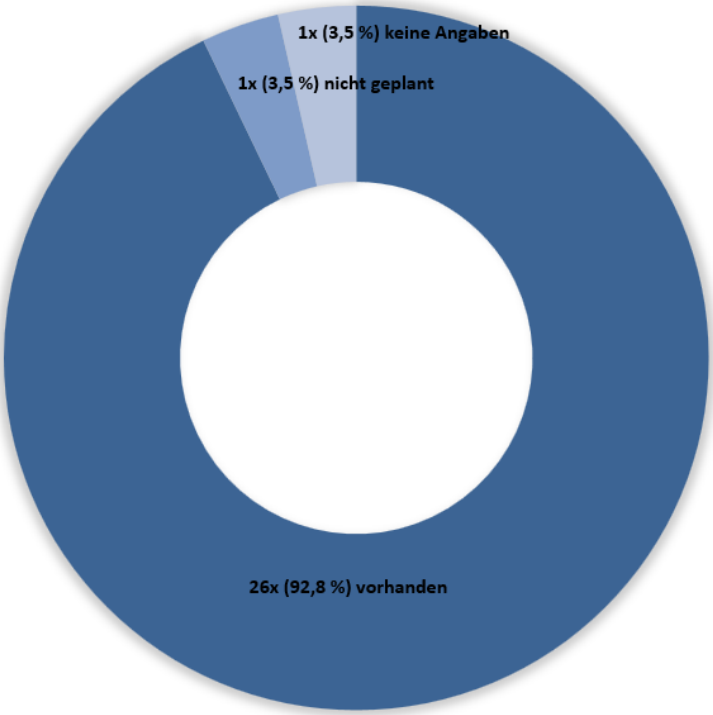
Frage: *Werden die Passwörter der Disponenten regelmäßig gewechselt? Wenn ja, in welchem Turnus?* (Mehrfachantworten möglich)




Ein Maximum ergibt sich bei sieben von 28 Leitstellen (25 %), bei denen ein Passwortwechsel für die Disponenten alle drei Monate stattfindet. In zwei Fällen wird der Passwortwechsel monatlich durchgeführt, in jeweils einem Fall alle zwei, alles sechs bzw. alle 12 Monate. Bei 16 der 28 Leitstellen gibt es keine Vorgaben zum turnusmäßigen Passwortwechsel; 22 Standorte haben darüber hinaus keine Änderungen des bestehenden Zustandes geplant.

## A.49 Passwörter der Disponenten – Wechsel bei Ausscheiden

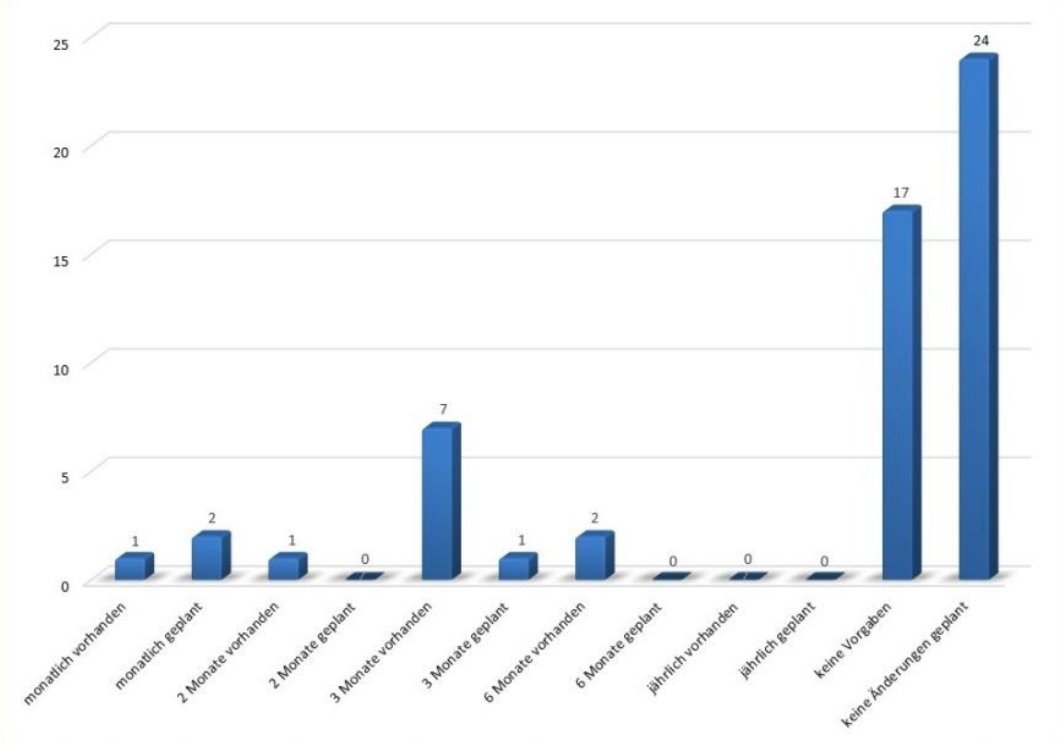
Frage: *Werden die Passwörter der Disponenten bei Ausscheiden gewechselt bzw. deaktiviert?*




Passwörter der Disponenten werden in 26 von 28 Leitstellen bei Ausscheiden deaktiviert. In jeweils einem Fall ist dies nicht gegeben und auch nicht geplant bzw. es wurden keine Angaben hierzu gemacht.

## A.50 Passwörter der Administratoren – Wechsel turnusmäßig

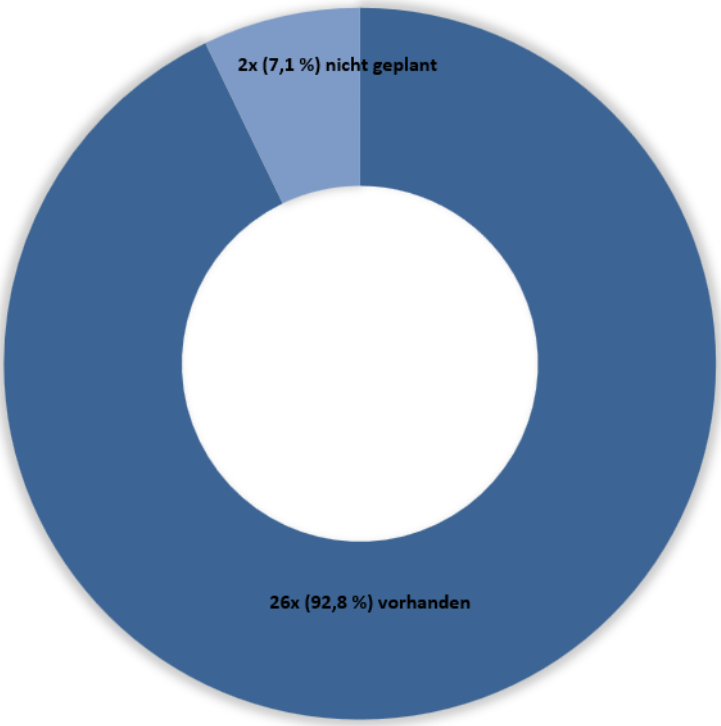
Frage: *Werden die Passwörter der Administratoren regelmäßig gewechselt? Wenn ja, in welchem Turnus?* (Mehrfachantworten möglich)




Die Passwörter de Administratoren werden in der Mehrzahl der Fälle (7 von 28, 25 %) alle drei Monate gewechselt. Wechsel im Turnus von einem, zwei oder drei Monaten finden in jeweils einem Fall statt; in jeweils zwei Fällen auch in einem sechsmonatigen Turnus. Zwei Standorte planen die Verkürzung auf einen monatlichen Turnus, einer der Standorte mit sechsmonatigem Turnus plant eine Verkürzung auf drei Monate. Bei 24 Standorten sind keine Änderungen des Ist-Standes geplant, 17 Leitstellen gaben an, dass es keine Vorgaben zum turnusmäßigen Passwortwechsel gibt und dieser daher auch nicht stattfindet.

## A.51 Passwörter der Administratoren – Wechsel bei Ausscheiden

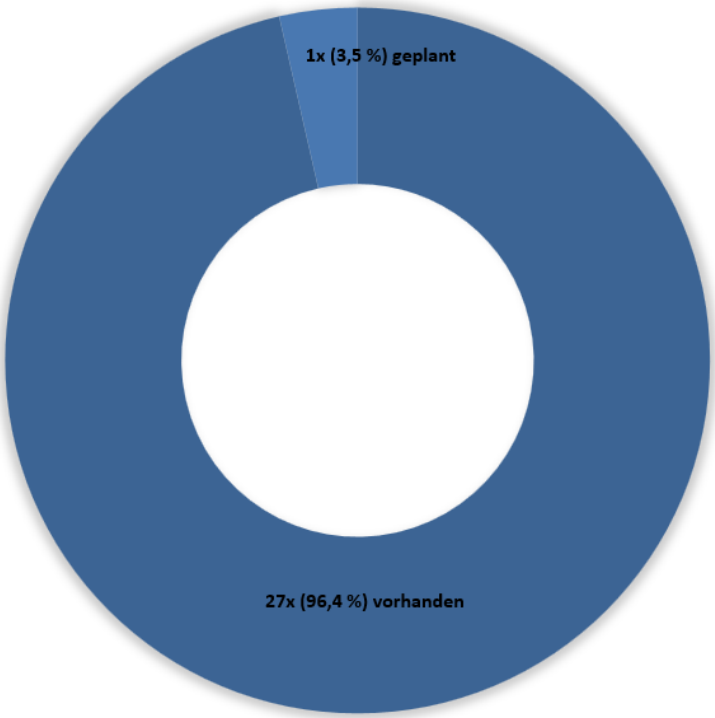
Frage: *Werden die Passwörter der Administratoren bei Ausscheiden gewechselt bzw. deaktiviert?*




Die Passwörter de Administratoren werden in 26 von 28 Leitstellen bei Ausscheiden gelöscht; lediglich an zwei Standorten erfolgt dies nicht und ist auch nicht geplant.

## A.52 Schulung Rückfallebenen

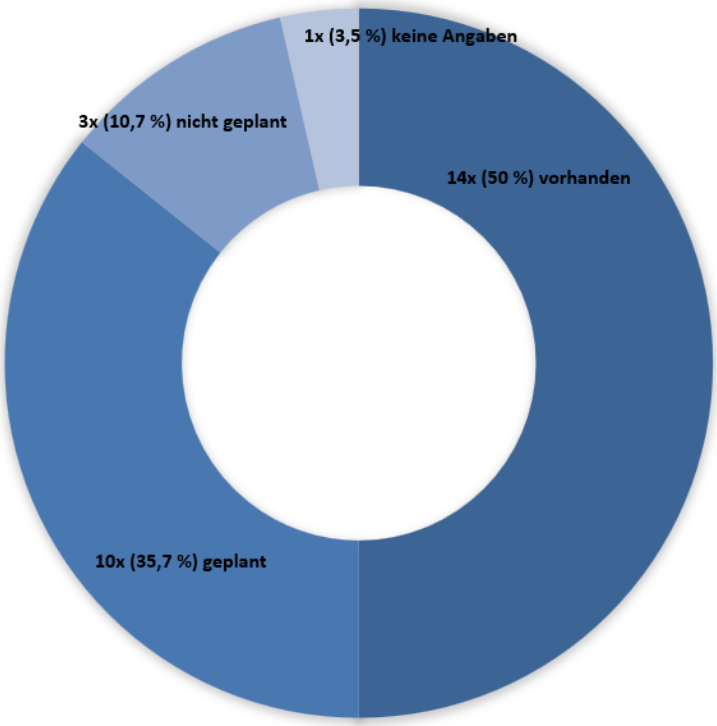
Frage: *Werden die Disponenten in der Nutzung der Rückfallebenen geschult?*




An 27 der 28 Leitstellenstandorte (96,4 %) finden Schulungen zur Nutzung der Rückfallebenen im Falle einer technischen Störung statt, an einem Standort ist dies nicht gegeben, aber geplant.

## A.53 Schulung Informationssicherheit

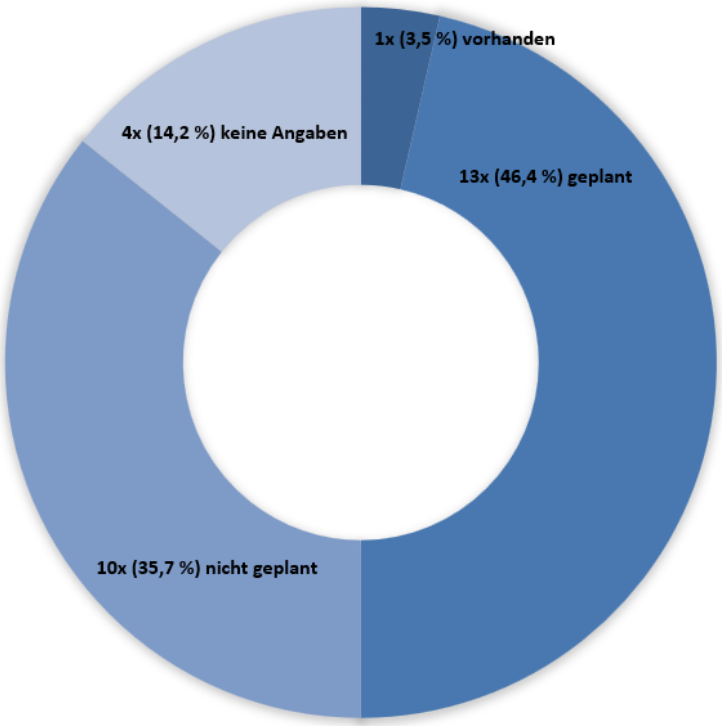
Frage: *Werden die Mitarbeiter hinsichtlich Informationssicherheit geschult?*




Bei der Hälfte der rückmeldenden Leitstellen (14 von 28) werden die Mitarbeiter hinsichtlich Informationssicherheit geschult, bei zehn Standorten ist dies in Planung, bei drei Standorten nicht geplant und in einem Fall erfolgten keine Angaben.

## A.54 Schulung IT-Grundschutz

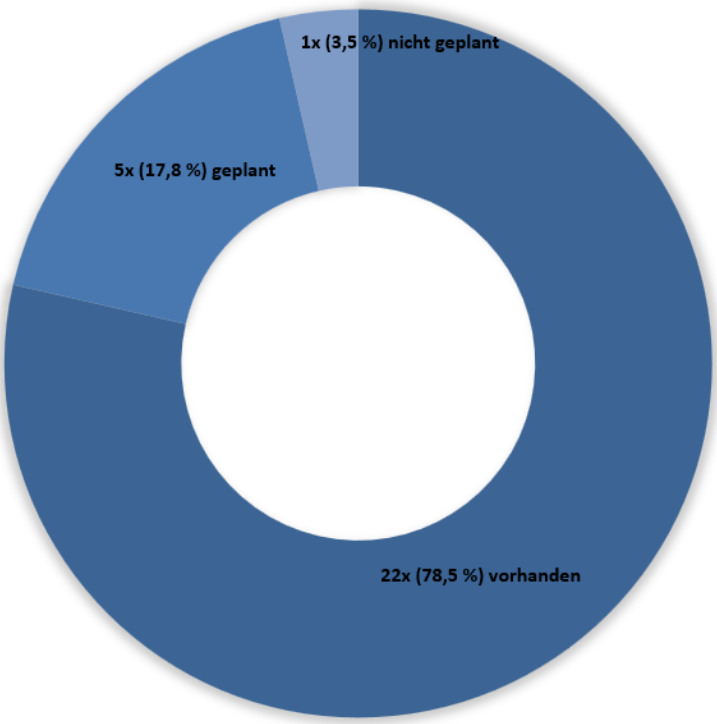
Frage: *Werden die Mitarbeiter zum IT-Grundschutz geschult?*




Schulungen der Mitarbeiter zum IT-Grundschutz sind nur in einem Fall vorhanden, bei 13 der 28 rückmeldenden Leitstellen ist dies geplant, bei zehn Standorten nicht geplant und von vier Standorten liegen keine Rückmeldungen hierzu vor.

## A.55 Schulung Notfallkonzept

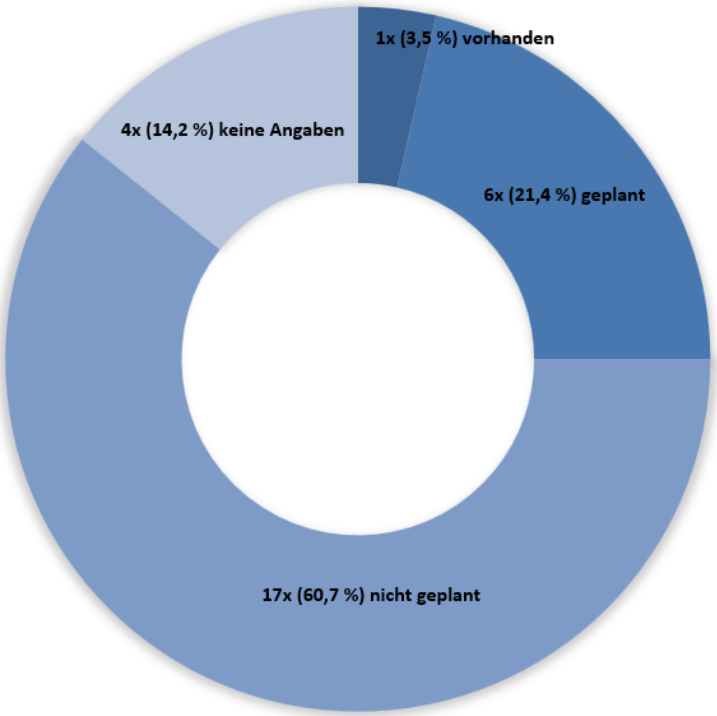
Frage: *Werden die Mitarbeiter zum Notfallkonzept geschult?*




Schulungen zum Notfallkonzept sind in 22 von 28 Leitstellen gegeben sowie an fünf Standorten in Planung befindlich. Eine Leitstelle gibt an, dass Schulungen zum Notfallkonzept nicht geplant sind.

## A.56 Schulung ITIL

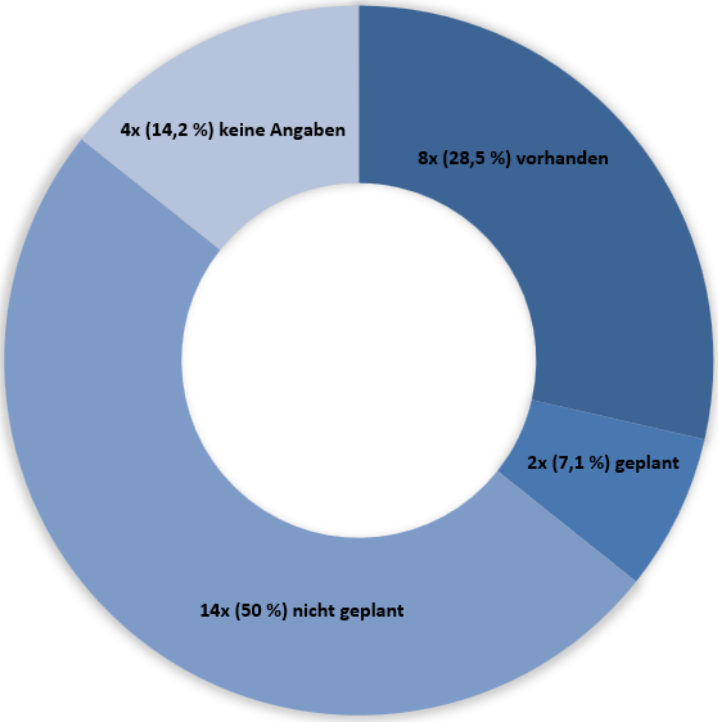
Frage: *Werden die Mitarbeiter in ITIL geschult?*




ITIL kommt nicht allen Leitstellen zur Anwendung (siehe A.101), dies ist bei der Einordnung der Antworten zu berücksichtigen. Nur bei einer Leitstelle finden ITIL-Schulungen für die Mitarbeiter statt, in sechs weiteren Leitstellen ist dies in Planung. An 17 Standorten sind keine ITIL-Schulungen geplant, vier Standorte machten hierzu keine Angaben.

## A.57 Sicherheitsaudits

Frage: *Finden regelmäßig Audits zur IT-Sicherheit statt?*




Sicherheitsaudits finden in acht der 28 Leitstellen statt, bei zwei weiteren ist dies geplant. An 14 Standorten bestehen keine derartigen Planungen; vier Leitstellen machten keine Angaben.

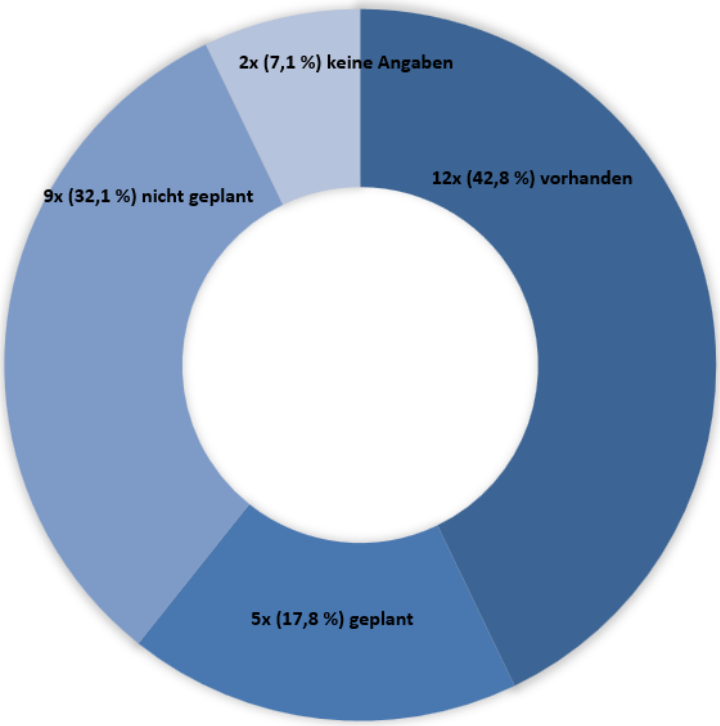
## A.58 Turnus der Audits

Frage: *In welchem Turnus finden die Audits zur IT-Sicherheit statt?*


Von den acht Standorten, an denen Sicherheitsaudits stattfinden (siehe 3.58) finden an einem Standort die Audits in dreimonatigem Turnus statt, bei vier Leitstellen im 12-monatigen Turnus und bei einer weiteren Leitstelle alle 24 Monate. An einem Standort gibt es keinen festen Turnus; ein Standort machte keine Angaben zum Turnus der Sicherheitsaudits.

## A.59 Vier-Augen-Prinzip

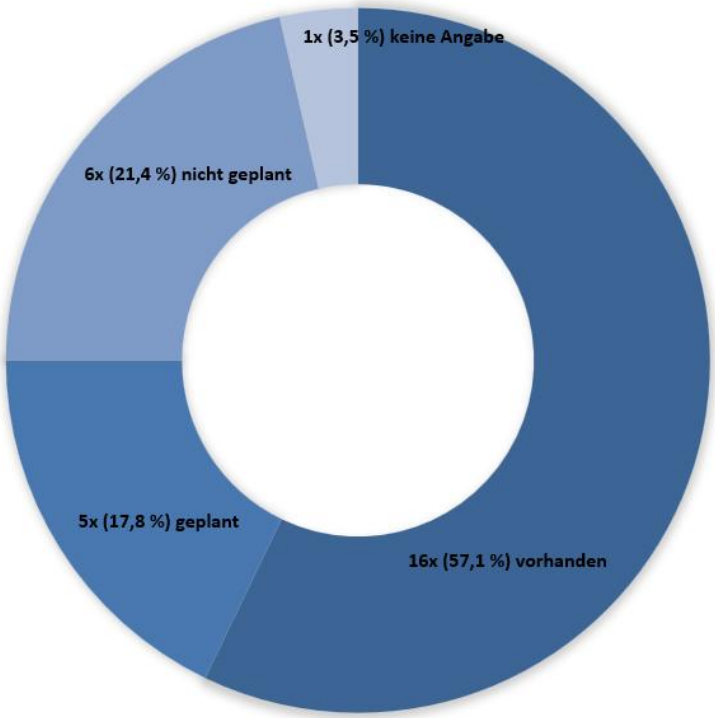
Frage: *Wir bei grundlegenden Systemänderungen das Vier-Augen-Prinzip angewendet?*




In 12 der 28 Leitstellen kommt das Vier-Augen-Prinzip zum Tragen, bei fünf Leitstellen ist es geplant. Neun Standorte meldeten, dass kein Vier-Augen-Prinzip geplant ist; zwei Leitstellen machten keine Angaben.

## A.60 Dokumentation Gebäudezugang

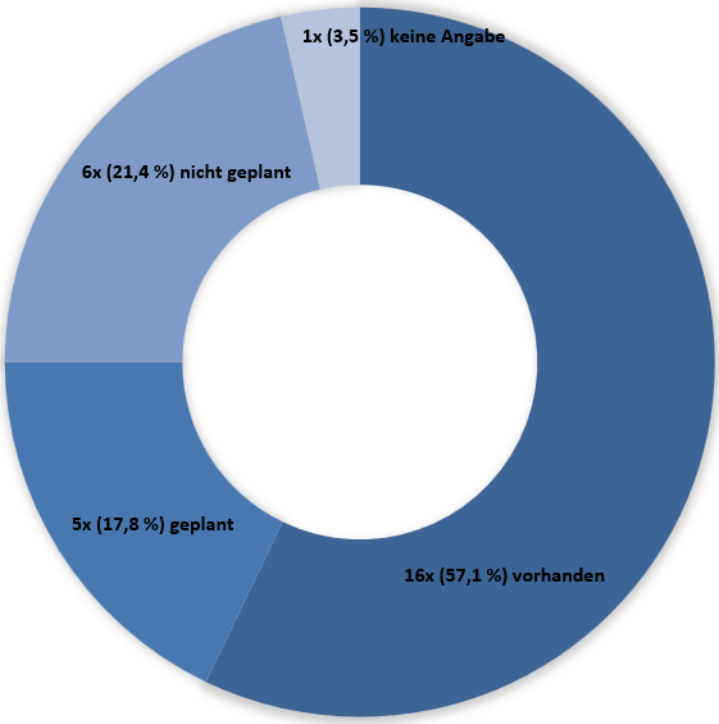
Frage: *Wird der Zugang zum Gebäude dokumentiert?*




Bei 16 der 28 Leitstellen wird der Zugang zum Gebäude dokumentiert (eigenes Personal und Fremdpersonen), bei fünf weiteren ist dies in Planung. Bei sechs Standorten ist dies nicht vorgesehen, ein Standort machten keine Angaben.

## A.61 Dokumentation Zugang Leitstellenbereich

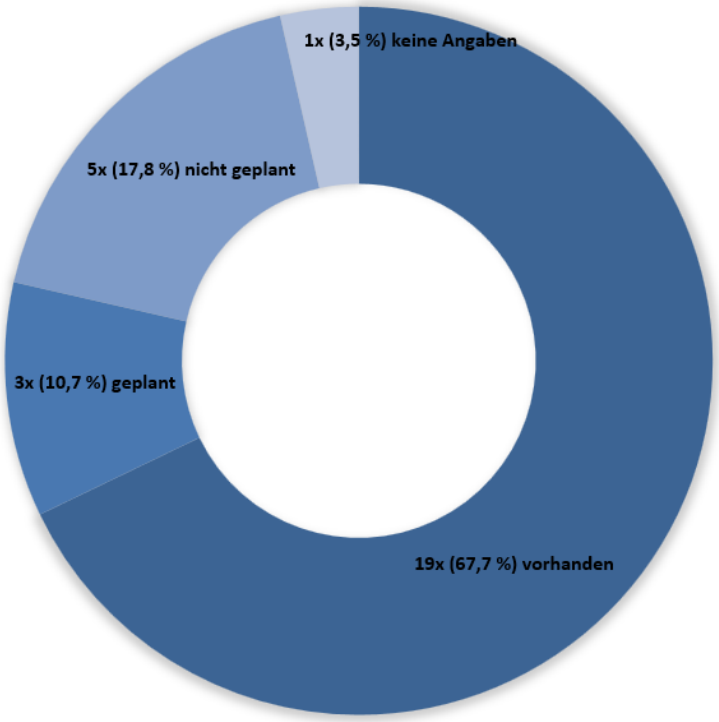
Frage: *Wird der Zugang zum Leitstellenbereich dokumentiert?*




In Kombination mit der Dokumentation des Zugangs zum Gebäude (3.61) wird der Zugang zum Leitstellenbereich innerhalb der Liegenschaft bei 16 Standorten gesondert dokumentiert. Bei fünf Standorten ist dies geplant, bei weiten sechs Standorten bestehen keine Planungen. Eine Leitstelle machte keine Angaben.

## A.62 Dokumentation Zugang Technikraum

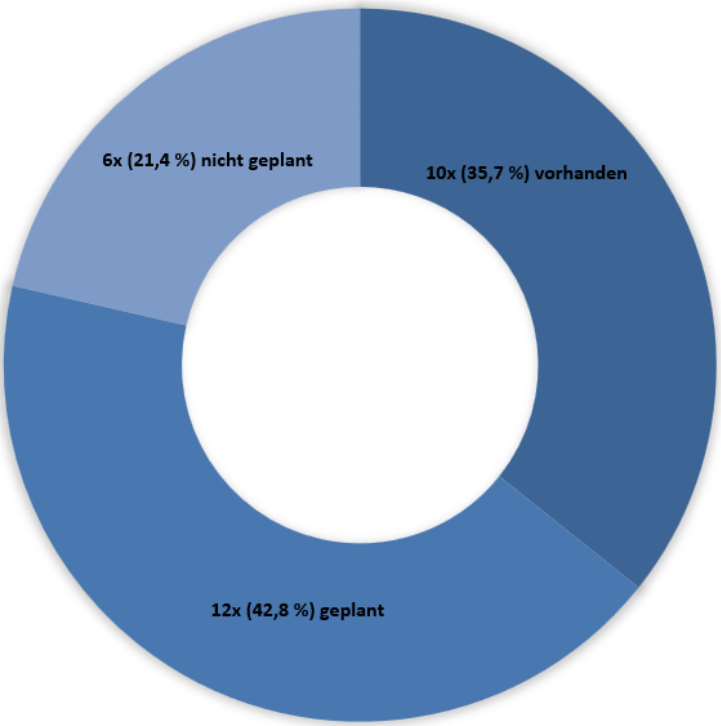
Frage: *Wird der Zugang zum Leitstellen-Technikraum dokumentiert?*




Der Zugang zum Technikraum wird bei 19 der 28 Leitstellen dokumentiert, bei drei weiteren Standorten ist dies geplant. Fünf Leitstellen meldeten, dass dies nicht geplant ist, in einem Fall wurden keine Angaben gemacht.

## A.63 Qualitätsmanagement

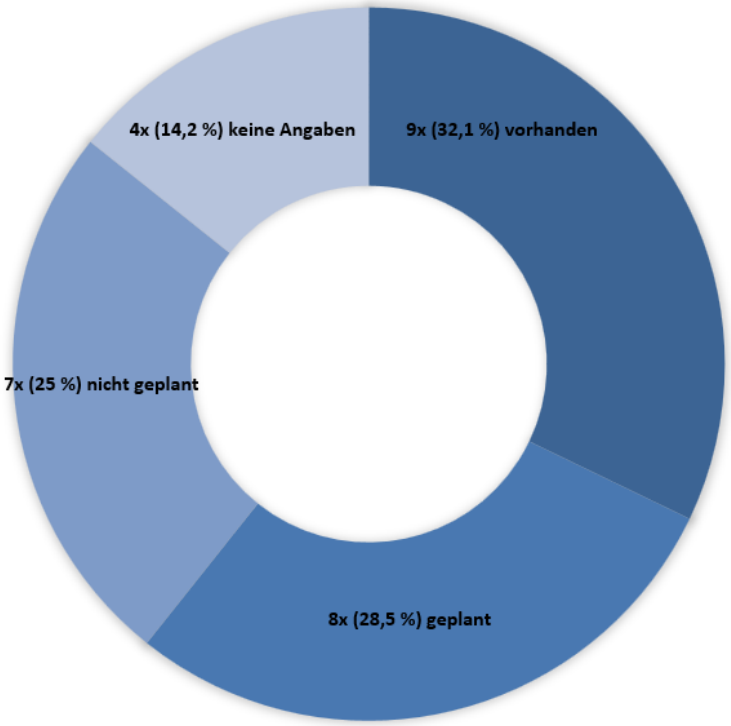
Frage: *Besteht ein eigenes Qualitätsmanagement für die Leitstelle?*




Bei zehn der 28 Leitstellen ist ein Qualitätsmanagement etabliert, bei 12 weiteren Standorten ist dies in Planung. Sechs Leitstellen meldeten, dass kein Qualitätsmanagement geplant ist.

## A.64 Fortschreibung QM-Handbuch

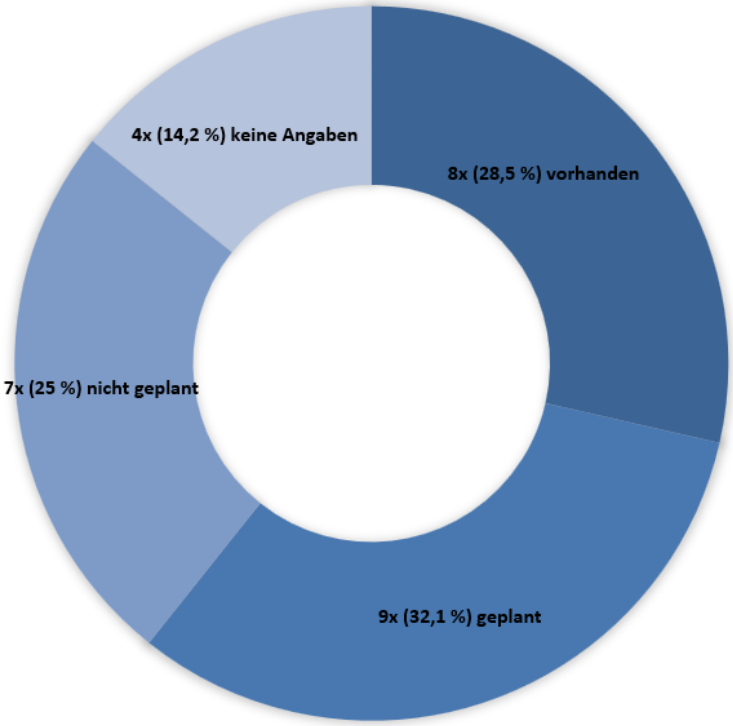
Frage: *Wird das QM-Handbuch regelmäßig fortgeschrieben?*




Von den Leitstellen, die Qualitätssicherung betreiben oder dies planen (siehe 3.64), findet an neun Standorten eine regelmäßige Fortschreibung des QM-Handbuches statt. Bei acht Standorten ist die Fortschreibung geplant (sofern auch die Einführung geplant ist, siehe 3.64). Sieben Standort planen keine Fortschreibung; in vier Fällen liegen keine Angaben vor.

## A.65 Störungen im QM-Handbuch enthalten

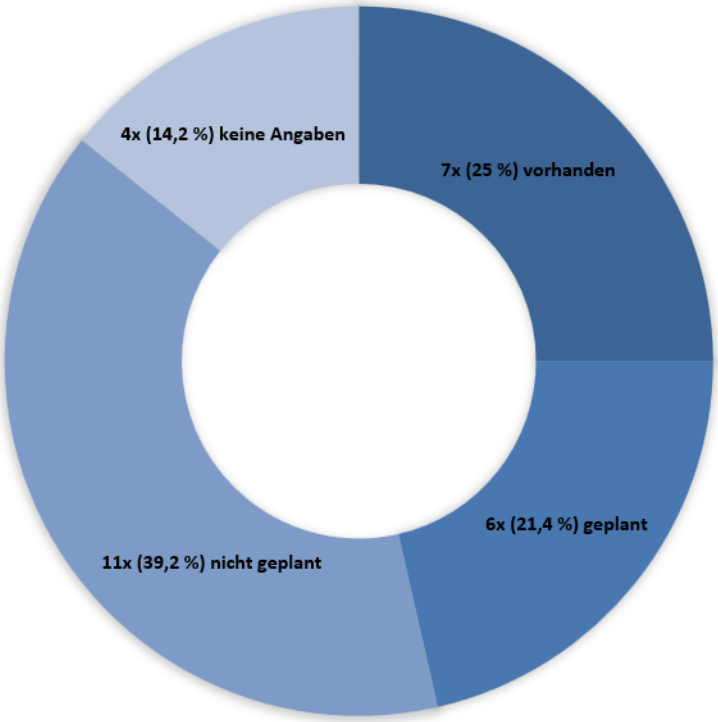
Frage: *Sind technische Störungen Bestandteil des QM-Handbuches?*




Bei acht Leitstellen sind technische Störungen und deren Behebung Bestandteil des QM-Handbuches, bei neun Standorten ist geplant, dies ins QM-Handbuch mit aufzunehmen. Sieben Leitstellen sehen dies nicht vor, vier Standorte machten keine Angaben. Die Anzahl der Rückmeldungen deckt sich exakt mit Zahlen des vorigen Punktes A.65 bzgl. Fortschreibung des QM-Handbuches.

## A.66 Zertifizierung nach ISO 9001

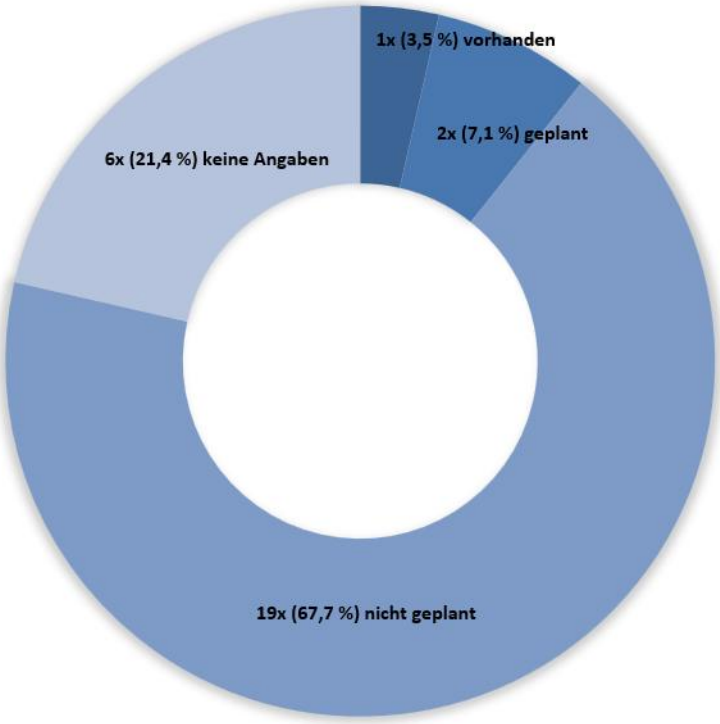
Frage: *Ist Ihre Leitstelle nach ISO 9001 zertifiziert?*




Sieben der 28 Leitstellen (25 %) sind nach ISO 9001 zertifiziert [Bau17], bei sechs Leitstellen ist die Zertifizierung geplant. Elf Standorte haben keine Zertifizierung geplant; vier Standorte machten keine Angaben.

## A.67 Zertifizierung nach DIN 15224

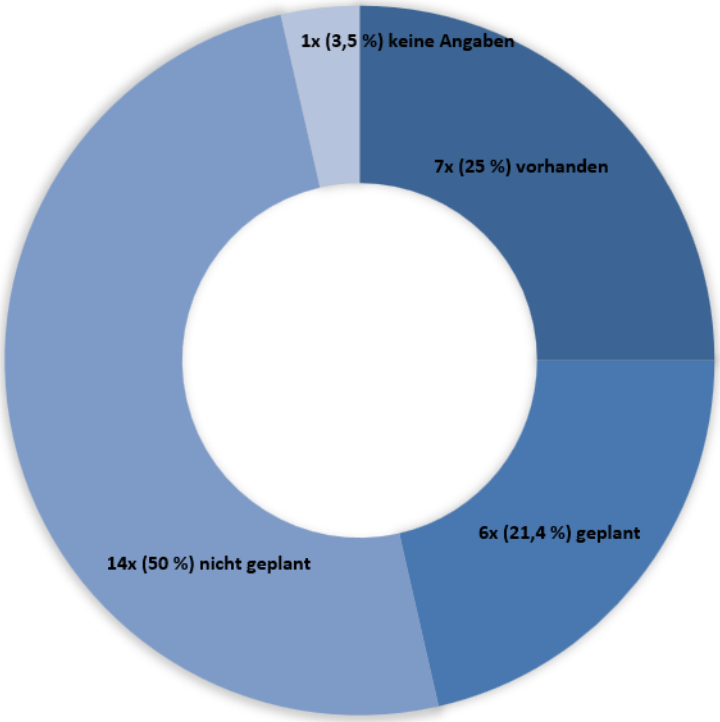
Frage: *Ist Ihre Leitstelle nach DIN 15224 zertifiziert?*




Die Zertifizierung nach DIN 15224 (Qualitätsmanagement im Gesundheitswesen) betrifft ausschließlich Leitstellen der Notfallrettung und des Krankentransportes, d.h. auch Integrierte Leitstellen (Erläuterung siehe 2.2.5). Bei einer der 28 Leitstellen liegt eine Zertifizierung nach DIN 15224 vor, bei zwei weiteren Leitstellen ist dies geplant. Bei der Mehrzahl der Standorte (19 von 28) ist keine Zertifizierung nach DIN 15224 vorgesehen, sechs Standorte machten keinen Angaben.

## A.68 Reserveleitstelle

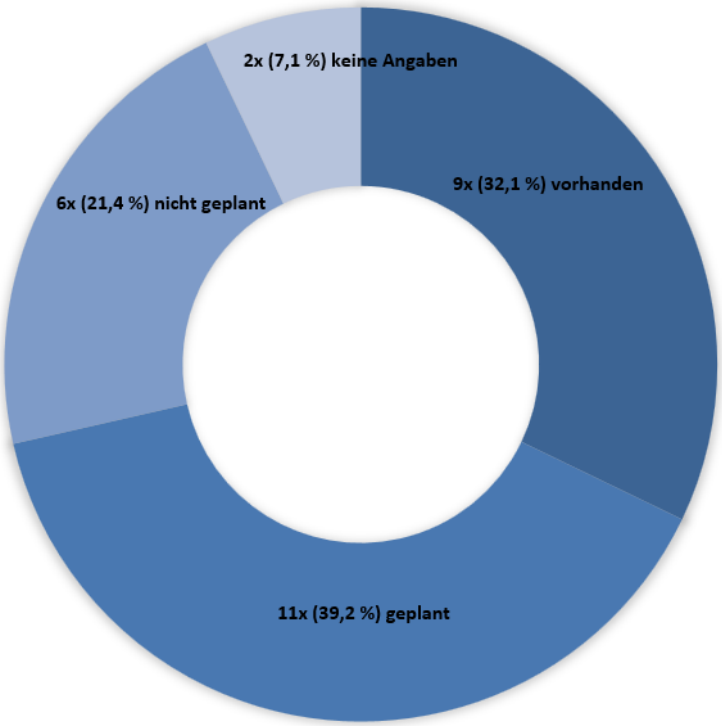
Frage: *Existiert eine unbemannte Reserveleitstelle, die bei Ausfall der „Hauptleitstelle“ genutzt werden kann?*




Ein Viertel der Zuständigkeitsbereiche der Leitstellen (7 von 28) verfügt über eine regulär unbemannte Reserveleitstelle, die im Bedarfsfall genutzt werden kann. Bei sechs Standorten ist eine Reserveleitstelle geplant. Bei der Hälfte der Leitstellen (14 von 28) ist keine unbemannte Reserveleitstelle geplant; ein Standort machte keine Angaben.

## A.69 Partnerleitstelle

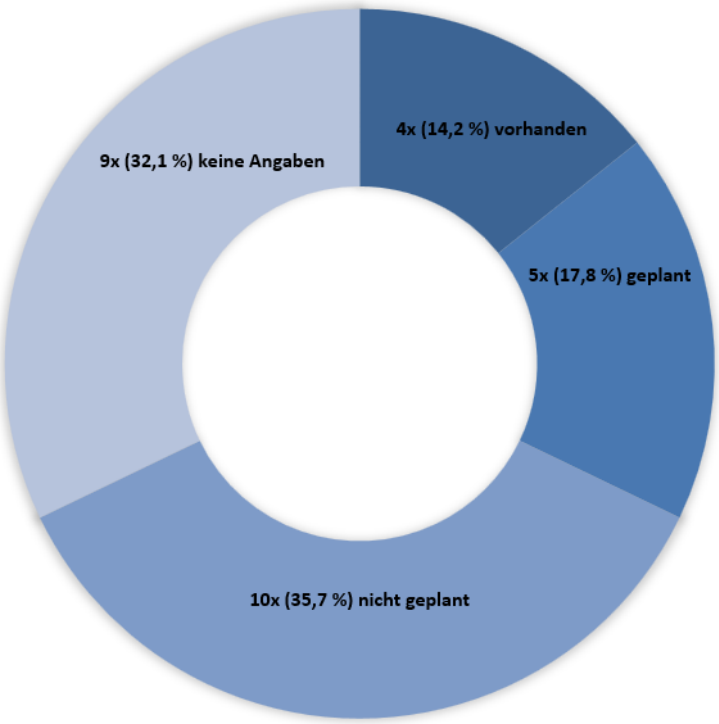
Frage: *Existiert eine Partnerleitstelle, die bei Ausfall der eigenen Leitstelle (mit)genutzt werden kann?*




Die Kooperation und technische Vernetzung mit einer Partnerleitstelle für den gegenseitigen Ausfallersatz und einer entsprechenden Anzahl an Reserveplätzen ist bei bzw. für neun Leitstellenstandorte vorhanden; bei elf Leitstellen ist dies geplant. Sechs Standorte sehen keine Partnerschaft mit einer anderen Leitstelle vor, zwei Leitstellen machten keine Angaben.

## A.70 andere Leitstelle

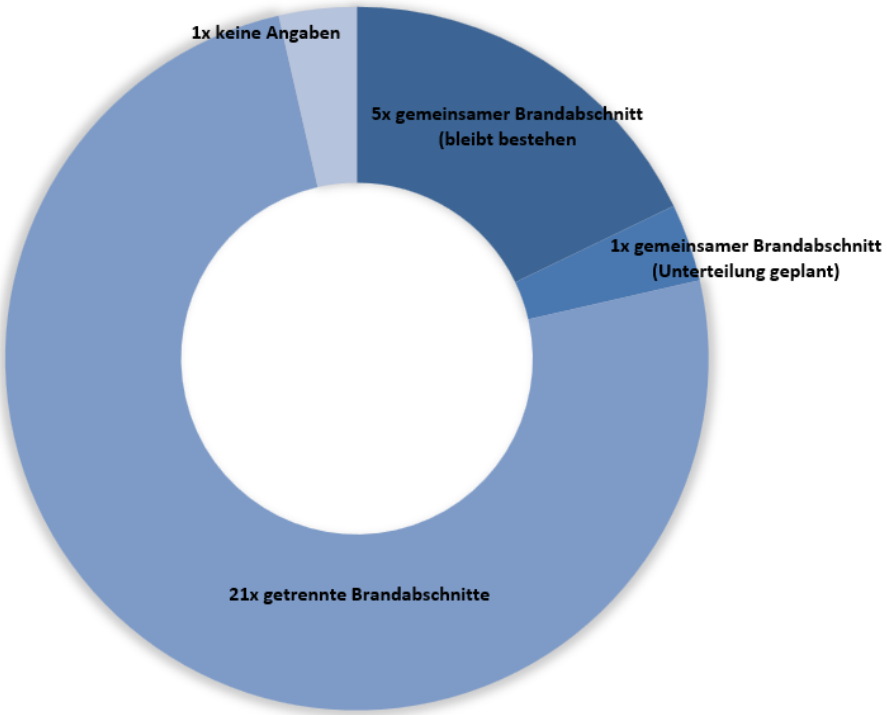
Frage: *Existiert eine andere Leitstelle, die bei einem Ausfall der eigenen Leitstelle den Dienstbetrieb mit ihrem eigenen Personal und eigener Technik vollständig übernehmen kann?*




Diese Form der Kooperation, den Ausfallersatz über die personellen und technischen Ressourcen einer anderen Leitstelle vollumfänglich sicherzustellen, ist in vier Fällen gegeben. Bei fünf Leitstellen ist dies in Planung, zehn Leitstellen sehen dies nicht vor. Neun Standorte machten keine Angaben.

## A.71 Brandabschnitte

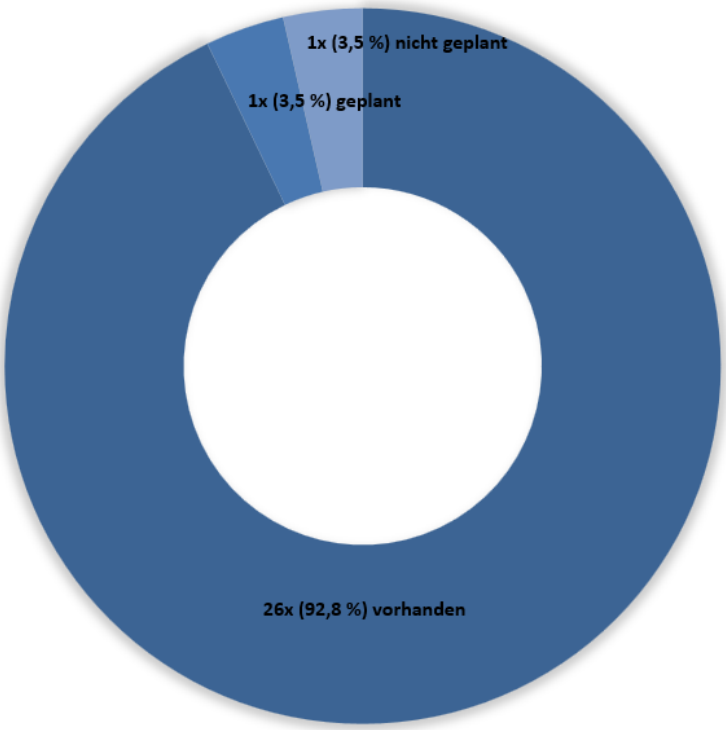
Frage: *Befinden sich der Leitstellenbetriebsraum und der Technikraum im gleichen Brandabschnitt oder in getrennten Brandabschnitten?*




Bei 21 der 28 Leitstellen befinden sich Betriebs- und Technikraum in getrennten Brandabschnitten, bei fünf Leitstellen sind beide Räume im gleichen Brandabschnitt untergebracht (Unterteilung nicht geplant), in einem Fall ist eine Aufteilung in zwei Brandabschnitte durch bauliche Maßnahmen geplant. Von einem Standort liegen keine Angaben vor.

## A.72 Brandmeldeüberwachung Betriebsraum

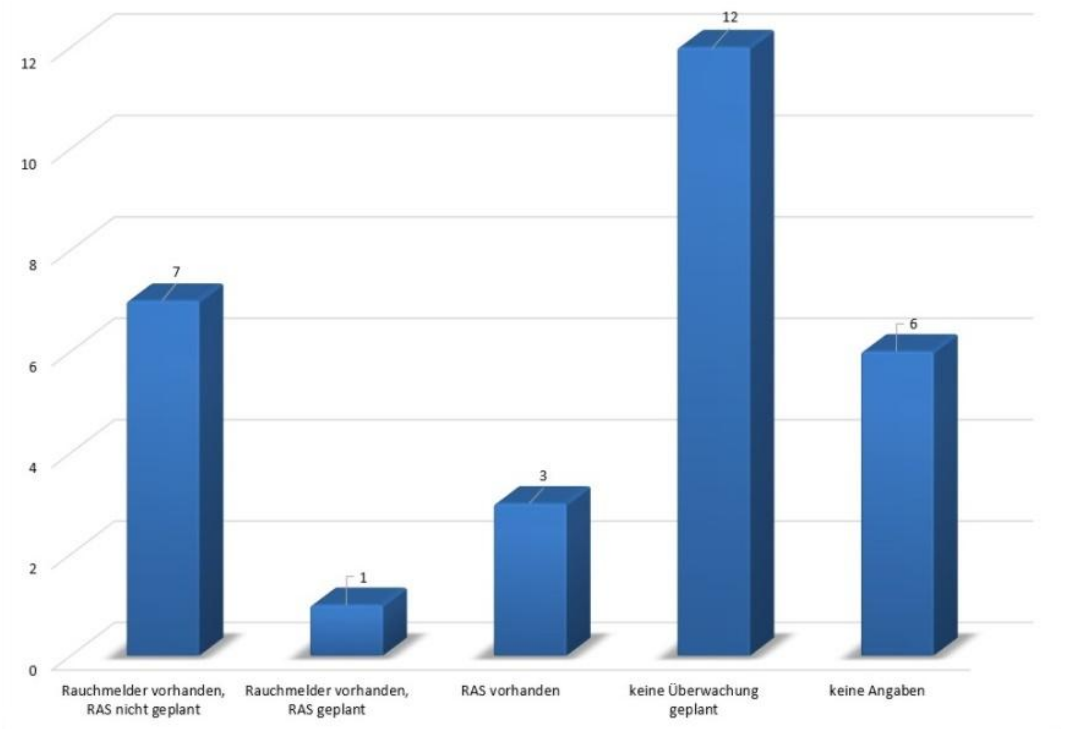
Frage: *Ist der Leitstellenbetriebsraum brandmelderüberwacht?*




Bei 26 der 28 Leitstellen (92,8 %) ist der Betriebsraum durch automatische Brandmelder überwacht, an einem Standort ist dies geplant; in einem Fall wurden keine Angaben zur Brandmeldeüberwachung gemacht.

## A.73 Brandmeldeüberwachung Technikraum/-schränke

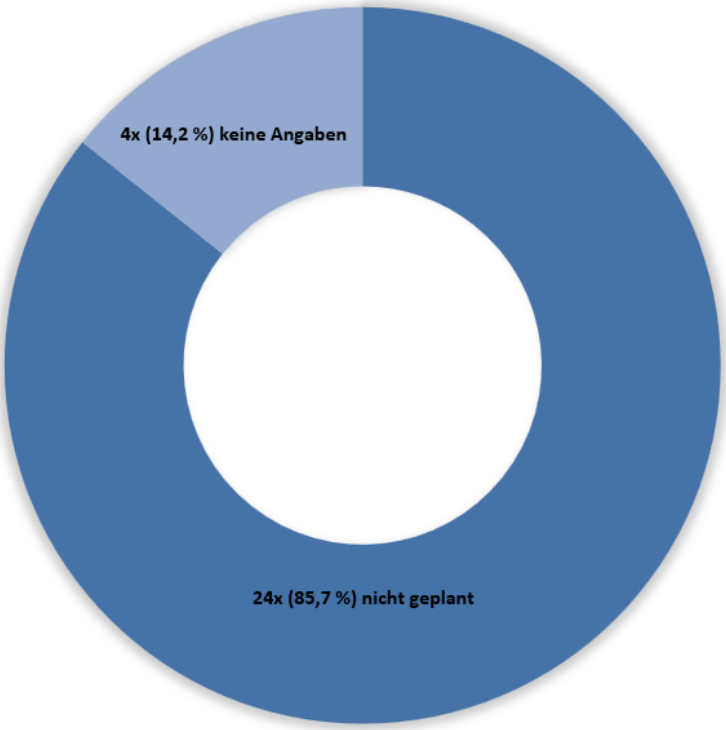
Frage: *Besteht im Technikraum bzw. in den Technikschränken eine Brandmeldeüberwachung?* (Mehrfachantworten möglich)




In sieben der 28 Leitstellen (25 %) wird der Technikraum mit Rauchmeldern überwacht, bei drei Leitstellen ist zusätzlich ein Rauchansaugsystem (RAS) in den Technikschränken vorhanden. Bei einem Standort ist ein RAS für die Überwachung der Schränke geplant. Bei 12 Leitstellen ist keine Brandmeldeüberwachung im Technikraum vorhanden bzw. geplant; sechs Standorte machten keine Angaben hierzu.

## A.74 Löschanlage Betriebsraum

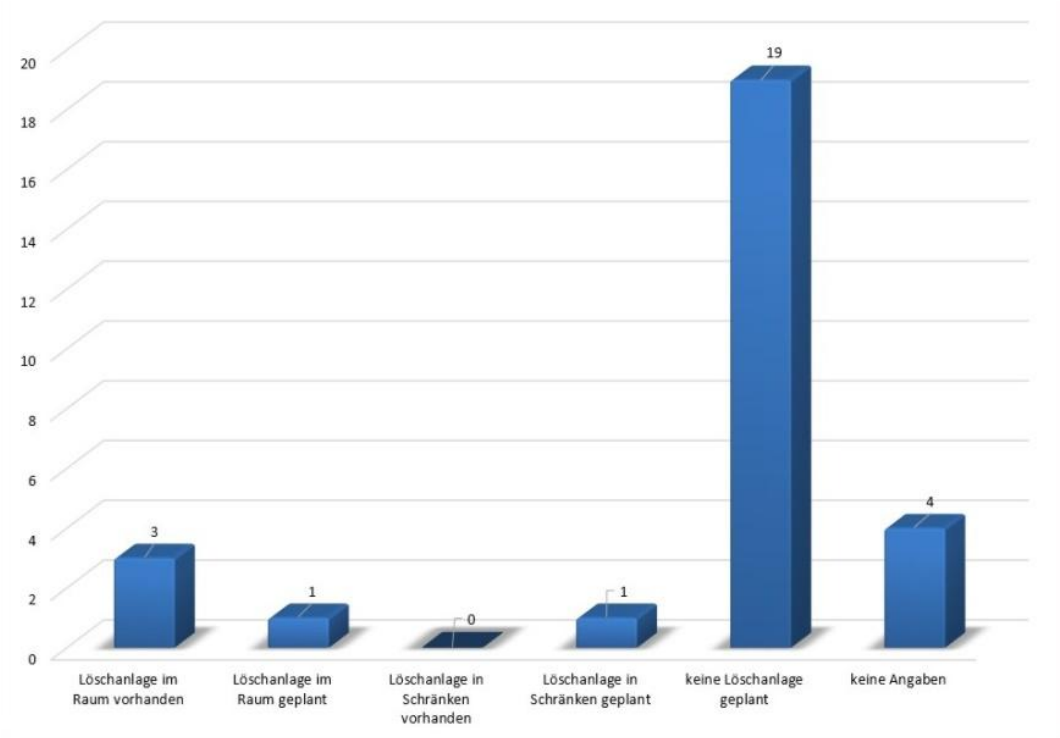
Frage: *Ist der Leitstellenbetriebsraum mit einer Löschanlage ausgestattet?*




Eine Löschanlage im Betriebsraum ist bei 24 der 28 Leitstellen weder vorhanden noch in Planung, vier Standorte machten keine Angaben.

## A.75 Löschanlage Technikraum/-schränke

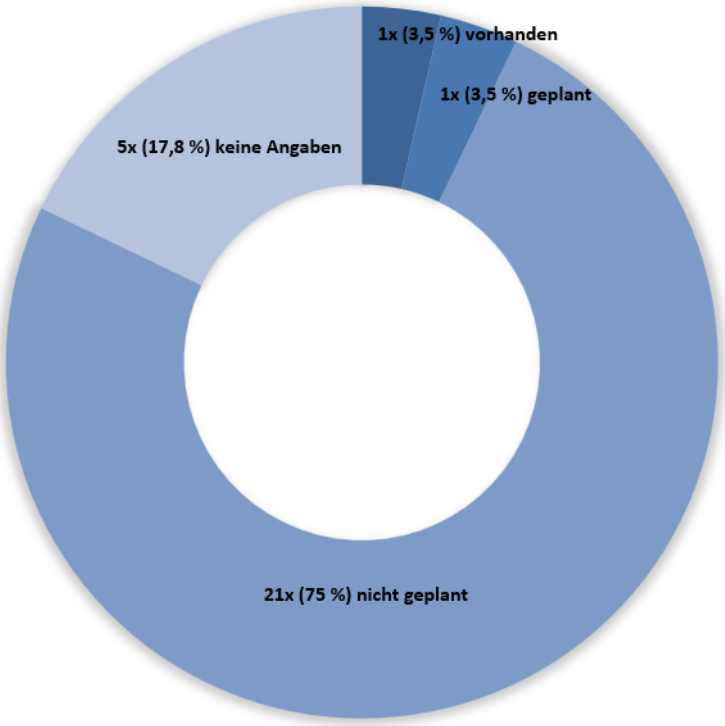
Frage: *Besteht im Technikraum bzw. in den Technikschränken eine Löschanlage?*
(Mehrfachantworten möglich)




Drei Leitstellen meldeten, dass eine Löschanlage im Technikraum vorhanden ist, bei einem Standort ist dies geplant. Eine Löschanlage in den Schränken ist bei den 28 Leitstellen nirgendwo vorhanden, aber an einem Standort geplant. Bei 19 der 28 Leitstellen ist eine Löschanlage im Technikraum bzw. den Schränken nicht geplant, vier Standorte machten keine Angaben.

## A.76 Sauerstoffreduktion Technikraum

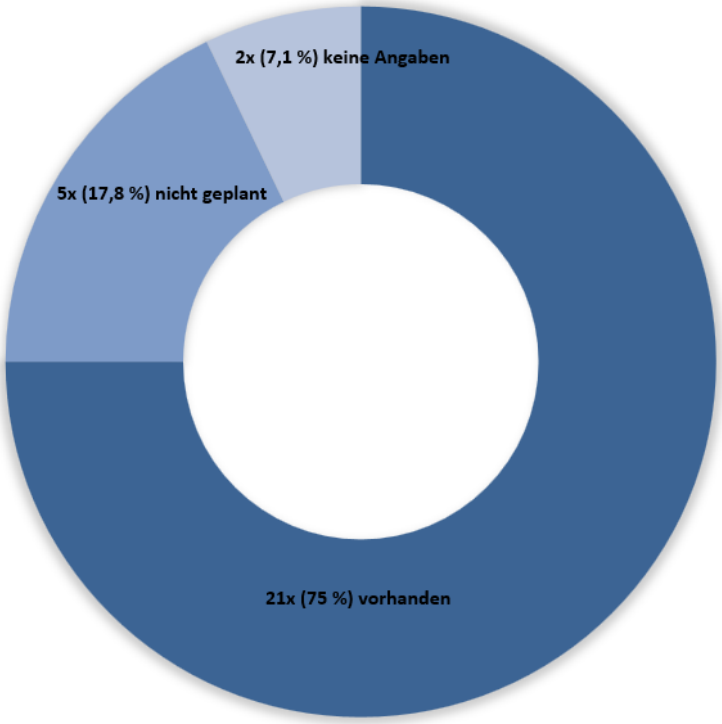
Frage: *Ist im Technikraum eine Sauerstoffreduktion vorhanden?*




Sauerstoffreduktion ist in einer Leitstelle vorhanden und bei einer weiteren geplant. Bei 21 der 28 Leitstellen (75 %) ist keine Sauerstoffreduktionsanlage geplant, fünf Standorte machten keine Angaben.

## A.77 USV Wachalarm / Elektroakustische Anlage

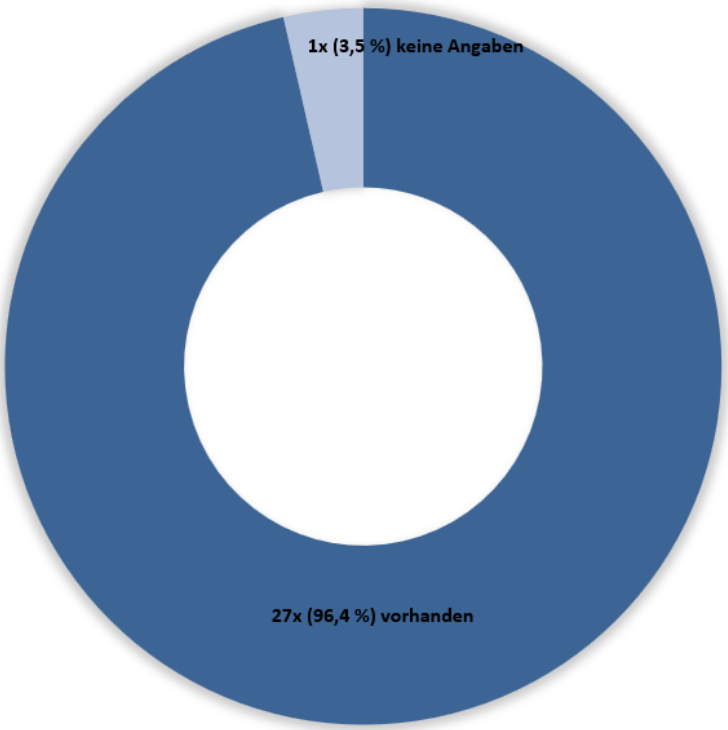
Frage: *Besteht eine Unterbrechungsfreie Stromversorgung (USV) für den Wachalarm bzw. die Elektroakustische Anlage (ELA)?*




Eine USV-Abstützung für Wachalarm bzw. ELA ist bei 21 der 28 Leitstellen vorhanden, bei fünf Leitstellen bestehen keine entsprechenden Planungen. Zwei Standorte machten keine Angaben.

## A.78 USV Gefahrenmeldeanlage

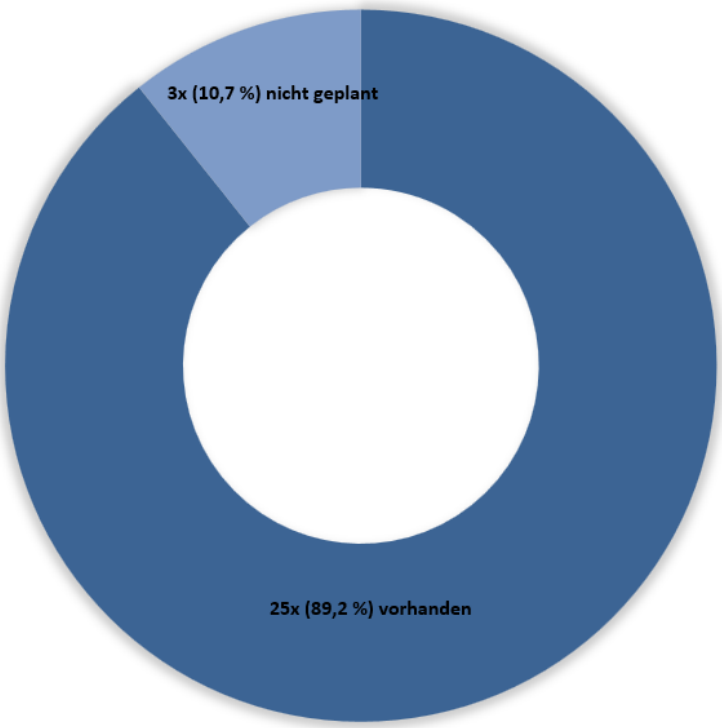
Frage: *Besteht eine Unterbrechungsfreie Stromversorgung (USV) für die Empfangstechnik der Gefahrenmeldeanlagen?*




Eine USV-Versorgung für die Empfangstechnik von Gefahrenmeldeanlagen (Brandmeldeanlagen) ist bei 27 der 28 Leitstellen vorhanden, ein Standort machte keine Angaben.

## A.79 USV Beleuchtung Betriebsraum

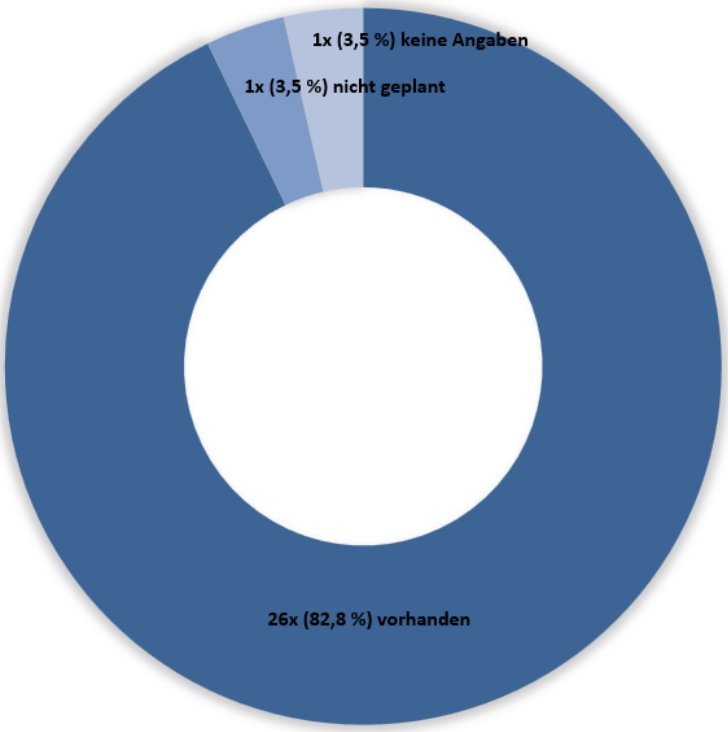
Frage: *Besteht eine Unterbrechungsfreie Stromversorgung (USV) für die Beleuchtung im Leitstellenbetriebsraum?*




Bei 25 der 28 Leitstellen ist die Beleuchtung des Betriebsraums USV-gestützt, bei drei Leitstellen ist dies weder vorhanden noch geplant.

## A.80 USV Steckdosen Betriebsraum

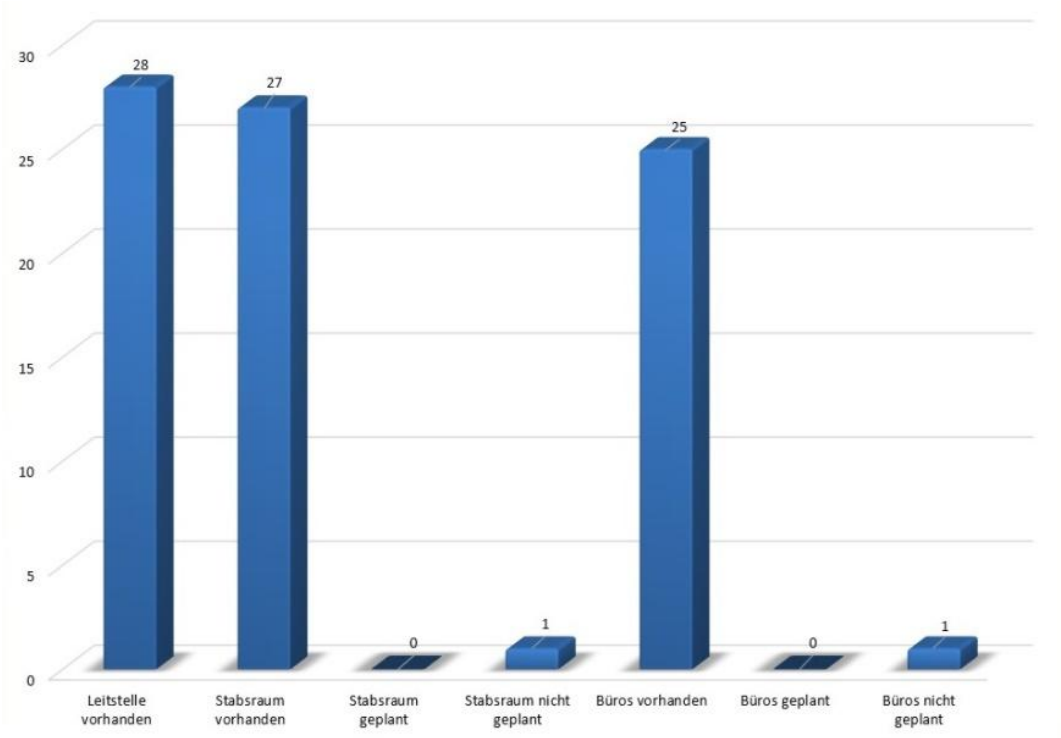
Frage: *Besteht eine Unterbrechungsfreie Stromversorgung (USV) für die 230 V-Steckdosen im Leitstellenbetriebsraum?*




In 26 der 28 Leitstellen sind die Steckdosen des Betriebsraums USV-gestützt, bei einem Standort ist dies weder vorhanden noch geplant, ein weiterer Standort machte keine Angaben.

## A.81 Netzersatzanlage

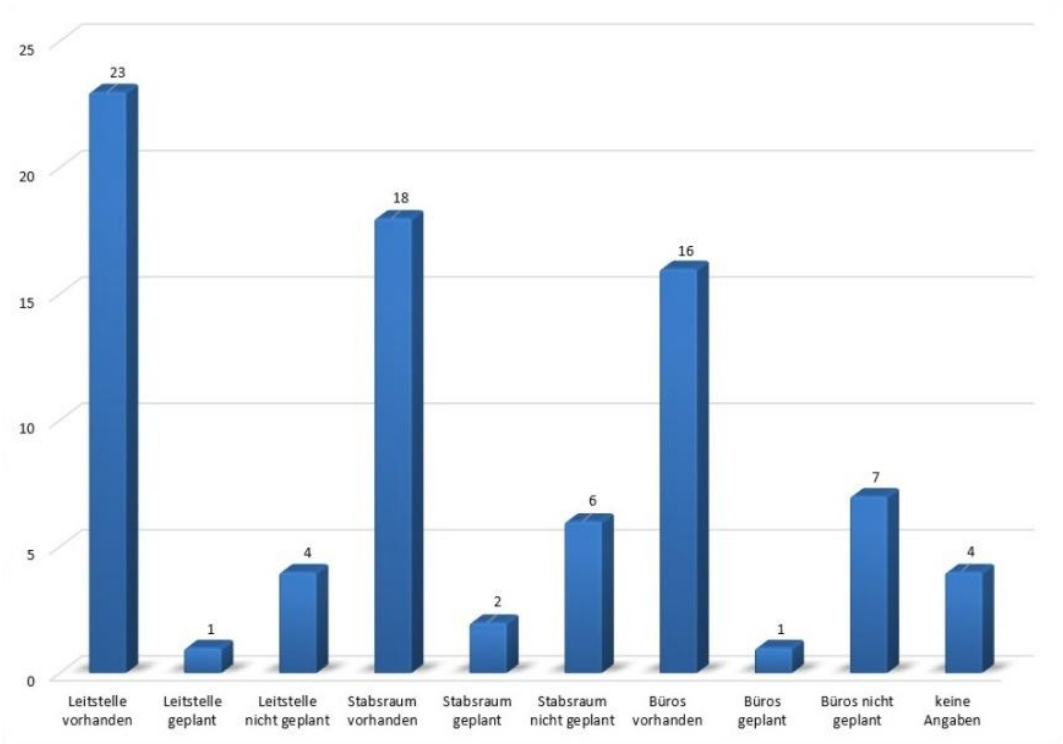
Frage: *Ist eine Netzersatzanlage (NEA) vorhanden? Welche Bereiche/Räume werden damit abgedeckt?* (Mehrfachantworten möglich)




Alle 28 Leitstellen verfügen über eine Netzersatzanlage, die die Leitstellentechnik (Komponenten im Betriebs- und Technikraum) versorgen kann. Bei 27 Standorten wird zudem der Stabsraum mit von der NEA versorgt; der verbleibende Standort gab an, dass die Einbeziehung des Stabsraums nicht vorhanden und auch nicht geplant ist. Bei 25 Standorten sind zudem die zugehörigen Büroräume mit in die NEA-Versorgung integriert, bei einem Standort ist die Einbeziehung der Büroräume nicht geplant.

## A.82 Einspeisung extern

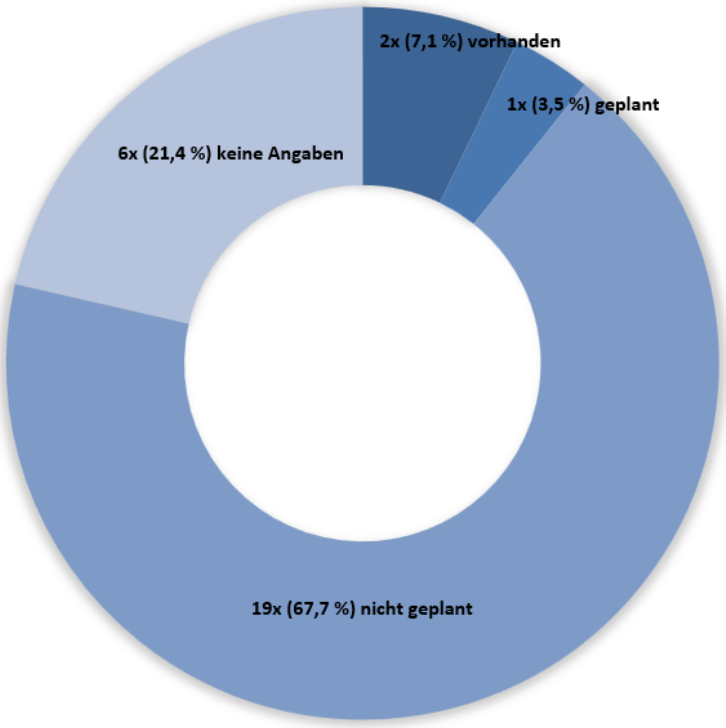
Frage: *Ist eine externe Stromeinspeisung vorhanden? Welche Bereiche/Räume werden damit abgedeckt?*




Ein externer Einspeiseanschluss ist bei 23 der 28 Leitstellen vorhanden; in einem Fall ist dies geplant, bei zwei Standorten ist dies nicht geplant. Bei 18 Liegenschaften wird auch der Stabsbereich von der externen Einspeisung mit abgedeckt, bei zwei weiteren Standorten ist dies geplant, in sechs Fällen nicht geplant. Die Büroräume sind an 16 Standorten mit in die externe Einspeisung einbezogen, bei einem weiteren Standort ist dies geplant. Bei sieben Liegenschaften ist dies nicht geplant; in vier Fällen wurden keine Angaben gemacht.

## A.83 Heizung redundant

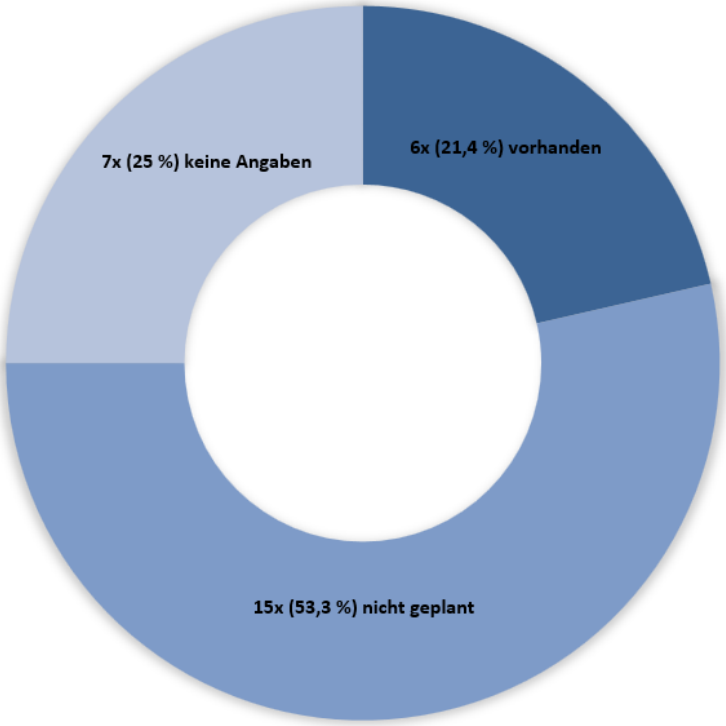
Frage: *Ist die Heizungsanlage des Leitstellengebäudes redundant ausgeführt?*




In zwei der 28 Leitstellen ist die Heizungsanlage redundant ausgeführt, bei einem weiteren Standort ist dies geplant. Bei 19 der 28 Standorte (ca. 2/3) ist die Heizungsanlage einfach ausgeführt und keine Redundanz geplant, sechs Standorte machten keine Angaben.

## A.84 Blockheizkraftwerk

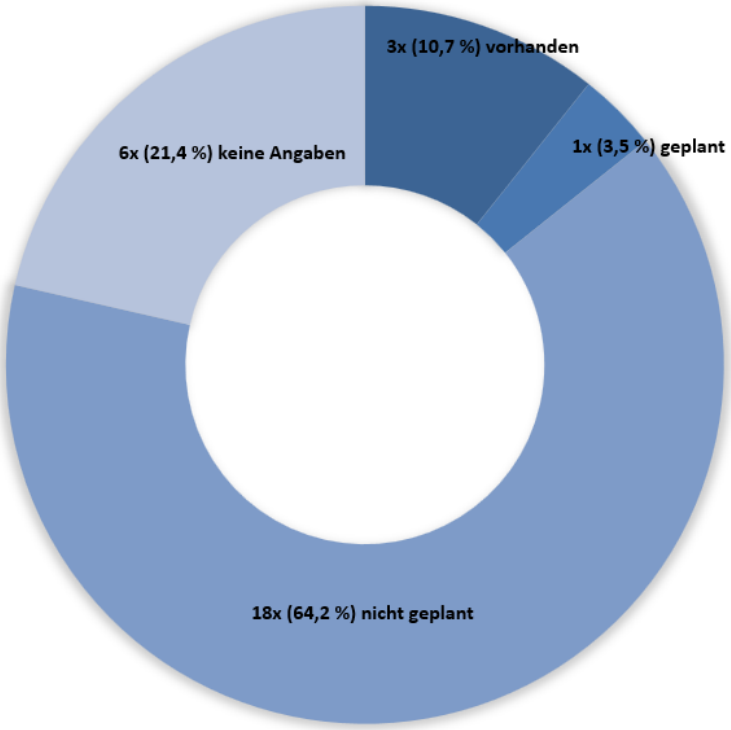
Frage: *Ist ein Blockheizkraftwerk (BHKW) vorhanden, mit dem neben der Wärmegewinnung (Heizen) auch Elektrizität erzeugt werden kann?*




An sechs Standorten ist ein BHKW vorhanden, bei 15 Leitstellenliegenschaften ist ein BHKW weder vorhanden noch geplant. Sieben Standorte machten keine Angaben.

## A.85 Heizlüfter

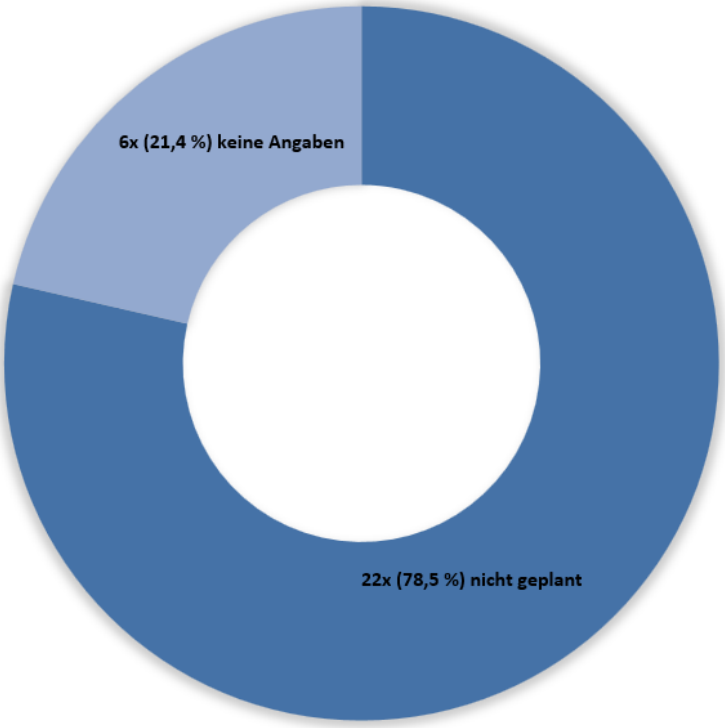
Frage: *Sind Heizlüfter als „Notheizung“ vorhanden?*




Bei drei Leitstellen werden Heizlüfter vorgehalten, um bei einem Ausfall der Heizungsanlage den Betriebsraum beheizen zu können; bei einem weiteren Standort ist dies geplant. An 18 Standorten ist dies nicht geplant, sechs Standorte machten keine Angaben hierzu.

## A.86 Einspeisung extern

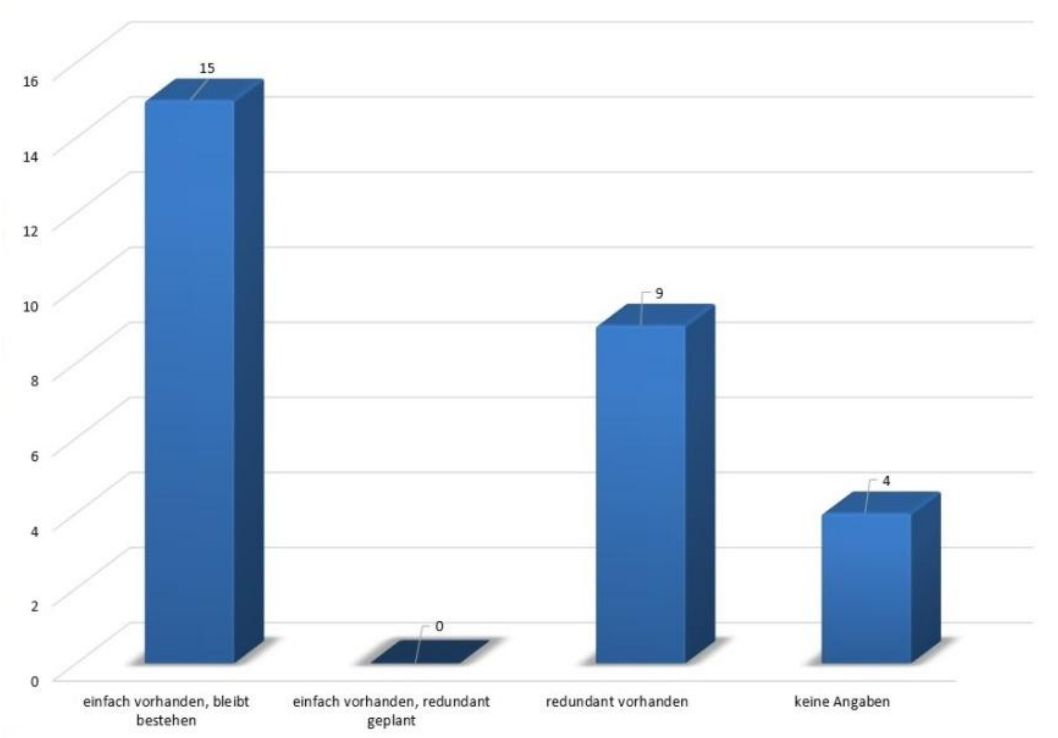
Frage: *Ist eine externe Heizungseinspeisung vorhanden?*




Anschlüsse für eine externe (mobile) Heizungsanlage sind bei keiner der 28 Leitstellen als vorhanden gemeldet worden; 22 Standorte verneinten entsprechende Planungen, sechs Standorte machten keine Angaben.

## A.87 Klimatisierung

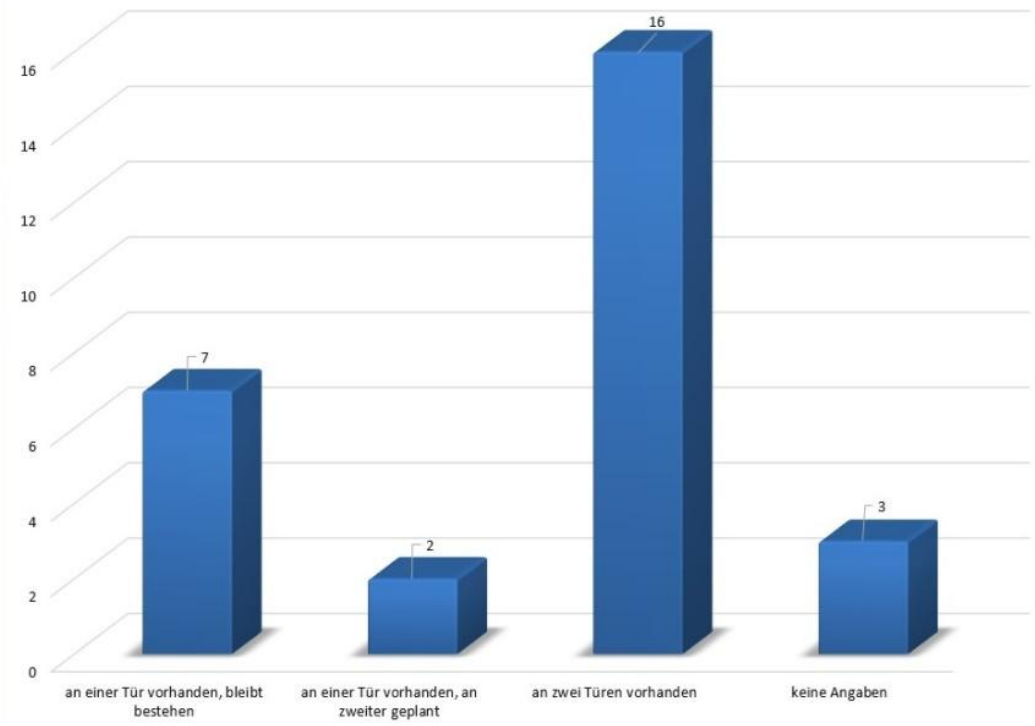
Frage: *Ist die Klimatisierung einfach oder redundant ausgeführt?* (Mehrfachantworten möglich)




In 15 Leitstellen ist eine einfach ausgeführte Klimaanlage vorhanden, wobei keine Änderungen (Erweiterung auf redundante Auslegung) vorgesehen sind. An neun Standorten ist redundante Klimatechnik vorhanden; vier Standorte machten keine Angaben.

## A.88 Zugangskontrolle

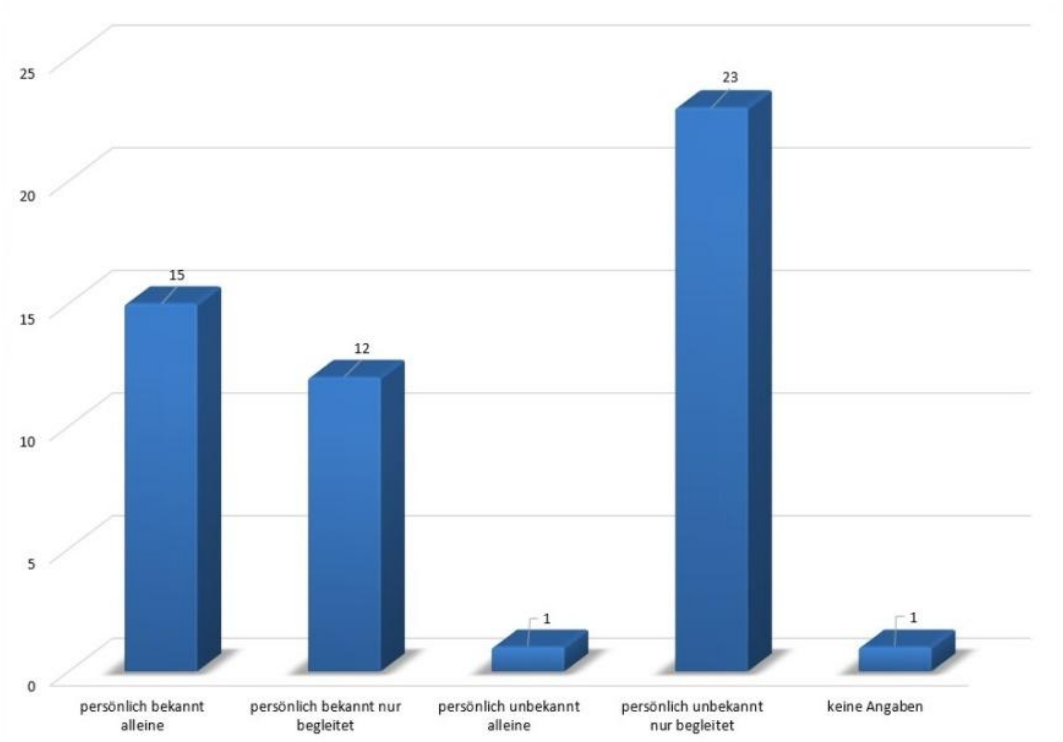
Frage: *Findet eine Zugangskontrolle an einer oder an zwei Türen statt, um den Leitstellenbereich betreten zu können?* (Mehrfachantworten möglich)




Bei 16 der 28 Leitstellen findet die Zugangskontrolle zweistufig, d.h. an zwei Türen nacheinander statt. In sieben Fällen nur an einer Tür, ohne dass Änderungen geplant sind. AN zwei Standorten findet ebenfalls nur an einer Tür eine Zugangskontrolle statt, wobei eine Erweiterung auf eine zweite Tür geplant ist. Drei Leitstellen machten keine Angaben.

## A.89 Zugang Begleitung

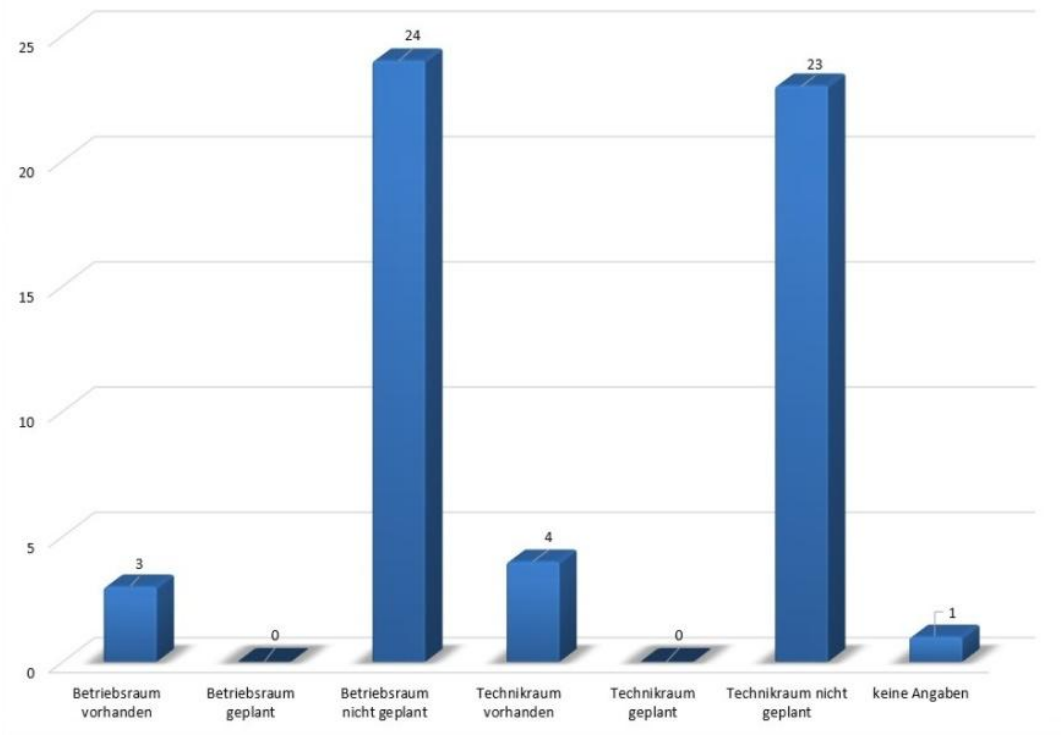
Frage: *Dürfen sich Besucher nach dem Einlass alleine im Leitstellenbereich bewegen oder ist eine ständige Begleitung durch eigenes Personal festgeschrieben?* (Mehrfachantworten möglich)




In 15 Liegenschaften dürfen sich Besucher, die persönlich bekannt sind, alleine aufhalten und bewegen. An 12 Standorten dürfen sich auch persönliche bekannte Besucher nur in Begleitung bewegen. Bei persönlich nicht bekannten Besuchern ist an 23 der 28 Standorte eine Begleitung erforderlich, nur in einem Fall dürfen sich auch persönlich nicht bekannte Besucher alleine in den Räumlichkeiten der Leitstelle aufhalten. In einem Fall wurden keine Angaben gemacht.

## A.90 Gasmelder

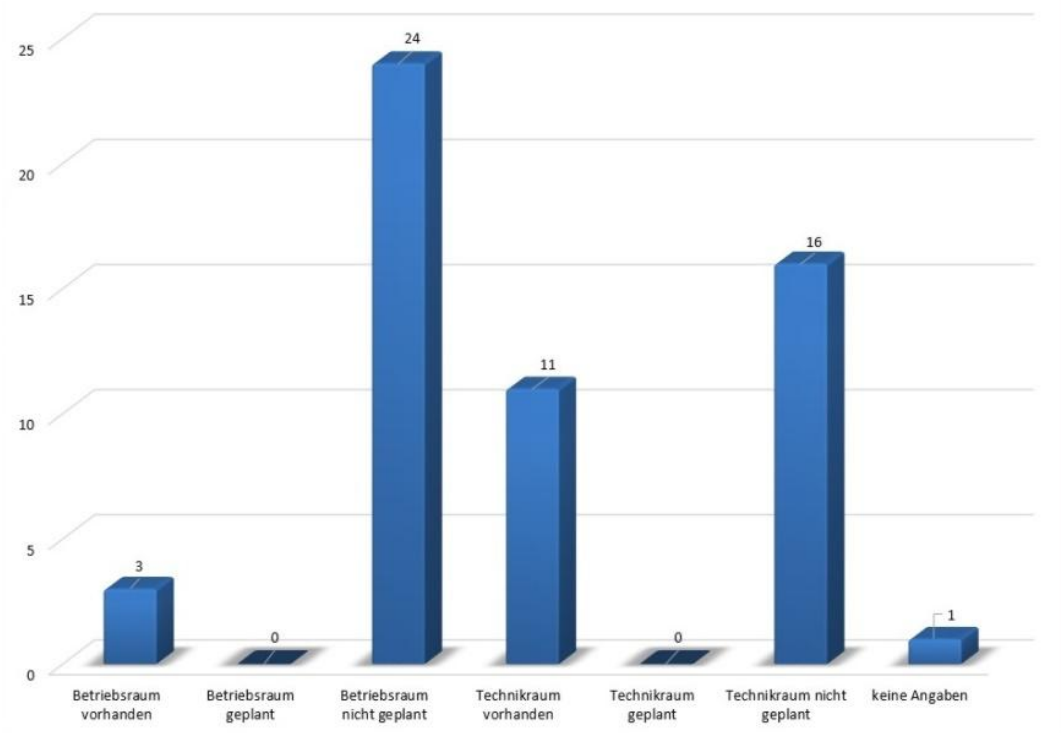
Frage: *Sind Gasmelder vorhanden? Welche Bereiche/Räume werden damit abgedeckt?* (Mehrfachantworten möglich)




Gasmelder sind an drei Standorten im Betriebsraum vorhanden bzw. an vier Standorten im Technikraum. Planungen zur Erweiterung der Gasmelderüberwachung bestehen nicht; 24 Leitstellen teilten mit, dass keine Gasmelder im Betriebsraum vorgesehen sind, an 23 Standorten ebenso wenig im Technikraum. Ein Standort machte keine Angaben bzgl. Gasmelderüberwachung.

## A.91 Wassermelder

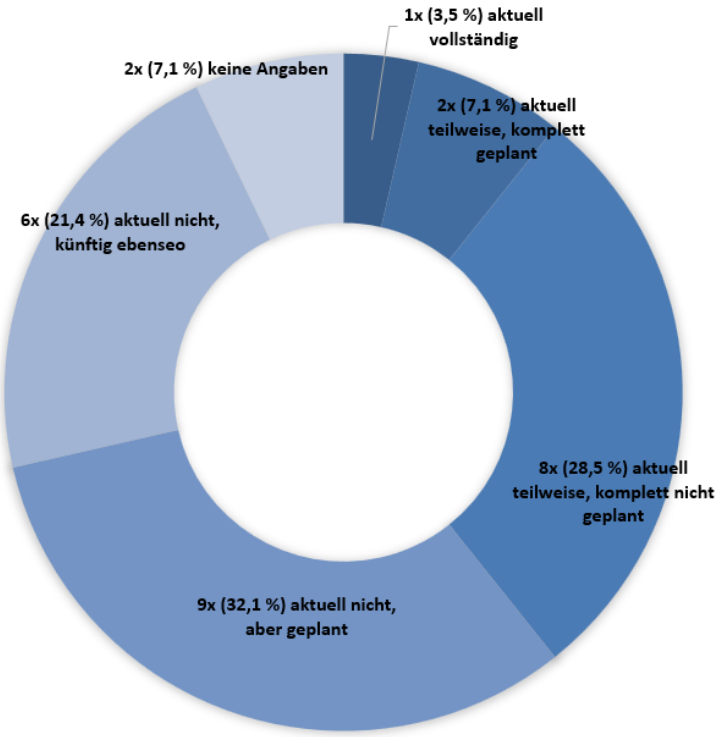
Frage: *Sind Wassermelder vorhanden? Welche Bereiche/Räume werden damit abgedeckt?* (Mehrfachantworten möglich)




Bei drei Leitstellen wird der Betriebsraum (bzw. dessen Rohboden) mit Wassermeldern überwacht, an elf Standorten gilt dies für den Technikraum. Eine Überwachung des Betriebsraums ist an 24 der 28 Standorte nicht geplant bzw. in 16 Fällen auch nicht für den Technikraum. In einem Fall wurden keine Angaben gemacht.

## A.92 DIN EN 50518

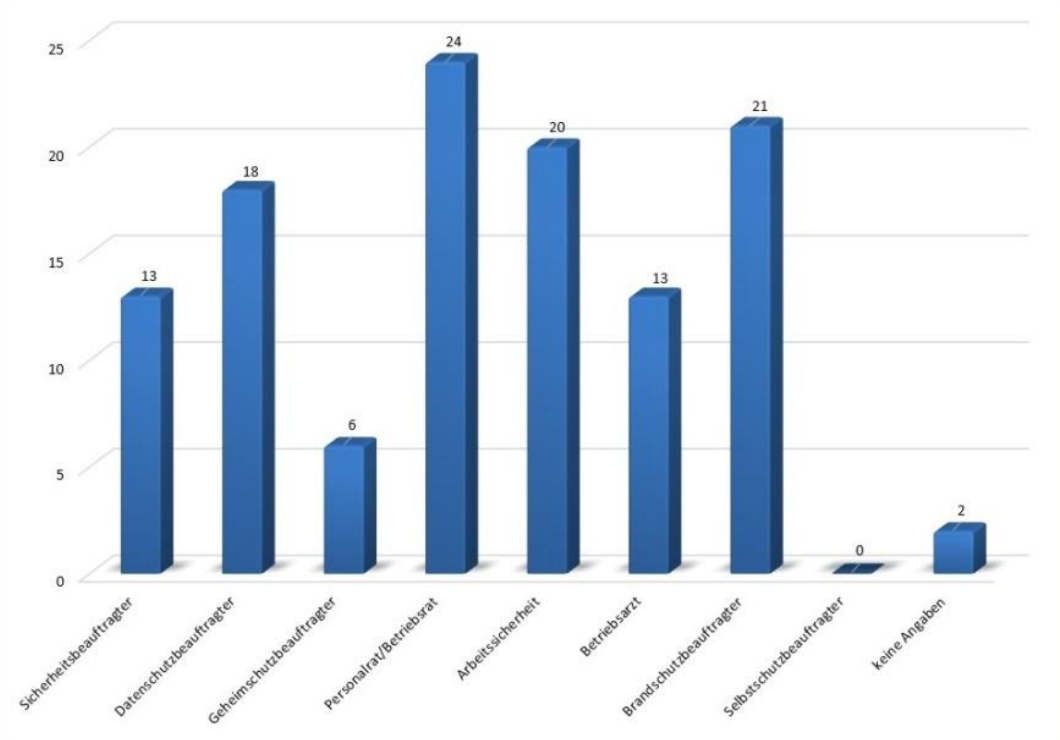
Frage: *Fand bzw. findet die DIN EN 50518 bei der Planung und dem Betrieb der Leitstelle Anwendung bzw. in welchem Umfang?*




Eine der 28 Leitstellen wendet die DIN EN 50518 vollumfänglich an, zwei weitere Leitstellen wenden die Norm in Teilen an, planen aber eine komplette Umsetzung. Acht Standorte wenden die Norm ebenfalls teilweise an und wollen dies auch beibehalten. Neun Standorte wenden die Norm derzeit nicht an, planen aber eine teilweise Umsetzung. Sechs Leitstellen wenden die Norm derzeit nicht an und wollen dies auch künftig nicht tun. In zwei Fällen wurden keine Angaben gemacht.

## A.93 Interne Stellen

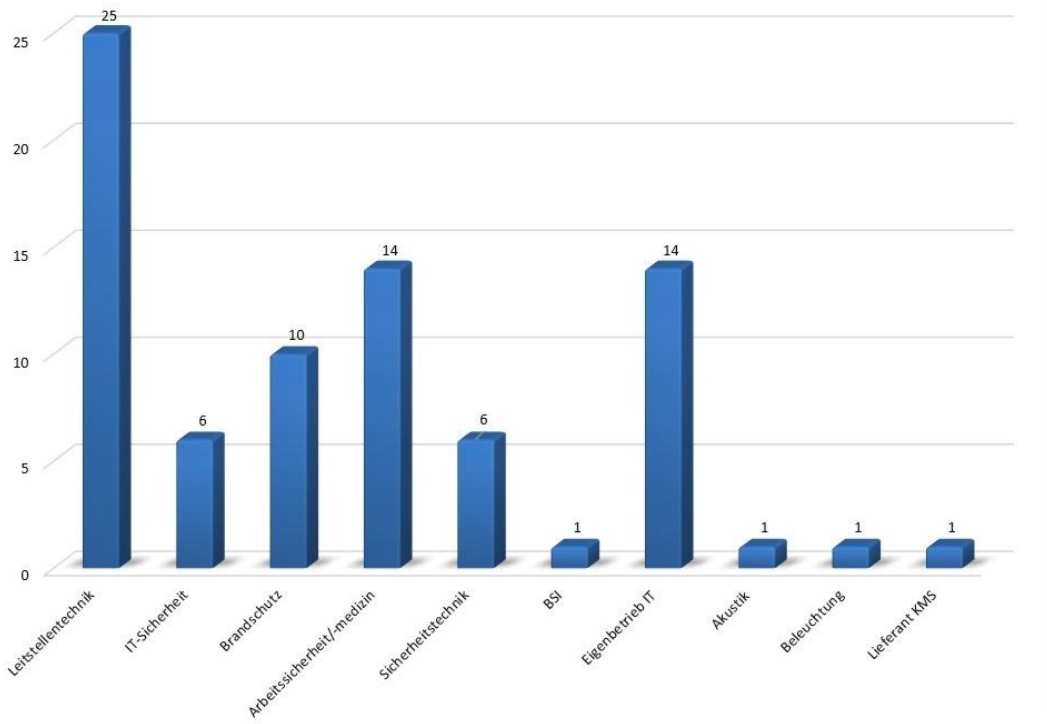
Frage: *Welche internen Stellen wurden bzw. sind in die Planung der Leitstelle mit einbezogen (worden)?* (Mehrfachantworten möglich)




In 13 von 28 Fällen wurde der Sicherheitsbeauftragte mit einbezogen, in 18 Fällen der Datenschutzbeauftragte, in sechs Fällen der Geheimschutzbeauftragte und in 24 Fällen der Personal- bzw. Betriebsrat. Fachkräfte für Arbeitssicherheit wurden in 20 Fällen hinzugezogen, Betriebsärzte in 13 Fällen und Brandschutzbeauftragte in 21 Fällen. Die Beteiligung eines Selbstschutzbeauftragten fand in keinem Falls statt; zwei Standorte machten keine Angaben.

## A.94 Externe Stellen

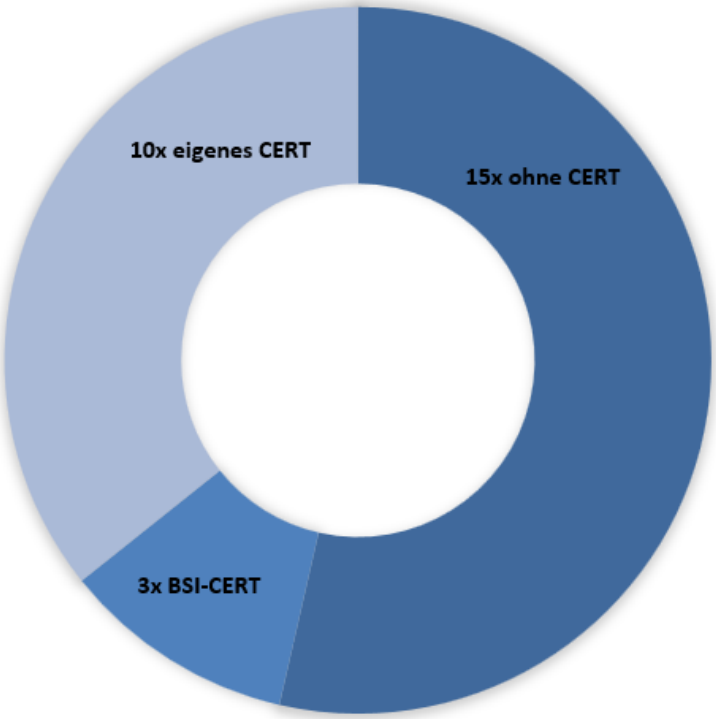
Frage: *Welche externen Stellen wurden bzw. sind in die Planung der Leitstelle mit einbezogen (worden)?* (Mehrfachantworten möglich)




Fachplaner für Leitstellentechnik wurden in 25 von 28 Fällen hinzugezogen; externe Beratung zur IT-Sicherheit wurde in 6 Fällen, für Brandschutz in 10 Fällen, für Arbeitssicherheit/Arbeitsmedizin in 14 Fällen und für Sicherheitstechnik in sechs Fällen hinzugezogen. In einem Fall wurde das BSI um Unterstützung ersucht, in 14 Fällen der Eigenbetrieb IT der Kommune bzw. des Landes. Fachplaner für Akustik und Beleuchtung wurden in jeweils einen Fall hinzugezogen und der Lieferant des Kommunikationsmanagementsystem wurde ebenfalls in einem Fall mit einbezogen,

## A.95 CERT

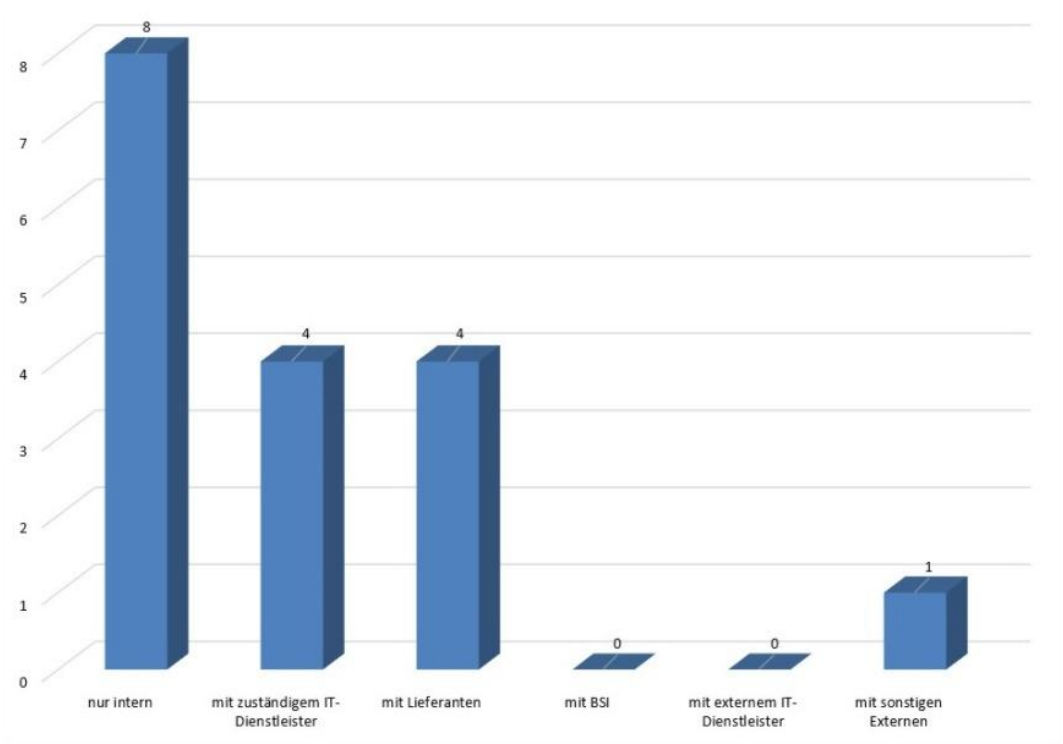
Frage: *Wird bei einem IT-Sicherheitsvorfall ein Computer Emergency Response Team (CERT) mit einbezogen bzw. ist dies vorgesehen?*




Bei 15 der 28 Leitstellen ist die Unterstützung durch ein CERT nicht vorgesehen, in zehn Fällen wird ein behördeneigenes CERT hinzugezogen, in drei Fällen wird auf das CERT des BSI zurückgegriffen.

## A.96 Abarbeitung von IT-Sicherheitsvorfällen

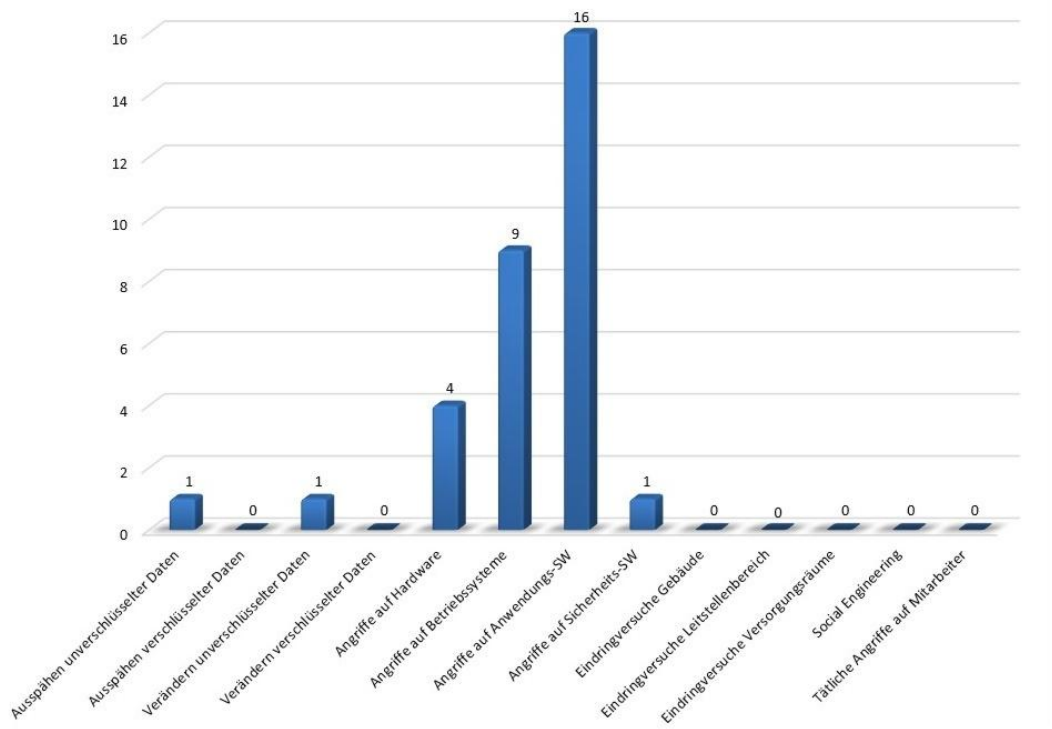
Frage: *Wie wurden bisherige IT-Sicherheitsvorfälle abgearbeitet?* (Mehrfachantworten möglich)




Bisherige Sicherheitsvorfälle wurden in acht Fällen rein intern abgearbeitet; in vier Fällen wurde zuständige IT-Dienstleister mit einbezogen, in weiteren vier Fällen die Systemlieferanten. Das BSI bzw. andere externe IT-Dienstleister wurden in keinem Fall hinzugezogen. In einem Fall wurde die Unterstützung eines sonstigen externen Dienstleisters in Anspruch genommen.

## A.97 Sicherheitsvorfälle IT

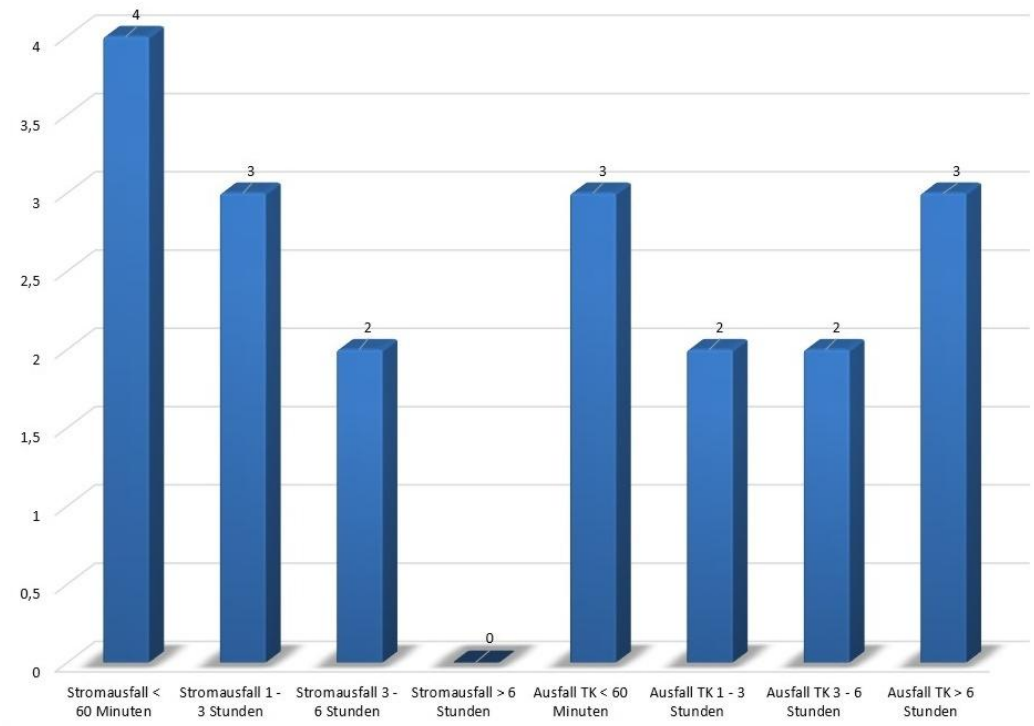
Frage: *Welcher Art und Anzahl waren die IT-Sicherheitsvorfälle?* (Mehrfachantworten möglich)




In einem Fall wurden unverschlüsselte Daten ausgespäht, in einem weiteren Fall wurden unverschlüsselte Daten verändert. In vier Fällen erfolgten Angriffe auf die Hardware, in neun Fällen waren Betriebssysteme betroffen. Angriffe auf Anwendungssoftware stellt mit 16 Fällen das Maximum unter den IT-Sicherheitsvorfällen dar. In einem Fall die Sicherheitssoftware das Ziel eines Angriffs. Das Ausspähen bzw. Verändern unverschlüsselter Daten, Eindringversuche in das Gebäude, Eindringversuche in den Leitstellenbereich, Eindringversuche in Versorgungsräume, Social Engineering oder tätliche Angriffe auf Mitarbeiter waren bei keinem der 28 Leitstellenstandorte zu verzeichnen.

## A.98 Versorgungsausfälle

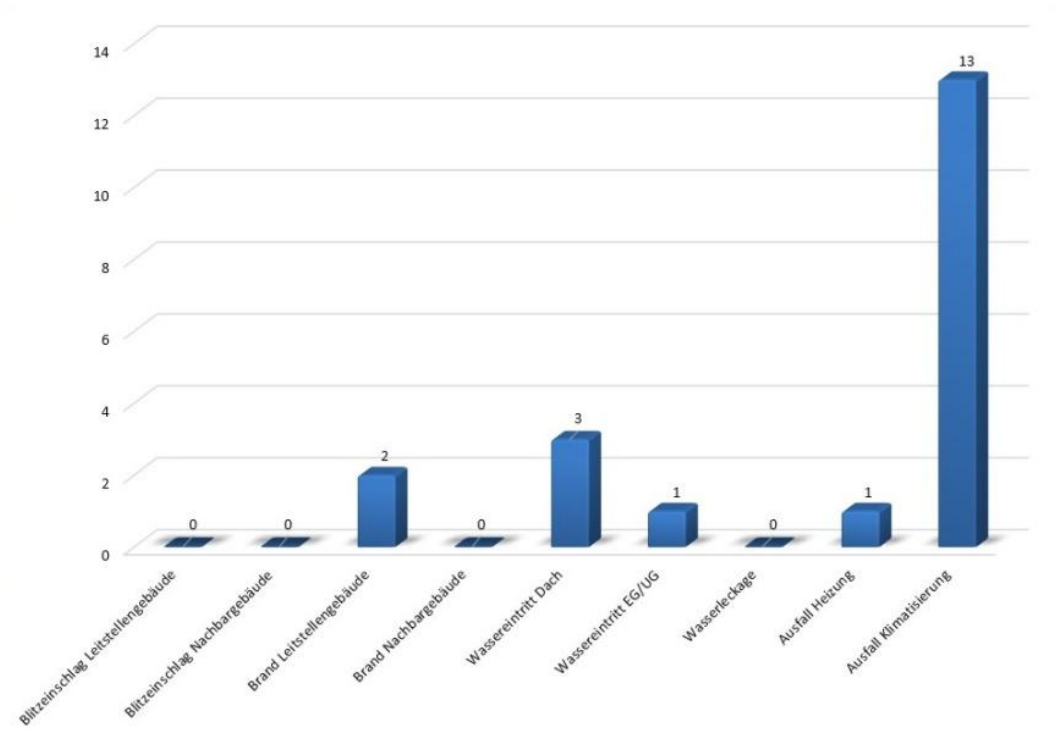
Frage: *Welcher Art und Anzahl waren die Versorgungsausfälle?* (Mehrfachantworten möglich)




Die Stromversorgung war in vier Fällen weniger als 60 Minuten betroffen, in drei Fällen zwischen einer und drei Stunden und in zwei Fällen zwischen drei und sechs Stunden. Stromausfälle von mehr als sechs Stunden waren nicht zu verzeichnen. Die Festnetzanbindung der Telekommunikation (Telefonie, Datenanbindung) war in drei Fällen weniger als 60 Minten betroffen, in zwei Fällen zwischen einer und drei Stunden, in weiteren zwei Fällen zwischen drei und sechs Stunden und in drei Fällen mehr als sechs Stunden.

## A.99 Sicherheitsvorfälle Bau, Technik, Personal

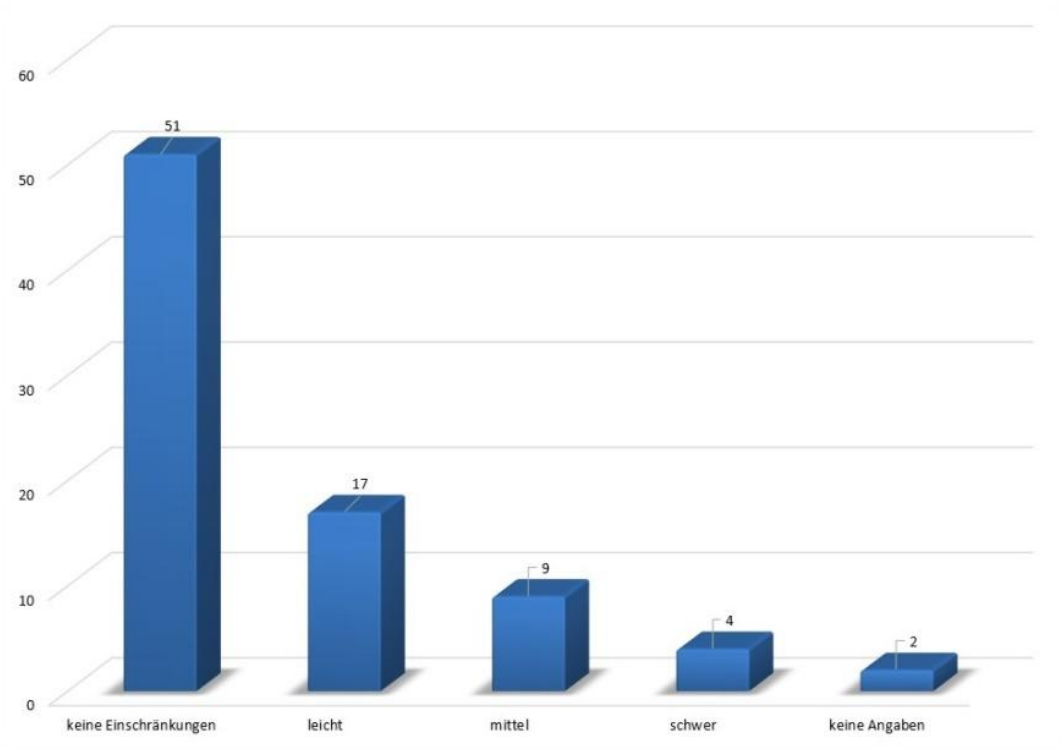
Frage: *Welcher Art und Anzahl waren die Sicherheitsvorfälle in Bezug auf Bau und Haustechnik?* (Mehrfachantworten möglich)




Das Maximum der Vorfälle bzw. Ausfälle sind Beeinträchtigungen der Klimatisierung in 13 Fällen. In zwei Fällen kam es zu Brandereignissen in den Leitstellengebäuden, in drei Fällen war ein Wassereintritt im Dachbereich zu verzeichnen und einem Fall drang Wasser ins Erd- bzw. Untergeschoss ein. In einem weiteren Fall kam es zu einem Ausfall der Heizungsanlage. Blitzeinschläge in das Leitstellen- oder das Nachbargebäude, Brandereignisse im Nachbargebäude oder Wasserleckagen im eigenen Gebäude waren nicht zu verzeichnen.

## A.100 Auswirkungen

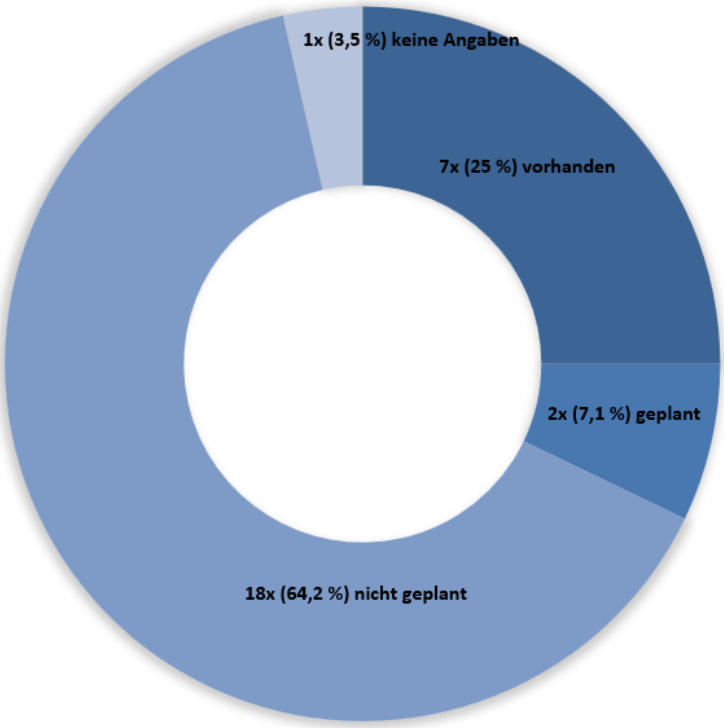
Frage: *Welche Auswirkungen hatten die zuvor genannten Vorfälle auf den Leitstellenbetrieb?* (Mehrfachantworten möglich)




Bei den unter A.98, A.99 und A.100 aufgeführten Vorfällen gab es in 51 Fällen keine betrieblichen Einschränkungen. In 17 Fällen waren leichte Einschränkungen zu verzeichnen, bei denen die Leitstelle ihre Aufgaben nach wie vor erfüllen konnte. Neun Fälle wurden als mittlere Betriebsstörungen eingestuft, bei denen die Leitstellenaufgaben nur mittels Rückfallebenen und/oder personeller Verstärkung erfüllt werden konnten. Vier Vorfälle konnten nur unter Zuhilfenahme von Notebenen bzw. der Aktivierung von Notfallkonzepten bewältigt werden. In zwei Fällen wurden keine Angaben zu den Einschränkungen gemacht.

## A.101 ITIL

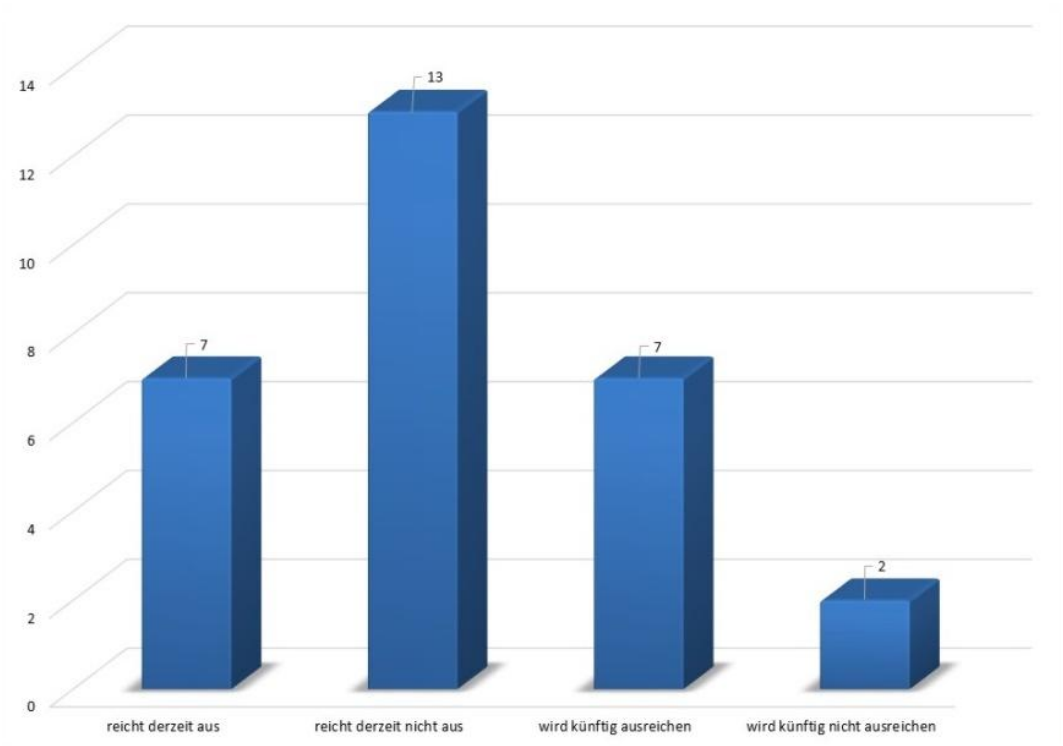
Frage: *Erfolgt der IT-Betrieb der Leitstelle auf Grundlage der IT Infrastructure Library (ITIL)?*




ITIL kommt in sieben der 28 (25 %) Leitstellen zur Anwendung, bei zwei weiteren Standorten ist die Einführung geplant. Bei 18 Standorten ist die Einführung von ITIL nicht geplant, in einem Fall wurden keine Angaben gemacht.

## A.102 Personalbedarf Disponenten

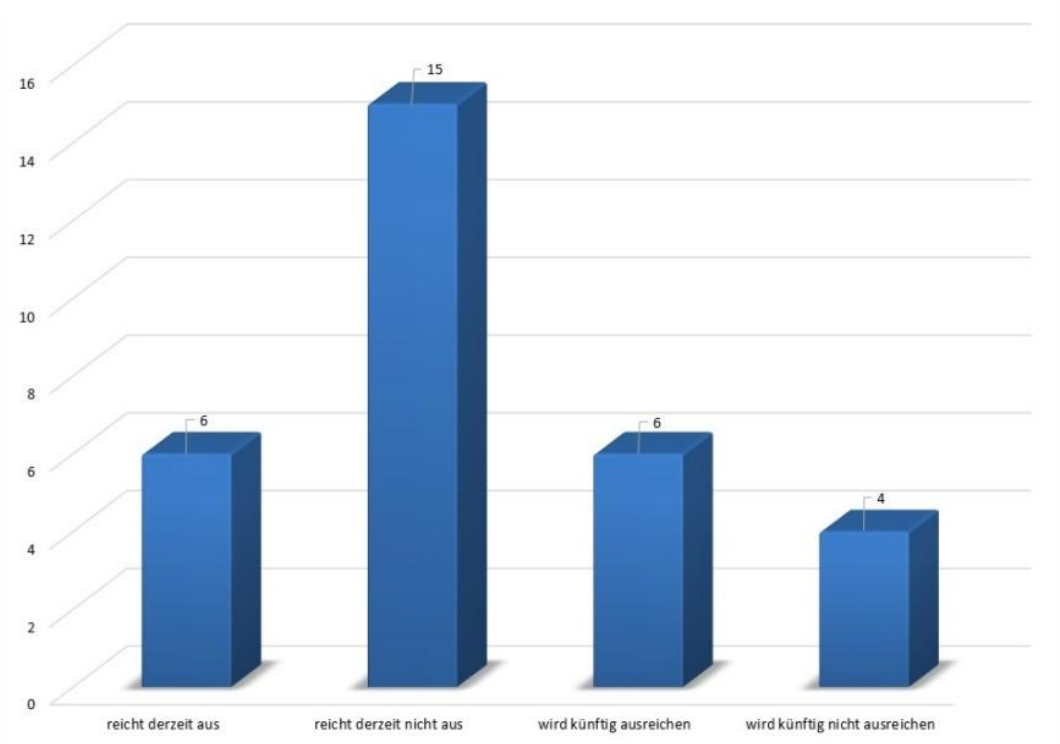
Frage: *Wie beurteilen die Aufwände für Informationssicherheit in Ihrer Leitstelle in Bezug auf den Personalbedarf bei den Disponenten?* (Mehrfachantworten möglich)




In sieben Fällen wird der aktuelle Personalansatz bei den Disponenten als ausreichend angesehen, in 13 Fällen als nicht ausreichend. Bei sieben Leitstellen geht man davon aus, dass der derzeitige Personalansatz auch zukünftig ausreichen wird, in zwei Fällen wird erwartet, dass der Personalansatz künftig nicht ausreichen wird.

## A.103 Personalbedarf Administration

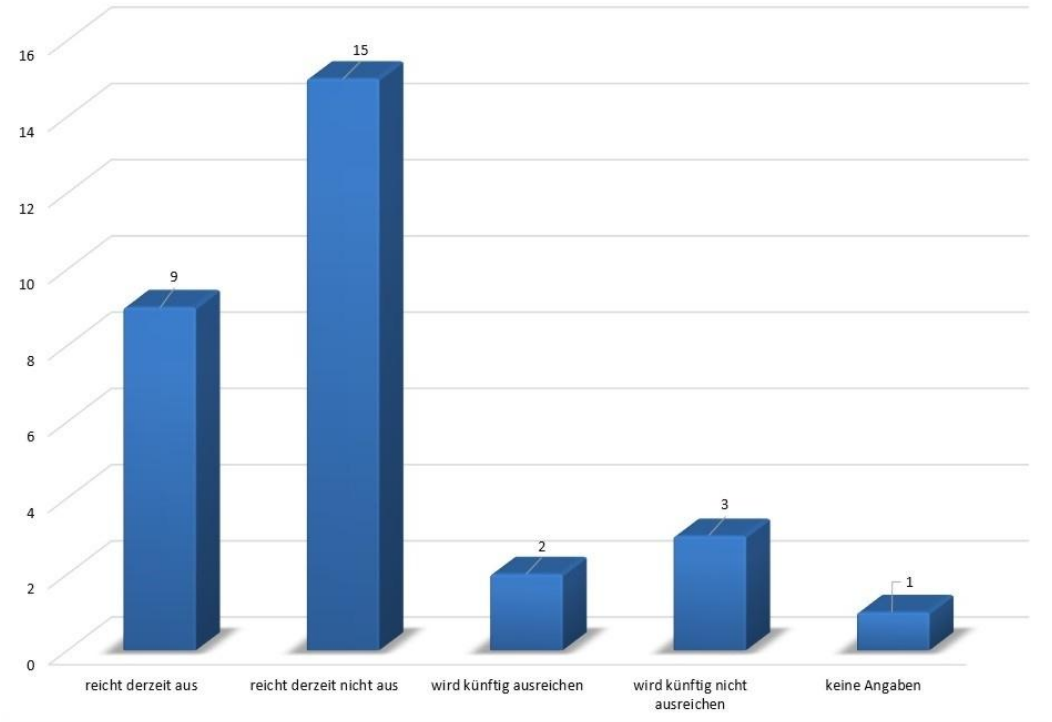
Frage: *Wie beurteilen Sie die Aufwände für Informationssicherheit in Ihrer Leitstelle in Bezug auf den Personalbedarf bei den Administratoren?* (Mehrfachantworten möglich)




In sechs Fällen wird der aktuelle Personalansatz bei den Administratoren als ausreichend angesehen, in 15 Fällen als nicht ausreichend. Bei sechs Leitstellen geht man davon aus, dass der derzeitige Personalansatz auch zukünftig ausreichen wird, in vier Fällen wird erwartet, dass der Personalansatz künftig nicht ausreichen wird.

## A.104 Sachmittel für Ausbildung

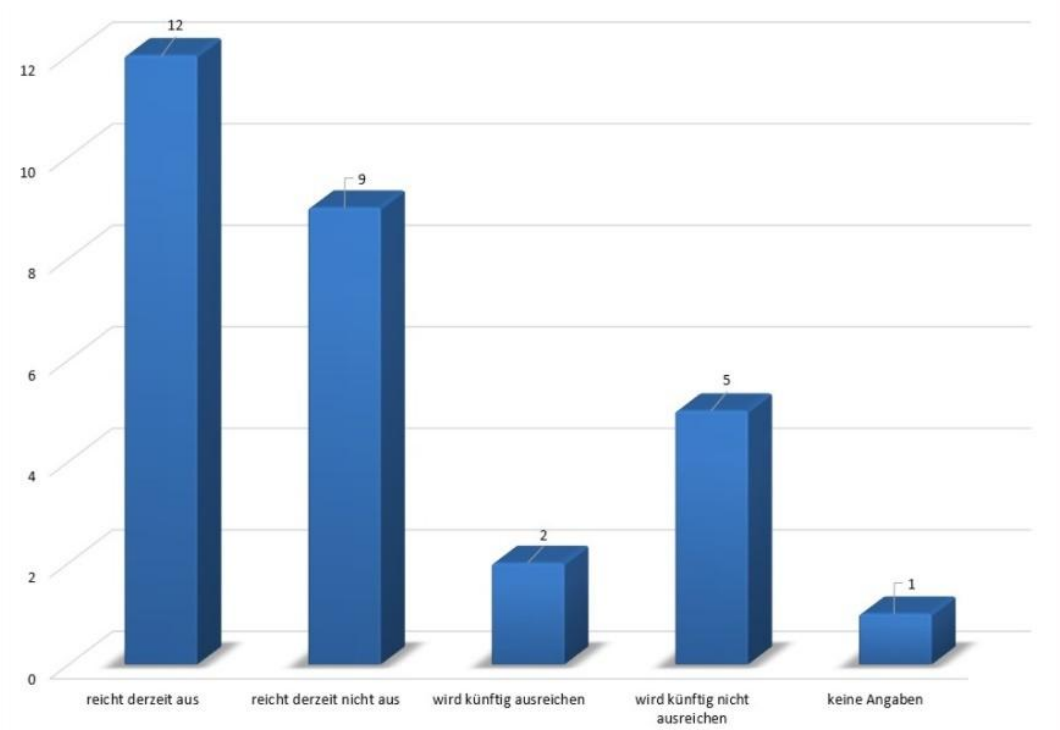
Frage: *Wie beurteilen Sie die Aufwände für Informationssicherheit in Ihrer Leitstelle in Bezug auf die Sachmittel für die Ausbildung?* (Mehrfachantworten möglich)




In neun Fällen wird der aktuelle Ansatz für Sachmittel zur Ausbildung der Mitarbeiter als ausreichend angesehen, in 15 Fällen als nicht ausreichend. Bei zwei Leitstellen geht man davon aus, dass der derzeitige Mittelansatz auch zukünftig ausreichen wird, in drei Fällen wird erwartet, dass der Mittelansatz künftig nicht ausreichen wird. In einem Fall wurden keine Angaben gemacht.

## A.105 Sachmittel für Technik

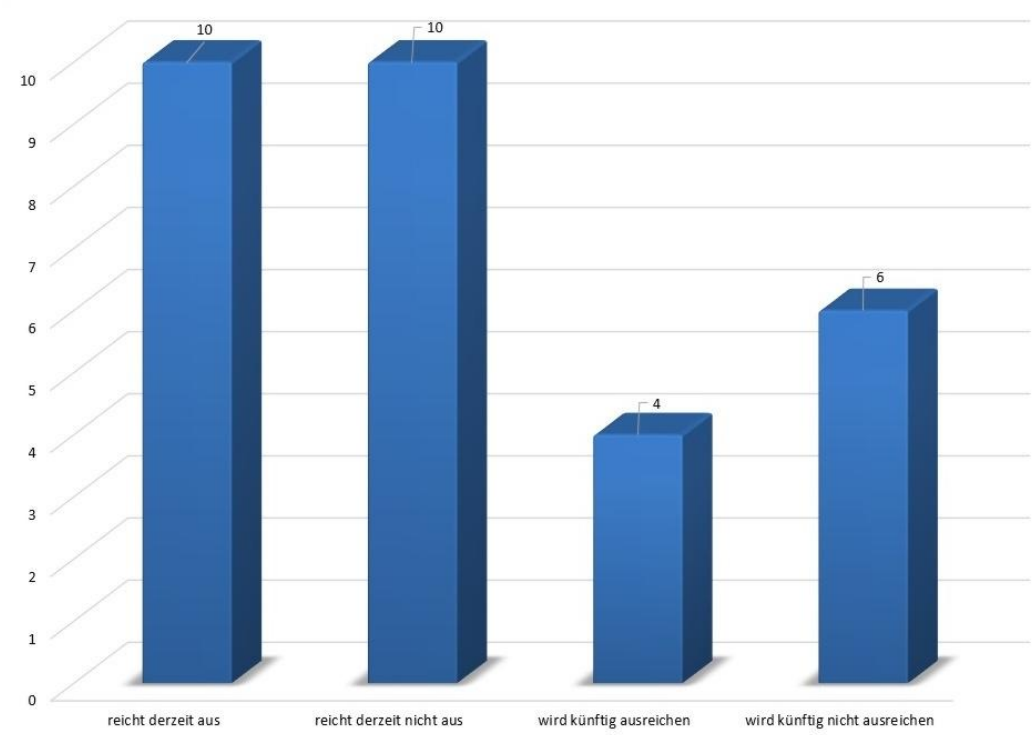
Frage: *Wie beurteilen Sie die Aufwände für Informationssicherheit in Ihrer Leitstelle in Bezug auf die Sachmittel für technische Maßnahmen?* (Mehrfachantworten möglich)




In 12 Fällen wird der aktuelle Ansatz für Sachmittel für technische Maßnahmen als ausreichend angesehen, in neun Fällen als nicht ausreichend. Bei zwei Leitstellen geht man davon aus, dass der derzeitige Mittelansatz auch zukünftig ausreichen wird, in fünf Fällen wird erwartet, dass der Mittelansatz künftig nicht ausreichen wird. In einem Fall wurden keine Angaben gemacht.

## A.106 Sachmittel für Bauunterhaltung

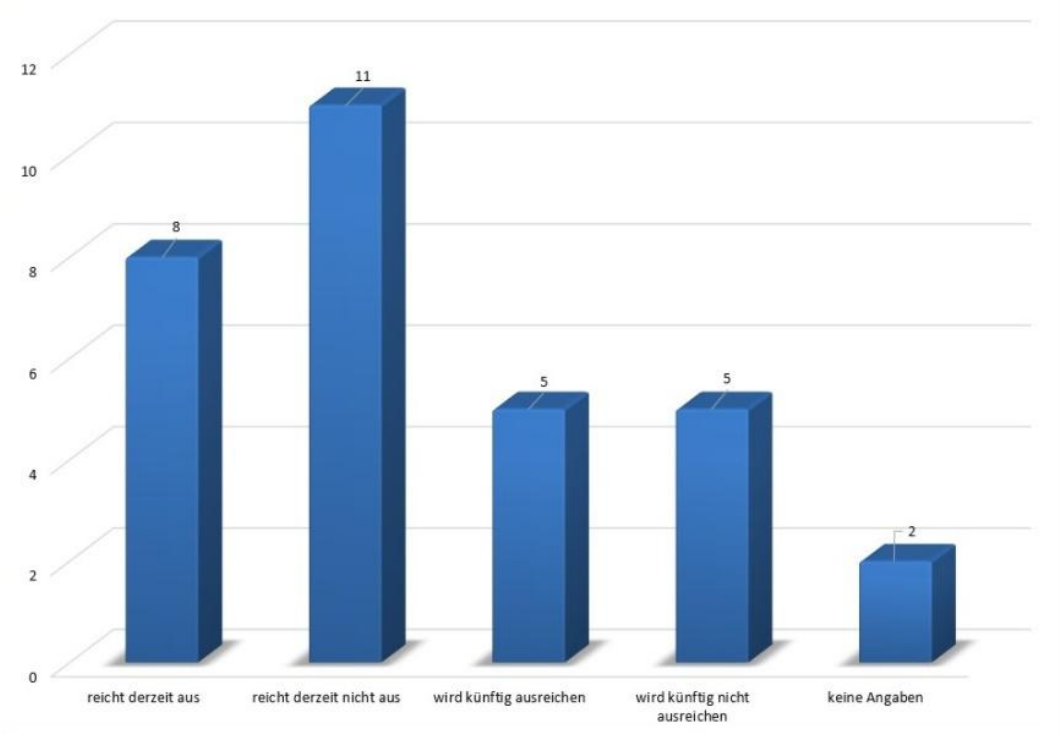
Frage: *Wie beurteilen Sie die Aufwände für Informationssicherheit in Ihrer Leitstelle in Bezug auf die Sachmittel für die Bauunterhaltung?* (Mehrfachantworten möglich)




In zehn Fällen wird der aktuelle Ansatz für Sachmittel für die Bauunterhaltung als ausreichend angesehen, in weiteren zehn Fällen als nicht ausreichend. Bei vier Leitstellen geht man davon aus, dass der derzeitige Mittelansatz auch zukünftig ausreichen wird, in sechs Fällen wird erwartet, dass der Mittelansatz künftig nicht ausreichen wird.

## A.107 Sachmittel für Organisatorisches

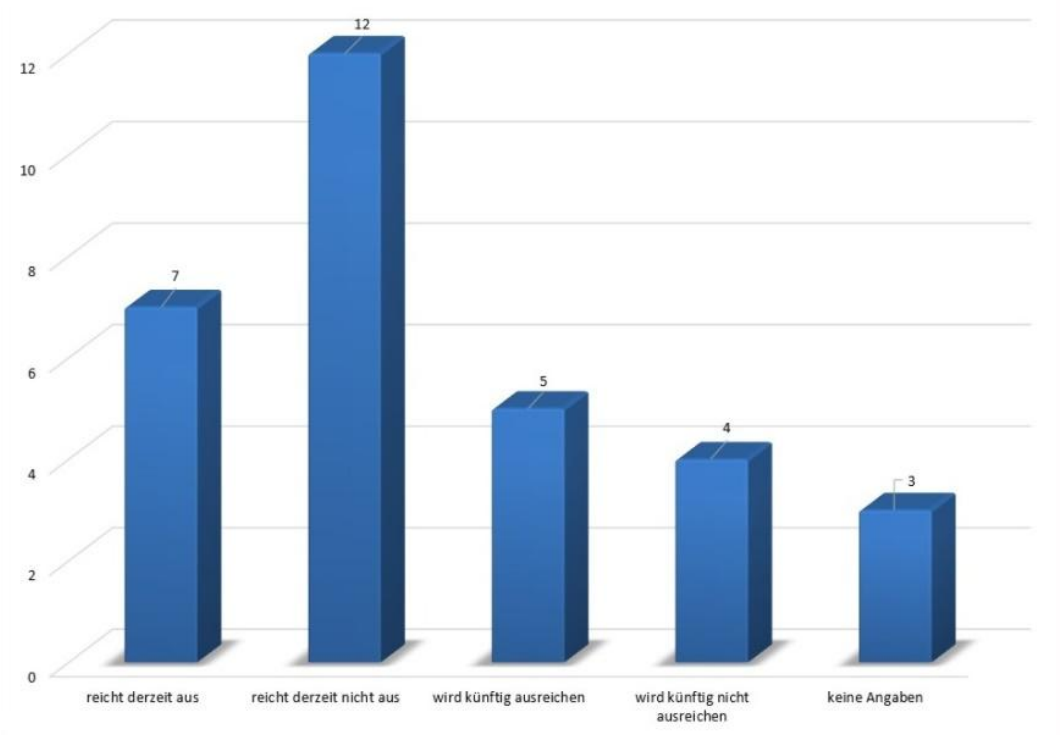
Frage: *Wie beurteilen Sie die Aufwände für Informationssicherheit in Ihrer Leitstelle in Bezug auf die Sachmittel für organisatorische Maßnahmen (externe Beratung, Audits usw.)?* (Mehrfachantworten möglich)




In acht Fällen wird der aktuelle Ansatz für Sachmittel für organisatorische Maßnahmen als ausreichend angesehen, in elf Fällen als nicht ausreichend. Bei fünf Leitstellen geht man davon aus, dass der derzeitige Mittelansatz auch zukünftig ausreichen wird, in weiteren fünf Fällen wird erwartet, dass der Mittelansatz künftig nicht ausreichen wird. In zwei Fällen wurden keine Angaben gemacht.

## A.108 Vorgaben

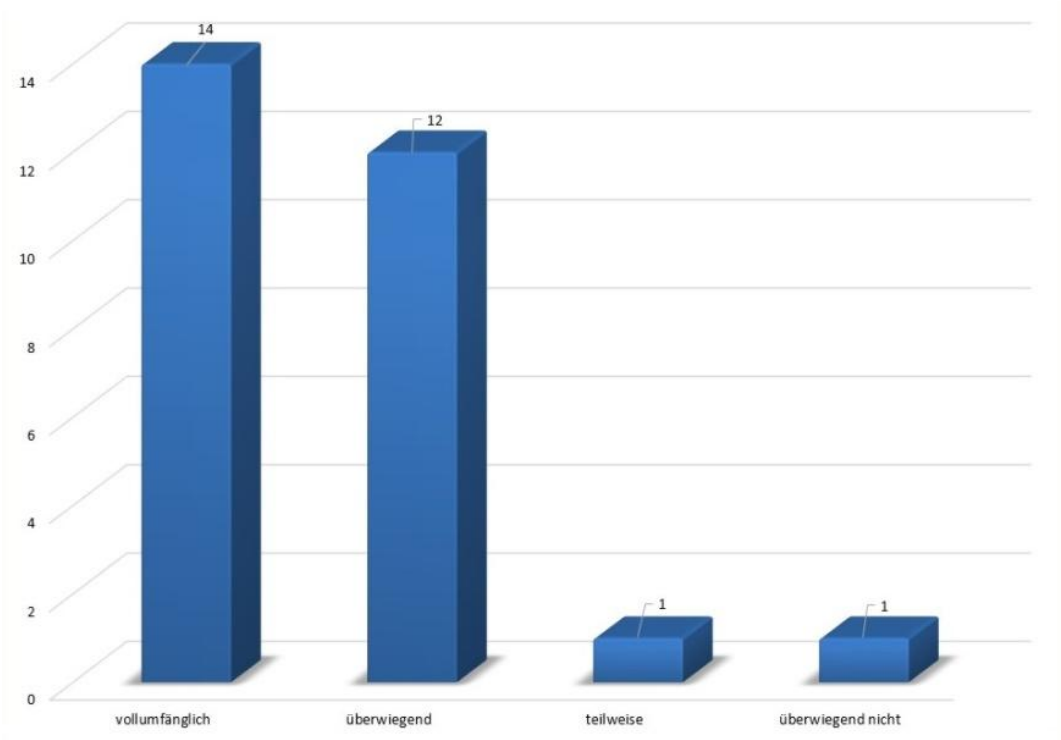
Frage: *Wie beurteilen Sie organisatorische und betriebliche Vorgaben der übergeordneten Stelle/Behörde?* (Mehrfachantworten möglich)




In sieben Fällen werden die aktuellen Vorgaben für organisatorische und betriebliche Vorgaben übergeordneter Stellen/Behörden als ausreichend angesehen, in 12 Fällen als nicht ausreichend. Bei fünf Leitstellen geht man davon aus, dass der derzeitige Regelungsumfang auch zukünftig ausreichen wird, in vier Fällen wird erwartet, dass der Regelungsumfang künftig nicht ausreichen wird. In drei Fällen wurden keine Angaben gemacht.

## A.109 Akzeptanz

Frage: *Wie schätzen Sie aktuell und künftig die Akzeptanz von IT-Sicherheitsmaßnahmen bei Ihren Mitarbeitern ein?* (Mehrfachantworten möglich)




Bei 14 der 28 Standorte (50 %) geht man davon aus, dass die Sicherheitsmaßnahmen aktuell und zukünftig vollumfängliche Akzeptanz bei den Mitarbeitern finden. In 12 Fällen wird von einer überwiegenden Akzeptanz ausgegangen, in jeweils einem Fall von teilweiser Akzeptanz bzw. einer überwiegenden Ablehnung der Sicherheitsmaßnahmen.