IABG

Whitepaper

INFOKOM.
digital.
sicher.
vernetzt.

Anforderungen an eine moderne Leitstelle

Leitstellen sicherer machen

Mitarbeiterinnen und Mitarbeiter einer Leitstelle wissen, wie zuverlässig diese funktionieren muss. Dass es bei einem Notruf auf jede Sekunde ankommt, ist der Ansporn aller Beteiligten. Die Dauer, bis die Rettungs- oder Sicherheitskräfte am Einsatzort eintreffen, kann zwischen Leben und Tod entscheiden. Eine Leitstelle leitet den Einsatzbetrieb der zugeordneten Organisationen, nimmt Informationen entgegen, wertet sie aus und koordiniert die angeschlossenen Dienste.

Leitstellen gibt es in vielen Bereichen: zur medizinischen und technischen Rettung von Menschenleben, zur Brandbekämpfung, im Katastrophenschutz und für die öffentliche Sicherheit und Ordnung.

Eine sichere Leitstelle ist die Grundlage der täglichen Arbeit – rund um die Uhr – an jedem Tag im Jahr. Sie ist eine kritische Infrastruktur – sicher und resilient gegenüber menschlichem Versagen, natürlichen Bedrohungen sowie physischen wie virtuellen Angriffen von innen und außen.

Die IABG ist ein verlässlicher Partner bei der Konzeption, Umsetzung und dem Betrieb von Leitstellen und Lagezentren. Es ist uns ein Anliegen, unsere Partner auf dem Weg zu einer sicheren Leitstelle zu begleiten.

Mit diesem Whitepaper wollen wir unsere Kunden sensibilisieren, welche Anforderungen an eine sichere Leitstelle der Zukunft gestellt werden und wie diese Anforderungen umzusetzen sind.

Die Veränderungen in der Leitstellenwelt betreffen alle Betreiber dieser kritischen Infrastruktur. Denn die Anforderungen an eine Leitstelle wachsen stetig und leider steigen parallel auch die Bedrohungen. **Lassen Sie uns gemeinsam Ihre Leitstelle gestalten: vernetzt und integriert sowie resilient und sicher.**

Einsatz sicherer IT für die resiliente Leitstelle von morgen

Der Einsatz sicherer IT ist für eine moderne Leitstelle unerlässlich. Neben dem Einsatzleitsystem als Kernanwendung spielen dabei querschnittliche IuK-Funktionalitäten/-Dienste, die zum Betrieb der Leitstelle notwendig sind, eine wichtige Rolle. Beispielsweise betrifft dies die Übertragung von Daten innerhalb der Leitstelle, den Anschluss an ein übergreifendes IT-Netz und die Systemadministration.

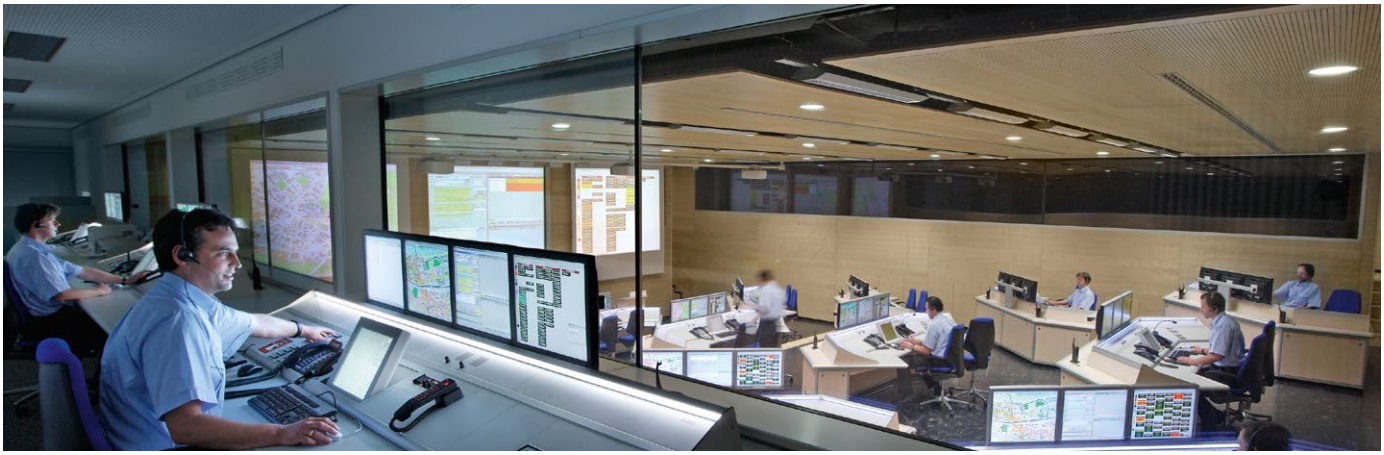
Leitstellen sind rund um die Uhr erreichbar und kommunizieren sowohl untereinander als auch mit den Einsatzmitteln und der Bevölkerung mittels Datenverbindungen, Digitalfunk, Mobil- und Festnetztelefon und Sonderkommunikationseinrichtungen. Wesentliche Entscheidungen einer Leitstelle beruhen auf der Integrität und der Verfügbarkeit von Informationen, welche in Datenbanken oder anderen Informations-Verarbeitungs-Systemen gespeichert und verarbeitet werden. Mehr und mehr spielt dabei die Erfassung und Analyse der Daten in Echtzeit eine tragende Rolle.

Eine funktionsfähige Informationstechnik und ein sicherheitsbewusster Umgang mit dieser sind wesentliche Voraussetzungen die Aufgaben zu erfüllen. Der Schutz der Vertraulichkeit von Informationen ist besonders dann hervorzuheben, wenn personenbezogene Daten betroffen sind oder weitere sensitive Daten, die nicht offen zugänglich sein sollen. Basierend auf dem Schutzbedarf und den Risiken muss jede Organisation Anforderungen definieren und die erforderlichen Sicherheitsmaßnahmen planen, umsetzen, betreiben, kontrollieren und kontinuierlich verbessern.

Leitstellen sicherer machen

INFOKOM.
digital.
sicher.
vernetzt.

IABG
Whitepaper



Nachfolgend einige Anforderungen an Betreiber und Technologieneinsatz für den sicheren Betrieb einer Leitstelle:

01. Daten, Verfahren und IT-Systeme müssen im erforderlichen Umfang verfügbar sein. Meldungsannahme, Disposition, Einsatzunterstützung, weitere Prozesse und Entscheidungen dürfen nicht durch IT-Ausfälle verhindert oder maßgeblich behindert werden.

02. Die Integrität der Daten und Verfahren ist zu gewährleisten. Verfälschte Daten bzw. manipulierte Systemfunktionen sind mindestens im Sinne eines Verlustes der Verfügbarkeit zu bewerten. Im schlimmsten Falle, wenn gezielte Verfälschungen/Manipulationen nicht erkannt werden, kann auch ein höherer Schaden entstehen als beim bloßen Verlust der Verfügbarkeit.

03. Daten sind gegen Missbrauch, unberechtigte Zugriffe und gegen Verlust zu schützen.

04. Zur Gewährleistung der Authentizität, Integrität der Daten und Vertraulichkeit bei der Datenübertragung sind die erforderlichen Maßnahmen zu ergreifen.

05. Die Beteiligung an einem sicherheitsrelevanten IT-Vorgang darf nicht erfolgreich geleugnet werden können (Verbindlichkeit als Teilaspekt der Integrität).

06. Gesetzliche, verwaltungsinterne vertragliche und aufsichtsrechtliche Regelungen und Verpflichtungen müssen eingehalten werden.

07. Es ist sicherzustellen, dass die IT-Nutzer in ihrem Zuständigkeitsbereich für die Datensicherheit, die Systemsicherheit, die Rechtssicherheit bei der Datenerfassung und die Netzwerksicherheit Sorge tragen.

08. IT-Sicherheit lebt, d.h. es ist ein fortlaufender Prozess zu implementieren mit regelmäßigen und anlassbezogenen Überprüfungen und Verbesserungen.

09. Festlegungen und Ergebnisse zum IT-Sicherheitsprozess sind angemessen zu dokumentieren.

10. Die IT-Sicherheitsanforderungen sind durch Maßnahmen aus den Bereichen Infrastruktur, Organisation, Personal und Technik zu ergänzen bzw. zu verstärken.

11. Der Zugriff auf sicherheitskritische IT-Systeme, IT-Anwendungen und Daten, ist auf den unbedingt notwendigen Personenkreis einzuschränken. Dabei ist verboten, was nicht explizit erlaubt ist. Jeder Nutzer erhält nur die Zugriffsrechte auf IT-Systeme, IT-Anwendungen und Daten, die zur Erfüllung der jeweiligen Aufgabe, insbesondere unter Wahrung der datenschutzrechtlichen Bestimmungen, erforderlich sind.

12. Die Mitarbeiterinnen und Mitarbeiter sind im erforderlichen Umfang bezüglich der IT-Sicherheit zu sensibilisieren und zu qualifizieren. Alle Mitarbeiterinnen und Mitarbeiter sind einer Überprüfung mindestens nach Ü1 zu unterziehen.

13. Die Grenzen des lokalen Netzwerkes sind mit effektiv konfigurierten Firewall-Systemen zu schützen. Es darf keine verdeckten Zugangsmöglichkeiten zum LAN geben.

14. Wichtige Systeme sind redundant auszulegen.

15. Das Betriebsrisiko bzw. der Schutzbedarf des jeweiligen IT-Systems bestimmt den notwendigen Sicherheits- und Kontrollumfang. Üblicherweise wird die Angemessenheit bereits durch die Grundschutzvorgehensweise gewährleistet.

16. Für alle Teile des gesamten IT-Verbundes (Rechner, Daten und Verfahren) müssen namentlich Systemverantwortliche ernannt werden.

17. Jeder Nutzer ist für die sachgerechte Nutzung der IT-Systeme in seinem Wirkungsbereich verantwortlich und entsprechend zu sensibilisieren.

18. Durch Protokollierung, Interpretation und Korrelation von Aktionen und Ereignissen ist zu gewährleisten, dass alle sicherheitsrelevanten IT-Vorgänge nachvollziehbar sind.

Leitstellen sicherer machen

INFOKOM.
digital.
sicher.
vernetzt.

IABG
Whitepaper

Sicherheitsstrategie und Schutzziele für Leitstellen

Die Daten, Verfahren, Systeme, Netze und Infrastrukturkomponenten des Informationsverbunds einer Leitstelle sind hinsichtlich der drei Grundwerte **Vertraulichkeit, Integrität und Verfügbarkeit** zu schützen. Der Schutz sollte mindestens das Niveau des IT-Grundschutzes des BSI umfassen.

Besondere Risiken erfordern weitergehende Schutzmaßnahmen. Die besondere Herausforderung ist hierbei, dass eine Leitstelle kein „geschlossenes System" darstellt, sondern in vielfältiger Weise Kommunikations-/Datenverbindungen mit anderen unterhält.

Kommunikations-/Datenverbindungen einer Leitstelle

Zukünftige Herausforderungen

Einsatzleitsysteme und Leitstelleninfrastruktur sind oftmals gewachsene Technologien und Strukturen, die über einen längeren Zeitraum genutzt werden. Um die Funktionalität zu verbessern und die Leistungsfähigkeit zu halten, gibt es vermehrt neuartige Technologien und Verfahren. Die damit einhergehenden Chancen und Risiken für die Informationssicherheit müssen analysiert und entsprechende Sicherheitsmaßnahmen umgesetzt werden.

Beispiele sind:

- Künstliche Intelligenz / Maschinelles Lernen
- Big Data
- Datenerfassung in Echtzeit
- Virtualisierung und Containertechnologien
- Cloudnutzung
- Internet of Things
- OT Security

Leitstellen sicherer machen

INFOKOM.
digital.
sicher.
vernetzt.

IABG Whitepaper

Schritte zu einer sicheren Leistelle

Wir haben nachfolgend einige Schritte aufgeführt, wie eine sichere Leitstelle implementiert werden kann:

- Frühzeitig Sicherheitsanforderungen – bereits bei der Planung von Leitstellen – berücksichtigen
- Ressourcen für Informationssicherheit einplanen
- Sicherheitsziele und –strategie in einer Sicherheitsleitlinie dokumentieren
- Sicherheitsorganisation festlegen
- IT-Sicherheitskonzept erstellen
- Leitstelle für eine Zertifizierung nach ISO 27001 auf Basis BSI IT-Grundschutz vorbereiten
- Fehlende Maßnahmen umsetzen
- Leitstelle auf Basis von BSI IT-Grundschutz auditieren und zertifizieren lassen
- Interne Audits und IS-Revisionen in der Leitstelle durchführen
- IT-Sicherheitsmanagement im operativen Betrieb durchführen
- Mitarbeiterinnen & Mitarbeiter zu Themen der Informationssicherheit sensibilisieren und schulen lassen

Wenn Ihre Leitstelle im Verbund mit mehreren Leitstellen betrieben wird oder werden soll, so ist auch dieser Verbund zu betrachten. Dann sind die folgenden zusätzlichen Schritte notwendig:

- IT-Sicherheitsrahmenkonzept für den Leitstellenverbund erstellen und regelmäßig aktualisieren
- IT-Sicherheitskonzepte mit IT-Rahmenkonzept abgleichen, konkretisieren und individuell ergänzen

Wir führen Ihre Leitstelle zu einer erfolgreichen Zertifizierung

Die integrierte Leitstelle Hochfranken des Bayerischen Roten Kreuzes und die Integrierte Leitstelle Allgäu sind die ersten Leitstellen in Deutschland, die vom Bundesamt für Sicherheit in der Informationstechnik nach ISO 27001 auf BSI Grundschutz zertifiziert wurden.

Auch Ihre Leitstelle soll zertifiziert werden?
Dann brauchen Sie einen Partner, der Sie auf diesem Weg begleitet. Mit unserer jahrelangen Expertise können wir Ihre Leitstelle auf eine Zertifizierung vorbereiten und führen diesen Prozess auch gemeinsam mit Ihnen durch. Alternativ können wir bei Leitstellen, in denen wir nicht beratend tätig waren, das Zertifizierungsaudit durchführen.

Wir rücken mit Ihnen die sichere Leitstelle in den Vordergrund Ihrer Arbeit

Die IABG ist ein deutsches, herstellerneutrales und unabhängiges Unternehmen, welches seit Jahren ein anerkannter Partner der öffentlichen Hand und insbesondere der BOS ist. Wir sind ein vom BSI zertifizierter IT-Sicherheitsdienstleister für IS-Revision und IS-Beratung.

WIR SIND EIN VOM BSI ZERTIFIZIERTER IT-SICHERHEITS-DIENSTLEISTER FÜR IS-REVISION UND IS-BERATUNG.

Die IABG verfügt über zertifizierte Auditteamleiter für ISO 27001 auf der Basis von BSI IT-Grundschutz, welche auch persönlich umfangreiche Erfahrungen zu Leitstellen besitzen. Vom BSI zertifizierte IS-Revisions- und Beratungsexperten (IS-Revisoren), welche diese Prüfungen an Leitstellen durchführen bzw. Leitstellen dazu anleiten können, runden diese Expertise ab. Für ein effektives Management der Informationssicherheit unterstützt Sie die IABG gerne als kompetenter Partner.

Nachstehend ein **Auszug aus unserem Portfolio**: Wir führen ein *Informations-Sicherheitsmanagement-System* ein und optimieren die IT-Sicherheit der Leitstelle:

- Grundschutz-Sicherheitskonzepte erstellen
- Risikoanalysen durchführen
- Ersatzbausteine erstellen
- Vorlagen für eine Sicherheitsdokumentation werden bereitgestellt
- Schulungen durchführen
- Auditierung und Zertifizierung, IS-Revision

ISMS nach ISO 27001

Mit der internationalen Standardreihe ISO 2700x kann auch ohne Grundschutz und BSI Standards ein Managementsystem zur Informationssicherheit aufgebaut und betrieben werden. Dies ist sicherlich eine Option, die in einigen Anwendungsgebieten sinnvoll ist – die fundiertere und nachhaltigere Lösung ist allerdings ISO 27001 auf Basis von BSI IT-Grundschutz.

Leitstellen sicherer machen

Referenzen

Integrierte Leitstelle Hochfranken

Die IABG hat die Integrierte Leitstelle Hochfranken bei der Zertifizierung ISO 27001 auf Basis IT-Grundschutz begleitet. Bei der Integrierten Leitstelle Hochfranken handelt es sich um die erste von 26 bayerischen Leitstellen, die diese Zertifizierung erfolgreich durchlaufen hat.

Kooperative Leitstelle Berlin

Bei der Kooperativen Leistelle für die Berliner Polizei und Berliner Feuerwehr haben wir die IT-Sicherheitsberatung im Rahmen der Planung und Vergabe dieser neuartigen Leitstelle durchgeführt. Die beiden ursprünglichen Notrufleitstellen werden mit einem gemeinsamen IT-Verfahren auf Basis einer gemeinsamen Technikplattform zusammengeführt und bieten dann eine gegenseitige technische wie räumliche Redundanz. Zudem führen wir hier die IT-Qualitätssicherung durch, zu der auch regelmäßige Revisionen gemäß BSI Grundschutz gehören.

Bayerische integrierte Leistellen

Die IABG mbH hat bereits mehrfach das IT-Sicherheitsrahmenkonzept für die integrierten Leitstellen in Bayern erstellt bzw. fortgeschrieben. Zuletzt erfolgte dies in 2020. Das IT-Sicherheitsrahmenkonzept dient dazu, den Leitstellen eine Vorlage zur Erstellung eigener Sicherheitskonzepte bzw. zur Vorbereitung einer Zertifizierung zu geben.

Die IABG besitzt in beiden "Welten" Erfahrungen und Expertise, beispielsweise in dem sie auch über mehrere ausgebildete Lead Auditoren für den internationalen Standard ISO 27001 verfügt.

Auf Wunsch können diese Sie beim Aufbau und der Zertifizierungsvorbereitung eines ISMS nach dem internationalen Standard ISO 27001 unterstützen.

Für weitere Informationen wenden Sie sich bitte an:

Konrad Rosmus
Leiter Zertifizierte Prüfstelle IS
rosmus@iabg.de
www.iabg.de

Dr. Stephan Gottwald
Leiter Leitstellen & Lagezentren
gottwald@iabg.de
www.iabg.de