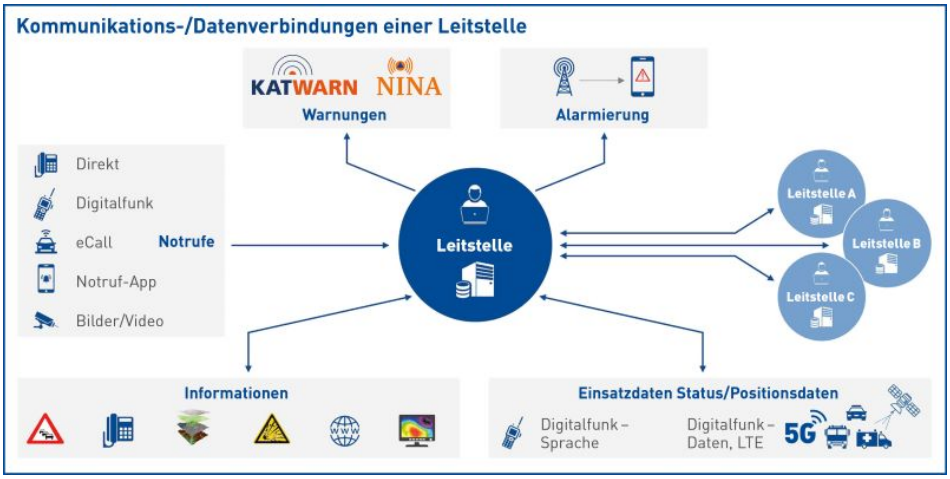
Vernetzt und sicher – aktuelle Herausforderungen für Leitstellen und Lagezentren

Artikel vom **3. August 2022**
ITK und Dienstleistungen

Die Dauer, bis die Rettungs- oder Sicherheitskräfte am Einsatzort eintreffen, kann zwischen Leben und Tod entscheiden. Eine Leitstelle nimmt Notrufe entgegen, sammelt Informationen, wertet diese aus und alarmiert die Einsatzkräfte: täglich – rund um die Uhr – an jedem Tag im Jahr. Insbesondere die Bürger verlassen sich auf die Organisation, die Technik und die Mitarbeiter in den Leitstellen, damit Leben gerettet, Brände gelöscht, Güter geborgen und Menschen, Objekte und die Umwelt geschützt werden.



Beispielhafte Kommunikationsverbindungen einer Leitstelle. (Abb. 1, Bilder/Grafiken: IABG mbH)

Neben Finanzinstitutionen, Technologieunternehmen oder ausländischen Organisationen sind auch deutsche Krankenhäuser, Kreisverwaltungen, Gerichte, anerkannte Institutionen wie das Rote Kreuz und auch BOS-Leitstellen Ziele von Cyberangriffen.

Aktuelle Cyber-Vorfälle

• Laut einer Umfrage des Bayerischen Rundfunks und Zeit Online 1) ist es Tätern im Juni 2021 in mehr als 100 Fällen gelungen, den Zugriff von Behörden und öffentlichen Organisationen auf IT-Systeme zu verhindern. Hacker haben Server verschlüsselt und Geld erpresst. Ähnliche Vorfälle gab es in Schwerin, im Landkreis Ludwigslust-Parchim sowie in Wismar, Greifswald und Stralsund.

- Die Stadt Witten ist im Oktober 2021 Opfer eines massiven Hackerangriffes geworden, der die gesamte Stadtverwaltung lahmlegte.
- Im September 2020 verstarb eine Patientin in einem Rettungswagen, da die Uniklinik Düsseldorf wegen eines Hackerangriffs auf ihre IT-Systeme den Rettungswagen abweisen musste. Eigentlich galt der Angriff einer benachbarten Universität 2).
- Die Feuerwehr St. Ruprecht an der Raab wurde im Mai 2021 Opfer eines Cyberangriffs. Alle Daten waren nach dem Angriff verloren.
- Im Februar 2022 wurde öffentlich 3), dass das Internationale Rote Kreuz im Januar 2022 Opfer eines Cyberangriffs wurde. Die Spuren des Angriffs ließen sich über 2 Monate bis November 2021 zurückverfolgen. Analysen zeigten, dass es sich um einen »Advanced Persistent Threat« handelte und die Angreifer Verschleierungstechniken nutzten. Mehrere Server wurden kompromittiert, Active Directory und andere Daten exfiltriert.
- Inwieweit die kritische Sicherheitslücke in der bei Leitstellen beliebten Fernzugriffssoftware Citrix es Angreifern ermöglicht hat 4), unbemerkt in Systeme einzudringen, ist öffentlich nicht bekannt.

Kommunikationsverbindungen und Cyberbedrohungen

Leitstellen sind rund um die Uhr erreichbar und kommunizieren sowohl untereinander als auch mit den Einsatzkräften, -mitteln 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 IT-Systemen gespeichert und verarbeitet werden. Eine exemplarische Übersicht der Kommunikationsverbindungen einer Leitstelle zeigt Abbildung 1. Im Folgenden sind Szenarien beschrieben, wie Leitstellen über diese Kommunikationsverbindungen angegriffen werden können – sie sind alle vorhanden und bereits zur Anwendung gekommen. Das Fluten von IT-Systemen, damit diese durch die Masse an Anfragen zum Erliegen kommen, gehört zur Kategorie der »Denial-of-Service«(»DoS«)-Angriffe. Solche Angriffe stören nicht nur Serversysteme und Webseiten, sondern auch die notwendige Erreichbarkeit einer Leitstelle. Daher ist eine »DoS«-Attacke mittels Hoax-Notrufen, d. h. Notrufen, die keine Notsituation oder Hilfeersuchen darstellen, eine ernst zu nehmende Bedrohung für die Verfügbarkeit einer Leitstelle. Ein perfider Angriff ist das »Swatting«. Notrufe scheinen echt zu sein, täuschen aber einen Notfall vor und provozieren damit, dass Einsatzmittel zu Orten geschickt oder von anderen Einsatzorten womöglich abgezogen werden, ohne dass ein realer Anlass bzw. Hintergrund besteht. Die Verlässlichkeit von Notrufen, weiterer Informationsquellen (z. B. Gefahrstoffdatenbanken, Wetter-, Verkehrs- oder sonstiger geobasierter Daten) oder recherchierten Daten ist ein wesentlicher Aspekt der Leitstellenarbeit. Manipulationen dieser Informationen, der entsprechenden Webseiten oder Informationssysteme gefährden die Verlässlichkeit, d. h. die Integrität der Daten, erheblich. Dies führt zu potenziellen Fehlentscheidungen in der Bearbeitung von Notrufen und Hilfeersuchen. Eine weitere Störung der Datenintegrität stellt das folgende Szenario dar: Jede Leitstelle hat ihre Prozesse auf die genaue Kenntnis des Einsatzortes sowie der eigenen

Einsatzmittel ausgerichtet. Das passende Fahrzeug wird schnell bestimmt, alarmiert und durch Navigationssysteme unterstützt, um es auf kürzestem Weg zum Unfallort zu schicken. Hierbei verlassen wir uns derzeit auf das satellitengestützte GPS. Dessen Signale nutzen unsere Handys, Tablets, Digitalfunkgeräte oder Navigationsgeräte, um eine genaue Positionsbestimmung vornehmen zu können. Doch was passiert, wenn dieses von Satelliten ausgestrahlte Signal gestört wird? Statt präziser, realer GPS-Daten, aus denen genaue Positionen errechnet werden können, erhält man ein unverständliches Rauschen, so dass die auf realen Ortsdaten basierenden Algorithmen eines Einsatzleitsystems nicht mehr sauber funktionieren oder das Navigationssystem nicht mehr den schnellsten Weg zum Einsatzort weist. Diese Bedrohung ist zwischenzeitlich real, denn das GPS-»Jamming« ist durch einfache Geräte umsetzbar. Der in Deutschland zwar verbotene, aber durchaus verbreitete Einsatz dieser Geräte hat teilweise eine völlig andere Ursache, nämlich die Verhinderung der Überwachung von Transportlogistik. Diese Verbreitung stellt damit auch eine ernste Gefahr für den Betrieb von Leitstellen dar. Übertroffen wird diese Gefahr durch sogenannte »Spoofing«-Angriffe. Normalen GPS-Empfängern werden dabei reale Positionen vorgegaukelt, was bei geringeren Abweichungen vom eigentlichen Ort schwer erkannt wird. Ungeeignete Einsatzmittel werden somit alarmiert oder die Navigation bei der Anfahrt empfindlich gestört.

Vernetzung mit anderen Leitstellen und Lagezentren

Die Zusammenarbeit und der Informationsaustausch mit anderen Leitstellen ist Teil der täglichen Arbeit in einer Leitstelle. Dabei sind situationsabhängig vielfältige Nachbarleitstellen zu involvieren, Leitstellen anderer BOS oder benachbarter Gebiete, Leitstellen von Versorgern oder Verkehrsunternehmen und vieles mehr (vgl. Abbildung 2). Wie überall steigt die Anzahl der zu bearbeitenden Vorgänge, und es ist das Bestreben, die Daten (Einsatzorte, Einsätze, Einsatzmittelanforderungen oder -bereitstellungen) so effizient wie möglich weiterzuleiten und zu verarbeiten. Es gilt, die Disponenten von Routinetätigkeiten zu entlasten und dennoch das gesamte Geschehen (z. B. Position und Status aller Einsätze und Einsatzmittel) transparent im Blick zu haben. Aktuell wird noch in großem Umfang auf das Telefon zurückgegriffen und die Information per Sprache übermittelt. Die Notwendigkeit, dies über einen schnellen Datenaustausch von und zu den benachbarten Leitstellen abzuwickeln, ist unbestritten. Aber jede Schnittstelle nach außen birgt auch neue Risiken:

- Kommuniziere ich wirklich mit »dem Richtigen«?
- Interpretiert mein Nachbar die Daten genauso wie ich?
- Hört/Liest jemand mit oder manipuliert die Daten auf dem Übertragungsweg?

Die meisten dieser Fragen stellen sich auch bei einer verbalen Kommunikation wie einem persönlichen Anruf: Aber wir machen uns relativ wenig Gedanken, da wir an Sprache und Äußerungen des (bekannten) Gesprächspartners sofort erkennen, ob der Sachverhalt verstanden wurde. Wechselt man zu einer rein elektronischen Kommunikation, so steht die Authentizität der adressierten Nachbarleitstelle bzw. des angesprochenen Systems im Vordergrund. Wie kann man zudem sicherstellen, dass sich auf dem Übertragungsweg kein Angreifer (»man-in-the-middle«) in die Kommunikation einklinkt? Reicht hier eine einfache VPN-Verbindung oder sollte ich hier weitergehende Sicherheitsmaßnahmen integrieren? Die Adressierung der zweiten, oben aufgeworfenen Frage zielt u. a. auf die Nutzung standardisierter Datenformate ab, wie sie beispielsweise die vom PMeV veröffentlichte UCRI-Schnittstelle 5) bzw. Datenübertragungsprotokolle wie »REST« definieren. Eine weit größere Herausforderung stellt jedoch die gemeinsame Sprache bzw. Bezeichnung der Fachlichkeit von Einsatzstichworten, Ortsbezeichnungen, Definition von Einsatzmitteln etc. dar. Interpretieren die Einsatzleitsysteme bzw. die sie nutzenden Disponenten alle Angaben gleich? Die dritte Frage berührt wieder die Sicherstellung der Integrität der

übermittelten Daten sowie den im Leitstellenkontext sehr wesentlichen Aspekt des Datenschutzes.

Herausforderungen für eine sichere Vernetzung

Da die in Abbildung 2 dargestellten Kommunikationsbeziehungen und Vernetzungen sowie die damit verbundenen Risiken nahezu alle Leitstellen betreffen, besteht die gemeinsame Herausforderung darin, diesen Risiken auch gemeinsam zu begegnen 6):

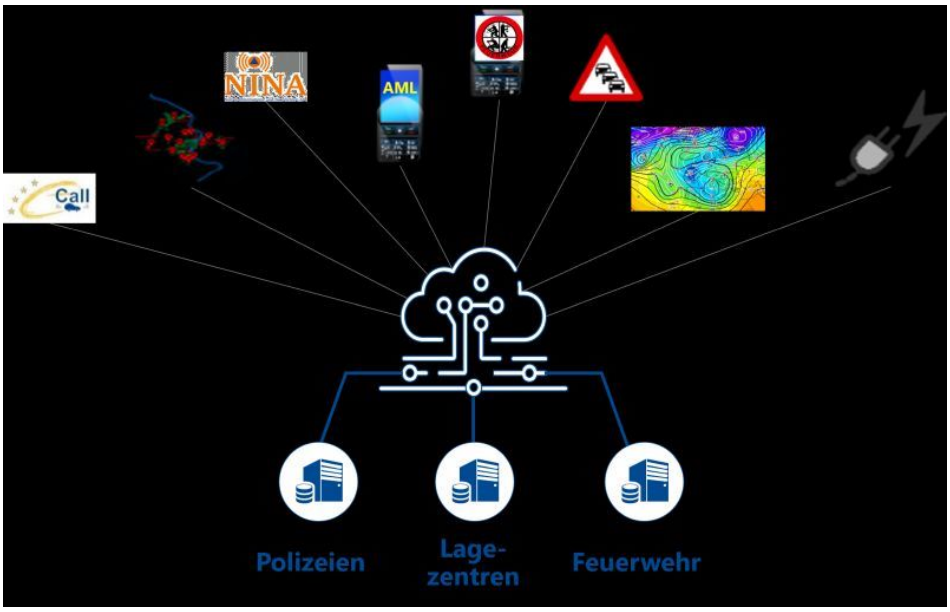
Vernetzung von Leitstellen mit angrenzenden Organisationen (Abb. 2).

• Gemeinsame IT-Sicherheitsmaßnahmen: Hierzu zählen technische Maßnahmen wie Netzsegmentierungen, Sicherheitsgateways, Zertifikatsprüfungen, Patchmanagement und ein technisches Monitoring mit entsprechenden Alarmierungen. Ebenso wichtig ist auch das Vorhandensein von qualifizierten IT-Spezialisten, die nicht nur die Komplexität beherrschen und stets auf einem aktuellen Wissensstand, sondern auch 24x7 verfügbar sind.

- Gemeinsame Anforderungen und Umsetzungen beispielweise auf Basis des BSI-Grundschutzes sowie Verfahrensweisen, die ein abgestimmtes Vorgehen sowohl im Normalbetrieb als auch im Störungs- bzw. Ausnahmefall gewährleisten.
- Gegenseitiges Vertrauen oder besser eine neutrale Prüfung/Auditierung, denn individuelle Fehler oder Nachlässigkeiten können leicht zu Gefährdungen vieler benachbarter Leitstellen führen.

Ausblick

Die Vernetzung von Leitstellen und Lagezentren mit der Nutzung vielfältiger neuer Informationsdienste und Schnittstellen erfordert die Identifikation, Bewertung und frühzeitige Mitigation der angesprochenen Risiken. Dies verursacht in jeder Leitstelle einen großen technischen, organisatorischen und personellen Aufwand. Vor diesem Hintergrund wurde die Idee entwickelt, zentral ein Gateway bzw. einen Hub zu schaffen, an dem sich alle Leitstellen und Lagezentren anschließen können (Abbildung 3).



Zentral bereitgestellte Leitstellendienste (Abb. 3).

Die Vorteile liegen hier vor allem in einem einmaligen Anpassungsaufwand bei neuen, sich ändernden Schnittstellen und einem »standardisierten« Anschluss für alle Leitstellen, wodurch insbesondere auch die IT-Sicherheit durch die Aggregation der Schnittstellen über einen zentralen Anbieter deutlich erhöht wird und eine technische/administrative Entlastung der Leitstellenbetreiber erfolgt. Die Diskussionen in der nächsten Zeit werden zeigen, ob und wie eine derartige Idee umgesetzt wird. Autor: Dr. Stephan Gottwald Programm-Manager IABG mbH 10117 Berlin Fussnoten: 1) https://www.tagesschau.de/investigativ/br-recherche/ransomware-103.html 2) https://www.handelsblatt.com/technik/sicherheit-im-netz/cyberkriminalitaet-todesfall-nach-hackerangriff-auf-uni-klinik-duesseldorf/26198688.html 3) https://www.icrc.org/de/document/cyberangriff-ikrk-was-wir-wissen 4) https://www.sueddeutsche.de/digital/citrix-sicherheitsluecke-1.4755894?print=true 5) Universal Control Room Specification 6) Vgl. WhitePaper »Anforderungen an eine moderne Leitstelle – Leitstellen sicherer machen«, IABG mbH

Hersteller aus dieser Kategorie

---

medDV GmbH
Rudolf-Diesel-Str. 10
D-35463 Fernwald
06404 20517-0
info@meddv.de
www.meddv.de
Firmenprofil ansehen

Eurocommand GmbH
Schnackenburgallee 217-223
D-22525 Hamburg
040 2396963-0
contact@eurocommand.com
www.eurocommand.com
Firmenprofil ansehen

Vomatec Innovations GmbH
Riegelgrube 7
D-55543 Bad Kreuznach
0671 796140-0
info@vomatec.de
www.vomatec.de
Firmenprofil ansehen