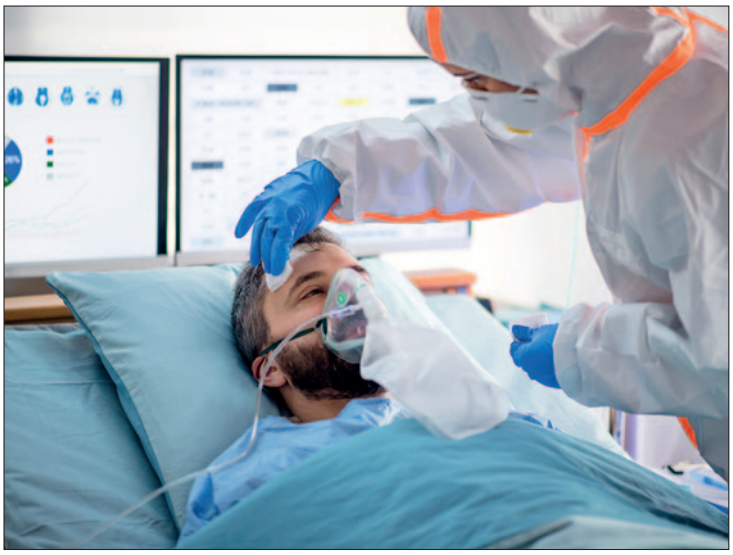
Funktionsfähigkeit erhalten

BVT-Expertinnen und -Experten schulen Sicherheitsverantwortliche von Krankenhäusern, um Bedrohungen und Schwachstellen im Gebäude, am Gelände und in der IT zu erkennen.

Krankenhäuser müssen als Teil der kritischen Infrastruktur wegen ihrer Bedeutung für das Wohlergehen der Bevölkerung besonders geschützt werden. Neben der Gefahr eines Anschlags durch Terroristen oder Computerhacker, technische Pannen, Naturkatastrophen, Stromausfall, Sabotage oder Bombendrohungen ist seit dem Auftreten des Coronavirus deutlich geworden, wie wichtig die Aufrechterhaltung der Funktionalität der Spitäler, der Pharmaunternehmen und der Nahrungsmittelversorgung ist. Gesundheitseinrichtungen sind von Strom, Trinkwasser, Informations- und Kommunikationstechnologie, Transport- und Logistikdienstleistungen und von spezialisiertem Personal abhängig. Auch wenn im Falle einer Pandemie rigorose Einschränkungen im gesellschaftlichen Leben stattfinden, muss die Versorgung der Gesellschaft mit lebensnotwendigen Dienstleistungen oder Gütern sichergestellt werden.



Krankenhäuser müssen als wesentliche Einrichtungen der kritischen Infrastruktur vor Ausfall und Bedrohungen geschützt werden.

Für den vorbeugenden Schutz von Pharmazieherstellern- und händlern, Rettungsorganisationen sowie Krankenhäusern sind die Sicherheitsbehörden gem. § 22 Sicherheitspolizeigesetz (SPG) verantwortlich. Zuständig ist das Bundesamt für Verfassungsschutz und Terrorismusbekämpfung (BVT) mit den Landesämtern für Verfassungsschutz und Terrorismusbekämpfung (LVTs) der Landespolizeidirektionen.

„Schützenswertes Krankenhaus". 2018 wurde die Workshop-Reihe „Schützenswertes Krankenhaus" des BVT gestartet. Ziel der Workshop-Reihe ist es, mögliche Risiken zu erkennen, die die Funktionsfähigkeit von Krankenhäusern beeinträchtigen könnten und Strategien dagegen zu entwickeln. Gefahren bestehen durch veraltete Technik, unzureichende Schutzmaßnahmen, mangelnde Überprüfung von Notfallmaßnahmen oder durch unzufriedene Mitarbeiter. Die Schulung zielt darauf ab, Betriebsausfälle zu verhindern, Schäden zu begrenzen und Menschen zu schützen. In den Workshops werden drei Themenbereiche behandelt, die für die Sicherheit der Spitäler als besonders wichtig erachtet wurden: „Cyber-Sicherheit für Krankenhäuser", „Objektschutz von Krankenhäusern" und „medizinischer Krisen- und Katastrophenschutz".

Cyber-Sicherheit. Die Funktionsfähigkeit von Krankenhäusern ist unter anderem nicht nur von der Strom- und Wasserversorgung abhängig, sondern auch von der Informationstechnologie. Für die medizinische Versorgung und Pflege der Patienten sowie für die Verwaltung wird immer mehr Informationstechnik eingesetzt.

Da die Cyber-Kriminalität zunimmt, werden auch Krankenhäuser vor Erpressung mittels Schadsoftware, Hackerangriffen, Computerviren oder Sabotage nicht verschont. Der Schutz der IT-Infrastruktur eines Krankenhauses ist daher eminent wichtig. In den Workshops geht es unter anderem um Schutz der IT-Anlagen, Sicherheit der Patientendaten, Zutrittsbeschränkungen für sensible IT-Bereiche, Netzwerksicherheit und Cyber-Krisenmanagement.

Objektschutz. Neben der Cyber-Sicherheit ist es wichtig, dass Gebäude, Gelände und das Personal eines Krankenhauses geschützt werden. Zu den Gebäuden zählen neben den Krankenhausgebäuden auch Lager- und Verwaltungsgebäude sowie Parkgaragen; zum Gelände alle freiliegenden Verkehrs-, Lager- und Parkflächen, Grünanlagen sowie Zufahrtswege.

Gefahren bestehen etwa durch Hochwasser, Sturm oder Brand sowie Ausfälle in der Strom- oder Wasserversorgung. In Krankenhäusern kann es zu Diebstahl, Vandalismus, Gewalt gegen Personal, Patienten oder Besucher kommen, die zum überwiegenden Teil von Personen verübt wird, die unter Drogen- oder Alkoholeinfluss stehen. Auch unterschiedliche kulturelle Auffassungen (Besuchszeiten, Behandlung nur durch gleichgeschlechtliches medizinisches Personal etc.) können zu Auseinandersetzungen führen, die häufig von Gewalt begleitet sind.

In den Workshops werden unter anderem der Schutz der Einrichtung und Personen, Sicherstellung der Versorgungskette für Lebensmittel, Medikamente, Diesel etc., Hausordnung, Sicherheitspersonal sowie Zutrittsbeschränkungen für sensible Bereiche wie Apotheke, Geburtenstation, Nuklearmedizin etc. behandelt.

Medizinischer Krisen- und Katastrophenschutz. Ein Massenanfall von Verletzten oder Erkrankten z. B. wegen eines Terroranschlags, Zugsunglücks, Epidemien etc. stellt eine große Herausforderung für den Rettungsdienst und die Spitäler dar. Krankenhäuser sind im Rahmen der Regelung zur Krankenhausalarmplanung per Gesetz verpflichtet, darauf vorbereitet zu sein. Zur Vorbereitung für Großschadensereignisse gehören neben der spezifi-

FOTO: BURITOKA/STOCK.ADOBE.COM

Cybersicherheit ist für die Funktion von Krankenhäusern ein wichtiger Faktor.

schen Infrastruktur ein Mitarbeiterschulungsprogramm sowie regelmäßige Übungen. Die Abläufe und Strukturen bei einem Massenanfall sind in einem Krankenhaus an die jeweiligen Rahmenbedingungen anzupassen. In den Workshops geht es unter anderem um Sicherstellung der Ressourcenverfügbarkeit, Ausfallsicherheit der Geräte, Schaffung von Isolationscamps, Dekontaminationsplätzen, andersgeartete Verletzungsmuster, Einrichtung von Triageplätzen.

Workshops. Auf diesen Szenarien basierend, verfolgen die Workshops das Ziel der Sensibilisierung der Mitarbeiterinnen und Mitarbeiter in Krankenhäusern sowie die Entwicklung von Mindestsicherheitsstandards in den Bereichen Cyber-Sicherheit, Objektschutz und medizinischer Krisen- und Katastrophenschutz unter Berücksichtigung des Schutzes, der Abwehr und der Widerstandsfähigkeit.

Vor Beginn des Workshops wird das jeweilige Krankenhaus besichtigt, um den Vortragenden eine Übersicht über die baulichen und technischen Einrichtungen zu ermöglichen. Es werden drei Gruppen zu den Bereichen Cyber-Sicherheit, Objektschutz und medizinischer Krisen- und Katastrophenschutz gebildet. Diese Gruppen erarbeiten mit dem jeweiligen Spezialisten ihr Thema.

Workshop-Teilnehmer sind die kollegiale Führung, Notfallmediziner, Sicherheitsbeauftragte für IKT, Datenschutz, Objektschutz und Brandschutz. Vom BVT fanden bisher 37 Begehungen in Krankenhäusern statt, und es wurden zwölf Workshops abgehalten (Stand März 2020). Weitere Workshops sollen 2020 und 2021 stattfinden.

Siegbert Lattacher

FOTOS: VADIM/STOCK.ADOBE.COM, ALEXANDER TUMA

Kommunizieren in der Krise

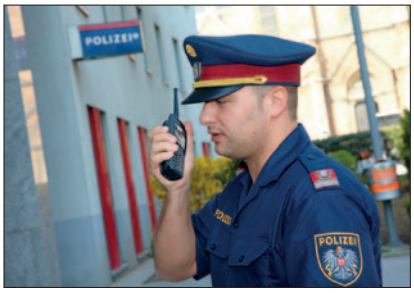
Wenn das Mobilfunk- oder Festnetz ausfällt, kann das in der Bevölkerung für Unmut sorgen oder Panik auslösen, wenn der Ausfall länger dauert. Die Menschen können nicht mehr miteinander kommunizieren, sie erreichen auch nicht mehr die Notrufnummern der Feuerwehr (122), Polizei (133) oder Rettung (144). Wer in Österreich eine Notrufnummer wählt, wird über das Festnetz der *A1 Telekom* in die Notrufzentrale weitergeleitet.

Am 14. Oktober 2019 fiel das Netz der *A1 Telekom* aufgrund eines Hardware-Fehlers für einige Stunden aus. In einer Krisenlage ist es wichtig, dass die Behörden miteinander kommunizieren können und dass jeder Bürger notfalls auch die erforderliche Hilfeleistung anfordern kann.

Digitalfunk. Extreme Schneefälle vergangenen Winter in Osttirol hatten zu längeren Stromausfällen geführt. „Mit dem Digitalfunk haben die Einsatzkräfte miteinander kommunizieren und die Schäden beheben können“, sagt Wolfgang Müller, Leiter der Abteilung IV/8 (Design und Betrieb kritischer Kommunikationsinfrastrukturen) im Bundesministerium für Inneres. Der Digitalfunk funktionierte auch, als der Strom mehrere Tage ausgefallen war, da die Sendemasten in Zusammenarbeit mit den Hilfsorganisationen des Landes mit Notstromaggregaten versorgt werden.

Wenn Telekomnetze aufgrund von technischen Pannen, Sabotage, Stromausfall oder Naturkatastrophen ausfallen, können die Behörden miteinander über das vom Bundesministerium für Inneres betriebene Digitalfunknetz für „Behörden und Organisationen mit Sicherheitsaufgaben“ (BOS) kommunizieren. Bürgerinnen und Bürger können sich an jeden Uniformierten mit Funkgerät wenden und über diesen auf Verlangen mit anderen staatlichen Einrichtungen Kontakt aufnehmen, wenn die Notrufnummern aufgrund eines Netzausfalls nicht erreichbar sind“, sagt Müller.

Der BOS-Digitalfunk ist nach dem NATO-Standard verschlüsselt und ermöglicht es, sensible Daten zu übertragen sowie ausfall- und abhörsicher zu kommunizieren. Mit dem BOS-Digitalfunk können auch Telefonate geführt oder Nachrichten verschickt werden. Bundesweit sind etwa 87.000 Geräte bei Polizei, Rettung, Feuerwehr und sonstigen Hilfs- und Einsatzorganisationen im Einsatz. Die Technik des Digitalfunknetzes wird vom Innenministerium im Zusammenwirken mit den Ländern errichtet und betrieben.



Digitalfunk ermöglicht Kommunikation der Behörden miteinander.

KI-Betreiber. In den Kreis der Digitalfunknutzer wurden Betreiber kritischen Infrastruktur (KI) aufgenommen. Das sind etwa 120 in Österreich. „Dadurch können Behörden in einer Krise mit den Verantwortlichen dieser Unternehmen oder Einrichtungen Kontakt aufnehmen“, erklärt Wolfgang Müller. Im Fall der Corona-Epidemie wäre das etwa der Kontakt zu Unternehmen der Pharmaindustrie oder der Nahrungsmittelversorgung.

Sektoren. Für die KI-Betreiber wurden nach Sektoren Sprechgruppen eingerichtet, in denen die Kommunikation innerhalb des Sektors gesichert stattfinden kann. Neben diesen Gruppenrufen, ist auch die direkte Kommunikation über Einzelrufe möglich. Per Einzelruf kann auch mit jedem anderen Teilnehmer eine Verbindung hergestellt werden. Jeder KI-Betreiber hat ein Digitalfunkgerät erhalten, die dafür verantwortlichen Personen wurden vom BVT sicherheitsüberprüft.

Die Erreichbarkeit der Betreiber wird durch 24/7-besetzte Bereiche (Leitstelle, Sicherheitsverantwortliche) sichergestellt. Die Erreichbarkeit wird vom zuständigen Referat im BVT durch sektorspezifische Kommunikations-Checks überprüft. *S. L.*