

Hinweise zur IT-Sicherheit in medizinischen Einrichtungen

Funktionssicherheit von vernetzten Geräten, Informations- und Kommunikationsmitteln gewährleisten

Im Zusammenhang mit der Pandemie COVID-19 stehen medizinische Einrichtungen vor besonderen Herausforderungen. Das Virus beansprucht in vielen Bereichen eine erhöhte Aufmerksamkeit und die Verlagerung von Kapazitäten. Dabei ist es wichtig Sicherheitslücken auch in kurzfristig eingerichteten IT-Lösungen zu vermeiden und Schutzmechanismen gegen Cyberangriffe aufrechtzuerhalten.

Der Ausfall der IT-Infrastruktur in medizinischen Einrichtungen kann unmittelbare Auswirkungen auf die Leistungsfähigkeit der Einrichtung und damit auf die Gesundheit von Patienten haben.

1. Vorbeugung von Cyberangriffen

Sensibilisierung aller Mitarbeitenden

Erfahrungsgemäß haben die meisten Cyberangriffe, die zu einem Ausfall ganzer IT-Infrastrukturen führen, ihren Anfang im Öffnen von E-Mail Dateianhängen. Daher ist eine besondere Sorgfalt im Umgang mit Dateianhängen obligatorisch. Sensibilisieren Sie Ihre Mitarbeiter, ausschließlich die E-Mail Anhänge zu öffnen, deren Absender sie persönlich kennen. Wenn Ihre Mitarbeiter sich unsicher sein sollten, empfehlen Sie, zunächst den IT-Support zu kontaktieren. Dies gilt auch bei vorhandenem Virenschutz. Raten Sie ebenfalls eine telefonische Überprüfung des Absenders einer E-Mail an.

Sensibilisieren Sie Ihre Mitarbeiter weiterhin hinsichtlich einer zurückhaltenden Weitergabe persönlicher Informationen und dem Aufrufen von Links.

Kontakt:

Landeskriminalamt Nordrhein-Westfalen

Völklinger Straße 49

40221 Düsseldorf

cybercrime.lka@polizei.nrw.de

0211 / 939-4040

Erhaltung der Backup-Fähigkeit

Bei Veränderungen in den Systemstrukturen oder Neuinstallationen muss sichergestellt sein, dass regelmäßig Sicherheitskopien ("Backups") Ihrer Daten erstellt werden, um diese vor Verlust zu schützen.

Führen Sie regelmäßige Überprüfungen Ihrer aktuellen Datenwiederherstellungsmöglichkeiten durch.

Überprüfen Sie, ob die nachfolgenden Aussagen auf Sie zutreffen:

- Sie führen regelmäßige Backups aller notwendigen Daten, Softwareprodukte und Systemelemente durch.
- Sie speichern alle Backups ausschließlich vom Netzwerk getrennt.
- Ihre Backups enthalten alle notwendigen Informationen zur Wiederherstellung ihrer Systeme (Seriennummern, Passwörter, Informationen zur Netzwerkstruktur, Redundanzsysteme).
- Mehrere Ihrer Mitarbeitenden sind zur Wiederherstellung befähigt.

Sicherheitsupdates

Gewährleisten Sie bei Neuinbetriebnahmen von Systemen oder Geräten eine Aktualität der entsprechenden Sicherheitsupdates der Betriebssysteme und der installierten Programme.

2. Sofortmaßnahmen bei erfolgreichem Cyberangriff

Frühzeitige Aktivierung des Notfallplans

Stellen Sie sicher, dass Ihre Mitarbeitenden auch in einem frühen Verdachtsstadium Kontakt zu Ihren Fachabteilungen aufnehmen. Nur bei frühzeitiger Aktivierung des Cyber-Notfallplans können IT-Systeme effektiv vor Ausfällen geschützt werden. Erstellen Sie Anzeige bei der Polizei.

Kontakt:

Landeskriminalamt Nordrhein-Westfalen

Völklinger Straße 49

40221 Düsseldorf

cybercrime.lka@polizei.nrw.de

0211 / 939-4040

Hotline des Landeskriminalamtes Nordrhein-Westfalen

Nehmen Sie bei einem konkreten Verdacht eines Cyberangriffes Kontakt mit der Zentralen Ansprechstelle Cybercrime (ZAC) des Landeskriminalamtes Nordrhein-Westfalen auf:
Tel.: 0211-939-4040.

Hier sind Experten für Sie 24 Stunden erreichbar und helfen Ihnen Angriffe zu unterbrechen und weiteren Schaden abzuwenden. In weniger dringenden Fällen können Sie uns auch unter cybercrime.lka@polizei.nrw.de erreichen.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat weitere Informationen für Sie zusammengestellt:

https://www.bsi.bund.de/DE/Themen/Cyber-Sicherheit/Empfehlungen/fuer_Wirtschaft/CS_Empfehlungen_node.html

Zusätzliche Informationen zu Gefahren von Ransomware und möglichen Entschlüsselungsoptionen erhalten Sie auch auf der Webseite <https://www.nomoreransom.org>.

Kontakt:

Landeskriminalamt Nordrhein-Westfalen
Völklinger Straße 49
40221 Düsseldorf
cybercrime.lka@polizei.nrw.de
0211 / 939-4040