POLIZEI
Nordrhein-Westfalen
Landeskriminalamt

bürgerorientiert • professionell • rechtsstaatlich

Hinweise zur IT-Sicherheit

Funktionssicherheit von vernetzten Geräten, Informations- und Kommunikationsmitteln gewährleisten

Im Zusammenhang mit der Pandemie COVID-19 stehen alle 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 kann unmittelbare Auswirkungen auf die Leistungsfähigkeit der Einrichtung und damit auf die Arbeitsfähigkeit und Verfügbarkeit Ihres Betriebs haben.

1. Vorbeugung von Cyberangriffen

Sicherer Umgang mit E-Mail Dateianhängen

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.

Eine besondere Gefahr besteht dann, wenn der Computer für den Email Empfang zugleich für die tägliche Arbeit genutzt wird. Versehentlich ausgeführte Schadsoftwareprogramme haben somit einen direkten Zugriff auf wichtige Daten und das Firmennetzwerk. Für besonders kritische Breiche empfielt sich daher die Einhaltung folgender Punkte

- Strikte Geräte- und Netztrennung zwischen E-Mail Eingang und allen weiteren Tätigkeiten.
- Nutzung von Systemen für den E-Mail Eingang, die weniger im Fokus von Straftätern stehen wie z.B. Linux oder Mac OS. Ggfls können auch mobile Geräte wir Andoid oder iOS Tablets für die E-Mail Verwaltung genutzt werden.

Sollten diese technischen Maßnahmen in Ihrer Firma nicht umsetzbar sein, ist eine besondere Aufmerksamkeit der Mitarbieter das wichtigste Mittel zur Abwehr von Cyberangriffen. 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

Erstellen Sie Regelmäßig Sicherheitskopien ("Backups") Ihrer Daten, um diese vor Verlust oder Verschlüsselung zu schützen.

Eine Datensicherung, die über das Firmennetzwerk zugreifbar ist, bietet keinen Schutz vor Datenverlust!

Führen Sie zudem 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 entahlten alle notwendigen Informationen zur Widerherstellung 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 bei den installierten Programmen.

Informationen des Bundesamtes für Sicherheit in der Informationstechnik (BSI):

Das Bundesamt für Sicherhheit 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

2. Sofortmaßnahmen bei erfolgtem 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 werde. Erstatten Sie Anzeige bei der Polizei.

Hotline des Landeskriminalamtes Nordrhein-Westfalen

Nehmen Sie bei dem 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. Diese können Sie auch unter cybercrime.lka@polizei.nrw.de erreichen.

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