SOFORTHILFE

Was bei einem IT-Sicherheitsnotfall zu tun ist

1 RUHE BEWAHREN

Bevor Sie etwas tun: Die Umsetzung von Maßnahmen muss gut überlegt sein, da sie sich auf die spätere Spurensicherung auswirkt.
Machen Sie sich also zunächst einen Plan, holen Sie sich Unterstützung und leiten erst dann gezielte Maßnahmen ein. Klären Sie als erstes, ob es sich um einen Cyber-Angriff oder einen technischen Defekt handelt.

2 VERANTWORTLICHEN FESTLEGEN

Legen Sie als zweites eine Person als Verantwortliche fest, bei der alle Schritte zusammenlaufen und die den Überblick behält. Diese sollte bestenfalls über Sachverstand und entsprechende Befugnisse verfügen. Dies können IT-Verantwortliche oder jemand aus der Geschäftsführung sein.

3 PROTOKOLLIEREN

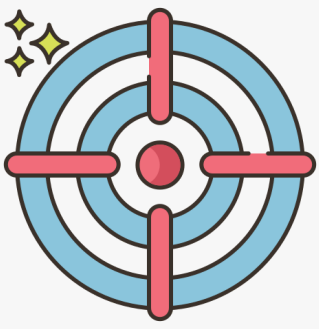
Dokumentieren Sie sowohl die einzelnen Vorkommnisse bei den betroffenen Systemen als auch bereits getroffene Maßnahmen. Das hilft Ihnen, den Überblick zu behalten und ist eine wichtige Grundlage für Behörden und Dienstleister.
Für die Dokumentationen gelten die 4-W-Regel:
Was – Wer – Wann – Warum.

4 LAGEZENTRUM BILDEN

Informationen müssen an einem Ort zusammenlaufen – dem Lagezentrum. Dort befinden sich alle Personen, die Entscheidungen treffen müssen. Eine kontinuierliche und ungestörte Kommunikation ist immens wichtig. Lagezentren können digital aufgestellt werden, besser ist eine physische Lokation, auch wenn es das Lager oder der Putzraum ist.

5 LAGEBILD ERSTELLEN

Eine offene Fehlerkultur ist ein zentraler Erfolgsfaktor: Motivieren Sie Ihre Mitarbeiter, offen mit Fehlern und Versäumnissen umzugehen. Machen Sie sich ein Bild von der Gesamtlage, stoppen Sie Backup-Prozesse oder setzen Sie diese aus. Auffälligkeiten sollten auch hierbei dokumentiert werden, machen Sie Snapshots von virtuellen Maschinen und Fotos von Bildschirmausgaben (Screenshots).



6 BEHÖRDEN KONTAKTIEREN

Wenden Sie sich an Behörden. Diese verfügen über deutlich weitergehende technische und rechtliche Werkzeuge, insbesondere zur Strafverfolgung, Forensik und Aufklärung.
Notfall-Kontaktstellen:

- Landeskriminalamt NRW: 0211 939-4040 – cybercrime.lka@polizei.nrw.de
- Verfassungsschutz NRW: 0211 871 2821 – wirtschaftsschutz@im1.nrw.de

7 PROFESSIONELLE HILFE

Ziehen Sie ein Dienstleistungsunternehmen Ihres Vertrauens hinzu, das Ihnen bei allen Aufgaben zur Eindämmung und Beseitigung des Vorfalls helfen kann. Bestehen Sie auf einen fest verantwortlichen, qualifizierten Ansprechpartner.

8 KOMMUNIKATION UND STELLUNGNAHMEN

Sie sollten bei einem Sicherheitsvorfall genau abwägen, welche Informationen Interne und Externe erhalten müssen. Benachrichtigen Sie Ihre Mitarbeiter und bereiten Sie eine oder ggfs. mehrere Stellungnahmen vor, die Kunden, Partner und Öffentlichkeit informieren und einen Ansprechpartner benennen.

9 MELDEPFLICHT

Im Fall von relevanten Datenschutzverletzungen müssen Sie den Vorfall innerhalb von 72 Stunden der zuständigen Datenschutzaufsichtsbehörde melden.

Melden Sie den Vorfall außerdem der Allianz für Cybersicherheit. Hier wird Ihr Vorfall anonymisiert erfasst, um andere Unternehmen rechtzeitig zu warnen.

WEITERFÜHRENDE INFORMATIONEN

Scannen Sie den QR-Code, um zur Seite des Kompetenzzentrums für Cybersicherheit in der Wirtschaft in NRW zu gelangen. Hier erhalten Sie weitere Informationen und Hinweise zum Verhalten im Notfall.

DIGITAL SICHER NRW
Kompetenzzentrum für Cybersicherheit in der Wirtschaft