Richtig handeln im Notfall

Die Bewältigung eines Cyber-Angriffs ist stets individuell. Die Maßnahmen müssen auf:

- die Gegebenheiten der IT-Infrastruktur vor Ort,
- die Art des Angriffs und
- die Zielsetzungen des Betriebes

angepasst werden.

Meldung oder Entdeckung des Cyberereignis
durch Überwachung, Benachrichtigung durch Mitarbeiter, Kunden/Anbieter oder Folgen wie Website- oder Systemausfälle.

Bewahren Sie Ruhe und handeln Sie nicht übereilt.

Wissen alle, die intern davon wissen müssen, vom mutmaßlichen IT-Notfall?
Benachrichtigung des IT-Verantwortlichen/IT-Dienstleisters, des Datenschutzbeauftragter der Geschäftsführung.

Verschaffen Sie sich einen Überblick
Sammeln Sie möglichst schnell und möglichst viele Informationen, um fundierte Entscheidungen treffen zu können. Ermitteln Sie:

- ☐ Was ist eigentlich passiert?
  Dokumentieren Sie den Angriff (Fotografieren Sie mit dem Smartphone die Anzeige)
- ☐ Wie ist es aufgefallen?
- ☐ Welche Systeme sind betroffen?
  - Sind alle angegriffenen Systeme identifiziert?
- ☐ Welche Auswirkungen ergeben sich auf Funktionen und Informationen?
  - Waren besonders zeitkritischen und damit vorrangig zu schützenden Geschäftsprozesse im Fokus?
- ☐ Gibt es eine Vermutung für die Ursache (infizierte E-Mail, Technikausfall etc.)?
- ☐ Sind bereits Maßnahmen durchgeführt worden (z. B. Herunterfahren des Rechners, Trennen der Netzwerkverbindung)?

Richten Sie einen Krisenstab ein
Abklären, ob es sich um einen technischen Defekt oder einen IT-Vorfall handelt. Richten Sie bei einem Cyber-Angriff (**IT-Vorfall**) einen Krisenstab bestehend aus Geschäftsführung, IT-Verantwortlichem (technischer Sachverstand), IT-Dienstleister (ggf. Branchensoftwareanbieter), Datenschutzbeauftragtem, Hausjurist (Klärung Haftung, Strafanzeige) und Personal-/Betriebsrat, falls vorhanden, ein.

Sofortmaßnahmen

Das Sicherheitsteam ergreift Maßnahmen, um den Vorfall einzudämmen und entgegenzuwirken.

- ☐ Internetverbindungen zu den betroffenen Systemen trennen
- ☐ betroffene Systeme vom Netzwerk und Kommunikationsverbindungen (WLAN, Bluetooth) trennen (erst Netzwerk, dann Strom) - Produktivitätseinbußen sind zu ignorieren
- ☐ alle unautorisierten Zugriffe unterbinden
- ☐ Backups stoppen, vom Netzwerk und Geräten trennen und vor möglichen weiteren Einwirkungen schützen

Verhindern Sie eine weitere Ausbreitung

- ☐ Arbeiten Sie nicht mehr an den Geräten.
- ☐ Schalten Sie ausgeschaltete Rechner nicht ein
- ☐ Fahren Sie die Systeme herunter. (Beachten Sie dabei, dass dies eine forensische Untersuchung erschwert)
- ☐ Vermeiden Sie eine Anmeldung mit Administratorrechten.
- ☐ Schalten Sie alle Funknetze ab (WLAN, 5G Netz)
- ☐ Trennen Sie alle Netzwerkverbindungen des Unternehmens nach außen
- ☐ IT-Endgeräte vom Netzwerk trennen – ACHTUNG: Fast alle modernen elektrischen Geräte haben eine Internetschnittstelle (Drucker, Server, Notebooks, PCs, Smart-TV, Präsentationsgeräte, Kaffeemaschine…)
- ☐ Interne Router und Switches abschalten (Router in das Produktionsnetz, Stockwerk-Switch, etc.)
- ☐ Ändern Sie sämtliche Benutzer- und Netzwerkkennwörter auf Ihren nicht infizierten Geräten

Untersuchen und analysieren Sie den Vorfall

- ☐ Prüfen Sie ob es sich um einen Einzelfall handelt, oder ob mehrere Rechner befallen sind. Prüfen Sei hierzu das gesamte Netzwerk, insbesondere die Antiviren-Lösung.
- ☐ Prüfen Sie, ob Sie über aktuelle, saubere, integre Backups verfügen

Wird externe Unterstützung benötigt?

Kontaktieren Sie den zuständigen Cyberexperten (IT-Verantwortlichen gemäß IT-Notfallplanung) um den Infektionsvektor zu finden zu schließen und um eine erneute Infektion zu verhindern

- ☐ **Cybersicherheitsnetzwerk** (CSN)
  Montag bis Freitag von 08:00-18:00 Uhr
- ☐ **IT-Sicherheitsbotschafter im Handwerk** (Sibo)
- ☐ **Zentrale Ansprechstelle Cybercrime** (ZAC)
  steht den Opfern zur Seite, wenn es um die Beweissicherung und die Erstattung einer Anzeige geht.

Beachten Sie die Melde- und Informationspflichten

- ☐ Informieren Sie die Angestellten darüber was passiert ist und welche Maßnahmen ergriffen wurden
- ☐ Besteht eine Melde- oder Informationspflicht gegenüber Dritten (Lieferanten, Kunden, Datenschutz-Aufsichtsbehörde)?
- ☐ Sind personenbezogene Daten betroffen informieren Sie mit dem Datenschutzbeauftragten und dem Hausjuristen, die Aufsichtsbehörde (LDSB).
- ☐ Erstatten Sie unverzüglich Strafanzeige bei Ihrer örtlich zuständigen Polizeidienststelle

Meldepflichten

- **Landesdatenschutzbeauftragte**: Sind bei einer Cyberattacke personenbezogene Daten abgeflossen, so MUSS nach DSGVO (Art. 33. DSGVO) innerhalb von 72 Stunden die zuständige Aufsichtsbehörde, der Landesdatenschutzbeauftragte, benachrichtigt werden.
- **Betroffene Personen:** Direkt betroffene Personen (Mitarbeiter, Kunden, Newsletter-Empfänger, …), deren Daten abgeflossen sind, müssen ebenso benachrichtigt werden. Erklären Sie, welche Daten abhandengekommen sind und wie hoch das Missbrauchspotential ist. Informieren Sie außerdem über die eigenen ergriffenen Schutzmaßnahmen.
- **BSI:** Betreiber kritischer Infrastrukturen müssen eine Datenpanne an das Bundesamt für Sicherheit in der Informationstechnik melden.
- **Vertragspartner:** Aus Verträgen ergeben sich eventuell auch Meldepflichten gegenüber den Vertragspartnern.
- **Cyber-Versicherung:** Sollte Ihr Unternehmen über eine Cyber-Versicherung verfügen, informieren Sie diese umgehend. Auch hier gibt es häufig Vorgaben über das notwendige Vorgehen.

Ziehen Sie Lehren aus dem Sicherheitsvorfall

- ☐ Überprüfen Sie welche Sicherheitsmechanismen versagt haben.
- ☐ Wurden die beim Cyber-Angriff ausgenutzten Schwachstellen in Systemen oder (Geschäfts-) Prozessen gefunden und behoben?
- ☐ Wurden die Zugangsberechtigungen und Authentisierungsmethoden für betroffene (geschäftliche und ggf. private) Accounts überprüft (z.B. neue Passwörter, 2FA)?
- ☐ Wird das Netzwerk nach dem Vorfall weiter überwacht, um mögliche erneute Anomalien festzustellen?

Denkbar wären:

- ☐ Konfigurationsänderungen an den technischen Systemen,
- ☐ Systemerweiterungen,
- ☐ organisatorische Anpassungen und die
- ☐ laufende Schulung bzw. Sensibilisierung von Mitarbeitern.

Passen Sie auch dementsprechend Ihre Dokumentationen an!