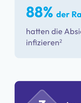
proliance

Chronologie eines Cyberangriffs

Ablauf, Folgen und wirksame Schadensbegrenzung

Warum müssen sich Unternehmen mit Cybersicherheit beschäftigen?

1 Cyberbedrohungen nehmen zu



2,2 Mrd. € Schaden
verursachte ein Cyberangriff 2025 in Großbritannien[1]

2 Backups allein reichen nicht

88% der Ransomware-Angriffe
hatten die Absicht, gezielt Backups zu infizieren[2]

3 Immer strengere EU-Vorgaben

30.000 Unternehmen
sind etwa allein in Deutschland von NIS2 betroffen

Tag X: Das droht wirklich bei einem Cyberangriff

Sehen wir uns an, was im Falle einer Cyberattacke passiert. Nehmen wir an, Ihr Unternehmen wird Opfer eines Ransomware-Angriffs.

58 Tage
sind Angreifer im Schnitt bis Tag X im Netzwerk aktiv und korrumpieren Software[3].

Vor dem Angriff

Die Hacker installieren bereits unbemerkt Schadsoftware und infizieren erste Systeme.

- Ausbreitung, um möglichst viele Systeme zu kapern
- Ausspionieren von Schwachstellen und vertraulichen Daten
- Kompromittierung von Software, Backups & Co.

Wie wir helfen können

- Aufbau ISMS
- Risiko- und GAP-Analyse
- Business Continuity Management (BCM)

9 Tage
benötigen Organisationen im Schnitt, um aktiv zu reagieren, nachdem ein Angriff entdeckt wurde[4].

Tag X

Die Hacker haben das Unternehmen erfolgreich angegriffen.

- Angreifer übernehmen die Kontrolle wichtiger Systeme
- Daten werden gestohlen und verschlüsselt
- Forderungen nach Lösegeld werden abgesetzt

Wie wir helfen können

- Ansprechpartner
- Meldung an BSI

180 Tage
oder oft mehr als 6 Monate dauert die Wiedererlangung des „normalen" Geschäftsbetriebs.

Nach dem Angriff

Nach dem Entdecken des Angriffs sollte größerer Schaden verhindert und der Betrieb wiederhergestellt werden.

- Isolierung betroffener Systeme sowie forensische Analyse
- Benachrichtigung der Behörden (Meldepflichten beachten)
- Passwörter ändern und Zugriffsrechte prüfen
- Wiederherstellung von Systemen
- interne Kommunikation sicherstellen
- Prävention (z. B. Schulungen und BCM)

Wie wir helfen können

- Betrieb wiederherstellen
- ISMS optimieren
- Learnings ableiten

Wer früher handelt, ist schneller geschützt

Je schneller auf erste Anzeichen eines Angriffs reagiert wird, desto größer ist die Chance, die Kontrolle über das eigene System zu behalten und größeren Schaden zu verhindern. Schon ein Tag Verzögerung kann große Auswirkungen haben.

So schützen Sie Ihr Unternehmen vor Schäden durch Cyberangriffe

Notfallplan + Patches + ISMS (Informationssicherheitsmanagementsystem) + BCM (Business Continuity Management)

Schadensbewältigung mit und ohne BCM

Sie wissen, welche Systeme zuerst wiederhergestellt werden müssen.

Sie wissen, wer im Notfall welche Aufgaben übernimmt.

Sie wissen, wie interne Kommunikation auch ohne funktionierende IT abläuft.

Quellen:
1 - https://www.manager-magazin.de/unternehmen/autoindustrie/jaguar-land-rover-cyberangriff-verursacht-milliardenverlust-fuer-britische-wirtschaft-a-c574d844-9bd9-46f0-a2a7-bfb32437d53e
2 - veeam.com
3 - https://www.microsoft.com/en-us/corporate-responsibility/cybersecurity/microsoft-digital-defense-report-2025/

proliance

Compliance. Sicher erledigt.

Proliance GmbH · Leopoldstr. 21 · 80802 München · +49 89 / 250 039 220 · www.proliance.ai · info@proliance.ai