Cyberattacke – und jetzt?

Tipps und Hinweise für den Ernstfall

Cyberattacke oder doch „nur" IT-Störung?

Wer kennt es nicht: das Programm reagiert anders als erwartet. Aber nicht jedes auffällige Ereignis ist auch gleich ein Sicherheitsvorfall.

Ernst wird die Lage meist dann, wenn ...

- das Antivirenprogramm einen Fund meldet,
- der Computer bzw. das Programm sich anders verhält als üblich oder sogar eigenständig agiert,
- ein Link oder Anhang in einer E-Mail angeklickt wurde, der merkwürdig aussieht,
- fälschliche Aufforderungen zur Passwortänderung erscheinen,
- Daten an anderen Orten auftauchen (andere Laufwerke, Ordner, Programme oder schlimmstenfalls im Internet),
- merkwürdige Weiterleitungen passieren,
- Anwendungen sich selbst installieren,
- kein oder nur ein eingeschränkter Zugriff auf Daten besteht.

Ernstfall Cyberattacke: schnell reagieren – aber richtig!

Wer? Wann? Wie? – und vor allem was zuerst?

UNVERZÜGLICH!

1. Trennen Sie das betroffene System vom Netzwerk. Schalten Sie das System nicht aus und verändern Sie das System nicht, damit nach Spuren gesucht werden kann.
2. Sperren Sie alle Zugänge auf anderen Systemen, die von diesem System aus per Passwort oder Zertifikat möglich waren.
3. Trennen Sie das Back-Up-System des betroffenen Systems vom Netzwerk.
4. Benachrichtigen Sie Ihren Datenschutzbeauftragten und sofern vorhanden Ihren Informationssicherheitsbeauftragten und Ihre Cyberversicherung.

WEITERE SCHRITTE

5. Werten Sie zusammen mit Ihrer IT, Ihrem Datenschutzbeauftragen und ggf. Informationssicherheitsbeauftragten die Schwere und Verbreitung des Vorfalls im Rahmen eines Incident Reports aus.
   - Sofern personenbezogene Daten betroffen sind, muss der Sicherheitsvorfall innerhalb von 72 Stunden an die Datenschutzaufsichtsbehörde gemeldet werden.
6. Große Unternehmen: je nach Schwere des Vorfalls aktivieren Sie Ihren Notfall- und Krisenstab
7. Binden Sie bei einem schweren Vorfall externe Experten und Spezialisten ein (siehe Ansprechpartner)
8. (Freiwillig) Einbindung von Polizei oder der „Allianz für Cyber-Sicherheit" des BSI
9. Krisenkommunikation nach innen und außen
10. Schließen/Entfernen der Sicherheitslücken durch die IT-Abteilung
11. IT-Abteilung spielt die Back-Ups der betroffenen Systeme auf neuer Hardware / neuen virtuellen Maschinen ein. An dieser Stelle werden neue Passwörter und neue Zertifikate vergeben!
12. Nachbereitung und Lessons Learned! Präventive Maßnahmen gegen Vorfälle ergreifen

IHK Lübeck

AK ITK

ANSPRECHPARTNER BEI EINER CYBERATTACKE

Cyberattacken sind komplex, daher bedarf es unterschiedlichster Kompetenzen und Ansprechpartner. Die folgende Auflistung soll Anhaltspunkte bieten, wer bei einem Cyberangriff unterstützen kann bzw. informiert werden sollte.

Eigenes Netzwerk & Know-how – informieren und mobilisieren

IT-Team, Datenschutzbeauftragter, IT-Sicherheitsbeauftragter, IT-Dienstleister, Jurist, Öffentlichkeitsarbeit, Personal- bzw. Betriebsrat, IT-Versicherung

Externes Know-how – qualifiziertes und objektives Lagebild

Zertifizierte IT-Sicherheitsdienstleister:
Liste BSI - Bundesamt für Sicherheit in der Informationstechnik
Öffentlich bestellte und vereidigte IT Sachverständige
ihk.de/schleswig-holstein/bsi-it-liste

Behördliche Institutionen – Beratung, Meldung, Ermittlung & Strafverfolgung

Zentrale Ansprechstelle Cybercrime (ZAC)
0431 160-42727
polizei.de/zac

Allianz für Cyber-Sicherheit (ACS)
0800 2741000
allianz-fuer-cybersicherheit.de

Unabhängiges Landeszentrum für Datenschutz
0431 988-1200
datenschutzzentrum.de

5 TIPPS FÜR MEHR IT-SICHERHEIT

 # 1 Mitarbeiter sensibilisieren: Ausdauer zählt (und zahlt sich aus)
Die wichtigste Maßnahme gegen Viren, Phishing und Datenpannen ist ein geschultes Team. Bieten Sie regelmäßig Schulungen an und halten Sie Hinweise und Leitfäden für Ihre Mitarbeiter leicht zugänglich.

 # 2 Passwörter: na klar – aber sind die auch sicher?
Fast alle digitalen Anwendungen sind passwortgeschützt. Aber nur komplexe und individuelle Passwörter bieten einen ausreichenden Schutz. Bei der stetig wachsenden Anzahl an Accounts und Anwendungen ist es gar nicht so einfach den Überblick zu behalten. Unterstützung bieten hier Passwortmanager. Aber auch bei einem noch so komplexen Kennwort kann es gerne noch ein bisschen mehr sein. Mit einer Multi-Faktor-Authentifizierung erhöhen Sie Ihr Sicherheitslevel um ein Vielfaches.

 # 3 Zugriffsrechte: weniger ist mehr
Ebenso wichtig ist es, die Zugriffsrechte richtig zu verwalten. Hier sollte nach dem Least Privilege Prinzip verfahren werden. Jeder Nutzer sollte nur die Zugriffsrechte haben, die er für seine Arbeit wirklich benötigt. In der Realität sieht es häufig anders aus, mit dem Ergebnis, dass sich IT-Sicherheitsvorfälle schneller und umfassender ausbreiten.

 # 4 Immer up-to-date bleiben
Update, Patch, Aktualisierung oder Bugfix: viele Begriffe, ein Ziel. Nur durch die ständige Aktualisierung aller Anwendungen können Fehler beseitigt, Sicherheitslücken geschlossen und neue Funktionen hinzugefügt werden. Bei jährlich über 20.000 identifizierten und beseitigten Schwachstellen, sind aktuell gehaltene Systeme ein Must-have.

 # 5 Notfallplan & Back-up – ohne geht`s nicht
100%-Sicherheit gibt es nicht. Daher sollte jedes Unternehmen für den Ernstfall gewappnet sein. Wichtig ist, dass bei einem IT-Sicherheitsvorfall schnell und richtig gehandelt wird. Ein Notfallplan mit schriftlich geregelten Abläufen und Ad-hoc-Maßnahmen ist hierfür ebenso unerlässlich wie ein regelmäßiges Back-up.

AK ITK Unterstützungs- und Beratungsangebot des Arbeitskreises ITK & Digitalisierung der IHK zu Lübeck

MEET THE EXPERTS – IT-Sicherheit

jeder 4. Dienstag im Monat, 12 – 16 Uhr
individuelle Einzelberatung (ca. 30 Minuten) mit einem IT-Experten
ihk.de/schleswig-holstein/mte

IT-Sicherheitsquickcheck

jeder 1. Dienstag im Monat, 12 – 16 Uhr
individuelle Onlineanalyse der IT-Sicherheitssituation
ihk.de/schleswig-holstein/it-check

Mediathek

Umfangreicher Wissensspeicher rund um die Themen IT-Sicherheit und Datenschutz
ihk.de/schleswig-holstein/webinare

Webinare & Veranstaltungen

Aktuelle Veranstaltungshinweise rund um das Thema Digitalisierung
ihk.de/schleswig-holstein/it4b-termine

Kontakt
Industrie- und Handelskammer zu Lübeck
Fackenburger Allee 2 | 23554 Lübeck
Telefon: 0451 600- 0 | www.ihk.de/schleswig-holstein

Ansprechpartner
Christian Wegener
Mail: christian.wegener@luebeck.ihk.de
Telefon: 0451 6006-142 | www.it4b.info