Verhalten bei Cyber-Angriff

Cyberrisiken und Schutzmassnahmen

Gemäss Umfragen hat jedes dritte Schweizer KMU bereits einen erfolgreichen Cyberangriff erlebt. Jedes noch so kleine Unternehmen sollte sich bewusst sein, was ein Cyberangriff auslösen kann. Sei es bloss ein zeitlich verwehrter Zugang zu IT-Anwendungen oder doch ein schwerwiegender Imageverlust durch Datenklau mit öffentlicher Publikation oder gar strafrechtliche Folgen durch mögliche Verletzungen der Sorgfaltspflicht. Es ist deshalb äusserst wichtig, vorbeugende Massnahmen umzusetzen, um sich effizient gegen Angriffe zu schützen. Einerseits gilt es, die eigene Technik entsprechend zu konfigurieren oder aufzurüsten, interne Prozesse so zu definieren, dass diese nicht extern beeinflusst werden können und Mitarbeitende zu sensibilisieren. Dieses Merkblatt dient als Weckruf für alle Verantwortlichen.

Inhalt:

Bahnhofstrasse 94, 5000 Aarau
T +41 44 388 53 00
info@jardinsuisse.ch | jardinsuisse.ch

JardinSuisse
Unternehmerverband Gärtner Schweiz
Hier wächst Zukunft.

1. Massnahmen für einen wirkungsvollen Schutz gegen Cyberangriffe

- Managementaufgaben wahrnehmen und Verantwortlichkeiten teilen
- Daten regelmässig sichern mit externen Backups (Diebstahlschutz). Zeitintervall: Solange wie der Geschäftsvorgang ohne IT-Anwendungen sichergestellt werden kann
- Software regelmässig aktualisieren
- Internetzugang mit einer Firewall schützen
- Antivirusprogramm aktualisieren
- Sichere Passwörter (mindestens 12 Zeichen mit Klein- und Grossbuchstaben, Ziffern, Satzzeichen), in Kombination mit einem Passworttresor und der Zwei-Faktoren-Authentifizierung verwenden
- IT-Benutzerrichtlinie an alle Mitarbeiter kommunizieren
- Daten klassifizieren und Zugriffsberechtigungen kontrollieren
- Anpassungen kontrollieren an produktiven Systemen mittels Changemanagements (Prozess der Planung, Umsetzung und Kontrolle von Veränderungen in IT-Systemen, um einen reibungslosen Übergang sicherzustellen)
- Umgebung der IT-Infrastruktur schützen (z.B. Zugangskontrollen, Einbruchschutz)

2. Cyberattacke erkennen

Hacker sind wie Einbrecher. Sie versuchen möglichst wenig Verdacht zu erregen und ihre Spuren zu verbergen. Oft ist nicht sofort erkennbar, wenn ein Cyberkrimineller bereits ins System eingedrungen ist. Es kann Wochen oder sogar Monate dauern, bis die Schadsoftware aktiviert wird.

Anzeichen für eine laufende Cyberattacke:

- Langsames System
- Daten sind nicht verfügbar
- Passwörter funktionieren nicht mehr
- Flimmernder Bildschirm
- Der Computer führt scheinbar selbstständig Aktionen aus
- Programme starten nicht oder reagieren unerwartet
- Computer produziert viele Fehlermeldungen
- Auf dem Bildschirm erscheint eine Lösegeldforderung

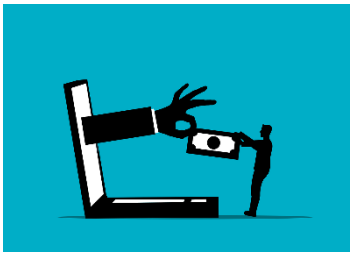
Handeln Sie schnell, wenn Sie solche Anzeichen entdecken. Diese Liste ist nicht abschliessend.

3. So reagieren Sie bei einem Cyberangriff richtig

1. Alle Systeme umgehend vom Netz nehmen und das WLAN ausschalten
2. Zuständige IT-Sicherheits-Person informieren
3. Mitarbeitende informieren
4. Problem und Schäden analysieren (ev. in Zusammenarbeit mit Fachpersonen)
5. Falls vorhanden, die Cyber-Versicherung informieren:
   Die Versicherung hat spezialisierte Partnerfirmen, welche Unterstützung bieten können. Im Idealfall übernimmt sie die Kosten für die Reinigung der IT-Systeme, die Datenwiederherstellung und entschädigt den Betriebsunterbruch.

Bei grösseren Angriffen wird vor der Reinigung und Wiederherstellung der Systeme gewartet, bis die Polizei die Spuren gesichert hat. Selbst wenn keine Schäden entstehen, sollten sowohl die Polizei als auch das Nationale Zentrum für Cybersicherheit NCSC (www.report.ncsc.admin.ch/de/) über den Vorfall unterrichtet werden. Die Täter werden selten gefasst, aber die Meldungen können zur Prävention und Sensibilisierung anderer potenzieller Opfer beitragen.
Wichtig: Zahlen Sie kein Lösegeld! Denn wer einmal zahlt, wird für Hacker erst recht zum attraktiven Opfer.

3.1. Die fünf grössten Fehler bei einer Cyberattacke



- IT-System am Netz lassen, WLAN nicht ausschalten
- Nichts tun und den Angriff aussitzen
- Lösegeld zahlen
- Niemanden informieren, um einen Reputationsschaden abzuwenden
- Meinen, dass es nur die anderen trifft – und keine Massnahmen für Cybersicherheit ergreifen

4. Cyber-Sensibilisierungstraining für Mitarbeitende

Es ist schnell passiert: Ein Mitarbeiter öffnet unbedacht eine E-Mail und plötzlich steht Ihr ganzes Unternehmen still. Es ist deshalb wichtig, die Mitarbeitenden im Umgang mit Internet und Mail zu informieren und zu sensibilisieren. Verschiedene Anbieter wie auch Versicherungen bieten Cybertrainings für Unternehmen an. Durch das Versenden von simulierten Phishing-Mails kann der Kursanbieter dem Unternehmen über die Reaktionen der Mitarbeiter berichten. Auf diese Weise sehen Sie, ob weitere Sensibilisierungsmassnahmen nötig sind.

5. Links

Weitere Informationen zu organisatorischen sowie technischen Massnahmen liefert das Nationale Zentrum für Cybersicherheit NCSC (www.ncsc.admin.ch) des Bundes.

Quellen: dergartenbau Ausgabe 20/2023, www.mobiliar.ch