EXPERT suisse
Wirtschaftsprüfung
Steuern
Treuhand

Cyberangriff-Checkliste

Vorbeugende Massnahmen

1. Mitarbeitende sensibilisieren und schulen. Dies kann mithilfe von Phishing-Tests und Cybersicherheitsschulungen durchgeführt werden.
2. Schutz der IT-Infrastruktur laufend prüfen. Patches und Updates laufend installieren.
3. Regelmässig Backups durchführen und die Firewall kontrollieren.
4. Einsatz von Anti-Malware-Software.
5. Berechtigungen zur Installation von Software einschränken.
6. Starke und sichere Passwörter verwenden. Passwörter regelmässig ändern.
7. Aktivieren Sie wo möglich die Multi-Faktor-Authentifizierung (MFA).
8. **Vorsichtig** sein bei Social Media.
9. Nutzen Sie stets eine **sichere Internetverbindung** (VPN) und verwenden Sie generell Verschlüsselungen.

Checkliste bei einem Cyberangriff

1. Zuerst **Ruhe bewahren** und bedacht vorgehen. Gehen Sie **niemals** auf die Forderung der Kriminellen ein. Sonst wird das Unternehmen als lukratives Ziel gesehen und weitere Angriffe können folgen.
   Wichtig! Jeder Schritt muss **dokumentiert** werden, um später die Vorgehensweise zu rekapitulieren.
2. Trennen Sie infizierte Systeme umgehend vom Netz. Dazu trennen Sie das Netzwerkkabel vom Computer und schalten allenfalls vorhandene WLAN-Adapter ab. Leiten Sie Massnahmen ein, um die Ausbreitung des potenziellen Angriffs zu verhindern (Umleitung des Netzwerkverkehrs, Filtern oder Blockieren des Datenverkehrs und Isolierung des gesamten oder von Teilen des möglichen kompromittierten Netzwerks).
3. **Vorgesetzte** und **IT-Abteilung** telefonisch informieren.
4. Überprüfen Sie, ob es sich tatsächlich um einen Cyberangriff handelt oder um einen technischen Fehler. Bis dahin mögliche Kommunikation nach draussen vermeiden. Falls es sich um einen Cyberangriff handelt, Polizei informieren und Spezialisten hinzuziehen.
5. Überprüfen Sie, welche Systeme betroffen sind, und finden Sie heraus, wie der Angriff stattgefunden hat. Darüber hinaus soll festgestellt werden, ob und **welche Daten** entwendet wurden und welche Netzwerke betroffen sind. Stellen Sie fest, welche Knoten kompromittiert wurden, welche Dienste unterbrochen sind und evaluieren Sie das Ausmass und die Art des Schadens an den Systemen.
6. Falls sensible Daten entwendet wurden, welche grosse Risiken für die Persönlichkeit oder die Grundrechte der betroffenen Personen beinhalten, sollte unbedingt der **Eidgenössische Datenschutzbeauftragte (EDÖB)** informiert werden.
7. Schliessen Sie alle Sicherheitslücken, welche der Angreifer verwendet hat.
8. Setzen Sie betroffene Mitarbeitende oder Kunden in Kenntnis.
9. Auf keinen Fall **ohne polizeiliche Unterstützung** mit den Kriminellen verhandeln!
10. Versuchen Sie, Massnahmen zu Wiederherstellung der Daten und Systeme einzuleiten.
11. **Analyse:** Wie hätte der Angriff verhindert werden können? Welche Massnahmen müssen in Zukunft umgesetzt werden?

Datum der Erstellung: 20. Mai 2022