# Cyber-Angriffe – wie können Sie sich schützen? Datenschutz: Szenario „Cyber-Angriff“

© © psdesign1 - Fotolia.com

**Die weltweite Vernetzung über das Internet bringt immense Vorteile mit sich. Allerdings steigen die Herausforderungen für den Schutz der Privatsphäre und der Unternehmensdaten erheblich. Cyber-Angriffe können von überall herkommen.**

**Es beginnt mit Leichtsinn im Umgang mit E-Mails und geht bis zu gezielten Angriffen auf das Unternehmen. Es gibt eine Reihe von vorsorglichen Schutzmaßnahmen – wir haben ein Szenario beispielhaft ausgewählt.**

**Szenario:**

Ein Unternehmen hat eine Stelle ausgeschrieben und die Bewerbungen treffen ein. Ein Bewerber schickt seine Bewerbung per Post und legt einen USB-Stick bei, der weiterführende Unterlagen enthält. Das Personalwesen vertraut dem Bewerber (warum auch nicht?) und der Mitarbeiter steckt deshalb den USB-Stick in seinen Rechner.

**„Vertrauen ist gut – Kontrolle ist besser“.**

Auf dem USB-Stick kann sehr leicht ein Trojaner in das Unternehmen geschleppt werden, der sich erst durch Öffnen, z. B. einer PDF-Datei, zeigt und selbst installiert. In unserem Szenario haben wir den USB-Stick als Trojaner-Träger ausgewählt.

Wie gut kennen Sie die IT-Firma, die Sie betreut? Auch eine Fernwartung kann vom Prinzip her ein „universelles trojanisches Pferd“ sein.

Was der Trojaner dann auf dem Rechner des Personalmitarbeiters oder möglicherweise auf allen Rechnern im Unternehmensnetzwerk „anstellt“, hängt davon ab, was der Ersteller des Trojaners damit bezwecken möchte. Er kann

- alle Daten auf der Festplatte verschlüsseln,
- Ihre Datenbank (Personalakten, Kunden, ...) auf einen Rechner außerhalb ihrer Firma übertragen
- die Daten in den Unternehmens-Datenbeständen verändern
- etc.

Der Trojaner wird auf jeden Fall die Unternehmens-Datenschutzziele „Verfügbarkeit, Vertraulichkeit oder Integrität“ verletzen, in den meisten Fällen sogar alle drei.

**Schutzmöglichkeiten**

Um sich vor solchen Cyber-Angriffen oder auch ganz allgemein vor Bedrohungen zu schützen, gibt es ein Standardvorgehen:

Erster Schritt: Analyse der Risiken / Bedrohungen

Zunächst erstellt man eine Liste der möglichen Bedrohungen, Angriffspunkte und Risiken. Zu jedem der aufgelisteten Punkte bestimmt man möglichst grob (niedrig – mittel – hoch) die mögliche Schadenshöhe für das eigene Unternehmen und die Wahrscheinlichkeit, dass dieses Risiko eintritt (Eintrittswahrscheinlichkeit). Üblicherweise nimmt man sich dann zuerst die Risiken mit dem größten Faktor aus Schadenshöhe und Eintrittswahrscheinlichkeit vor.

Zweiter Schritt: Maßnahmendefinition:

Zu den im Schritt 1 ausgewählten Risiken überlegt man sich Maßnahmen, wie das Risiko gemindert oder ausgeschlossen werden kann.

Grundsätzlich gibt es hierbei immer drei Lösungswege:

a) ein konkret selbst tragbares Risiko übernehmen und eingehen,
b) das Risiko mit technischen und organisatorischen Maßnahmen minimieren und möglichst eliminieren,

oder

c) das Risiko wirtschaftlich transferieren, d. h., vor allem bei unternehmens- und existenzgefährdenden Risiken, sich gegen den wirtschaftlichen Schaden daraus zu versichern.

Lösung a) Die maximale Schadenhöhe nur schätzen und abwarten. Wenn das Risiko irgendwann eintritt, gilt es den Schaden, wenn möglich, selbst zu begleichen. Danach wird man sicherlich erneut prüfen müssen, ob ein anderer Lösungsweg doch geeigneter ist, vor allem wenn der Schaden zu einer wirtschaftlichen „Unzeit“ eintritt.

Für die Lösung b) gibt es die unterschiedlichsten Maßnahmen. Einige typische technische und organisatorische Maßnahmen sind:

- Infrastruktur: bauliche Schutz-Maßnahmen, intern wie extern
- Organisation: Zuständigkeiten klären, Dokumentationen und Arbeitsanweisungen erstellen, einführen und Einhaltung kontrollieren
- Personal: Vertretungsregelung, Schulung, Bewusstseinsförderung
- Hardware/Software: Passwortgebrauch, Protokollierung, Vergabe von Berechtigungen

- Elektronische Kommunikation: Konfiguration, Datenübertragung, E-Mail-Verschlüsselung, SSL, Firewall
- Notfallvorsorge: Notfallpläne erstellen, Datensicherung planen und durchführen, weitere Vorsorgemaßnahmen treffen

Gerade der MENSCHLICHE Faktor ist nicht zu vernachlässigen. Dieser Punkt gehört zwar hauptsächlich zu den organisatorischen Maßnahmen, jedoch ist es sehr wichtig, diesen explizit mit zu bedenken:

- Bei Menschen fehlt meistens das Verständnis für noch nicht erfahrene, selbst erlebte Risiken. Dieses mangelnde Verständnis führt häufig zu Unachtsamkeit und zu Fehleinschätzung, welche die Risiken sogar begünstigen.
- In Situationen, die selten vorkommen, reagieren die Mitarbeiter ungeübt und deswegen womöglich falsch. Deshalb ist es wichtig, Notfallübungen durchführen. Bestes Beispiel dafür sind Feuerwehrübungen.
- Viele Menschen haben ein nahezu grenzenloses Vertrauen in die Technik und gehen davon aus, dass der Computer immer Recht hat. Computerexperten wissen, dass dieses Vertrauen zu einem hohen Prozentsatz ungerechtfertigt ist.
- Unbequemlichkeiten werden von Menschen abgelehnt. Sicherheit und Risiken entstehen und wirken im Verborgenen. Dieses Wissen sollte bei der Auswahl der Maßnahmen berücksichtigt werden.
- Enttäuschte und böswillige Mitarbeiter (Insider) können sehr hohe Schäden verursachen, gegen die kaum eine der oben genannten Maßnahmen greift. Diese Mitarbeiter sind im Gebäude, haben die Berechtigung die Software zu nutzen usw. Echten Schutz bieten neben persönlichen Gesprächen zum Verständnis und zur Prävention eigentlich nur das wirtschaftliche Auffangen des Schaden durch eine Versicherung, die auch einen begangenen Vertrauensschaden mit berücksichtigt.
- Angriffe durch „Social Engineering“: Experten wissen, dass es einfacher ist, einen Berechtigten dazu zu bringen, den Angriff durchzuführen, als sich selbst die entsprechende Mühe machen zu müssen.

Dritter Schritt: Maßnahmen umsetzen und Wirksamkeit kontrollieren.

Zur Minimierung des möglichen Schadens für das eingangs genannte Szenario sind folgende konkrete Maßnahmen möglich:

Dateien auf mobilen Datenträgern sind zu behandeln wie Downloads aus dem Internet. Sie dürfen nur von Berechtigten nach Virenscan geöffnet und ggfs. bearbeitet werden.

Es wird eine sogenannte Dateischleuse angewendet.

Für die Nutzung von USB-Sticks könnte noch eine Trennung von „nur internen“ oder „extern verwendeter“ USB-Sticks eingeführt werden. Dies erfordert jedoch von Allen eine hohe Konsequenz und löst das Risiko „Empfang eines fremden USB-Sticks von außen“ nicht vollständig.

**Warum sollten Schutzmaßnahmen in Unternehmen eingeführt werden?**

Zu allererst helfen eingeführte Schutzmaßnahmen einem Unternehmen, seine Daten zu schützen und handlungsfähig zu bleiben. Die Erreichung des obersten Unternehmensziels erhält durch die Einführung der EU-DSGVO noch ein paar weitere Aspekte, die man nicht außer Acht lassen sollte: **es erhöht sich die Dokumentationspflicht sowie die Meldepflicht von Datenschutzverletzungen an die Aufsichtsbehörden!** Zudem erhöhen sich die zu erwartenden Strafen für die Verletzung dieser Pflichten: Es können Bußgelder von bis zu vier

Prozent des globalen Unternehmensumsatzes beziehungsweise bis zu 20 Millionen Euro für betroffene Manager oder andere Entscheidungsträger verhängt werden.

Für Fehleinschätzungen der Risiken und deren Auswirkungen, die sogar zur Insolvenz führen können, z. B. aufgrund von unzureichendem Versicherungsschutz oder wegen sehr hoher Ansprüche Dritter aufgrund eingetretener Datenschutzverletzungen, haften die verantwortlichen Unternehmensleiter und Manager auch mit ihrem Privatvermögen.

Fordern Sie direkt Ihr persönliches Angebot für eine Cyber-Versicherung bei der CONAV Consulting ab: Risikoermittlungsbogen

**Pressekontakt:**

Ralf W. Barth
Telefon: 07138 81099970
Fax: 07138-81099922
E-Mail: info@conav.de

**Unternehmen**

CONAV Consulting GmbH & Co. KG
Birkenweg 5
74193 Schwaigern

Internet: www.conav.de

**Über CONAV Consulting GmbH & Co. KG**

Die CONAV steht Unternehmen, Vermittlern und Beratern als CoNavigator in unternehmerischen, strategischen, absicherungstechnischen und vertrieblichen Themen zur Seite. Als Versicherungsmakler fokussiert sich die CONAV auf nettobasierte Absicherungen für Gewerbetreibende sowie kleinere und mittlere Unternehmen (KMU). Sie bietet Analysen zum Risikomanagement und praxisnahe Lösungen für Führungskräfte, Gewerbetreibende, Unternehmer und Unternehmen.

**Pressekontakt:**

Rose Müller
Telefon: 07142 3392343
Fax: 07142 9669588
E-Mail: dsb@startklar-rosemueller.de

**Unternehmen**

Startklar
Bei der Kelter 5
74321 Bietigheim-Bissingen

Internet: www.startklar-rosemueller.de