Quelle: putilov_denis – stock.adobe.com

Datenschutz: Szenario „Cyber-Angriff“

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 präventiver Schutzmaßnahmen – wir haben ein Szenario beispielhaft 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,
- die Datenbank (Personalakten, Kunden, etc.) auf einen Rechner außerhalb ihrer Firma übertragen
- die Daten in den Unternehmens-Datenbeständen verändern
- usw.

Der Trojaner wird auf jeden Fall die Vorgaben des Datenschutzes in einem Unternehmen wie „Verfügbarkeit, Vertraulichkeit oder Integrität“ verletzen, in den meisten Fällen sogar alle drei zu einem Zeitpunkt.

Schutzmöglichkeiten

Um sich vor Cyber-Angriffen wie diesen oder auch ganz allgemein vor Bedrohungen zu schützen, gibt es einige Standards zur Prävention:

Erster Schritt: Analyse der Risiken / Bedrohungen

Zunächst sollte eine Liste der möglichen Bedrohungen wie Angriffspunkte und Risiken erstellt werden. Zu jedem der aufgelisteten Punkte sollte eine möglichst valide Einschätzung vorgenommen werden:

- Schadenhöhe insgesamt möglichst grob (niedrig – mittel – hoch)
- die mögliche Schadenshöhe für das eigene Unternehmen
- die Schadenwahrscheinlichkeit
- das Risiko einer Eintrittswahrscheinlichkeit

Daraus geht eine Prioritätenliste für Abwehrmaßnahmen hervor.

Zweiter Schritt: Maßnahmendefinition

Zu den im Schritt 1 ausgewählten Risiken werden Maßnahmen definiert, wie das Risiko gemindert oder ausgeschlossen werden kann. Grundsätzlich gibt es hierbei drei Lösungswege:

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

oder

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

Zu 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 sicherlich erneut zu prüfen sein, ob ein anderer Lösungsweg geeigneter erscheint, vor allem wenn der Schaden zu einer wirtschaftlichen „Unzeit“ eintritt.

Zu Lösung b)

Einige typische technische und organisatorische Maßnahmen sind:

- die Infrastruktur: bauliche Schutz-Maßnahmen, intern wie extern
- die Organisation: Zuständigkeiten klären, Dokumentationen und Arbeitsanweisungen erstellen, einführen und Einhaltung kontrollieren
- das Personal: Vertretungsregelung, Schulung, Bewusstseinsförderung
- die Hard- und Software: Passwortgebrauch, Protokollierung, Vergabe von Berechtigungen
- die elektronische Kommunikation: Konfiguration, Datenübertragung, E-Mail-Verschlüsselung, SSL, Firewall
- die Notfallvorsorge: Notfallpläne erstellen, Datensicherung planen und durchführen, weitere Vorsorgemaßnahmen treffen

Gerade der Faktor „Mensch“ ist nicht zu vernachlässigen. Dieser Punkt gehört zwar hauptsächlich zu den organisatorischen Maßnahmen, jedoch ist es sehr wichtig, diesen explizit einzubeziehen:

- Menschen fehlt häufig das Verständnis für noch nicht erfahrene, selbst erlebte Risiken. Dieses mangelnde Verständnis führt in Folge zu Unachtsamkeit und zu Fehleinschätzungen, was wiederum Risiken begünstigen kann.
- In Situationen, die selten vorkommen, reagieren Mitarbeiter oft ungeübt und möglicherweise falsch. Deshalb ist es wichtig, dass auch Notfallübungen durchgeführt werden. 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 bietet neben persönlichen Gesprächen zum Verständnis und zur Prävention 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 möglicher Schäden 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 nicht außer Acht gelassen werden sollten. Es erhöhen sich die Dokumentationspflicht sowie die Meldepflicht von Datenschutzverletzungen an die Aufsichtsbehörden und in Folge auch 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. Fehleinschätzungen der Risiken und deren Auswirkungen, können sogar zur Insolvenz führen, beispielsweise aufgrund eines unzureichenden Versicherungsschutz oder wegen sehr hoher Ansprüche Dritter aufgrund eingetretener Datenschutzverletzungen. Verantwortliche Unternehmensleiter und Manager haften mit ihrem Privatvermögen.

Bild: © putilov_denis / fotolia.com

Versicherungs- und Finanznachrichten

expertenReport

https://www.experten.de/id/4943619/datenschutz-szenario-cyber-angriff/