SICHERHEITSHALBER
MORGEN JUNG

Cyberabwehr ist Chefsache

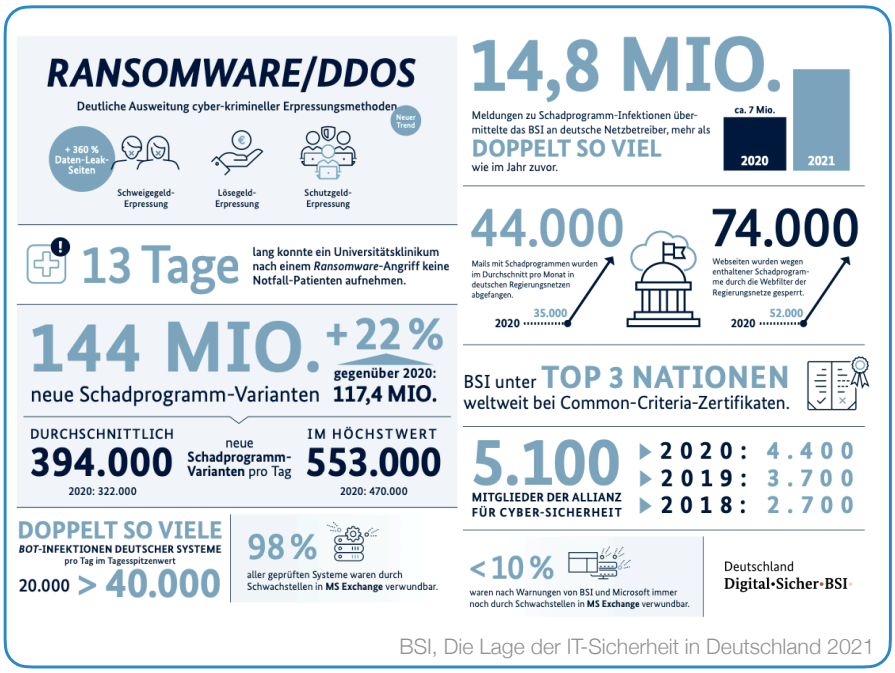
Internetkriminalität und ihre Folgen für Unternehmen

Die Gefährdungslage der Unternehmen durch die Cyber-Kriminalität ist erneut in den Fokus gerückt, besonders durch den Krieg in der Ukraine. Nichts funktioniert ohne IT – ihr Ausfall führt zum Lockdown einzelner Abteilungen bis hin zum Stillstand des ganzen Betriebs. Im Extremfall steht die Existenz des Unternehmens auf dem Spiel. Daher gilt: Cyber-Abwehr ist Chef-Sache!

Unternehmensprozesse werden stetig digitalisiert und die Covid-19-Pandemie hat diesen Trend zum überlebenswichtigen Faktor gemacht. Mit anderen Worten: Ohne eine funktionsfähige IT geht nichts mehr. Gleichzeitig ist die Cyber-Gefahrenlage in den letzten Monaten stetig gestiegen und die Kosten für den Höchstschaden sowie der Median der Schadenkosten sind explodiert.

Unabhängig von der Branche sind alle Unternehmen zunehmend mit dieser Problematik konfrontiert: Kundendaten werden ins System eingegeben. Kalkulationen, Bankverbindungen, Verträge, Bilanzen, Gewinn- und Verlust-Rechnungen und vieles mehr an vertraulichen Daten werden digital erfasst und durch IT-Systeme des Unternehmens verarbeitet.

Laut dem Bundesamt für Sicherheit in der IT (BSI) sind es insbesondere die Schadprogramme, komplexe Phishing-Angriffe, Daten-Leaks und das Ausnutzen von Softwareschwachstellen, die beim Datendiebstahl das Gefährdungspotential erhöhen. Ein Verlust oder die Ausspähung von Kunden- und/oder Personaldaten kann zum Supergau werden beziehungsweise erhebliche Kosten, Ertragseinbrüche und Haftungsansprüche verursachen.



BSI, Die Lage der IT-Sicherheit in Deutschland 2021

Die Kommunikation und der Informationsaustausch mit Kunden und sonstigen Dritten basiert in der Regel auf positiven Beziehungen und Vertrauen zwischen den handelnden Personen. Genau an dieser „menschlichen Schnittstelle“ zum Firmennetzwerk liegt das höchste Gefahrenpotential für einen Cybervorfall.

Die Mitarbeiter müssen ihre Resilienz gegen Cyberangriffe aufbauen und kontinuierlich erweitern. Schon ein kleiner Fehler beim Umgang mit einem nicht erkannten Schadprogramm führt schnell zum Ausspähen von Administrator-Rechten. Mit diesen Rechten nimmt das Virus im Netzwerk Fahrt auf und der Cyberangriff breitet sich dort ungebremst aus.
Ein weiterer Angriffspunkt ist das sogenannte Social Engineering. Durch das Ausspähen von Netzbeziehungen macht sich ein möglicher Angreifer zu einem bekannten und vertrauensvollen Kontakt und schon wird die Tür zum Datenklau von den eigenen Mitarbeitern voller Vorfreude und serviceorientiert aufgestoßen.

Erfolgreiche Digitalisierung braucht Cybersicherheit

Bei der Überprüfung des konkreten Cyber-Risikos für die Unternehmen ist zunächst die Gefährdungslage im Detail zu analysieren. Zur Risikovermeidung und -minderung sind neben technischen Abwehrmaßnahmen insbesondere auch menschliche Abwehrkompetenzen gefragt. Am Ende ist nicht zuletzt der Risikotransfer zu prüfen.

Datensicherung ist das A und O

Die Datensicherung ist das A und O in der Gefahrenabwehr. Bei einer Infizierung mit einem Schadprogramm ist ein funktionsfähiges Backup in der Regel die einzige Rettung. Grundsätzlich kann man sich bei Bezahlung eines Lösegeldes nicht auf die Dienstleistungsqualität des Cyber-Angreifers verlassen. Damit das Cyber-Risiko sinkt, müssen alle Geräte mit einem aktuellen Virenschutz ausgestattet und die Firewall des Netzwerks muss auf die aktuelle Cyber-Gefahrenlage eingestellt sein.
Alle technischen Maßnahmen können allerdings nur unterstützen. Häufig wird der „Faktor Mensch“ als Ausgangspunkt eines Cyberangriffes unterschätzt. Die Unternehmen sollten daher alle Nutzer des Firmennetzwerkes sensibilisieren und die nachstehenden Mindestanforderungen durchsetzen:

- Komplexe Passwörter
- Passwort-Manager als Kennwort-Tresor einsetzen
- Mehr-Faktor-Authentifizierung
- Regelmäßige Updates
- Vorsicht bei dubiosen Mails und Anfragen
- Informationen ernst nehmen und entsprechend handeln

Kurzum: Um Cyberrisiken effektiv begegnen zu können, muss ein Verständnis geschaffen werden: Risiken erkennen, Risiken beeinflussen, Training und permanente Kontrolle.

Die wesentlichen Aspekte der Cyberkriminalität in Deutschland 2021

Bundeskriminalamt, Bundeslagebild Cybercrime 2021

Transfer des Restrisikos

Die Unternehmen, die sich auf diese Weise umfänglich auf das Cyber-Risiko vorbereitet haben, können schließlich das Restrisiko auf einen Risikoträger übertragen und so den Handlungskreis zur erfolgreichen Cyber-Abwehr schließen. Die Möglichkeit, sich gegen Cyberrisiken zu versichern, ist allerdings vielen Unternehmen noch nicht bekannt. Nachfolgend wird deshalb erläutert, welche Voraussetzungen bei Unternehmen vorliegen müssen, was sich versichern lässt und wie im Schadensfall am besten zu agieren ist.
Bei einer entsprechenden Versicherungslösung werden im Wesentlichen Präventions- und Assistance-Leistungen zur Abwehr und Bewältigung von Cyber-Risiken eingekauft, daneben kommt es aber auch auf die Schadenregulierungskompetenz an. Eine Cyber-Versicherung sollte unter anderem folgende Punkte abdecken:

1. Prävention und Notfallplan
2. Sofortmaßnahmen 24/7
3. Beratung und Maßnahmen zur Schadenminderung
4. Ertragsausfall und Mehrkosten
5. Wiederherstellung von Daten und Systemen
6. Informationspflichten bei Datenschutzverletzungen
7. Betrugsschäden und Identitätsdiebstahl
8. Haftpflichtansprüche aus Cyberangriffe

Als Fazit lässt sich festhalten: Die Gefahrenabwehr von Cyber-Risiken ist durch drei Bausteine gekennzeichnet – technische Gefahrenabwehr, Steigerung der Mitarbeiterkompetenzen und Risikotransfer durch einen umfassenden Versicherungsschutz.

Beispiele für Schaden-Szenarien bei Cyberangriffen

Ransomware-Schaden

Cyber-Vorfall: Der Unternehmens-Server wird gehackt. Es kommt zum kompletten Systemausfall. Die Erpresser verschlüsseln alle Daten und fordern **10.000 Euro** für die Datenfreigabe.

SICHERHEITSHALBER Cyber-Abwehr:
Der Risikoträger beauftragt sofort seinen Cyber-IT-Dienstleister, der gemeinsam mit dem Unternehmen das Problem löst. Im Idealfall entsteht somit kein Schaden. Zudem zeigen die IT-Spezialisten Präventionsmaßnahmen auf. Ein Beispiel für die sinnvolle Erweiterung des Versicherungsschutzes auf Sofortmaßnahmen im Schadenfall und auf Beratungskosten für Cyber-IT-Spezialisten.

Laptop Diebstahl

Cyber-Vorfall: Einem Geschäftsführer wurde der Arbeitsrechner gestohlen. Darauf gespeichert: Vertrauliche Namen und Finanzdaten von großen deutschen Industrieunternehmen.

SICHERHEITSHALBER Cyber-Abwehr:
Das Unternehmen muss seine Kunden informieren, eine PR-Agentur engagieren und ein Callcenter einrichten. Außerdem muss er Anwälte für die Sicherstellung der Benachrichtigungs- und Compliance-Richtlinien hinzuziehen. Es entsteht ein Schaden von **einer Million Euro**. Die Cyber-Versicherung kommt für die Kosten auf. Ebenfalls übernimmt der Versicherer die Abwehr von Schadenersatzansprüchen und erwirkt einen Vergleich über **zwei Millionen Euro**.

Verschlüsselte Kundendaten

Cyber-Vorfall: Ein Mitarbeiter öffnet versehentlich einen E-Mail-Anhang mit einem Trojaner. Die Schadsoftware verschlüsselt alle Dateien auf dem Netzwerk. Es erscheint der Hinweis, dass die Entschlüsselung nur gegen Bezahlung von Bitcoins erfolgt.

SICHERHEITSHALBER Cyber-Abwehr:
Ein IT-Sicherheitsexperte unterstützt den lokalen IT-Dienstleister des Unternehmens. Er empfiehlt Sofortmaßnahmen, um die Ausbreitung der Schadsoftware einzudämmen. Auch hilft er bei der Daten-Rekonstruktion. Die Cyber-Versicherung übernimmt die Kosten für IT-Forensik und Datenwiederherstellung (**circa 250.000 Euro**).

Autor: Christoph H. Neumann

Weitere Artikel und Newsletter finden Sie auf unserer Website:
www.sicherheitshalber.de unter dem Abschnitt „News“, oder auf direktem Wege über den QR-Code.

Fotos: © Adobe Stock und eigene Bilder