Laut einer repräsentativen Umfrage des IT-Branchenverbandes Bitkom wurden 61 Prozent der Internetnutzer im Jahr 2020 Opfer von Cyber-Kriminalität.

INTERNETKRIMINALITÄT UND IHRE FOLGEN FÜR DEN GEBÄUDEDIENSTLEISTER

CYBERABWEHR IST **CHEFSACHE**

In Zeiten der Pandemie ist die Gefährdungslage der Unternehmen durch Cyberkriminalität erneut in den Fokus gerückt. 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: Cyberabwehr ist Chefsache!

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

Christoph H. Neumann
ist spezialisierter Versicherungsmakler für Gebäudedienstleister.
c.neumann@sicherheitshalber.de

Auch Gebäudedienstleister sind zunehmend mit dieser Problematik konfrontiert: Mitarbeiterdaten werden ins System eingegeben, Stundenzettel gefertigt sowie Ausschreibungsunterlagen und Leistungsverzeichnisse erstellt. Genau an dieser „menschlichen Schnittstelle" zum Firmennetzwerk liegt das höchste Gefahrenpotential für einen Cybervorfall.
Laut dem Bundesamt für Sicherheit in der Informationstechnik (BSI) sind es insbesondere die Fortentwicklung der Schadprogramme, komplexe PhishingAngriffe, Daten-Leaks und das Ausnutzen von Softwareschwachstellen, die beim Datendiebstahl das Gefährdungspotential erhöhen. Ein Verlust oder das Ausspähen von Kunden- und/oder Personaldaten kann zum Supergau führen beziehungsweise erhebliche Kosten und Ertragseinbrüchen verursachen. Und da Gebäudedienstleistung „People Business" ist, steigt das Cyber-Schadenpotenzial mit

BEISPIELE FÜR SCHADENSZENARIEN BEI CYBERANGRIFFEN

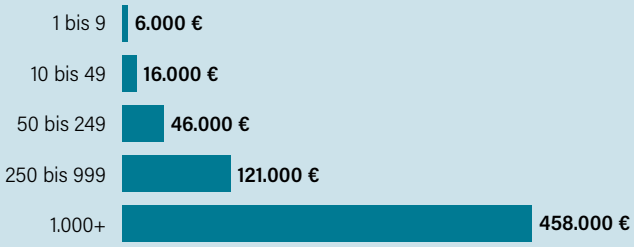
Übersicht verschiedener Szenarien

	Cybervorfall	Cyberabwehr
Ransomware-Schaden	Der Unternehmens-Server wird gehackt. Es kommt zum kompletten Systemausfall. Die Erpresser verschlüsseln alle Daten und fordern 10.000 Euro für die Datenfreigabe.	Der Risikoträger beauftragt sofort seinen IT-Dienstleister, der gemeinsam mit dem Gebäudedienstleister 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.
Mailing an falschen Verteiler	Ein Gebäudedienstleister versendet per E-Mail versehentlich ein vertrauliches Dokument mit Adress- und Bestelldaten sowie Bankverbindungen von Kunden.	Für das Unternehmen entsteht zwar kein Schaden. Allerdings ist die gesetzliche Meldepflicht zu beachten. Der Versicherer vermittelt umgehend den Kontakt zu einer auf Datenschutzverletzungen spezialisierten Kanzlei, mit der die weiteren Schritte abgestimmt werden. Die Beratungskosten trägt die Cyberversicherung.
Verschlüsselte Kundendaten	Ein Mitarbeiter eines Gebäudedienstleisters 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.	Ein IT-Sicherheitsexperte unterstützte den lokalen IT-Dienstleister des Unternehmens. Er empfiehlt Sofortmaßnahmen, um die Ausbreitung der Schadsoftware einzudämmen. Auch hilft er bei der Daten-Rekonstruktion. Die Cyberversicherung übernimmt die Kosten für IT-Forensik und Datenwiederherstellung (circa 25.000 Euro).

der Mitarbeiteranzahl. Somit ist die Gefährdungslage für die Branche als sehr hoch anzusehen.
Schon ein kleiner Fehler beim Umgang mit einem Schadprogramm führt schnell zum Ausspähen von Administrator-Rechten. Mit diesen Rechten nimmt das Virus im Netzwerk Fahrt auf und der Cyberangriff breitet sich im Firmennetzwerk 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 vom Mitarbeiter voller Vorfreude und serviceorientiert aufgestoßen. ▶

Gesamtkosten der Cyber-Vorfälle

Der Cyber-Readiness-Report-2020 eines Spezialversicherers zeigt: Die Schadenkosten steigen überproportional im Verhältnis zur Anzahl der Mitarbeiter.



Bei der Überprüfung des konkreten Cyberrisikos für das 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 Cyberangreifers verlassen. Damit das Cyberrisiko sinkt, müssen alle Geräte mit einem aktuellen Virenschutz ausgestattet und die Firewall des Netzwerks muss auf die aktuelle Gefahrenlage eingestellt sein.
Alle technischen Maßnahmen können allerdings nur unterstützen. Häufig wird der „Faktor Mensch" als Ausgangspunkt eines Cyberangriffes unterschätzt. Der Gebäudedienstleister sollte daher alle Nutzer des Firmennetzwerkes sensibilisieren und die nachstehenden Mindestanforderungen durchsetzen:

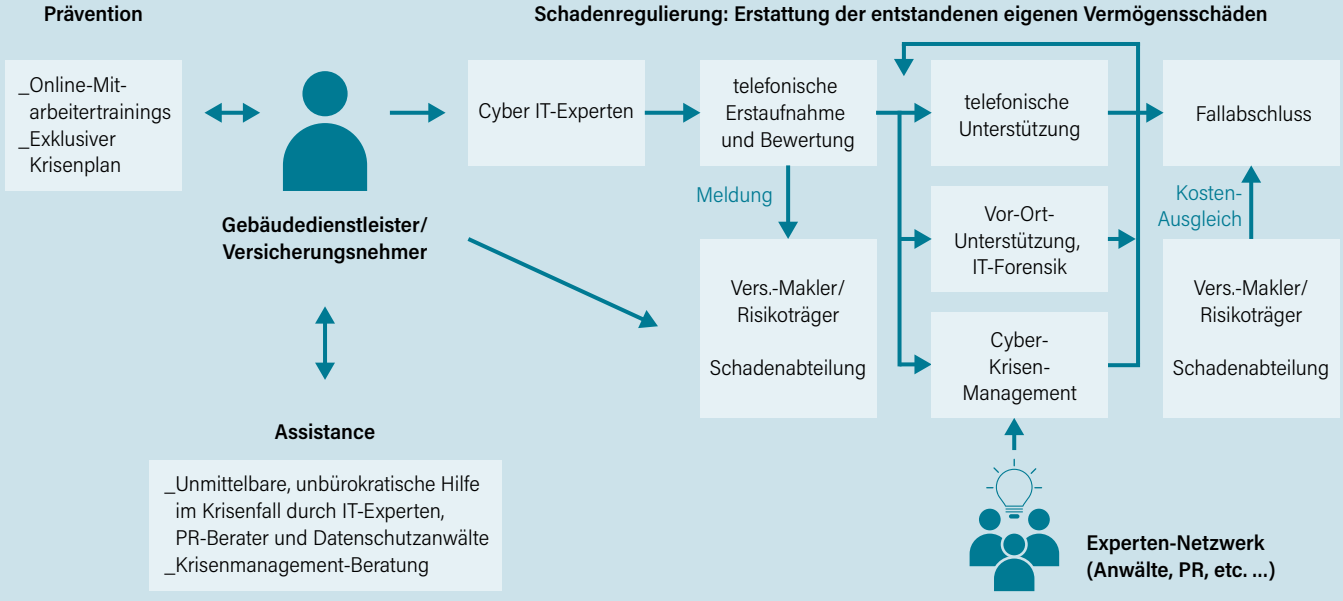
- komplexe Passwörter
- Passwort-Manager als Kennwort-Tresor einsetzen
- Mehr-Faktor-Authentifizierung
- regelmäßige Updates
- Vorsicht bei dubiosen Mails und Anfragen
- Informationen ernst nehmen und entsprechend handeln

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

TRANSFER DES RESTRISIKOS

Der Gebäudedienstleister, der sich auf diese Weise umfänglich auf das Cyberrisiko vorbereitet hat, kann schließlich das Restrisiko auf einen Risikoträger übertragen und so den Handlungskreis zur erfolgreichen Cyberabwehr schließen. Diese Möglichkeit, sich gegen Cyberrisiken zu versichern, ist allerdings vielen Gebäudedienstleistern noch nicht bekannt.

Mit einer Cyberversicherung erhält der Gebäudedienstleister die Unterstützung von Cyber-IT-Spezialisten, Cyber-Forensik sowie spezialisierten Rechtsanwälten und Sachverständigen.



Grafiken: Sicherheitshalber

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 AssistanceLeistungen zur Abwehr und Bewältigung von Cyberrisiken eingekauft. Folgende Punkte sollte eine Cyberversicherung abdecken:

Sofortmaßnahmen

Der Versicherungsschutz muss eine 24/7-Hotline mit Cyber-IT-Spezialisten und Sachverständigen bereitstellen. Mit gezielten Sofortmaßnahmen lässt sich eine Ausweitung des Schadens vermeiden.

Beratung und Maßnahmen zur Schadenminderung

Um einen Schaden gering zu halten, ist ein wirkungsvolles Krisenmanagement und eine angemessene Kommunikation nach außen notwendig.

Ertragsausfall und Mehrkosten

Kosten entstehen vor allem dadurch, dass Daten nicht mehr zur Verfügung stehen, die Erbringung der (Dienst-)Leistung ausfällt oder die Website offline ist.

Wiederherstellung von Daten und Systemen

Datenordnung und Systeme müssen wiederhergestellt werden, eventuell ist eine Datenrettung notwendig.

Informationspflichten bei Datenschutzverletzungen

Wenn Unternehmen personenbezogene Daten verwalten und diese Daten die in fremde Hände geraten, sind sie gesetzlich verpflichtet, die Betroffenen sowie die Behörden zu informieren.

Betrugsschäden

Betrugsdelikte, wie zum Beispiel Manipulation von Websites oder Identitätsdiebstahl, können erhebliche Vermögensverluste auslösen.

Haftpflichtansprüche

Berechtigte Forderungen Dritter müssen ausgeglichen, unberechtigte Ansprüche abgewehrt werden. Wichtig: Die Cyberhaftpflicht sollte auch verschuldensunabhängige Tatbestände mit abdecken.

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

Christoph H. Neumann
guenter.herkommer@holzmann-medien.de