Ganz ausschließen lässt sich ein Cyberangriff nie – bestmöglich vorbeugen hilft jedoch, die Folgen in Grenzen zu halten.

CYBERANGRIFFE GEFÄHRDEN DIE GEBÄUDEDIENSTLEISTER

RESILIENZ AUF DREI EBENEN

Prominente Schadenfälle in der nahen Vergangenheit machen die Risiken deutlich: Keine Auftragsbearbeitung ohne IT, Löhne- und Sozialversicherungsbeiträge werden nicht fristgerecht gezahlt und die Anforderungen des Datenschutzbeauftragten nach einem Cyberangriff blockieren die gesamte Unternehmensleistung des Gebäudedienstleisters. Wie man sich davor wappnet.

Laut dem aktuellen Bericht des Bundesamtes für Sicherheit in der Informationstechnik (BSI) spitzte sich die bereits zuvor angespannte Lage der IT-Sicherheit in Deutschland im Jahr 2022 weiter zu – unter anderem im Zusammenhang mit dem russischen Angriffskrieg auf die Ukraine. Die Bedrohung im Cyberraum ist damit so hoch wie nie! Und es stellt sich auch nicht mehr die Frage, ob ein Gebäudedienstleister durch Cyberkriminalität geschädigt wird, sondern wann und in welchem Ausmaß der Angriff die Existenz des Unternehmens gefährdet.

Ein prominentes Beispiel dafür, welche Folgen eine Cyberattacke nach sich ziehen kann, ist die Wisag. Bereits Ende Januar 2022 wurde der Dienstleister Ziel eines gezielten Angriffes: Zwar liefen damals die operativen Geschäfte weiter, aber die Abläufe waren etwa eine Woche lang stark gestört. Unter anderem konnten die Löhne für 55.000 Mitarbeiter erst verspätet ausgezahlt werden.

Fast genau ein Jahr später hat es die Wisag erneut getroffen. Wie die Frankfurter Allgemeine Zeitung berichtete, habe die IT-Abteilung Anfang Februar laut einer Sprecherin des Unternehmens „Unregelmäßigkeiten“ auf den Servern festgestellt. Daraufhin wurden umgehend alle Systeme und Anwendungen vom Netz genommen und mit der Entstörung der Systeme begonnen. Der Konzern habe nach dem Angriff vor einem Jahr seine Hausaufgaben gemacht und in die IT-Sicherheit investiert und es sei nicht ersichtlich, „dass Kunden- oder interne Daten abgeflossen sind“.

Das Beispiel aus der Branche zeigt: Gänzlich ausschließen lässt sich ein Cyberangriff wohl nie – die negativen Folgen lassen sich jedoch in Grenzen halten, indem man einer möglichen Attacke bestmöglich vorbeugt und im Fall der Fälle weiß, wie man richtig und vor allem schnell darauf reagiert.

Christoph H. Neumann
ist spezialisierter Versicherungsmakler für Gebäudedienstleister.

Bilder: NicoElNino – stock.adobe.com; Sicherheitshalber

Vor dem geschilderten Hintergrund lässt sich allen Gebäudedienstleistern nur raten, ihre Resilienz auf drei Ebenen zu prüfen, zu aktualisieren und kontinuierlich fortzuschreiben.

EBENE 1: CYBERPRÄVENTION

Die Datensicherung ist das A und O in der Gefahrenabwehr. Bei einer Infizierung mit einem Schadprogramm ist ein funktionsfähiges Back-up in der Regel die einzige Rettung. Grundsätzlich kann man sich bei Bezahlung eines Lösegeldes nicht auf die Dienstleistungsqualität des Angreifers 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 (technische Abwehrkräfte).

Alle technischen Maßnahmen können allerdings nur unterstützen. Häufig wird der Faktor „Mensch" als Ausgangspunkt eines Cyberangriffes unterschätzt. Der Gebäudedienstleister sollte neben den technischen Abwehrmaßnahmen alle Nutzer des Firmennetzwerkes sensibilisieren – Stichwort: Cyber-Mitarbeiter-Resilienz – und die nachstehenden Mindestanforderungen durchsetzen. Dazu zählen:

- komplexe Passwörter,
- Passwortmanager als Kennworttresor einsetzen,
- Mehr-Faktor-Authentisierung,
- regelmäßige Updates,
- Vorsicht bei dubiosen Mails und Anfragen,
- Informationen ernst nehmen und entsprechend handeln.

Ein weiterer wichtiger Eckpfeiler der Cyberprävention ist der Notfallplan: Hier ist gute Vorbereitung des Gebäudedienstleisters gefragt. Im Fall der Fälle geht es vor allem darum, schnell zu reagieren und so den Cyberangriff möglichst rasch zu unterbinden, die Daten zu schützen und auch die Arbeitsfähigkeit des Unternehmens wiederherzustellen. Dafür legt der Notfallplan verschiedene Sofortmaßnahmen und externe sowie interne Berichts- und Kommunikationswege fest, beispielsweise wenn die Bürokommunikation oder die digitale Zeiterfassung lahmgelegt wird, wichtige Webseiten nicht mehr erreichbar sind oder die Auftragsbearbeitung und die Lohnbuchhaltung wegen eines digitalen Angriffs stillsteht. Grundsätzlich stellt der Cybernotfallplan die Überlebensstrategie des Gebäudedienstleisters bei einem Hackerangriff dar, denn mit Stecker ziehen allein ist es nicht getan.

> **Mit „Stecker ziehen" allein ist es bei einem Hackerangriff nicht getan.**
>
> Christoph H. Neumann

EBENE 2: 24/7 CYBER TASK FORCE

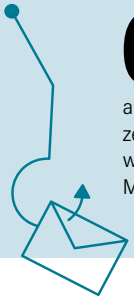
Im Überlebenskampf nach einem Hackerangriff muss der Notfallplan mit Leben gefüllt werden und der Gebäudedienstleister muss sich bereits vor dem Cybervorfall alle notwendigen Dienstleistungen gesichert haben, damit eine zielgerichtete Abwehrschlacht unverzüglich beginnen kann. Dafür müssen IT-Spezialisten, Sachverständige und sonstige Cyberrisk-Spezialisten zur Verfügung stehen und im Schadenfall leistungsbereit und leistungsverpflich- ▶

Fakten aus dem aktuellen Lagebericht des BSI zur IT-Sicherheit in Deutschland

15 Millionen
Meldungen zu Schadprogramm-Infektionen in Deutschland übermittelte das BSI im Berichtszeitraum an deutsche Netzbetreiber.

34.000
Mails mit Schadprogrammen wurden monatlich durchschnittlich in deutschen Regierungsnetzen abgefangen.

78.000
neue Webseiten wurden wegen enthaltener Schadprogramme für den Zugriff aus den Regierungsnetzen gesperrt.



69 %
aller Spam-Mails im Berichtszeitraum waren Cyber-Angriffe wie z.B. Phishing-Mails und Mail-Erpressung.

90 %
des Mail-Betrugs im Berichtszeitraum war Finance Phishing, d.h. die Mails erweckten betrügerisch den Eindruck, von Banken oder Sparkassen geschickt worden zu sein.

tet sein. Der Gebäudedienstleister sollte sich die entsprechenden Dienstleistungen im Vorfeld eingekauft beziehungsweise die Verfügbarkeit eines 24/7 Cyber-Task-Force-Teams gesichert haben.

EBENE 3: TRANSFER AUF EINEN RISIKOTRÄGER

Eine Cyberversicherung beinhaltet alle vorab genannten Punkte sowie sonstige Schadenskosten. Neben der eigentlichen Entschädigungsleistung im Schadensfall stehen bei einem guten Cyberversicherungsschutz die Dienst- und Assistenzleistungen im Mittelpunkt des aktiven Leistungsversprechens.

Zunächst prüft der Versicherer beziehungsweise der mit dem Versicherungsvertrag eingekaufte, externe Cyberrisk-Dienstleister die technischen Abwehrfähigkeiten des Gebäudedienstleisters. Mit der Erstprüfung werden Maßnahmen zur Verbesserung der technischen Cyber-Sicherheit vorgeschlagen und zusammen mit dem Gebäudedienstleister besprochen.

Mit dem Abschluss einer Cyber-Police erhält man in der Regel auch eine digitale Mitarbeiterschulung, damit die Resilienz der Mitarbeiter gestärkt wird. Grundsätzlich ist eine dauerhafte und wiederkehrende Schulung der Mitarbeiter im Leistungsspektrum der Versicherungspolice zu verankern. Ebenso sollte die Aufmerksamkeit der Mitarbeiter durch dokumentierte Scheinattacken hochgehalten werden und in einem Cybercockpit beim Gebäudedienstleister dokumentiert werden.

Weiterhin erstellt der externe Cyber-Dienstleister mit dem Gebäudedienstleister den Notfallplan als Überlebensstrategie. Dieser Notfallplan kann in der Regel beim Versicherer als zusätzliche Leistung mitgebucht werden und sollte auch unbedingt eingekauft werden, da der so erstellte Notfallplan auf die mit dem Versicherer abgestimmten Versicherungs- und Assistenzleistungen im tatsächlichen Schadensfall abgestimmt ist.

Schließlich muss der Versicherungsschutz auch eine 24/7-Hotline mit Cyber-IT-Spezialisten und Sachverständigen bereitstellen, um mit gezielten Sofortmaßnahmen eine Ausweitung des Schadens zu vermeiden. Dazu zählen nicht zuletzt ein wirkungsvolles Krisenmanagement und eine angemessene Kommunikation nach außen.

Neben diesen essenziellen Bestandteilen einer Cyberversicherung werden je nach abgeschlossener Police noch weitere Schadenskosten durch den Versicherer reguliert:

- Ertragsausfall- und Mehrkosten, die etwa dadurch entstehen, dass Daten nicht mehr zur Verfügung stehen, die Wertschöpfung des Gebäudedienstleisters ausfällt oder die Website offline ist.
- Kosten für die Wiederherstellung von Daten und Systemen; eventuell ist eine Datenrettung notwendig.
- Informationspflichten bei Datenschutzverletzungen: Gebäudedienstleistung ist „Peoples Business“ und somit verwalten die Gebäudedienstleister personenbezogene Daten in erheblichen Umfang. Wenn diese relevanten Daten in fremde Hände geraten, sind die Gebäudedienstleister gesetzlich verpflichtet, die Betroffenen sowie die Behörden zu informieren. Die Informationspflicht zieht erhebliche Kosten für den Gebäudedienstleister nach sich.
- Betrugskosten: Delikte wie Manipulationen von Websites, das sogenannte „Fake President“ oder Identitätsdiebstahl können erhebliche Vermögensverluste beim Gebäudedienstleister auslösen.
- Der Versicherer übernimmt das Erpressungsgeld bei einer Cyberattacke.
- Cyber-Haftpflichtansprüche: Berechtigte Forderungen Dritter müssen ausgeglichen, unberechtigte Ansprüche abgewehrt werden. Wichtig: Die Cyberhaftpflicht deckt auch verschuldensunabhängige Tatbestände mit ab.

CYBERABSICHERUNG IST CHEFSACHE

Zusammenfassend lässt sich festhalten: Eine aktive Cyberprävention, die kontinuierliche Entwicklung der Cyber-Mitarbeiter-Resilienz, aktuelle und kontinuierlich fortgeschriebene Notfallpläne und eine funktionierende 24/7 Cyber Task Force sind absolut notwendige Absicherungsinstrumente beim Cyber-Risikomanagement. All diese Instrumente können über eine entsprechende Versicherung zielgerichtet abgedeckt werden. Und am Ende gilt: Cyberabsicherung ist und bleibt Chefsache! ■

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

Grafik: BSI