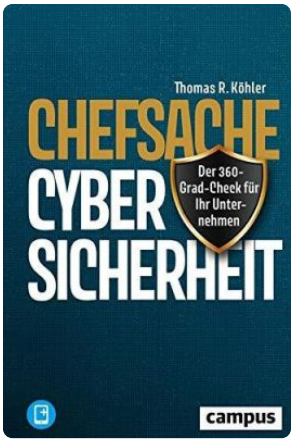
getabstract
compressed knowledge



Bewertung 9

Qualitäten
Umsetzbar
Augenöffner
Brisant

Buch oder Hörbuch kaufen

Chefsache Cybersicherheit

Der 360-Grad-Check für Ihr Unternehmen

Thomas R. Köhler • Campus © 2021 • 256 Seiten

Management / Risikomanagement / IT-Sicherheit

Take-aways

- Obwohl Cyberattacken eine große Bedrohung darstellen, nehmen viele Unternehmen das Risiko nicht ernst genug.
- Durch Cyberattacken können Schäden in zwei- bis dreistelliger Millionenhöhe entstehen.
- Bei Erpressung per Ransomware sollten Sie nicht auf Lösegeldforderungen eingehen.
- Sichern Sie Ihre Daten regelmäßig offline, segmentieren Sie Ihre IT-Systeme und sensibilisieren Sie Ihre Mitarbeiter für Risiken.
- Wenn Sie einen Angriff bemerken, schalten Sie Ihr Gerät sofort aus.
- Arbeiten Sie einen Notfallplan aus und bereiten Sie alternative Kommunikationswege vor.
- Schließen Sie auch Einfallstore wie ungesicherte Netzwerkdrucker oder vernetzte Produktionsgeräte.
- Kein Unternehmen ist zu klein, um für Cyberkriminelle interessant zu sein.
- Sie können Cyberattacken nicht verhindern, aber die Risiken minimieren.

Rezension

Nicht erst seit den jüngsten Ransomware-Attacken auf US-Unternehmen wissen wir: Cyberkriminalität ist ein enormes Risiko für Firmen aller Größen. Die Schäden liegen teils in dreistelliger Millionenhöhe. Anschaulich schildert der Autor, auf welchen Wegen Hacker in Firmennetzwerke eindringen, dort ihr Unwesen treiben und Daten klauen oder verschlüsseln. Er erklärt Schwachstellen und zeigt, wie Unternehmen sich schützen können. Ein höchst nützlicher Ratgeber, randvoll mit praktischen Tipps.

Zusammenfassung

Obwohl Cyberattacken eine große Bedrohung darstellen, nehmen viele Unternehmen das Risiko nicht ernst genug.

Cyberattacken auf Unternehmen und andere Organisationen verursachen hohe, teils existenzgefährdende Schäden. Allein für Deutschland werden die Kosten auf 100 Milliarden Euro jährlich geschätzt – etwa durch Datendiebstahl, Wirtschafts- und Industriespionage, Erpressung oder Sabotage. Im schlimmsten Fall kommen zum eigentlichen Schaden noch Strafzahlungen und behördliche Sanktionen wegen Verstößen gegen die Datenschutzgrundverordnung DSGVO hinzu.

> *„Wichtig ist, dass Sie Cybersicherheit als Marathon sehen und nicht als Sprint."*

Dennoch werden Cyberrisiken oft auf die leichte Schulter genommen. Entscheider in Unternehmen rechtfertigen ihre Sorglosigkeit unter anderem damit, dass man ja versichert sei, dass man sich später um Sicherheitslücken kümmern werde, dass man ja bereits vollständig geschützt sei und ja sowieso noch nie angegriffen wurde und dass das eigene Unternehmen doch gar nicht groß genug sei, um Cyberangriffe lohnenswert erscheinen zu lassen. Doch Versicherungen ziehen sich gern aus der Affäre. Es gibt auch keinen hundertprozentigen Schutz vor Hackerangriffen. Und selbst kleine Unternehmen können das Ziel von Attacken sein. Darüber hinaus hilft es nicht, auf die IT-Abteilung zu verweisen. Letztlich liegt die Verantwortung bei der Geschäftsleitung. Aktiengesetz und GmbH-Gesetz nennen bestimmte Grundpflichten wie Sorgfaltspflicht, Legalitätspflicht und Pflicht zur Einrichtung von Überwachungssystemen, die auch für die Cybersicherheit gelten.

Durch Cyberattacken können Schäden in zwei- bis dreistelliger Millionenhöhe entstehen.

Viele der wichtigsten Cyberrisiken gibt es schon seit Jahrzehnten. Viren, Würmer oder Trojaner, zusammenfassend Malware genannt, sowie Betrugsmaschen aller Art können erhebliche Schäden anrichten. Phishing-Mails enthalten Anhänge oder Links, die zu Schadprogrammen führen, die ihrerseits Zugangsdaten ausspähen, Dokumente stehlen oder Dateien verschlüsseln. Ransomware ist aktuell eine besonders gefährliche Bedrohung für Firmen. Dabei verschlüsseln die Täter Daten auf dem angegriffenen IT-System und geben sie nur nach Zahlung von Lösegeld wieder frei. Auf diese Weise erpressten Cyberkriminelle 2019 rund 11,5 Milliarden Dollar. Den Unternehmen entstanden aber darüber hinaus noch weit höhere Kosten.

„Rein wirtschaftlich gesehen ist Ransomware die größte Bedrohung für mittelständische Unternehmen."

Mit Wucht traf es 2017 das Logistikunternehmen Maersk: Über ein Update der Buchhaltungssoftware in einer ukrainischen Filiale gelangte Schadsoftware ins IT-System des Unternehmens, legte nahezu alle Aktivitäten mehrere Tage lang lahm und verursachte einen Schaden von rund 300 Millionen Dollar. Beim Automatisierungsunternehmen Pilz in Ostfildern konnte nach einer Ransomware-Attacke die Produktion erst nach rund drei Wochen wieder anfahren und brauchte rund sechs Wochen, bis sie wieder planmäßig lief. Der Schweizer Fensterhersteller Swisswindows mit 170 Beschäftigten konnte den Betrieb nach einem solchen Angriff nicht mehr aufnehmen und ging pleite.

Bei Erpressung per Ransomware sollten Sie nicht auf Lösegeldforderungen eingehen.

Eingeschleust wird Ransomware über E-Mails oder Sicherheitslücken. Die Angreifer können dann Datenbestände aller Art stehlen – von Aufträgen über Kundenlisten bis hin zu Konstruktionsplänen –, sie manipulieren und anschließend verschlüsseln. Dann fordern sie Geld für die Entschlüsselung der Daten – verbunden vielleicht mit der Drohung, das Lösegeld bei Verzögerungen zu erhöhen und sensible Daten bei Nichtzahlung zu veröffentlichen. Bei Vastaamo, einer psychotherapeutischen Einrichtung in Finnland, entwendeten Hacker 40 000 Patientenakten. Als sich das Unternehmen den Forderungen der Täter widersetzte, stellten sie zunächst Akten ins Internet und erpressten dann betroffene Patienten.

„Dem Großteil der Cyberkriminellen ist völlig egal, was Sie machen. Die meisten sehen die Schwächen in Ihrer IT-Infrastruktur und Ihrer Cyberabwehr als eine willkommene Gelegenheit, um Geld zu verdienen."

Oft fordern die Täter Lösegeld in Millionenhöhe. 2019 zahlte jedes dritte erpresste Unternehmen. Von diesen erhielt ungefähr jedes fünfte dennoch keinen Zugriff auf die Daten – viele wurden sogar mit weiteren Forderungen konfrontiert. Daher rät das Bundesamt für Sicherheit in der Informationstechnik (BSI), nicht zu zahlen. In den USA raten Analysten pragmatisch, zu zahlen und das Lösegeld als Betriebsausgabe anzugeben. Dies freilich stärkt die Position der Gangster und garantiert – wie gesehen – keineswegs die Freigabe der Daten.

Sichern Sie Ihre Daten regelmäßig offline, segmentieren Sie Ihre IT-Systeme und sensibilisieren Sie Ihre Mitarbeiter für Risiken.

Die Website nomoreransom.org der niederländischen Polizei bietet gratis Entschlüsselungssoftware zum Download an, mit der Unternehmen in vielen Fällen ihre Daten selbst wieder entschlüsseln können. Doch sollten Sie unbedingt Vorkehrungen treffen, damit es gar nicht erst zum Ernstfall kommt. Beachten Sie dazu folgende Tipps:

- Sichern Sie Daten regelmäßig offline.
- Kritische Datenbestände sollten Sie zusätzlich extern oder in der Cloud sichern. Diese Kopien sollten nicht aus dem Live-System heraus modifiziert werden können.

- Unterlagen der höchsten Wichtigkeitsstufe, Ihre „Kronjuwelen“ also, sollten Sie auf einem Computer speichern, der physisch von allen Netzwerken isoliert ist.
- Inventarisieren Sie Ihre Hardware – also sämtliche Systeme, Rechner, Server, vernetzte Geräte sowie alle Verbindungen.
- Katalogisieren Sie alle Softwaresysteme, Updates und Patches und halten Sie Ihre Software stets auf dem aktuellsten Stand.
- Nutzen Sie aktuelle Anti-Viren- und Anti-Schadsoftware-Technologien, Festplattenverschlüsselung und anspruchsvollen Passwortschutz.
- Beschränken Sie Benutzer- und Administratorenrechte nach dem „Need-to-know“-Prinzip auf das Nötigste. Gewähren Sie also jedem Mitarbeiter nur die Rechte, die er zur Erledigung seiner Aufgaben braucht.
- Allgemein gilt das „Zero Trust“-Prinzip: Kein Gerät, Nutzer oder Dienst innerhalb oder außerhalb des eigenen Systems ist vertrauenswürdig.
- Gestatten Sie keine privaten Geräte der Mitarbeiter in Ihrem Netz.
- Segmentieren Sie Ihre Netze in unabhängige Teilzonen, damit bei Angriffen nicht das gesamte Unternehmen betroffen ist.
- Trennen Sie IT- von Produktionstechnologien strikt, damit Hacker nicht über ein Netzsegment ins andere gelangen.
- Schaffen Sie einheitliche, gut abgesicherte Remote-Zugänge für Mitarbeiter im Homeoffice.
- Meiden Sie öffentliche WLAN-Netzwerke. Bieten Sie Ihren Mitarbeitern fürs mobile Arbeiten LTE- bzw. 5G-Zugänge.
- Wenn Sie im Unternehmen einen Gast-Internetzugang anbieten wollen, richten Sie diesen technisch komplett getrennt von Ihrem eigenen Netzwerk ein.
- An Cyberattacken sind oft Insider beteiligt. Achten Sie daher bei Mitarbeitern auf verdächtiges Verhalten.
- Überwachen Sie Ihr gesamtes System ständig im Hinblick auf Anomalien – etwa ungewöhnliche Datenströme.
- Nutzen Sie bei Anmeldungen die Zwei-Faktor-Authentifizierung.
- Sensibilisieren Sie Ihre Mitarbeiter für Cyberrisiken und führen Sie regelmäßig Schulungen durch.
- Sorgen Sie dafür, dass Anlagen und Links in nicht erwarteten Mails nie angeklickt werden.

Wenn Sie einen Angriff bemerken, schalten Sie Ihr Gerät sofort aus.

Als größte Bedrohung nennt das BSI Schadsoftware, die über externe Datenträger sowie über Internet oder Intranet das eigene Netzwerk befällt. Die nächstgrößte Gefahr ist menschliches Fehlverhalten oder Sabotage – mit stark steigender Tendenz. Angreifer können sich zudem über die Cloud, über per Internet erreichbare Steuerungskomponenten, Fernwartungszugänge und Smartphones Zugang verschaffen.

Wie aber sollten Sie reagieren, wenn es zu einer Attacke kommt? Erscheint auf Ihrem Bildschirm die Meldung „Oops, your files have been encrypted!“, ist es schon zu spät. Doch wahrscheinlich haben sich die Angreifer schon vorher in Ihrem System zu schaffen gemacht. Wenn Sie Anzeichen dafür erkennen, etwa weil einzelne Dateien plötzlich grundlos verschlüsselt sind oder Ihr Mauszeiger sich wie von Geisterhand bewegt, können Sie durch sofortiges Handeln Schlimmeres verhindern. Schalten Sie Ihr Gerät „hart“ aus,

ziehen Sie also Strom- und LAN-Stecker. Bei einem Laptop halten Sie den Aus-Schalter lange gedrückt. Bei Smartphone und Tablet schalten Sie Funkschnittstelle, WLAN und dann das Gerät aus. Trennen Sie eiligst die Verbindung zum Internet. So stoppen Sie die Ausbreitung der Malware. Informieren Sie umgehend Ihre IT-Abteilung.

Arbeiten Sie einen Notfallplan aus und bereiten Sie alternative Kommunikationswege vor.

Bereiten Sie sich auf einen GAU vor, um im Ernstfall planvoll und souverän zu agieren. Bedenken Sie, dass mit Ihren IT-Systemen auch Ihre Telefonanlage betroffen sein wird. Richten Sie also vorsorglich ein technisch unabhängiges Kommunikationszentrum ein, beispielsweise bei Ihrer PR-Agentur. Sorgen Sie dafür, dass Ihre Rufnummer binnen Minuten dorthin umgeschaltet werden kann. Halten Sie eine Schattenwebsite für die Kommunikation mit der Öffentlichkeit bereit, die Sie im Störfall aktivieren können.

> *„Bei Investitionen in Cybersicherheit geht es vor allem um die Vermeidung von Verlusten durch die Begrenzung von Risiken."*

Fahren Sie bei einem Vorfall unverzüglich alle erreichbaren Systeme herunter und trennen Sie sie vom Netz. Leiten Sie dann folgende Maßnahmen ein:

- Bilden Sie einen Krisenstab aus eigenen und externen Cybersecurity-Spezialisten. Die Externen sollten Ihre Systeme kennen. So sparen Sie im Ernstfall wertvolle Zeit. Der Krisenstab legt das weitere Vorgehen fest.
- Schalten Sie die Ermittlungsbehörden ein. Zentrale Anlaufstellen gibt es für Deutschland beim jeweiligen Landeskriminalamt. In Österreich gibt es eine Cyber-Security-Hotline bei den Wirtschaftskammern. Die Schweiz hat kantonale Regelungen.
- Informieren Sie Ihre wichtigsten Kunden und Geschäftspartner über die Situation und über etwaige Ausfälle.
- Prüfen Sie Meldepflichten, die etwa für bestimmte Branchen oder ab einer gewissen Unternehmensgröße bestehen.
- Nutzen Sie weitere Informationsquellen und Hilfsangebote der Sicherheitsbehörden und Wirtschaftsverbände.

Schließen Sie auch Einfallstore wie ungesicherte Netzwerkdrucker oder vernetzte Produktionsgeräte.

Trotz aller Bemühungen um Cybersicherheit lauern vielerorts Risiken und Lücken. Machen Sie sich diese bewusst, denn sie sind für Kriminelle Einfallstore zu Ihren IT-Systemen und Datenbeständen:

- Einen größeren Komplex stellt das Internet der Dinge dar, oft auch IoT genannt. Die meisten IoT-Geräte sind ungesichert und nahezu der gesamte Informationsaustausch zwischen diesen Geräten ist unverschlüsselt. Ein einziger unsicherer Wartungszugang kann für einen Angriff ausreichen.
- Netzwerkdrucker verfügen oft über große Datenspeicher für zu druckende Dokumente. Ein Krimineller, der sich als Wartungstechniker ausgibt, kann mit Leichtigkeit alle dort abgelegten Dateien klauen.

- Smartphone-Ladekabel sind zugleich Datenkabel. Öffentlich zugängliche Ladestationen – etwa auf Flughäfen oder in Hotels – können manipuliert sein, sodass vertrauliche Daten von angeschlossenen Geräten abgegriffen werden können.
- Seien Sie vorsichtig, wenn ein Fremder etwa auf einer Konferenz bittet, sein Smartphone per USB an Ihrem Laptop aufladen zu dürfen. Auf diesem Weg könnte er Ihre Daten stehlen.
- Nicht nur die Inhalte von Gesprächen und Mails können für Konkurrenten, Terroristen und Geheimdienste wertvoll sein, sondern auch Metadaten. Aus Bewegungs- oder Kommunikationsdaten lässt sich etwa auf geheime Vorhaben wie Übernahmegespräche schließen. Selbst anonymisierte Datensätze lassen sich anhand weniger konkreter Informationen de-anonymisieren.
- Über online erreichbare Haustechniksteuerung können Angreifer nicht nur Zugangskontrollen, Schließsysteme, Klimatisierung, Fahrstühle und andere Anlagen manipulieren, sondern teils auch ins unternehmenseigene Datennetz vordringen.

Kein Unternehmen ist zu klein, um für Cyberkriminelle interessant zu sein.

Cyberkriminelle kennen kein Pardon. Skrupellos nutzen sie jede Gelegenheit, um sich zu bereichern. Unternehmen können sich noch so viel Mühe mit der Absicherung ihrer Systeme geben – ein einziger Konfigurationsfehler, ein falsch definierter Zugang, ein fehlendes Update genügt.

> *„Technisch versierte Angreifer müssen nur eine einzige ausnutzbare Lücke oder eine passende Kombination von Lücken in den Verteidigungslinien Ihres Unternehmens finden und hinreichend Energie aufbringen, um diese aktiv auszunutzen.“*

Die Täter greifen nicht nur große Unternehmen an, sondern auch kleine und mittelständische. Clearaudio in Erlangen etwa baut High-End-Plattenspieler. Die Firma mit weniger als 50 Mitarbeitern hatte ein hochwertiges Lager für Plattenteller entwickelt und patentieren lassen. Dieses Lager wurde wundersamerweise 2011 auf einer Messe fast zeitgleich von einem chinesischen Hersteller angeboten.

Sie können Cyberattacken nicht verhindern, aber die Risiken minimieren.

Nach einer Umfrage von 2017 wird Industriespionage – mit 38,3 Prozent der Nennungen – von Unternehmensverantwortlichen als zweitgrößte Gefahr für die Sicherheit im Unternehmen gesehen. Als größtes Risiko wurden mit 39,3 Prozent die Mitarbeiter genannt. Dagegen meint der IT-Leiter eines süddeutschen Automobilzulieferers: „Wir haben hier nur ein Sicherheitsrisiko – und das ist der Chef“. Der mache sich um Cybersicherheit keine Gedanken und handelt selbst sorglos bis fahrlässig. Dabei ist Cybersicherheit grundsätzlich Chefsache.

> *„Mit Ihrem Wissen über die Methoden der Cyberkriminellen und Möglichkeiten zur Verbesserung Ihrer Cybersicherheit können Sie in Zukunft Ihr Bestes dafür tun, so lange wie möglich kein leichtes Ziel für Hacker zu sein.“*

Völlig gegen Cyberrisiken absichern können Sie Ihr Unternehmen nicht. Aber Sie können viel dafür tun, um Risiken zu minimieren und nach einem Angriff schnell wieder zum Alltag zurückzukehren. Eine gute Orientierung bietet das kostenlos abrufbare *IT-Grundschutz-Kompendium* des BSI.

Über den Autor

Thomas R. Köhler ist Geschäftsführer von CE21, einem Beratungsunternehmen mit Schwerpunkt Cybersicherheit. Zudem lehrt er am Center for International Innovation der Hankou University in China.