CYBERCRIME

Risikogruppe deutscher Mittelstand

Gefahren erkennen · Maßnahmen planen · Schutz sicherstellen

FINANZ CHEF 24
UNTERNEHMER? ABER SICHER!

Sind Sie sicher?

Im Jahr 2017 legte der Cyberangriff WannaCry hunderttausende Computer in mehr als 100 Ländern lahm. Opfer waren unter anderem Krankenhäuser, Autohersteller, Schulen und Verkehrsbetriebe. Damit ist WannaCry einer der schwersten Cyberangriffe der vergangenen Jahre – doch bei weitem nicht der einzige. Die Liste an Firmen und Institutionen, die bereits Opfer dieses und weiterer Angriffe wurden, lässt sich endlos weiterführen: AOL, Sony, die Deutsche Bahn sowie die Deutsche Telekom, LinkedIn, Uber, British Airways und auch das FBI. Allein im deutschen Wirtschaftssektor entstehen durch Cyberattacken jährlich Schäden in Höhe von 50 Milliarden Euro. (Quelle: Bitkom)

Das Thema hat folglich Brisanz. Und: es betrifft alle Länder, alle Branchen, alle Unternehmensgrößen. Doch gerade für kleine und mittlere Unternehmen (KMUs) ist Cybersicherheit von besonderer Bedeutung, da die finanziellen Schäden, die ein Hackerangriff mit sich bringt, für sie oft existenzbedrohend sind. Dennoch sind KMUs immer noch nicht ausreichend gegen die Gefahr aus dem Netz gewappnet.

Dieses E-Book soll Ihnen dabei helfen. Sie erhalten einen Überblick über die verschiedenen Gefahren sowie praxisnahe Tipps, wie Sie Ihr Unternehmen vor Cybercrime schützen.

Inhaltsverzeichnis

1. Risikogruppe: kleine und mittlere Betriebe

Wer davon ausgeht, dass es nur die Großen „erwischt“, der irrt. In Deutschland wurde in den letzten zwei Jahren jedes zweite kleinere Unternehmen (bis zu 100 Mitarbeiter) Opfer einer Cyberattacke (Quelle: Bitkom).

Laut Forsa-Umfrage 2018 (Quelle: GDV):

- erlitten **30 Prozent der KMUs** wirtschaftliche Schäden durch Cyberattacken, 11 Prozent davon mehrfach.
- mussten **43 Prozent der KMUs** in Folge eines Angriffs ihren Betrieb zeitweise stilllegen.

Gerade dieses Risiko kann für ein kleineres Unternehmen existenzbedrohend sein. Denn ein Cyberschaden verursacht durchschnittlich 55.000 Euro. Folgenschwer ist daher die verbreitete Annahme:

„Ich bin ein kleiner Betrieb. Was sollen Hacker von mir wollen?!“

Denn: Ein Hackerangriff wird selten gezielt ausgeführt. Gerade im Fall von infizierten E-Mails werden diese randomisiert – also zufällig verschickt. Ein Klick genügt und der Schaden ist passiert. Deshalb ist JEDER Betrieb, der in irgendeiner Form das Internet nutzt ein potenzielles Ziel. Das Gleiche gilt für Freiberufler / Freelancer.

Beispiele betroffener KMUs

- **Restaurant Auerbachs Keller**
  Hacker knackten das Kassensystem und spionierten monatelang die Kreditkartendaten von Gästen aus. Mit den Daten tätigten Sie Einkäufe im Ausland. (Quelle: LVZ)

- **Bäckerei Hesse**
  Durch einen Hackerangriff wurde die Verwaltung stundenlang lahm gelegt. Dadurch konnte auf Kundenbestellungen von 54 Filialen nicht zugegriffen werden. Alle Bestellungen mussten telefonisch erfragt werden. (Quelle: WP)

- **Hotelbuchungsseite FastBooking**
  Hier wurde Datenklau im großen Stil betrieben und Kundendaten im 6-stelligen Bereich abgezogen. (Quelle: Heise)

Diese drei Beispiele aus der Praxis zeigen, dass es **jedes Unternehmen** treffen kann, und dass der richtige/bewusste Umgang mit

Cyberrisiken heute ein unverzichtbarer Bestandteil Ihrer selbstständigen Tätigkeit sein muss.

2. Die größten Cyber-Risiken für KMUs

Häufig sind es alltägliche Dinge, die aufgrund mangelnder Sensibilität für das Thema Cybersicherheit zu einem Schaden führen. Ganz oben auf der Liste: das Öffnen einer E-Mail.

Rund zwei Drittel aller Cyberschäden werden durch infizierte E-Mail-Anhänge, sogenannte Phishing-Mails, verursacht. (Quelle: GDV) Einmal unbedacht auf einen Link geklickt oder einen Anhang geöffnet und schon verbreitet sich die Schadsoftware auf Ihrem Server wie ein Lauffeuer. Fake-E-Mails werden z. B. häufig als sehr professionell imitierte Nachrichten von Amazon, eBay, Paypal oder anderen bekannten Online-Shops, bei denen so gut wie jeder ein Kundenkonto hat, versendet. Aber auch vermeintliche Bewerbungen auf aktuelle Stellenanzeigen werden immer beliebter als Tool für Cyberkriminelle.

2.1. E-Mails

Fake-E-Mails zu identifizieren ist gar nicht so leicht. Die Betrüger versenden inzwischen sehr gute Kopien und sind vom Original kaum mehr zu unterscheiden. Wenn Sie jedoch folgende Hinweise beachten, können Sie den Betrugsversuch als solchen entlarven.

- **Werden Sie aufgefordert,** auf einen Link zu klicken, ist das bereits der erste Hinweis darauf, dass es sich nicht um eine echte E-Mail einer serösen Institution handelt. Klicken Sie auf keinen Fall, sondern fahren Sie stattdessen mit dem Mauszeiger über den Link. So wird die URL angezeigt. Stimmt diese nicht mit der in der E-Mail angegebenen Linkadresse überein oder beinhaltet sie merkwürdige Zahlen- und Buchstabenkombinationen, handelt es sich um einen Betrugsversuch.

! Schauen Sie genau hin. Manchmal weicht die Adresse auch nur um einen Buchstaben ab (z. B. Amzon statt Amazon).

- **Dringende Handlungsaufforderungen** in einer E-Mail sprechen ebenfalls dafür, dass es sich um eine gefälschte, sprich Fake-E-Mail handelt. Im Zweifel kontaktieren Sie den Absender (z. B. Amazon, Ihre Bank etc.) direkt und fragen Sie nach, ob die E-Mail wirklich von diesem stammt. Generell können Sie davon ausgehen, dass seriöse Institutionen niemals nach persönlichen Daten oder Logins per E-Mail fragen.

> ! Antworten Sie nie auf verdächtige E-Mails! Sonst erkennen die Betrüger, dass sie mit Ihrem Phishing-Versuch an eine reale E-Mail-Adresse geraten sind.

- **Klicken Sie niemals auf einen Anhang**, insbesondere bei Dateien mit Endungen wie .exe, .com, .sys oder .reg. Hierbei handelt es sich um Programmdateien. Einmal geklickt, beginnen diese sofort zu arbeiten – in der Regel, um einen Virus zu installieren.

- **Ziehen Sie einen IT-Experten zu Rate,** wenn Sie immer noch unsicher sind. Dieser kann den Header der E-Mail auslesen und anhand der hinterlegten IP-Adresse herausfinden, ob es sich um einen Betrugsversuch handelt.

2.2. Weitere Gefahren

- Übertragung eines Virus / Trojaners über einen externen Datenträger (z. B: USB-Stick)

- (ehemalige) Mitarbeiter, die z. B. einen Virus implementieren und die Dateninfrastruktur lahmlegen
- Hackerangriffe, z. B. DDoS-Attacken

Exkurs: Was ist eine DDoS-Attacke?

Bei einer „Distributed-Denial-of-Service“-Attacke (DDoS) wird die Nichtverfügbarkeit eines Dienstes oder Servers gezielt herbeigeführt. Der Angreifer infiziert einen oder mehrere Rechner mit Schadsoftware, die die Server überlastet und die Leistung der Internetverbindung stark verringert. Die Folge: Ihre Webseiten bauen sich nur noch ganz langsam auf oder lassen sich überhaupt nicht mehr aufrufen.

Aus der Praxis: Fremdgesteuerte Arbeitsmaschinen

Unternehmen im (Bau-)Handwerk, die mit funkgesteuerten Maschinen wie Kränen, Bohrern oder anderen Industriegeräten arbeiten, stellen ein potenzielles und leicht angreifbares Ziel für Hacker dar. Denn laut eine Studie der Sicherheitsfirma Trend Micro können Funksteuerungen leicht gehackt und damit sämtliche Arbeitsmaschinen willkürlich ferngesteuert werden.

Die resultierenden Risiken sind vielfältig und reichen von Betriebsunterbrechungen bis hin zu Gefahr für die Sicherheit von Mitarbeitern, Kunden und Passanten.

3. Teure Schäden durch Cyberangriffe

Die Schäden infolge einer Cyberattacke sind meist finanzieller Natur. Aber auch der Ruf Ihres Unternehmens kann stark leiden. Zu den am häufigsten auftretenden wirtschaftlichen Schäden, die durch einen Cyberangriff verursacht werden, zählen (Quelle: GDV):

- Aufklärungskosten (IT-Forensik) und Datenwiederherstellung
- Betriebsunterbrechung und damit einhergehende Umsatzeinbußen, z. B. aufgrund von Produktionsstillstand (gehackte Arbeitsmaschinen) oder Ausfall des IT-System
- Reputationsschäden (z. B. durch Shitstorm nach einer Attacke)
- Datendiebstahl (Kommunikationsdaten wie E-Mail, Kundendaten, vertrauliche Unternehmensdaten etc.)

So teuer kann ein Cyberschaden werden

Das Ausmaß des finanziellen Schadens, den ein Cyberangriff verursachen kann, zeigt Ihnen folgendes Beispiel: Sie betreiben einen Online-Shop. Eine DDoS-Attacke legt Ihre gesamte Website lahm. Dadurch können Ihre Kunden vier Tage lang nicht auf Ihren Shop zugreifen. Die Folge:

- Umsatzeinbußen
- Kosten für IT-Forensik (Untersuchung betroffener Systeme)
- Wiederherstellung der Systeme (u. a. Website)

Die verursachten Gesamtkosten belaufen sich auf 141.500 Euro.

Die weiteren Schadensbeispiele verdeutlichen, dass ein Cyberangriff jeden Unternehmer treffen kann:

- **Arztpraxis**
  Hacker stehlen sensible Patientendaten und veröffentlichen sie im Netz. Ihnen entstehen hohe Kosten für die Datenwiederherstellung sowie die Benachrichtigung der Patienten. Ferner haben Sie mit einem Reputationsschaden zu kämpfen.

  Kfz-Werkstatt
  Beim Öffnen des E-Mail-Anhangs eines vermeintlichen Bewerbers installiert sich ein Trojaner auf dem PC Ihres Betriebs und zerstört alle Daten. Sie können weder auf Bestellungen noch auf anstehende Auftragsdaten zugreifen. Bis das System wiederhergestellt ist, müssen Sie den Betrieb einstellen.

- **Garni-Hotel**
  Hacker gelangen über die Buchungswebsite Ihres Hotels an die Kreditkartendaten Ihrer Kunden. Zudem legen sie Ihre Website lahm – über Stunden können Ihre Kunden keine Buchungen online durchführen.

4. Vorsorge ist besser als Nachsorge

Um Ihren Betrieb gegen Cyberrisiken so gut wie möglich abzusichern, ist es unerlässlich, dass Sie sich und Ihre Mitarbeiter für das Thema Cybersecurity sensibilisieren.

Es muss ihnen in Fleisch und Blut übergehen, dass es sich dabei nicht um ein realitätsfremdes Problem handelt, sondern eine reelle Gefahr für Ihr Unternehmen darstellt. Nur wenn diese Sensibilisierung stattfindet, machen konkrete Maßnahmen zur Steigerung der Cybersecurity Ihrer Firma Sinn. Denn das beste Konzept nützt nichts, wenn sich niemand daran hält.

Ihr Bestreben sollte es sein, das Sicherheitsverständnis aller Mitarbeiter zu schulen (intern oder durch einen externen IT-Dienstleister) und beispielsweise darauf aufmerksam zu machen, dass eine E-Mail in der Regel kein sicheres Kommunikationsmedium ist und Schadsoftware durch private Datenträger wie USB-Sticks oder Smartphones auf die Unternehmenssysteme geraten kann.

Mit diesen 5 Tipps machen Sie Ihr Unternehmen sicherer

1. Firewall aktivieren und Virenscanner installieren

Ihren Firmenserver sollten Sie in jedem Fall mit einer Firewall schützen. Diese dient dazu, Angriffe aus dem Netz abzuwehren. Daneben ist es zwingend erforderlich, dass Ihre Firmen-PCs mit einem guten Antivirenprogramm zur Virenerkennung ausgestattet sind. Anbieter für Business-Lösungen sind beispielsweise Bitdefender, McAfee und Panda.

! Die Programme müssen regelmäßig geupdated werden, um fehlerfrei zu funktionieren. Grundsätzlich aktualisieren sie sich automatisch – unterbrechen Sie ein solches Update niemals, denn dadurch kann

Eine Sicherheitslücke entstehen, die Hacker gerne und schnell ausnutzen.

2. Sichere Passwörter erstellen und mittels Passwortmanager verwalten

Ob es um den Zugriff auf den eigenen PC, auf das E-Mail-Postfach oder andere webbasierte Anwendungen geht: Passwörter sind ein Muss! Denn nur mit ihnen können Sie vertrauliche Inhalte vor Angreifern schützen. Doch dazu müssen die Passwörter, die Sie verwenden, sicher sein. Und auch der Umgang mit diesen ist essenziell für Ihre IT-Sicherheit. Beachten Sie folgende Dinge beim Erstellen und Verwalten von Passwörtern und verwenden Sie:

- 12 Zeichen oder mehr
- keine einfachen Wörter oder Zahlenreihen
- keine Begriffe aus dem Wörterbuch
- kein Passwort mehr als einmal

Nutzen Sie einen Passwortmanager

Komplexe und lange Passwörter lassen sich schwer merken. Dennoch sollten Sie diese auf keinen Fall notieren oder auf Ihrem PC ungeschützt abspeichern. Verwenden Sie stattdessen einen Passwortmanager, wie z. B. KeePass. Dabei handelt es sich um ein sicheres Programm auf Ihrem Computer, in dem Sie unter anderem die Login-Daten Ihrer verschiedenen Anwendungen lokal speichern und verwalten können. Sie können den integrierten Passwortgenerator auch dazu verwenden, um sichere Passwörter zu erstellen. Die

Gesamtdatei wird dann schließlich mit einem Masterpasswort geschützt. So müssen Sie sich anstatt dutzender Passwörter nur eins merken.

3. Zugriffsmanagement innerhalb des Betriebs regeln

Es ist nicht sinnvoll, wenn jeder Ihrer Mitarbeiter Zugriff auf sämtliche Anwendungen und den entsprechenden Zugangsdaten hat. Je mehr Personen die Daten kennen, desto höher ist das Risiko einer Sicherheitslücke. Jeder Mitarbeiter sollte nur Zugriff auf jene Daten und Anwendungen erhalten, die er auch wirklich zum Arbeiten benötigt. Darüber hinaus sollte jeder **eigene Zugangsdaten** zugewiesen bekommen. Nur so lassen sich Aktivitäten ausreichend nachvollziehen (z. B. Löschung bestimmter Daten etc.)

Wenn möglich, stellen Sie einen IT-Sicherheitsbeauftragten ein bzw. ernennen Sie einen Ihrer IT-Mitarbeiter, der regelmäßig Kontrollen zur IT-Sicherheit durchführt und die diversen Accounts und Zugriffs-berechtigungen verwaltet.

4. Software-Updates regelmäßig durchführen

Ein verpasstes Update kann eine Sicherheitslücke im System bedeuten. Das macht Sie und Ihr Unternehmen für Hacker und Viren leicht angreifbar. Erstellen Sie (oder Ihr IT-Mitarbeiter) eine Liste all Ihrer Anwendungen und dokumentieren Sie die Updates. In der Regel führen die Programme ihre Updates selbstständig im Hintergrund aus. Sie müssen Sie also lediglich autorisieren.

Updates können unter Umständen ein Sicherheitsrisiko darstellen. Wenn es sich bei einem Programm um kritische Software handelt, sollte das Update zunächst auf einem Testsystem durchgeführt werden.

5. Für eine konsequente Datensicherung sorgen

Laut Bundesministerium für Wirtschaft und Energie führen gut ein Viertel der kleinen und mittleren Unternehmen keine regelmäßige Datensicherung durch. Dabei sind gesicherte Unternehmensdaten das A und O, sollten Sie einmal ins Visier eines Hackerangriffs geraten. Nach einem Hackerangriff können die verlorenen Daten häufig nicht wieder hergestellt werden, was im Umkehrschluss einen herben finanziellen Verlust für Sie bedeuten kann. Ein Backup ist hier Ihre Rettung. Das sollten Sie jedoch bei der Datensicherung beachten:

- **Nutzen Sie Datenträger,** die nicht an Ihre IT-Infrastruktur gekoppelt sind. Am besten werden diese auch nicht in Ihrem Betrieb gelagert. Denn Diebstahl, Feuer oder Leitungswasser können Ihre Elektronik beschädigen.
- **Vertrauliche Daten** sollten Sie außerdem an einem verschließbaren Ort, etwa in einem Safe, aufbewahren. Benennen Sie einen Mitarbeiter, der für die Datensicherung verantwortlich ist. Halten Sie den Sicherungsprozess schriftlich fest, damit mögliche Probleme nachvollzogen werden können.

Wie eingangs erwähnt, sind insbesondere E-Mails der größte Risikofaktor für Cyberschäden. Verwenden Sie deshalb Verschlüsselungsmechanismen und digitale Signaturen – sowohl für die interne als auch die externe E-Mail-Kommunikation.

5. Erkennen von Cyber-attacken

Trotz aller Sicherheitsvorkehrungen kann es dennoch jederzeit zu einer Cyberattacke kommen. Deshalb ist es zum einen wichtig, die Attacke frühzeitig zu erkennen. Zum anderen ist ein Notfallplan ratsam, um im Schadensfall richtig reagieren zu können. Dieser gibt genau vor, was zu tun ist und wie die

Zuständigkeiten geregelt sind. Bei folgenden Szenarien kann es sich um einen Cyberangriff handeln:

- Nach dem Öffnen einer E-Mail ist der PC langsamer oder gar nicht mehr nutzbar.
- Passwörter funktionieren nicht mehr.
- Der Zugriff auf ein Konto wird verweigert.
- Eine unbekannte Fehlermeldung erscheint kurz auf dem Bildschirm und verschwindet dann wieder.
- Ungewöhnliche Login-Aktivitäten werden verzeichnet.
- Auffälligkeiten bei Systemanwendungen, z. B. große Mengen an Systemressourcen werden beansprucht.
- Eine Schadsoftware wird von Ihrem Virenscanner erkannt.
- Innerhalb kürzester Zeit werden große Datenmengen von unterschiedlichen Absendern an Ihr System versendet.

! Stellen Sie einen Administrator für Ihren IT-Bereich ein, der entsprechend geschult ist. Häufig laufen Cyberangriffe im Hintergrund ab. Ungeschulte Mitarbeiter können diese kaum erkennen. Haben Sie keine eigene IT-Abteilung, engagieren Sie einen externen IT-Berater, der Ihr System regelmäßig überprüft.

6. Erstellen eines Notfallplans

Der Notfallplan muss individuell auf Ihren Betrieb zugeschnitten sein. Dafür sollten Sie vorab folgende Fragen beantworten:

- Welche Auswirkungen hat der Ausfall meines IT-Systems?
- Welche Ausfallzeiten verkraftet der Betrieb?
- Was muss ich/muss mein IT-Verantwortlicher tun, um die Funktion der Systeme wiederherzustellen?

- Wen muss ich bei Problemen informieren?
- Wie erreiche ich diese Personen?

Nachdem Sie diese Fragen beantwortet haben, geht es an die konkrete Erstellung Ihres Notfallplans

- **Verzeichnis anlegen**
  Legen Sie ein Verzeichnis für relevante Dokumentationen (z. B. Datensicherung) und Informationen an, die im Notfall benötigt werden.

- **Verantwortlichkeiten bestimmen**
  Benennen Sie Mitarbeiter, die für die im Fall einer Cyberattacke betroffenen Bereiche zuständig und die Umsetzung der Notfall-Maßnahmen verantwortlich sind.

- **Kontaktliste mit Experten anlegen**
  Erstellen Sie eine Telefonliste mit Experten und Ansprechpartnern, die Sie im Schadensfall unterstützen (IT-Forensik, Versicherung).

- **Ablaufplan festlegen**
  Legen Sie konkrete Vorgehensweisen zur Fehleranalyse und -behebung sowie zum Notbetriebs-verfahren fest.

- **Checklisten erstellen**
  Erstellen Sie Checklisten mit entsprechenden Handlungs-anweisungen.

- **Alarmkette festlegen**
  Wer muss wann informiert werden? (Name, Kontaktdaten, Verantwortlichkeit)

Hinweis zur Meldepflicht: Wurden personenbezogene Daten gestohlen, sind Sie gemäß Artikel 33 der DSGVO dazu verpflichtet, den Schaden innerhalb von 72 Stunden, nachdem Sie die Attacke bemerkt haben, der zuständigen Aufsichtsbehörde Ihres Bundeslandes (Sitz des Unternehmens) zu melden.

Alle Mitarbeiter sollten den Notfallplan kennen. Im besten Fall machen Sie regelmäßige Notfall-Übungen, damit der Ablauf im konkreten Schadensfall auch klappt.

Ein Beispiel für korrektes Verhalten im Schadensfall:

Einer Ihrer Mitarbeiter hat den Anhang einer E-Mail geöffnet und dadurch einen Verschlüsselungs-Trojaner aktiviert, der sofort beginnt, Ihre Daten auf dem Computer zu verschlüsseln. IT-Experten empfehlen hier, den PC sofort abzuschalten, da man unter Umständen so den Verschlüsselungsprozess noch aufhalten kann.

Im zweiten Schritt sollten Sie beziehungsweise Ihr Mitarbeiter den IT-Notfall-Beauftragten (intern oder extern) Ihres Betriebs informieren. Je nach Befugnis wird er zunächst identifizieren, welche Systeme betroffen sind und sich um die Systemwiederherstellung sowie Datenrettung kümmern. Alternativ kontaktiert er einen externen IT-Experten – je nachdem, wie Sie es in Ihrem Notfallplan festgelegt haben.

Häufig geht mit der Verschlüsselung eine Lösegeldforderung einher. Zahlen Sie dieses auf keinen Fall, denn in den meisten Fällen heben die Verbrecher die Verschlüsselung trotz Zahlung nicht wieder auf. Im Gegenteil! Meistens fordern sie danach immer wieder Geldbeträge von Ihnen. Werden Sie Opfer einer solchen oder andersartigen Cyberattacke, erstatten Sie auf jeden Fall Anzeige bei der Polizei. Denn es handelt sich bei einem Cyberangriff um eine Straftat. Und nur, wenn diese den Behörden angezeigt werden, kann insgesamt auch für mehr Sicherheit in diesem Bereich gesorgt werden. Ihren zuständigen Ansprechpartner können Sie unter anderem hier ausfindig machen: https://www.europol.europa.eu/report-a-crime/report-cybercrime-online

! Wenn Sie über eine Cyber-Versicherung verfügen, melden Sie den Schaden so schnell wie möglich Ihrem Versicherer.

Sofortmaßnahmen im Schadensfall

(Quelle: BKA)

- Identifizierung aller infizierten Systeme
- Isolierung von nicht infizierten Systemen, wenn möglich
- Sicherung relevanter Logdaten
- Ereignisprotokoll erstellen mit:
  - genauen Daten, wann der Angriff entdeckt wurde
  - Art der Beeinträchtigung aller infizierten Systeme, Konten, Dienste etc.
  - Angaben zum Ausmaß des Schadens

Krisenkommunikation im Schadensfall

Nach einem groß angelegten Cyberangriff fürchten Unternehmen vor allem eines: den Reputationsschaden. Deshalb scheuen sich viele davor, einen solchen Angriff öffentlich zu machen. Doch genau das ist der größte Fehler. Nur mit offener Kommunikation kann das Vertrauen in das betroffene Unternehmen bewahrt – oder zumindest wieder hergestellt werden. Und das gilt sowohl für die interne Kommunikation (Mitarbeiter, Investoren, etc.) als auch für die externe (Kunden, Presse, etc.).

Ein positives Beispiel ist hier ein Fall aus dem Jahr 2016:

Das Lukaskrankenhaus in Neuss wurde Opfer einer Cybererpressung. Ein Virus aus einem infizierten E-Mail-Anhang hatte das gesamte Kliniknetzwerk lahmgelegt. Die Notfallversorgung fiel für insgesamt 30 Stunden komplett aus. Die Verantwortlichen des Krankenhauses handelten überlegt und meldeten den Fall sofort dem Landeskriminalamt. Zudem wurden schnellstmöglich sowohl Mitarbeiter als auch Patienten informiert, eine Pressemitteilung wurde ebenfalls zeitnah herausgegeben.

Zwar entstand alles in allem ein hoher finanzieller Schaden von rund einer Million Euro. Eine Rufschädigung und einen damit einhergehenden Patientenrückgang konnte die Klinik jedoch nicht verzeichnen. Sowohl die Mitarbeiter als auch die Patienten bewerteten die Offenheit im Umgang mit der Cyberattacke als positiv. (Quelle: Ärztezeitung)

7. Absicherung von Cyber-risiken

Eine Cyber-Versicherung sichert Sie im Fall eines Cyberschadens finanziell ab. Je nach Art und Umfang des Versicherungspakets übernimmt der Versicherer sowohl Haftpflichtschäden wie auch Eigenschäden, die Ihnen im Fall einer Cyberattacke entstehen.

So schützt Sie die Cyberversicherung

Absicherung von Haftpflichtschäden:

Vermögensschaden zu Lasten Ihrer Kunden oder Firmenpartner z. B. durch:

- Datendiebstahl und - missbrauch
- von Kreditkartendaten
- Diebstahl und Veröffentlichung vertraulicher Informationen

Absicherung von Eigenschäden:

Bei finanziellen Schäden Ihres Unternehmens z. B. durch:

- DDoS-Attacken
- Betriebsausfall durch Trojaner
- Veröffentlichung von Betriebsinterna

Kostenübernahme u. a. für:

- finanziellen Schaden
- IT-Forensik
- Daten- und Systemwiederherstellung
- Krisenberatung
- Benachrichtigung betroffener Kunden
- Rechtsberatung bei Datenschutzverletzungen

Bedingungen für einen wirksamen Versicherungsschutz

Damit Ihr Versicherungsschutz im Schadensfall besteht, stellen einige Versicherer bestimmte Bedingungen, die Sie in Sachen Cybersicherheit erfüllen müssen. Das können beispielsweise sein:

- Einsatz von Antiviren-Programmen und Firewalls

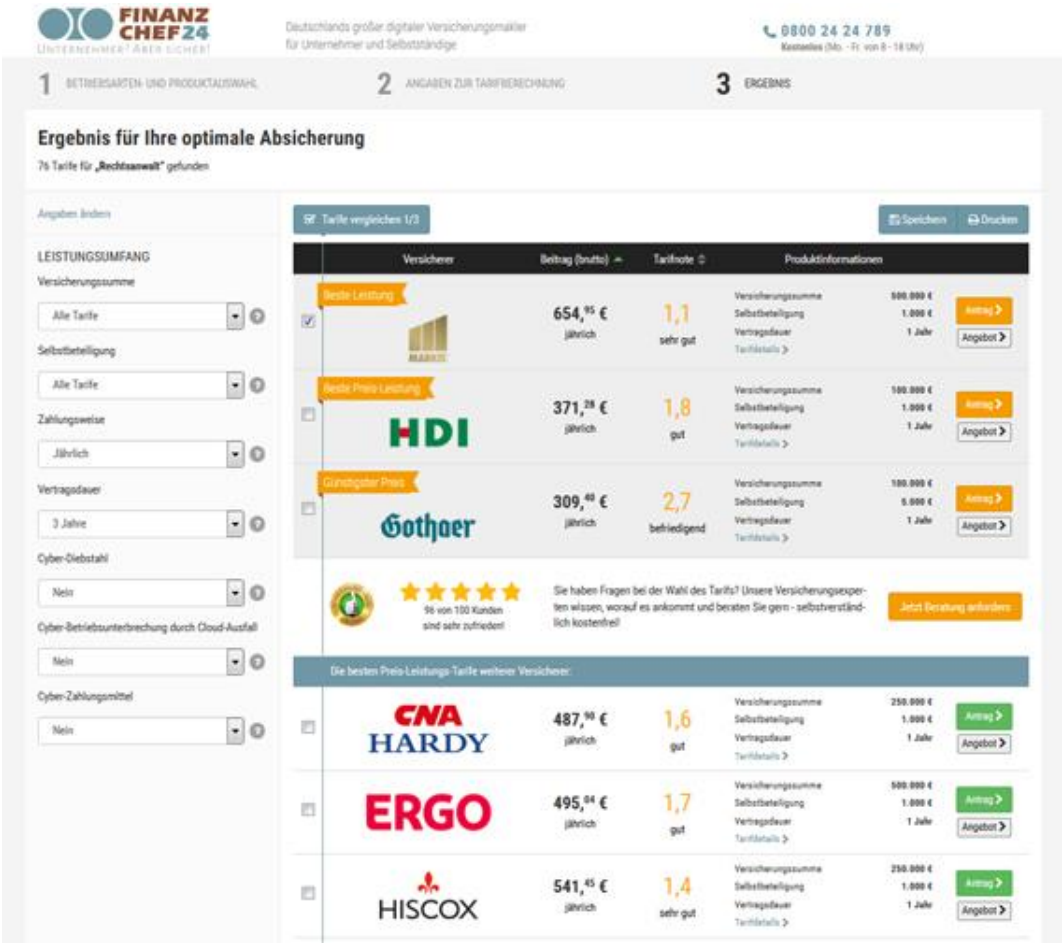
- Einsatz vom Hersteller unterstützter Software (Garantie regelmäßiger Updates, um Fehler zu beheben und Sicherheitslücken zu schließen)
- zeitnahe und regelmäßige Installation solcher Updates
- regelmäßige Datensicherung
- Änderungen von voreingestellten (Werkseinstellung) Passwörtern und PINs bei Inbetriebnahme neuer Anlagen / Geräte

Versicherungsvergleich mit Finanzchef24

Mit der steigenden Relevanz des Themas Cybercrime entwickeln auch immer mehr Versicherer Produkte, die Unternehmen Schutz bieten. Um den richtigen Tarif für Ihren individuellen Bedarf zu finden, empfehlen wir Ihnen, die Angebote miteinander zu vergleichen. Dies können Sie bequem mithilfe unseres unabhängigen Online-Rechners für Cyber-Versicherungen durchführen.

Auf Basis Ihrer unternehmensspezifischen Angaben ermittelt er Ihren Bedarf und spielt Ihnen passende Angebote individuell für Ihr Unternehmen aus. Diese können Sie hinsichtlich Preis und Leistung bequem online vergleichen und Ihren Wunschtarif direkt über unseren Rechner abschließen.

Unabhängiger Online-Vergleich für die Cyber-Versicherung



Kostenlose und unverbindliche Beratung

Wünschen Sie eine persönliche Beratung, stehen Ihnen unsere Versicherungsexperten jederzeit gern zur Verfügung. Schreiben Sie uns einfach eine E-Mail oder rufen Sie uns von Montag bis Freitag zwischen 8 und 18 Uhr kostenfrei an unter 0800 24 24 789.

8. Nützliche Websites zur Cybersicherheit

- **Mitarbeiter-Schulungen**
  Es gibt E-Learning-Plattformen, die Sie zur Schulung Ihrer Mitarbeiter nutzen können. Die Security-Awareness-Plattform von usd, gefördert vom Bundesministerium für Wirtschaft und Energie (BMWi), bietet beispielsweise ein solches Angebot.

- **Website-Check**
  Ebenfalls gefördert durch das BMWi bietet die Initiative-S einen speziellen Service an. Sie können dort Ihre Unternehmens-Webseite von Sicherheitsexperten überprüfen, reinigen und schützen lassen.

- **Cyber-Sicherheitscheck**
  Mithilfe des Cyber-Sicherheitschecks vom Gesamtverband der Deutschen Versicherungswirtschaft (GDV) können Sie online testen, wie gut Sie/Ihr Betrieb tatsächlich für Cyberattacken & Co. gerüstet sind. Das Tool stellt Ihnen die 10 wichtigsten Fragen und gibt Ihnen anschließend hilfreiche Tipps zur Verbesserung der IT-Sicherheit.

- **Für Selbstständige im Handwerk**
  Speziell für Handwerksbetriebe wurde das Projekt IT-Sicherheit im Handwerk ins Leben gerufen. Dort finden selbstständige Handwerker persönliche Ansprechpartner, viele Informationen zum Thema Cybersecurity sowie Unterstützung bei der Umsetzung ihrer IT-Sicherheitskonzepte. Das Projekt wird ebenfalls vom Bundesministerium für Wirtschaft und Energie unterstützt.

- **Datenlecks prüfen**
  Mit der Website Have I been pwnd des unabhängigen Sicherheitsforschers Troy Hunt können Sie prüfen, ob die Logins der von Ihnen genutzten Webdienste wie E-Mail-Anbieter, Cloudservices, Online-Verkaufsplattformen u. ä. möglicherweise gestohlen wurden und diese nun im Internet im Umlauf sind, wie es 2012 beispielsweise bei 68 Millionen Nutzern von Dropbox passiert ist.

Ebenso können Sie mit Identity Leak Checker vom Hasso Plattner-Institut testen, ob Ihre Identitätsdaten ausspioniert wurden. Sie erhalten eine E-Mail an ihre eingegebene Adresse und erfahren ob und welche persönlichen Daten betroffen sind.

Stand: 05. Februar 2019

Bildreferenzen:

Cover:	Adobe Stock	#177665532	© Sikov
Seite 4:	Adobe Stock	#122248676	© horimono
Seite 7:	Adobe Stock	#178952601	© SFIO CRACHO
Seite 10:	Adobe Stock	#208731473	© ipopba
Seite 12:	Adobe Stock	#37359192	© Woodapple
Seite 17:	Adobe Stock	#163401169	© vectorfusionart
Seite 19:	Adobe Stock	#40949459	© auremar
Seite 24:	Adobe Stock	#105852088	© Industrieblick
Seite 28:	Adobe Stock	#170031429	© Suteren Studio

Finanzchef24 GmbH
Hohenlindener Str. 1
81677 München
Tel: 089 / 716 772 700
E-Mail: info@finanzchef24.de
www.finanzchef24.de

FINANZ CHEF24
UNTERNEHMER? ABER SICHER!