RECHT 01.09.2018

Cyberrisiken – Wie groß ist die Bedrohung und welche Absicherungskonzepte gibt es?



Mit zunehmender Bedeutung und Vernetzung von IT-Systemen werden die wirtschaftlichen Folgen eines Systemausfalls immer größer. Gefahren bestehen nicht nur durch „Feinde“ von außen. Grundsätzlich können alle technischen Fehler an Hard- und/oder Software sowie menschliches Versagen bzw. Bedienfehler den IT-Systemen schaden. Das müssen nicht unbedingt vorsätzliche unerlaubte Handlungen sein. Solche Schäden können auch durch versehentliches Handeln, Verschleiß oder sonstige Einflüsse (Feuer, Leitungswasser usw.) entstehen. Hingegen ist jede vorsätzliche unerlaubte Handlung, die mittels eines Computers, Netzwerk- oder Hardwaregeräts begangen wird (z. B. unerlaubter Zugriff, Sabotagen durch Hackerangriffe und Phishingattacken) als Cybercrime zu bezeichnen.

Folgen eines Cyberangriffs

Es kann zu erheblichen Ertragseinbußen kommen, wenn IT-Systeme, die für den Betrieb eines Unternehmens notwendig sind, über einen längeren Zeitraum blockiert sind oder gar ausfallen. Zudem kann die Integrität der Daten (Korrektheit) Schaden nehmen, ebenso wie die Vertraulichkeit von personenbezogenen Daten. Die Kosten, egal ob finanzieller Art oder in Bezug auf die Reputation des Unternehmens, sind in jedem Fall nicht zu unterschätzen. Das folgende Schaubild führt einige Kostenpositionen auf, die die Höhe des Gesamtschadens bestimmen.

Die Liste macht deutlich, dass vielfältige Schadenszenarien möglich sind. Die Schadenabteilung der Ecclesia Gruppe hat den Überblick. Bei den folgenden Fallbeispielen handelt es sich um tatsächlich eingetretene IT-Schadenfälle bei Kunden der Ecclesia. Die Schadenhöhen bei den aufgeführten Beispielen belaufen sich je nach Größe der Einrichtung auf ca. 10.000 bis 20.000 Euro.

Absicherung von Cyberrisiken und Konditionen

Die Versicherer bieten unter der Überschrift „Cyberversicherung“ eine Vielzahl unterschiedlicher Absicherungskonzepte an. Bei einigen Konzepten liegt der Schwerpunkt im Sachschadenbereich (z. B. Betriebsunterbrechung, Hard- und Softwareschäden), bei anderen eher im Drittschaden-/Haftpflichtbereich. Die Verletzung von Datenschutzgesetzen führt in der überwiegenden Anzahl der Schadenfälle z. B. zu einer Verletzung des Persönlichkeitsrechts. Dieser Schadenfall wird in der Kommentierung und Rechtsprechung überwiegend als Vermögensschaden bewertet und fällt damit in den Bereich Haftpflicht.

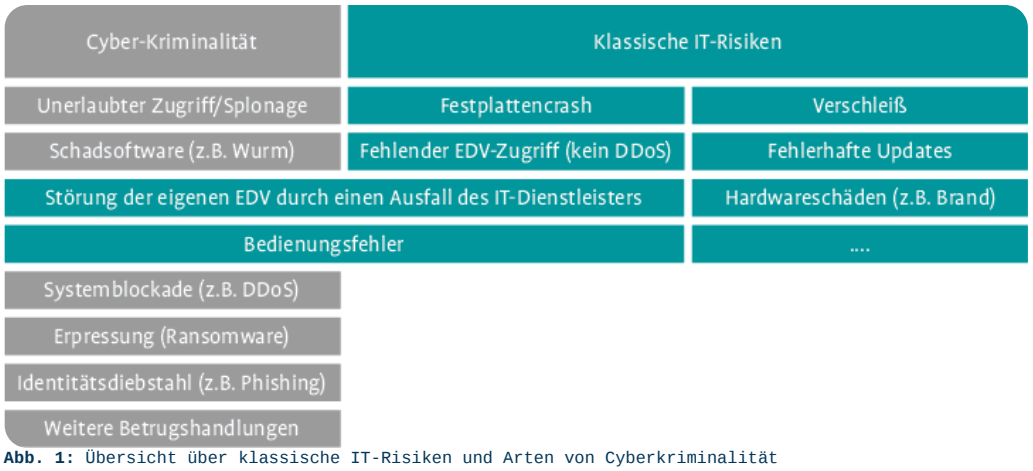


Abb. 1: Übersicht über klassische IT-Risiken und Arten von Cyberkriminalität



Abb. 2: Kostenpositionen bei einem IT-Ausfall/-Schaden

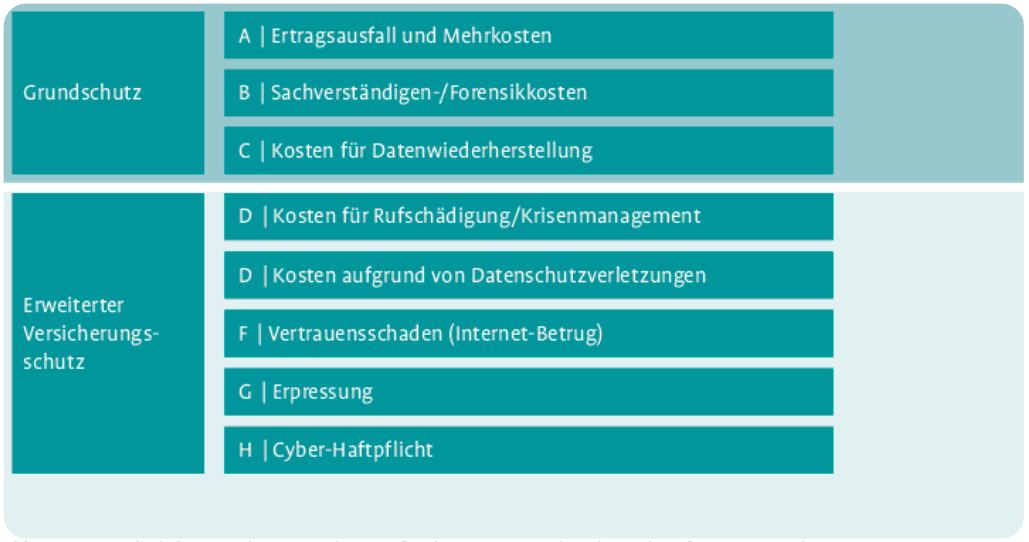


Abb. 3: Das Absicherungskonzept der Ecclesia Gruppe und seine einzelnen Bausteine

Fallbeispiel 1: Dateianhang mit verstecktem Virus

In einer ambulanten Gemeinschaftspraxis geht eine E-Mail mit einem Dateianhang ein. Die Mitarbeitenden öffnen den Anhang und setzen damit einen Virus frei. Der Virus zerstört die gespeicherten Daten auf dem Computer und führt zu einem vollständigen Ausfall der IT-Systeme. Bis zur Bereinigung des Systems ist die Behandlung von Patientinnen und Patienten nur eingeschränkt möglich. Die Praxis verzeichnet einen entsprechenden Ertragsausfall.

Fallbeispiel 2: Identitätsdiebstahl

Ein Mitarbeitender einer Praxis erhält eine E-Mail von einem Geschäftspartner für Praxisbedarf. Die Praxis wird aufgefordert, offene Rechnungsbeträge an eine geänderte Bankverbindung zu überweisen. Daraufhin weist die Praxis Zahlungen an die neue Bankverbindung an. Nach zwei Wochen erhält die Praxis eine weitere E-Mail, dieses Mal mit einer Zahlungserinnerung desselben Geschäftspartners. Infolge dessen stellt sich heraus, dass ein Dritter die Identität des Geschäftspartners gestohlen hat und sich als dieser ausgab.

Fallbeispiel 3: Sicherheitslücken im IT-System

In einem Medizinischen Versorgungszentrum besteht eine unerkannte Sicherheitslücke im IT-System. Diese führt dazu, dass das IT-System unbemerkt von einer neuen Schadsoftware, einem sogenannten Trojaner, befallen wird. Der Virenscanner erkennt die Schadsoftware erst nach dem täglichen Update. In der Zwischenzeit werden zahlreiche sensible Daten von Patientinnen und Patienten auf ein fremdes externes System übertragen. Für das MVZ entstehen erhebliche Kosten u. a. für die gesetzlichen Benachrichtigungspflichten

(Bundesdatenschutzgesetz), forensische Maßnahmen (einschließlich Bereinigung der Systeme) und öffentlichkeitswirksame Maßnahmen, um eine mögliche Rufschädigung abzuwenden.

Die Ecclesia Gruppe hat über einen speziellen Rahmenvertrag die Möglichkeit geschaffen, alle Arten von IT-Schäden mit nur einem Versicherungskonzept abzusichern. Dabei handelt es sich um ein modulares Konzept, in das alle Bausteine integriert werden können – aber nicht müssen.

Zusätzliche Dienstleistungsangebote exklusiv für BDC-Mitglieder: Risikobeurteilung (IT-Basis-Check, Penetrationstests etc.) und Präventionsmaßnahmen

BDC-Mitglieder erhalten von der Ecclesia Gruppe professionelle Unterstützung beim systematischen Management von Cyberrisiken. Im digitalen Datentransfer sollten drei zentrale Schutzziele im Fokus stehen:

- Systemausfälle verhindern (Verfügbarkeit).
- unbemerkte Datenänderungen verhindern bzw. nur nachvollziehbare Änderungen erlauben (Integrität).
- Daten nur autorisierten Benutzern zugänglich machen (Vertraulichkeit)

Ein IT-Basis-Check unterstützt dabei, Sicherheitsstrukturen zu bewerten und wichtige Optimierungsfelder zu erkennen. Durchgeführt werden der IT-Basis-Check und die Penetrationstests von dem Spezialdienstleister HiSolutions AG, mit dem die Ecclesia Gruppe zusammenarbeitet.

Einschätzungen und Wirklichkeit

1. **Unsere Einrichtung war bislang nicht Ziel eines Cyberangriffs. Unsere Unternehmensgröße und unsere Daten sind für Angreifer nicht interessant.**

Ungezielte Cyberangriffe (z. B. Ransomware) können jeden treffen, egal ob Privatpersonen oder Unternehmen. Die Unternehmensgröße und die Art und Größe der Daten sind für den Angreifer ebenfalls irrelevant.

Seit 2011 ist der Anteil der gezielten Angriffe auf kleine Unternehmen von 18 % auf 43 % gestiegen. Die Anzahl der gezielten Angriffe bei Großunternehmen ist hingegen zurückgegangen. Dieser Trend dürfte sich weiter fortsetzen, sodass die Wahrscheinlichkeit eines Angriffs steigt.

2.**Wir haben ausgezeichnete IT-Sicherheitssysteme. Ein Cyberangriff wird keinen Erfolg haben.**

Die Angreifer sind (hoch-)professionelle Hacker, Wettbewerber oder Mitarbeitende mit dem primären Motiv „Gewinnmaximierung“. Stark gesicherte Regierungseinrichtungen oder Großunternehmen werden trotzdem erfolgreich angegriffen (z. B. Bundestag, T-Mobile oder Sony). Pro Tag werden über 1,1 Mio. neue Schadprogramme entwickelt und in Umlauf gebracht. Die Angreifer sind somit immer einen Schritt voraus und die Sicherheitshersteller müssen erst reagieren. Ein Update der Sicherheitssoftware für neue Schadprogramme dauert einige Stunden bis Tage. Die Gefahren kommen zudem nicht nur von außen. Der Faktor Mensch ist nicht zu verkennen. Ein unachtsamer Klick auf den verseuchten Anhang einer E-Mail kann fatale Folgen für die gesamte IT-Infrastruktur eines Unternehmens haben.

3.**Das Risiko von Trojanern, Viren oder Würmer ist überschaubar. Wir haben eine Echtzeitspiegelung unserer Daten. Bei einem Befall werden wir unsere Datensicherung nutzen.**

Schadsoftware wird nicht immer direkt bemerkt und kann die Datensicherung ebenfalls infizieren (z. B. neuer Virus oder Trojaner wird erst nach sechs 6 Monaten aktiviert). Die Datensicherung läuft somit ins Leere. Aus der Schadenpraxis heraus sind Fälle bekannt, bei denen eine Datenwiederherstellung über die Datensicherung nicht möglich war (beschädigte Datensicherung).

Dahl A: Cyberrisiken – Wie groß ist die Bedrohung und welche Absicherungskonzepte gibt es? Passion Chirurgie. 2018 September, 8(09): Artikel 04_04.