CYBERVERSICHERUNG

# Cyberschäden: ...

Foto: Ken Schluchtmann, diephotodesigner.de

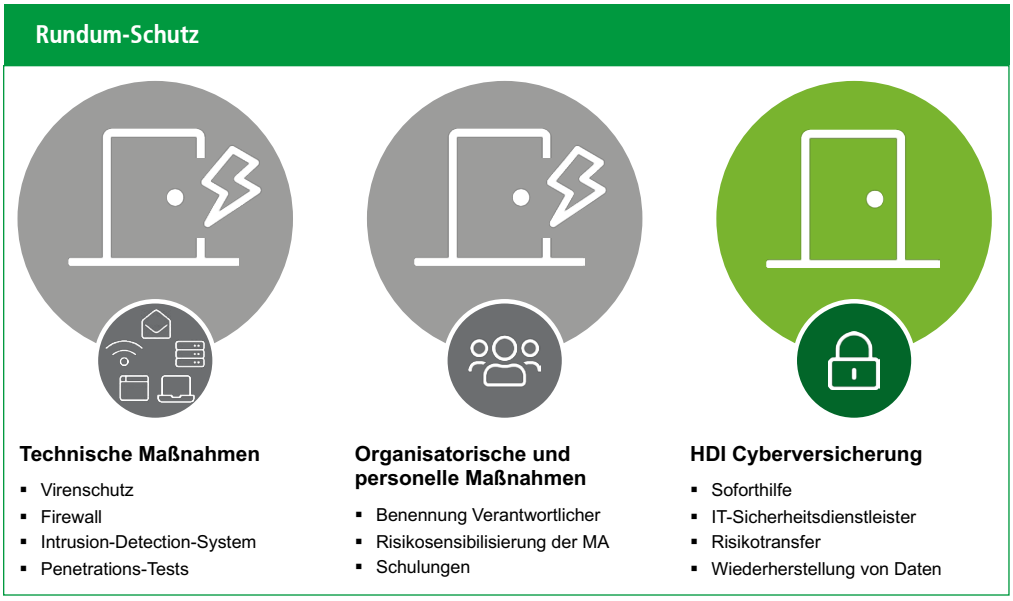
## ...Wenn ein technischer Ausfall der Anwendung zur Betriebsunterbrechung führt

Viele Planungbüros sind sich der Cybergefahren und Cyberkriminalität nicht bewusst und verdrängen im Zweifel die steigenden Gefahren aus dem Netz. Aber das ist ein Fehler, denn das Cyberrisiko ist allgegenwärtig und im Zusammenhang mit Corona kritischer als je zuvor.

Ganz gleich ob Gründer oder etablierte Unternehmen, die Netzwerksicherheit erhält in den wenigsten Fällen die Aufmerksamkeit, die sie eigentlich verdient. Ähnliches geht auch aus dem Report der Cyberrisiken im Mittelstand 2020 hervor. Bei einer Forsa-Umfrage wurden 300 Entscheider in kleinen und mittleren Unternehmen befragt. Ziel der Befragung war es, eine Sensibilisierung für Cybergefahren zu schaffen. Es ließ sich feststellen, dass viele Unternehmen der Annahme sind, zu klein, umfassend geschützt, nicht interessant genug zu sein oder einfach noch nie Opfer einer Cyberattacke waren und folglich nicht sein werden. Deutlich wird, dass man sich der Gefahr nicht bewusst ist.

Die Annahme, dass man zu klein oder uninteressant sei, geht leider nicht auf. Gerade kleinere Unternehmen werden eher Opfer von massenhaft gestreuten, ungezielten Angriffen. Aus unserer praktischen Erfahrung wissen wir, dass jeder betroffen sein kann – und noch schlimmer: Es kann für jeden existenzbedrohende Ausmaße annehmen.

Viele assoziieren mit einem Cyberangriff oft den böswilligen Hacker. Ein Mensch, der ausschließlich die finanzielle Bereicherung im Kopf hat. Die Motive können variieren und genau deswegen ist das Thema so brisant. Die Medien fundamentieren, dass nahezu wöchentliche Hackerangriffe auf große Konzerne stattfinden. Konzerne, die eine ausgesprochen vernünftige Sicherheitsstruktur vermuten lassen. Unweigerlich wird klar, dass sich keine Branche, so auch nicht die Planer allzu sicher fühlen sollten. Dazu kommt, dass Unternehmen oft nicht gezielt angegriffen werden. Kriminelle setzen ihre Schadsoftware auf eine große Zahl kleinerer Unternehmen an. Es sind dann immer einige dabei, die zum Beispiel mit Schadsoftware präparierte E-Mail-Anhänge öffnen, sodass die Schadsoftware Unternehmensdaten verschlüsseln kann. Die Motivation der Hacker ist so simpel wie einfach, nämlich der **Quotient aus Anreiz und Nutzen**. Der Aufwand bei dieser unwillkürlichen Streuung ist minimal und wird wohl in Summe durchaus lohnend sein.




**Besonderheiten im Kontext Building Information Modeling (BIM)**
Das digitale Arbeiten – insbesondere auch mit BIM – soll und wird zukünftig mehr und mehr zum Standard werden. Im Ausland hat sich die Einführung dieser Methode schon lange etabliert und in vielen Ländern wie Großbritannien, Schweden, Norwegen und den USA ist die Nutzung von BIM bei öffentlich finanzierten Bauvorhaben bereits Pflicht. In Deutschland wurde gemäß „Agenda 2020" BIM zum Standard bei Projekten des Infrastrukturbaus.

Durch die zunehmende Durchdringung von digitalen Planungsprozessen z. B. BIM kommt man nicht drum herum, Anwendungen dieser Art in Bezug auf Cybergefahren näher zu beleuchten.

Wir unterscheiden Cloud-Dienstleistungen in zwei Kategorien. Das ist für den Anfang ausgesprochen oberflächlich, wird der Erläuterung aber genügen:
Auf der einen Seite die reine Datenablage, also Cloud-Storage, in welcher wir Daten ab- oder zwischenspeichern. Umgangssprachlich ein Lager für virtuelle Daten. Hier findet keinerlei Bearbeitung statt. Ein gängiges Beispiel ist die Dropbox.
Auf der anderen Seite haben wir die virtuellen Maschinen der Cloud-Dienstleistungen. Zum Beispiel der vServer von IONES. In ähnlicher Funktion tritt die Anwendung BIM auf. Nennenswerte Vorteile bei Verwendung einer Cloud-Dienstleistung, wie beispielsweise BIM, ist, dass der Host das Patch-Management übernimmt, die ausreichende Kompetenz hat und die vermeintlich notwendigen Ressourcen für Stabilität und Verfügbarkeit sicherstellen kann. Weiter ist die eigens betriebliche Bandbreite im Büro oder im Homeoffice nur für den Transfer der Daten notwendig. Die Verarbeitung im Datenraum unterliegt der Bandbreite des Providers.

Habe ich überhaupt Nachteile als Anwender? Die Frage ist schwer pauschal zu beantworten, da jeder Nutzer unterschiedliche Präventionen für die eigene Hard- und Software initiiert hat. Bekannt ist, dass die Einfallstore von Cybergefahren, wie für einen virtuellen Datenraum typisch, einer DDoS-Attacke unterliegen nicht das Haupteinfallstor für erfolgreiche Cyberangriffe ist. Heißt, dass die Verwendung einer virtuellen Maschine mit höherwertigen Schutzmaßnahmen nicht den vollständigen Schutz des eigenen Betriebs sicherstellt. Das Haupteinfallstor für erfolgreiche Cyberangriffe sind E-Mails. Die Unwissenheit eines Mitarbeiters im eigenen Betrieb führt häufig zu einer erfolgreichen Attacke. Dies belegt o. g. Studie. Ein Grund, weswegen ordentliche Cyberprävention perspektivisch unumgänglich wird. Hier wird ein starker Partner, wie in unserer Cyberabsicherung beitragsfrei integriert, benötigt.

**Cyberattacke und ihre Folgen**
Setzen wir uns mit den Folgen einer Cyberattacke auseinander und stellen uns folgende Fragen: Was ist mit der Integrität, Datensicherheit und dem Datenschutz der Daten? Was passiert, wenn die Anwendung mehrere Tage ausfällt? Wie verhalten wir uns, wenn wir keinen Zugriff haben (Konnektivitätsprobleme)? Wie lange und wie kann man solche Unterbrechungen überstehen?
**Ab wann müssen Vertragspartner informiert werden, weil die Verbindlichkeiten in einem Vertrag kritisch werden?**

Wir stellen fest, dass wir bei der Verwendung digitaler Lösungen in ständiger Abhängigkeit zum Cloud-Host bzw. zum Datenraum stehen. Sollte der Datenraum aufgrund einer Attacke offline sein, ist eine Fortsetzung der Arbeit nicht möglich. Gründe für die Unerreichbarkeit müssen nicht zwangsläufig böswilliger Natur eines unbekannten Dritten sein. Es kann sich hierbei auch um gravierende Programmier- oder Bedienfehler handeln, die zu einem Absturz geführt haben. Diese zu identifizieren und zu beheben, wird im Zweifel mehrere Stunden in Anspruch nehmen. Wer stellt sicher, dass die Daten nicht verändert worden sind? Wird eine Überprüfung der bereits gesicherten Daten vorgenommen? Sind diese unbeschadet? Weiter kann ein Update zu Kompatibilitätsproblemen führen. Was sich als Vorteil schmückt, entpuppt sich in Teilen auch als Nachteil. Wir überlassen dem Provider das Patch-Management, somit auch die Abwägung von Dringlichkeit und Kritikalität der Updates. Ein Sicherheitspatch sollte unverzüglich eingespielt werden – teilt der Host diese Auffassung? Kann ich diese Entscheidung beeinflussen? Habe ich Kenntnisse über Backdoors und andere Zugriffsmöglichkeiten? Der Bonus der physischen Unabhängigkeit könnte doch auch anderen ein Zugang ermöglichen? Unterliege ich einer strengen Zwei-Faktor-Authentifizierung? Gibt es eine Passwortrichtlinie? Wird diese technisch unterstützt?

**Fazit:** Im Endeffekt fundamentiert sich die unausweichliche Wahrheit, dass aus Kosten- und Kapazitätsgründen keine lückenlose Überwachung gewährleistet werden kann. Außerdem übernehmen Dienstleister keine Haftung für eingetretene Schäden. Denn auch die wissen, dass es eine hundertprozentige Sicherheit nicht geben kann.

Schlussendlich sind bei einem Cyberangriff wie auch bei dem Thema IT-Sicherheit und Datenschutz viele Unternehmen noch nicht optimal aufgestellt und im Ernstfall hilflos. Dabei ist bei einer möglichen Datenpanne nach der Europäischen Datenschutz-Grundverordnung (DSGVO) bereits im Vorfeld eine Risikobewertung der Datensicherheit notwendig und bei Bekanntwerden einer sogenannten Datenpanne ein zügiges Handeln geboten. Nach Art. 33 Abs. 1 DSGVO muss eine Datenpanne binnen 72 Stunden nach Kenntnis der Datenschutzverletzung an die zuständige Datenschutzbehörde gemeldet werden.

Die zuvor genannten Risiken deckt eine Cyberversicherung ab. Die HDI Cyberversicherung bietet zudem Leistungen, die über den normalen Versicherungsschutz hinausgehen. Schulungs- und Präventionsmaßnahmen, eine 24/7-Hotline und einen IT-Sicherheitsdienstleister, der sich durch besondere Expertise in Sachen Cybersicherheit auszeichnet, sind dabei Dreh- und Angelpunkte.

Durch die zeitnahe und vollumfängliche Unterstützung mit allen Experten können wir unsere Kunden nicht nur monetär unterstützen, sondern insbesondere den zeitnahen, dringend benötigten Support bieten.

Als Veranschaulichung: Die Niedersächsische Bauordnung (NBauO) schreibt sinngemäß vor, dass bauliche Anlagen so errichtet, geändert und instand gehalten werden und so angeordnet, beschaffen und für die Benutzung geeignet sein müssen, dass der Entstehung eines Brandes sowie der Ausbreitung von Feuer und Rauch vorgebeugt wird und bei einem Brand die Rettung von Menschen sowie wirksame Löscharbeiten möglich sind. Ein Gebäude wird also mit der Intention errichtet, den Brandschaden möglichst gering und für die Fachmenschen beherrschbar zu halten. Nichts anderes ist die Aufgabe von IT-Spezialisten, Firewall und Anti-Virensoftware. Brandschutzmaßnahmen machen eine Feuerversicherung ebenso wenig obsolet wie zuvor genannte Punkte eine Cyberversicherung.

**Autor**

Sönke Glanz
Produktmanagement Underwriter Cyber
HDI Versicherung AG
Hannover

Fotos: Ken Schluchtmann, diephotodesigner.de