Cyber-Versicherungen

Nur ein Teil des Sicherheitspuzzles

HR-Daten sind ein beliebtes Ziel für Hacker. Das wissen auch die Versicherungsgesellschaften und bieten mittlerweile eine ganze Palette an Versicherungen für Grossfirmen und KMU an. Eine Police alleine bietet allerdings noch keinen Schutz. Unsere Umfrage bei Versicherungsexperten zeigt, was wirklich wichtig ist.
Text: Sandra Escher Clauss

HR-Daten sind so etwas wie das digitale Gold der kriminellen Hackerszene. Zu diesem Schluss kommt man, wenn man Stéphane Fleury von der Baloise Group zuhört: «HR-Daten werden auf dem digitalen Schwarzmarkt als noch wertvoller eingeschätzt als Finanz- oder IT-System-Daten.»

Das zeigt die Zweischneidigkeit der digitalen Welt. Sie bietet Unternehmen zwar beinahe unbegrenzte Möglichkeiten, öffnet aber auch Tür und Tor für Missbrauch. Gemäss der KPMG-Studie Clarity on Cyber Security haben im vergangenen Jahr rund neun von zehn Schweizer Unternehmen eine Cyberattacke erlebt. «Cyberkriminelle agieren schnell und erfinden laufend neue Angriffsmethoden. Daher besteht trotz modernster Sicherheitsmassnahmen immer das Restrisiko einer Attacke», sagt Alexander Tlili , Underwriter bei Zurich Schweiz.

Um dieses Restrisiko abzusichern, bieten mittlerweile die meisten grossen Versicherungsgesellschaften Cybersecurity-Versicherungen an. Das alleine schützt aber nicht vor Hackern und Konsorten. Davon ist Reto Zbinden, Gründer und CEO von Swiss Infosec, überzeugt. Seit fast 30 Jahren berät und schult sein Unternehmen Kunden rund um das Thema Sicherheit von Informationen. Zbinden weist darauf hin, dass eine Versicherung nur in den wenigsten Fällen den gesamten entstandenen Schaden decke. «Wichtiger ist die Schulung und Sensibilisierung aller Mitarbeitenden.»

Der Mensch als Schwachstelle

Diese Meinung teilen auch die befragten Versicherungsunternehmen (siehe Umfrage rechts). «Die grösste Angriffsfläche bieten immer noch Menschen, die mit ihrem Zugriff auf sensitive Daten zu wenig achtsam umgehen», betont etwa Christian Zeller, Leiter IT-Governance, Risk Management & Compliance bei der Mobiliarversicherung. Für Reto Zbinden ist der Faktor Mensch ebenfalls der Hauptgrund, um in erster Linie auf sichere Systeme zu setzen und erst in zweiter Linie auf eine Versicherung. «Ein sicheres System ist mehr als die Kombination von integren Personen und moderner Technik», mahnt Zbinden. «Um Daten zu schützen, braucht es physischen und logischen Schutz, Firewalls, sichere Passwörter oder angemessene Benutzerrechte. Andererseits gehören aber auch schriftliche Vereinbarungen mit internen und externen Mitarbeitenden und Partnern dazu.» Letztere, so Zbinden, würden sehr gerne vergessen gehen.

Eine Norm setzt sich durch

Informationssicherheit ist mehr als IT-Sicherheit und benötigt ein umfangreiches Managementsystem. Aus diesem Grund setzt sich mittlerweile die internationale Norm ISO/IEC 27001 in mehr und mehr Unternehmen durch. Auf dieser Norm basiert die Zertifizierung von Informationssicherheits-Managementsystemen (ISMS).

Auch wenn solche Zertifizierungsprozesse einen grossen zeitlichen und finanziellen Aufwand bedeuten, seien sie allemal empfehlenswert, ist Zbinden überzeugt: «Damit ist die Vertraulichkeit, die Verfügbarkeit und die Integrität der Daten gewährleistet, und die Mitarbeitenden sind bestmöglich sensibilisiert.» Die ISMS-Zertifizierung stellt u. a. auch die Konformität mit den Gesetzen und Regulatorien sicher. Deshalb sei sie gerade auch im Hinblick auf die Totalrevision des Datenschutzgesetzes eine lohnende Investition. «Mit der Gesetzesrevision werden auch die Bussen stark ansteigen, – und diese übernimmt keine Versicherung.» ■

Alle Angaben basieren auf Eigendeklaration der genannten Unternehmen.	Stéphane Fleury, Underwriter technische Versicherung, Baloise Group
1. Wie gross ist das Risiko einer Cyberattacke?	Das Risiko einer Cyberattacke ist inzwischen unabhängig von Unternehmensgrösse, Standort oder Branche gegeben. Die Zahlen der «Clarity on Cyber Security»-Studie von KPMG sprechen für sich: 2016 meldeten 56 Prozent von 60 teilnehmenden mittelgrossen bis grossen Schweizer Unternehmen eine Cyberattacke.
2. Inwiefern sind HR-Daten einem Risiko ausgesetzt und wo sehen Sie die grössten Angriffspunkte?	HR-Daten sind genauso gefährdet wie Finanz- oder IT-System-Daten. Oft werden HR-Daten auf dem digitalen Schwarzmarkt als noch wertvoller eingeschätzt, da sie sensible Informationen über Menschen enthalten und gegen diese verwendet werden können. Deshalb sind sie auch umso schützenswerter. Die grösste Schwachstelle in punkto Cybersicherheit ist in jedem Unternehmen der Mensch. Durch fehlende Kenntnis der Risiken und korrekter Verhaltensweisen ist er beispielsweise einer Phishing-Attacke hilflos ausgeliefert.
3. Sind HR-Fachleute auf diese Risiken und auf den Umgang damit vorbereitet?	In den meisten Fällen sind Mitarbeitende nicht genügend auf diese Risiken vorbereitet. Viele kennen zwar die wichtigen Begriffe der Cybersecurity, sind sich aber oft nicht sicher, wie sie im Ernstfall reagieren müssen. Wichtig ist, dass Unternehmen dieses Bewusstsein schaffen und alle Mitarbeitenden die Konsequenzen eines Cyberangriffs verstehen.
4. Braucht tatsächlich jedes Unternehmen eine Cyber-Versicherung? Wo macht eine solche Sinn, wo nicht?	Eine Auswertung des Eidgenössischen Finanzdepartements aus dem Jahr 2017 zeigte, dass bereits jedes dritte Schweizer KMU Opfer von Cyberattacken wurde. Betroffen sind nicht nur grosse Firmen, sondern auch kleine Handwerkerbetriebe, Coiffeure und andere KMU. Eine Cyber-Versicherung ist daher zu empfehlen, sobald Unternehmen Computer verwenden oder technische, beziehungsweise Produktionsanlagen betreiben, die mit einem digitalen Netzwerk verbunden sind.
5. Was beinhalten Ihre Versicherungsleistungen und an wen richten sie sich?	Diese zielt hauptsächlich auf KMU. Sie umfasst die Deckung von Eigenschäden wie die Entfernung von Schadsoftware, Wiederherstellung oder Wiederbeschaffung von elektronischen Daten und Programmen, den Betriebsertragsausfall. Sie ist erweiterbar auf die Beeinflussung des Zahlungsverkehrs oder von Warenflüssen und deckt Ansprüche infolge von Drittschäden, beispielsweise wegen beeinträchtigter IT-Systemverfügbarkeit, Datenverlusten, unerlaubtem Eingriff in IT-Systeme, Datenschutzverletzungen bis zur Deckung von Forensikkosten, Kosten für Krisenmanagement und Reputationsmassnahmen, Rechtsschutz und einer Erweiterung bei Cybererpressung.

Alexander Tlili, Underwriter Financial Lines Professional Indemnity & Cyber, Zurich Schweiz	Christian Zeller, Leiter IT Governance, Risk Management & Compliance, Schweizerische Mobiliarversicherungsgesellschaft	Alexandre Horvath, Cyber-Experte, Allianz Suisse
Mit der zunehmenden Digitalisierung steigt das Risiko einer Cyberattacke. Die Prozesse sind vermehrt automatisiert und Daten werden hauptsächlich digital gespeichert, wie dies beispielsweise beim Cloud-Computing der Fall ist. Cybersecurity-Massnahmen sind Reaktionen auf neue Trends, sie garantieren aber keinen Schutz.	Die Bedrohungslage im Cybersecurity-Umfeld hat in den letzten Jahren stetig zugenommen und wird weiter zunehmen. Die technischen Massnahmen der IT-Sicherheit greifen, müssen aber laufend ausgebaut und auf immer ausgefeiltere Methoden hin konzipiert werden. Fakt ist: Der Mensch bleibt der Schlüssel einer guten Sicherheit.	Durch die zunehmende Vernetzung der Wirtschaft werden Unternehmen immer anfälliger für Cyberattacken. Es drohen Schäden in Millionenhöhe, Imageverluste und sogar ein existenzgefährdender Betriebsunterbruch. Cyberkriminalität ist eine unterschätzte Gefahr: Weniger als zehn Prozent der Unternehmen verfügen über eine Cyber-Versicherung.
HR-Daten sind Personendaten und unterliegen dem Datenschutzrecht. Die regulatorischen Vorschriften werden immer strenger, ein umfassender Schutz von sensiblen Daten ist daher unerlässlich. Grundsätzlich sind zwei Risiken zu erwähnen: Innerhalb des Unternehmens können durch operative Fehler ungewollt Daten an Dritte versendet werden. Ausserhalb des Unternehmens droht Gefahr durch Hacker, die gezielt in HR-Systeme eindringen.	HR-Daten sind im Allgemeinen beliebte Angriffsziele von Hackern, welche diese Daten für verschiedenste Zwecke nutzen könnten. Die grösste Angriffsfläche bieten jedoch immer noch Menschen, die mit Zugriff auf solch sensitive Daten zu wenig achtsam umgehen.	Grösster Angriffspunkt sind infizierte Lebensläufe von potenziellen Mitarbeitenden mittels Malware, welche vortäuschen, legitim zu sein, aber in Wahrheit das Netzwerk infiltrieren und sich Zugriff auf sensible Daten verschaffen.
Fachleute sind sehr unterschiedlich auf die Risiken von Cyberattacken sensibilisiert. Insbesondere KMU fehlen häufig die Ressourcen, um Mitarbeitende im Umgang mit Risiken im Datenschutz und der Cybersecurity gezielt zu schulen.	Unsere HR-Fachleute werden laufend im Umgang mit sensitiven Daten geschult und sind sich der damit verbundenen Verantwortung durchaus bewusst. So werden Dossiers, die über Bewerbungsplattformen bei uns eingehen, auf deren Sicherheit überprüft. Schwächen sehe ich, wenn Dossiers über nicht gesicherte Plattformen ins Unternehmen gelangen, etwa, wenn sie per Mail geschickt werden.	HR-Fachleute sind nur zum Teil auf solche Risiken vorbereitet, sei dies durch Schulungen, bei denen sie für dieses Thema sensibilisiert werden, oder durch technische Lösungen.
Eine Cybersecurity-Versicherung allein schützt nicht. Sie ist eine von mehreren Sicherheitsmassnahmen. Eine Absicherung ist eine sinnvolle Ergänzung, um das Restrisiko zu minimieren und die finanziellen Folgen von Cyberkriminalität abzusichern. Zudem erhalten Firmen bei einem Abschluss einer Police den Zugang zu Sicherheitsexperten. Für KMU ohne eigene Rechts- oder IT-Abteilung ist dies sehr nützlich.	Das Internet öffnet leider nicht nur Unternehmen die digitale Tür zur Welt, sondern auch unerwünschten Gästen. Gemäss einer KPMG-Studie wurden 2017 über 80 Prozent der Schweizer Unternehmen Opfer einer Cyberattacke. Eine solche erfolgt in der Regel nach dem Giesskannenprinzip. Das beweisen Mails mit schadhaftem Inhalt, die wahllos an unterschiedlichste Empfänger gesendet werden. Daher benötigt praktisch jedes Unternehmen einen auf seine Bedürfnisse zugeschnittenen Versicherungsschutz gegen Cyberrisiken.	Da das Risiko immer grösser wird, macht es für jedes Unternehmen Sinn, eine Cybersecurity-Versicherung abzuschliessen. Viele Angebote sind vor allem auf Grossbetriebe zugeschnitten, die über mehr Ressourcen, Fachexpertise und somit auch Risikobewusstsein verfügen. Dies zu gewährleisten, ist für kleine und mittlere Unternehmen ungleich schwerer. Deshalb bieten wir nicht nur einen auf die Bedürfnisse von KMU zugeschnittenen Versicherungsschutz, sondern unterstützen sie auch in der Risikoanalyse.
Diese richtet sich an Firmen, die Prozesse automatisieren, Daten hauptsächlich digital speichern und dadurch der Gefahr von Cyberkriminalität ausgesetzt sind. Wir helfen, die Folgen eines Vorfalls zu bewältigen – sei es bei Betriebsunterbruch, Datenverlust oder Schadensersatzforderungen von Kunden und Partnern. Die Versicherungsleistung beinhaltet drei Elemente: Sensibilisierung mittels Beratung und Security Assessment mit Massnahmendialog, Risikotransfer mittels Cyberpolice zur finanziellen Absicherung, 24/7-Service mit Unterstützung und Hilfestellung bei einem Cybervorfall durch Versicherungs- und IT-Spezialisten sowie Rechtsberatung durch Juristen.	Unsere Versicherungsdeckung ist in Eigen- und Fremdschäden unterteilt. Erstere übernimmt die Kosten für notwendige IT-Experten, für die Datenwiederherstellung sowie die Entfernung oder Reinigung von Schadprogrammen. Zusätzlich können aus dem Ereignis resultierende Ertragsausfälle sowie die Kosten für ein Krisen- oder PR-Management versichert werden. Die Fremdschadendeckung umfasst die Ansprüche Dritter aus der Verletzung des Datenschutzes oder der Geheimhaltungspflicht sowie der Verletzung der Netzwerksicherheit. Als Opfer einer Persönlichkeitsverletzung, bei Online-Mobbing oder bei Kreditkartenmissbrauch wird betroffenen KMU Rechtsschutz gewährt.	Wir bieten ein KMU-Produkt an, das diverse Deckungspakete beinhaltet: Haftpflichtversicherung (Datenschutzverletzungen, Datenverlust, Zweckentfremdung und Ausfall der Funktionalität), Eigenschäden (Wiederherstellung, Diebstahl durch Cyberangriff, Cybererpressung und Schutz bei Datenschutzverfahren), Betriebsunterbruch (Cyberangriff, Datenschutzverletzung und Haftzeit), Krisenmanagement (forensische Dienstleistungen, Informationskosten, Krisenkommunikation und Notfallkosten), Rechtsschutz und E-Crime (Betrug). Für Grossfirmen und bei Spezialbedürfnissen für Cyberdeckungen besteht eine Kooperation mit der Allianz Global Corporate & Speciality.