SCHWACHSTELLE MENSCH
Tipps für mehr Sicherheit **03**

CYBERVERSICHERUNGEN
Präventiv statt reaktiv **06**

CLOUD Was macht eine sichere Cloud aus? **08**

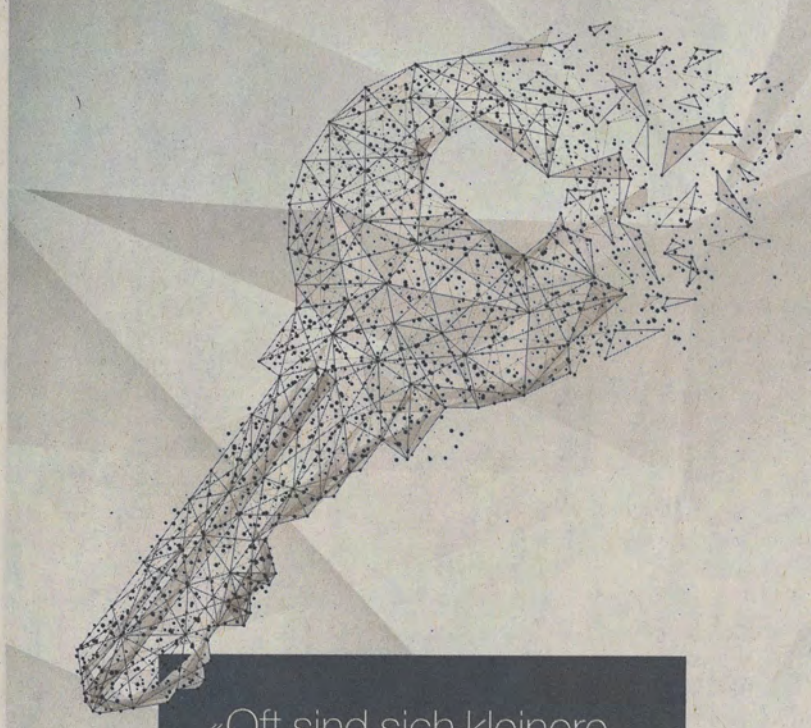
Cyber Security für KMU

Kevin Mitnick
Der berühmteste Hacker der Welt über seine Leidenschaft und seine persönlichen Tipps für Schweizer KMU

FOTO: TOLGA KATAS

NICHT VERPASSEN

Arié Malz fordert einen Grundschutz für KMU. Lesen Sie mehr dazu auf
business-ratgeber.ch



Mitarbeitende müssen E-Mails mit Schadsoftware erkennen

Um die Chancen der Digitalisierung zu nutzen, werden Unternehmensinfrastrukturen, -prozesse und -daten mit dem Internet vernetzt. Dies erhöht die Risiken aus dem Cyberspace und bedingt nebst technischen Sicherheitsmassnahmen die Sensibilisierung der Mitarbeitenden für Schadsoftware.

von Andreas W. Kaelin

«Oft sind sich kleinere Unternehmen der Bedrohung aus den Cyberspace nicht bewusst, was sie zu einer leichten Beute für Hacker macht.»

Erfolgreiche KMU sind stark mit dem Cyberspace vernetzt
Mehr als 98 Prozent der Schweizer Unternehmen sind KMU und bilden somit das Rückgrat der Schweizer Wirtschaft. Um langfristig erfolgreich zu sein, müssen KMU mittels digitaler Technologien Lieferanten, Mitarbeiter und Kunden in den betrieblichen Leistungserstellungsprozess einbeziehen. Dies bedingt eine zunehmende Vernetzung von Unternehmensinfrastrukturen, -prozessen und -daten mit dem Internet und erhöht somit die Risiken aus dem Cyberspace drastisch.

Mehr als ein Drittel der Schweizer KMU waren bereits Opfer von Cyberangriffen
Trotz dieser Tatsache zeigen die im Dezember 2017 publizierten Ergebnisse der Studie von SVV (Schweizerischer Versicherungsverband), SQS (Schweizerische Vereinigung für Qualitäts- und Management-Systeme), ICT Switzerland, ISSS (Information Security Society Switzerland), ISB (Informatiksteuerungsorgan des Bundes) und der Expertenkommission des Bundes, dass sich die Mehrheit der KMU gut bis sehr gut geschützt fühlt und nur vier Prozent der KMU-CEOs Cyberangriffe als existenzgefährdend einschätzen. Hacker richten ihre Cyberattacken vermehrt auf sogenannte «low hanging fruits» - nicht ausreichend geschützte KMU. Die Studie spricht hier eine deutliche Sprache: Rund ein Drittel der KMU waren schon einmal von Viren oder Trojanern betroffen. Auch Datenverlust und Erpressung übers Netz kamen bei fünf Prozent der befragten Unternehmen schon vor.

Andreas W. Kaelin
Geschäftsführer ICTswitzerland, Präsident ICT-Berufsbildung Schweiz

Besorgniserregend – horrende Zunahme von Angriffen mit Erpressungssoftware
Der Global Threat Intelligence Report von NTT Security zeigt auf, dass im Jahr 2017 die Angriffe mit Ransomware um 350 Prozent zugenommen haben. Diese Verschlüsselungstrojaner, auch Kryptoware oder Erpressungstrojaner genannt, sind eine Form von Schadprogrammen, die meist über E-Mails oder gehackte Websites in Systeme eindringen. Befallene Netzwerke und Daten sind für die Nutzer nicht mehr zugänglich. Stattdessen sehen sie eine Bildschirmnachricht, die sie auffordert, ein Lösegeld - meist in Bitcoin - zu bezahlen. Erst nach der Bezahlung geben die Hacker die Daten wieder frei. So verursachen diese Trojaner grosse Schäden in KMU, von denen folglich die ganze Schweiz betroffen ist. ■

Folgen Sie uns MediaplanetSwitzerland @MediaplanetCH @mediaplanetch MediaplanetCH mediaplanetch

Managing Director: **Fredrik Colfach** Produktions- und Redaktionsleitung: **Philipp Steiner** Layout und Bildbearbeitung: **Aline Hafen** Project Manager: **Thuy Dung Le** Business Developer: **Sepideh Baradaran**
Kontaktdaten Tel: **+41 (0)43 540 73 00** E-mail: **redaktion.ch@mediaplanet.com** Fotos: **iStock/ZVG** Druck: **DZZ Druckzentrum Zürich AG** Distribution: **Tages-Anzeiger**

Schweizer KMU bleiben von der Cyberkriminalität nicht verschont

Laut den Ergebnissen einer Umfrage der Wirtschaftsprüfungsgesellschaft KPMG wurden knapp neun von zehn Firmen in den letzten zwölf Monaten Opfer von Angriffen.

von Roland Rupp

Über 380000 verschiedene Schadprogramme warten täglich auf Opfer, schlüpfen durch Sicherheitslücken in Betriebssystemen und Internet-Browsern oder infizieren Websites. Wenn Software-Updates und Virenscanner installiert und aktualisiert wurden sowie Firewall und starke Passwörter vorhanden sind, bleiben aber die meisten Attacken erfolglos. Doch immer wieder schaffen es neueste Schadcode-Versionen an allen Abwehrmassnahmen vorbei, noch bevor ein Sicherheits-Patch als Gegenmassnahme zur Verfügung steht. Immer öfter greifen Kriminelle auch Computer mit Trojanern wie «Petya» an, um auszuspionieren, zu infizieren und zu erpressen.

Was geschieht, wenn Cyberkriminelle in einen Rechner eindringen und ihn kapern, mussten einige KMU bereits leidvoll erfahren: Man will sich abends noch kurz in den PC einwählen und merkt, dass dieser wie von Geisterhand gesteuert wird. Nach einem Neustart ist das ganze Netzwerk blockiert und alle Dateien sind verschlüsselt. Die Freigabe erfolge erst nach Überweisung eines Lösegelds in der Kryptowährung Bitcoin, lautet die Botschaft auf dem gesperrten Bildschirm. Die Höhe des Lösegeldes ist dann ganz unterschiedlich von mehreren Hundert bis mehreren Tausend Franken.

Die Konsequenz: Die Firmendaten können zwar dank Back-ups auch ohne Lösegeldzahlung gerettet werden, aber der Betrieb ist natürlich vorübergehend nicht mehr gewährleistet.

Schwachstelle Mensch

Die grösste Schwachstelle im System ist der Mensch und genau darauf zielen natürlich Cyberkriminelle. Ein Klick auf einen infizierten E-Mail-Anhang mit dem Betreff «Offertanfrage» oder «Bewerbungsmappe» schleust den Krypto-

Roland M. Rupp
Leiter der Geschäftsstelle SKV (Schweizer KMU Verband)

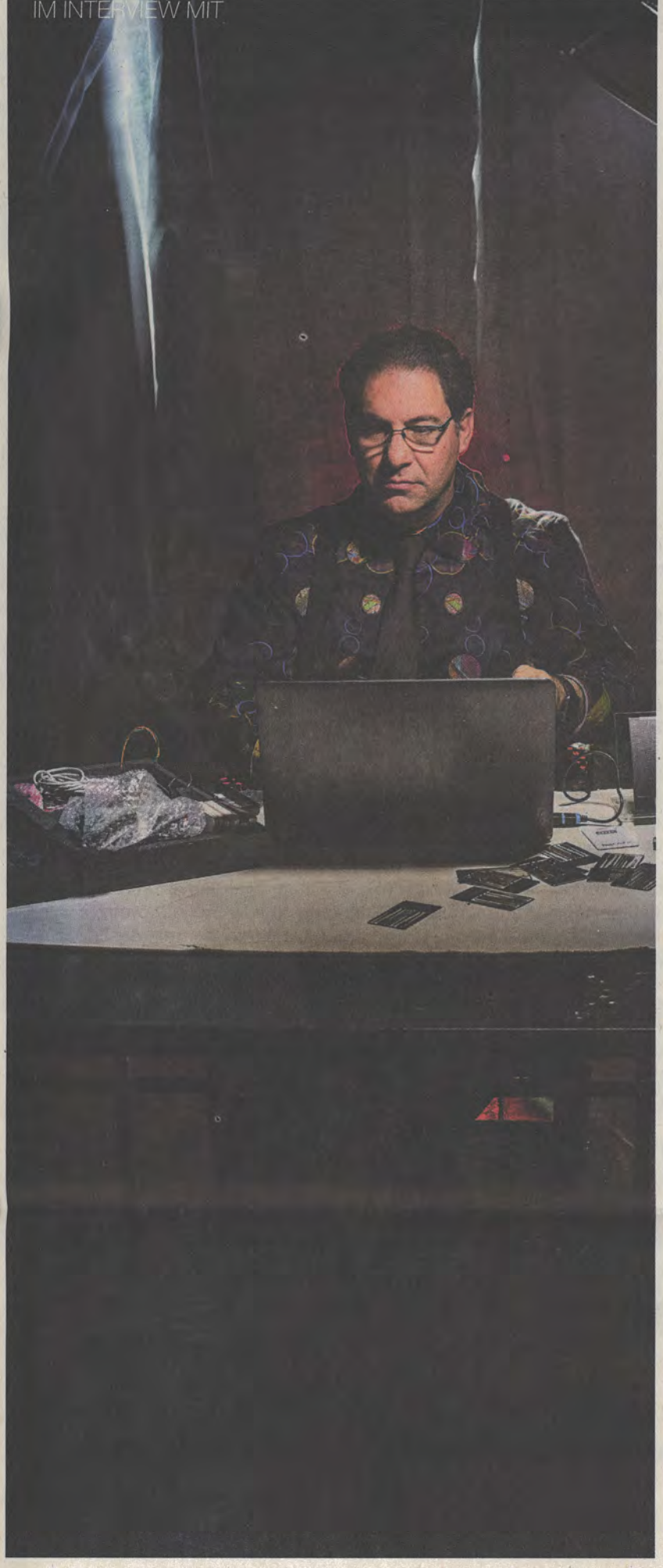
trojaner ins Netzwerk der Firma. Diese Cyberangriffe sind für die betroffenen Unternehmen bei Weitem nicht folgenlos: Bei mehr als der Hälfte (56 Prozent) kam es zu einer Unterbrechung der Geschäftstätigkeit. Zudem hatten mehr als ein Drittel (36 Prozent) finanzielle Verluste zu beklagen.

In nur fünf Jahren hat sich die Zahl der Meldungen bezüglich Cyberkriminalität beinahe verdreifacht. Gingen 2011 beim Bundesamt für Polizei (Fedpol) noch 5330 Meldungen im Bereich der Cyberkriminalität ein, waren es 2016 bereits 14033. Über 20 unterschiedliche Cybercrime-Formen listet ein Katalog des Fedpol derzeit auf - vom klassischen Phishing über die Infizierung eines Computers mit Spyware bis zur Bildung sogenannter Botnets.

Risiken erkennen

Eine umfassende Prävention ist unabdingbar und Investitionen in IT-Sicherheit und Risikomanagement sind elementar. Dabei hängt das Konzept vom eigenen IT-Know-how, von den finanziellen Ressourcen und der Firmenstruktur ab. Relevant sind nicht nur technische Massnahmen, sondern auch organisatorische und personelle Aspekte. Die Sensibilisierung und Schulung, also die «Security Awareness», muss jeder Internetnutzer als Basiskenntnis haben. Dass Mails mit unbekanntem Absender nicht einfach geöffnet oder Anhänge gar angeklickt werden, ist ebenso wichtig wie die Erstellung regelmässiger externer Back-ups.

Viele Firmen - vor allem Grossbetriebe - haben bereits umfangreiche Abwehrkonzepte implementiert. Doch nach wie vor unterschätzen Schweizer Unternehmen die Bedrohung durch Cyberkriminalität. Rund 88 Prozent der Firmen wurden in den letzten zwölf Monaten Opfer einer Cyberattacke. Teils mit gravierenden Störungen der Geschäftsprozesse, finanziellen Schäden und womöglich nachhaltigen Reputationseinbussen. Aus diesem Grund sollte man das Thema Cyberschutz nicht allzu lange vor sich herschieben, sondern sich dessen wirklich annehmen. ■



Vier Dinge, die wir vom berühmtesten Hacker der Welt gelernt haben

Fragen Sie den renommierten Computer-Sicherheitsberater Kevin Mitnick und er wird Ihnen sagen, dass sich unter unserer Nase ein stiller Cyber-Krieg entfaltet und jeder – vom Chef eines Fortune-500-Unternehmens mit einem riesigen Netzwerk bis hin zu jeder Person mit einem Smartphone – ist in Gefahr.

von James Diabri

1 Hacker haben sich weiterentwickelt.

«Als ich anfing, war es völlig legal und Hacking war cool. Hacker galten als Wunderkinder», sagt Mitnick. Er erinnert sich, dass «bis heute mein Lieblingshack aller Zeiten der Hack des Drive-in-Schalters von McDonald's war. Das war, als ich noch jung war.» Aber in den letzten paar Jahrzehnten haben sich Hacker von schlauen Teenagern, die auf dem Familien-Computer herumalberten, zu etwas viel Böswilligerem entwickelt.

Und Mitnicks Fastfood-Streich weist auf ein zugrundeliegendes Dilemma in der Cyber-Sicherheit hin. Durch die Zunahme der mit dem Internet verbundenen Technologien müssen nicht mehr nur die offensichtlichen Geräte wie Laptops, Smartphones und Tablets geschützt werden. Jetzt geht es auch um Thermostate, Kühlschränke, Baby-Phones, Überwachungskameras und vieles mehr.

2 Keine Information ist sicher.

Experten sagen voraus, dass anspruchsvolle Hacker bis zum Jahr 2018 eher Menschen als Maschinen ins Visier nehmen werden. Diese Cyberkriminellen sind mit einem sich ständig weiterentwickelnden Arsenal von Angriffsmethoden ausgestattet, die jeden mit einer Internetverbindung in Gefahr bringen.

«Private Informationen sind frei verfügbar, wenn Sie Zugriff auf die richtigen Datenbanken haben, die normalerweise von Informationsbrokern genutzt werden», erklärt Mitnick. Mit diesen Datenbanken können Sie die Sozialversicherungsnummer, das Geburtsdatum, die Adressen und Telefonnummern einer Person abfragen. «Hacker können Zugang zu allem bekommen, wenn sie genug Zeit, Geld und Ressourcen haben.»

3 Siri kann Sie nicht retten.

Eine neue Studie von Cisco legt nahe, dass WLAN und mobile Geräte bis 2020 66 Prozent des IP-Traffics ausmachen werden (2015 waren es 48 Prozent). Viele Verbraucher glauben, dass die Sicherheit durch einfaches Hinzufügen eines Passworts zu einem Gerät gewährleistet ist. Tatsächlich benötigen Hacker keinen physischen Zugriff auf Ihr Telefon, um persönliche Daten zu stehlen oder das Gerät mit Malware zu infizieren.

Um Sicherheitslücken zu vermeiden, empfiehlt Mitnick, einen virtuellen VPN-Dienst (Virtuelles Privates Netzwerk) zu verwenden. «Eine Sache, die die Leute in Betracht ziehen sollten, ist der Erwerb eines VPN-Abonnements, damit sie sich bei Verwendung öffentlicher WLANs sicher verbinden können», erläutert er. «Grundsätzlich ist es so, wenn Sie kein VPN verwenden, wird Ihr Internetverkehr möglicherweise überwacht. Sie könnten gehackt werden, wenn Sie offene drahtlose Netzwerke verwenden!»

4 Eine lukrative Karriere.

Vom Informationssicherheitsverantwortlichen, der das Gesamtbild betrachtet, bis hin zu den Ingenieuren, die sich mit den technischen Details befassen, gibt es eine ständig wachsende Nachfrage nach talentierten Mitarbeitern auf diesem Gebiet – und dieses Talent zahlt sich aus.

Wie wenig wusste der junge Mitnick davon, dass er an der Spitze einer aufkeimenden Branche war. Aber zuerst musste er die US-Regierung davon überzeugen, dass nicht er die Gefahr war. «Ich wurde als Aushängeschild für die neue böse Bedrohung angesehen: Hacker.» Aber heute erkennen intelligente Organisationen, dass «die Wahrheit einfach ist. Man braucht einen Hacker, um einen Hacker zu fangen.»

Jetzt, als CEO von Mitnick Security, wird er von Fortune-500-Unternehmen dafür bezahlt, Mängel in der Internetsicherheit aufzudecken. Er und sein Team «sind nachweislich zu 100 Prozent erfolgreich in der Lage, die Sicherheit eines jeden Systems, für dessen Hacking sie bezahlt werden, zu überwinden, indem sie eine Kombination aus technischen Exploits und Social Engineering einsetzen.» Wie Mitnick erklärt: «Unternehmen beauftragen meine Firma, in ihre Organisationen einzubrechen, um ihre Sicherheit zu testen», erklärt er. «Es ist wie ein Leben in einem Räuberfilm. Was kann einem daran nicht gefallen?» ■

BIOGRAPHIE

Vom gefürchteten Hacker zum geschätzten Security-Experten

von Frank Erdle

Zaubertricks faszinierten ihn schon als Kind – besonders, wenn sie einen technischen Background hatten: Ein Mitschüler weihte Kevin Mitnick in das sogenannte Phreaking ein, das die Manipulation von Telefonverbindungen ermöglicht. Später soll Mitnick einen Highschool-Lehrer mit einer selbstentwickelten Software verblüfft haben, die wie von Geisterhand Passwörter erraten konnte. Konsequenzen hatten diese Missetaten nicht, weil Hacking noch nicht verboten war.

Als 17-Jähriger brach Mitnick in die Telefonzentrale von Pacific Bell ein und landete für drei Monate in einem Erziehungsheim. Kurz danach hackte er sich in das North American Aerospace Defense Command (NORAD) und inspirierte damit die Macher des erfolgreichen Hollywoodfilms «War Games». Auch die IT-Systeme von Fujitsu, Motorola, Nokia und Sun Microsystems knackte der Cybergangster. Seit 1989 vor den Strafbehörden auf der Flucht, wurde Mitnick 1995 vom FBI verhaftet und zu fünf Jahren Gefängnis verdonnert.

Als Hacker wollte er nur auf Sicherheitslücken aufmerksam machen

Im Gegensatz zu 99,9 Prozent seiner Hacker-Kollegen nutzte es Kevin Mitnick jedoch nie aus, dass er auf die Server oder Datenbanken der gehackten Firmen zugreifen konnte: Er wollte lediglich die Sicherheitslücken der IT-Konzerne offenlegen. Mehr als 100 Mal soll er allein in das Netzwerk des Verteidigungsministeriums der Vereinigten Staaten und mehrfach in das Netz der Nationalen Sicherheitsbehörde NSA eingedrungen sein, dessen Überwachungspraktiken 2013 von Edward Snowden blossgestellt wurden.

Heute führt Mitnick ein vergleichsweise bürgerliches Leben: Einst von der IT-Sicherheitsfirma Kaspersky Lab auf Platz 1 der «Berüchtigtsten Hacker aller Zeiten» geführt, firmiert er nun als seriöser Security-Spezialist in den Top 500 des US-Wirtschaftsmagazins «Fortune». Mit seiner Firma Mitnick Security Consulting arbeitet der 54-Jährige für Regierungen und Unternehmen in aller Welt. Kevin und sein Global Ghost Team versprechen, in jedes Firmen- oder Behörden-Netzwerk eindringen zu können – mit einer streng geheimen Kombination aus technischen Exploits und Social Engineering.

Leichtsinnige Mitarbeiter sind die grösste Gefahr

Denn oft ist das schwächste Glied in der IT-Kette weder ein Computer noch ein Programm, sondern der Mensch. Deshalb wünscht sich Mitnick, dass gerade kleine Unternehmen und KMU, die oft wegen ihrer weniger aufwendigen technischen Ausstattung leichter angreifbar sind, das Sicherheitsbewusstsein der Mitarbeiter schärfen. So sollten sie keinesfalls Mail-Anhänge von Absendern öffnen, die ihnen nicht namentlich bekannt sind, da sich dahinter gefährliche Spionage-Software verstecken könne. Ausserdem kämpft der Amerikaner dafür, dass die Menschen lernen, ihre Privatsphäre als Grundrecht zu betrachten, das sie aktiv verteidigen müssen. Der von Behörden gerne vorgebrachte Verweis auf die Bedrohung durch Terroristen werde nur dazu benutzt, die Überwachung zu verstärken.

Kevin Mitnick will die Gesellschaft wachrütteln und gegensteuern – mit Vorträgen auf wichtigen Konferenzen wie dem Risk & Security Forum in Zürich, Interviews und Büchern. Kürzlich erschien das jüngste Werk «Die Kunst der Anonymität im Internet». Darin deckt der Security-Stratege auf, wie sich Unternehmen, Regierungen und kriminelle Hacker Zugriff auf die Daten der Bürger verschaffen. Wie aber schützen sich Firmen vor den Datenkraken? In 16 Kapiteln liefern Mitnick und sein Co-Autor Robert Vamosi zahlreiche Tipps für die Praxis – von der Passwort-Hygiene über effiziente Verschlüsselungs-Tools bis zur Verhinderung raffinierter Ausspähmethoden wie dem Tracking per Mausklick. Hier können selbst internetaffine Unternehmer noch einiges lernen. Und wenn Mitnick den Fall der Darknet-Ikone Ross Ulbricht schildert, der 2017 zu lebenslanger Haft verurteilt wurde, wird die Lektüre zum Thriller. ■

TOP 5 VIDEOS
ZU CYBERSECURITY
AUF YOUTUBE

Nützliches aus dem Netz.

How to be a Hacker

Where is Cybercrime really coming from

Fokus KMU TV Wie gut sind Schweizer KMU gegen Cyber Attacken geschützt

10 Cyber Security Facts

Cyber Security 101

Cyber-Risiken sind eine Management-aufgabe

Mit Cyber-Risiken umzugehen, ist nicht nur eine Aufgabe für die IT-Abteilung, sondern vor allem Chefsache. Sie beginnt mit dem Bewusstsein, dass es diese Risiken gibt und dass sie nicht zu unterschätzen sind.

von Stefan Kühnis

Ob gross oder klein, für jedes Unternehmen gilt: Risikomanagement ist eine strategische Aufgabe. «Es geht darum, die Unternehmensziele möglichst stresssicher zu erreichen, indem die vielen ganz unterschiedlichen Risiken erkannt, analysiert und dann bestmöglich bewirtschaftet werden», sagt Sabrina Hartusch, Global Head of Insurance Risk bei Triumph International und Präsidentin der Schweizerischen Vereinigung der Insurance und Risk Manager (SIRM).

Sabrina Hartusch
Expertin für Risikomanagement und Präsidentin der SIRM Vereinigung

Risiken erkennen und bewirtschaften

Es braucht eine Methodik, mit der Risiken und ihre internen oder externen Quellen und Ursachen entdeckt werden können. Dafür braucht es vor allem ein Bewusstsein, dass es diese Risiken gibt und dass man sie nicht unbedingt immer kennt. «Beispielsweise sind sich viele Unternehmen nicht bewusst, dass rund 30 Prozent der Cyber-Risiken von den eigenen Mitarbeitenden ausgehen», sagt Hartusch. «Das ganze Thema ist sehr unternehmensspezifisch und auch grosse Unternehmen haben oft noch viel Nachholbedarf. Aber auch ein KMU muss ein Risikomanagement betreiben, um weiter agil und im Business zu bleiben. Der Vorteil eines KMU ist es, dass man häufiger näher zusammenarbeitet und kürzere Wege hat.»

Mit Cyber-Risiken tun sich dennoch viele Unternehmen besonders schwer. «Es gibt hier teilweise eine Art subjektiver Unterschätzung der Risiken», sagt Hartusch. «Sie sind nicht gleichermassen greifbar wie beispielsweise ein Feuer oder ein physischer Diebstahl. Damit kommt man zurecht. Doch Cyber-Risiken, obwohl sie ähnlich sind, sind immateriell und ziehen sich wie ein Schleier über das Unternehmen. Man kann selten genau sagen, wo sie sind.» Ihre Empfehlung an KMU ist es deshalb: sich bewusstmachen, was ein Schaden durch Cyber-Risiken für das Unternehmen bedeutet, woher er kommen kann, wie er auftreten kann und dass Externe durchaus ein Interesse daran haben, an Kundendaten, Kompetenzen, Patente oder Prototypen des Unternehmens zu gelangen. «Man muss wissen, welche Kronjuwelen das eigene Unternehmen hat und wie man sie schützen möchte», sagt Hartusch. «Dafür muss man nicht unbedingt viel Geld ausgeben, aber man muss sich mit dem Thema auseinandersetzen, vielleicht auch mithilfe eines externen Beraters.»

Wer kümmert sich darum?

Das Unternehmen muss sich fragen, wer sich um diese Risiken kümmert, wer die Verantwortung übernimmt und wer welche Aufgaben löst. «Vorsorge ist zwar immer besser und versichern kann man nicht alles, aber man sollte auch wissen, wo beispielsweise die Haftpflichtversicherung greift und ob sie noch auf dem aktuellsten Stand ist», sagt Hartusch. «Auch Reputationsschäden, Eigenschäden und Drittschäden sind Themen, über die man sich im Klaren sein sollte. Und das sind keine IT-Themen, sondern Managementaufgaben.»

Sabrina Hartusch betont, dass ein Risikomanagement speziell rund um Cyber-Risiken eine vernetzte Aufgabe ist: «Der Geschäftsführer ist der Lead und muss in der Firma die richtigen Leute zusammenziehen. Der IT-Verantwortliche ist unersetzlich und eine tragende Säule in diesem Komitee. Je nachdem braucht es auch den CFO und den CCO, also den Chief Financial Officer und den Chief Commercial Officer. Dieser Kreis muss sich regelmässig treffen und die Risikokultur dann nach aussen tragen, in die Operations, und mit dem HR zusammen alle Mitarbeitenden schulen und sensibilisieren.» ■

Gunthard Niederbäumer
Dr. sc. nat. ETH, Leiter Schaden- und Rückversicherung, Schweizerischer Versicherungsverband SVV

Betriebe für Cyber-Risiken sensibilisieren

Cyber-Risiken können grossen Schaden anrichten und sind teuer – der Schutz muss gestärkt werden.

von Gunthard Niederbäumer

Cyber-Schäden sowie Schutz und Abwehr gegen Cyber-Risiken verursachen in der Schweiz gesamthaft jährliche Kosten von schätzungsweise 9,5 Milliarden Franken, Tendenz steigend. Für Unternehmen kann ein einzelner Cyber-Vorfall schnell zur existenziellen Bedrohung werden. Der verhältnismässig junge Bereich der Cyber-Risiken stellt auch die Versicherer vor neue Herausforderungen. Eine Aufarbeitung von Grund auf tut Not.

Versicherungsgesellschaften unterstützen Unternehmen in ihrem Risikomanagement, übernehmen deren Risiken und erfüllen dadurch eine Reihe von volkswirtschaftlich wichtigen Aufgaben. Die Betriebe können sich auf ihr Kerngeschäft konzentrieren und nach einem Schadenfall auf die Versicherer zählen. Dadurch können sie sich möglichst rasch wieder ihrem Alltagsgeschäft widmen.

Versicherer vor neuen Herausforderungen

Cyber-Risiken stellen die Versicherer jedoch vor neue Herausforderungen: Die Risiken sind schwer zu berechnen, weil Daten und Erfahrungswerte fehlen. Ausserdem bringt der rasante technologische Fortschritt immer wieder neue Cyber-Risiken hervor. Und: Cyber-Vorfälle haben das Potenzial, erheblichen volkswirtschaftlichen Schaden anzurichten, da sie in der heutigen vernetzten Wirtschaft viele Unternehmen gleichzeitig treffen können.

Eine repräsentative Umfrage im Herbst 2017 hat ergeben, dass die Mehrheit der KMU ungenügend auf einen Cyber-Vorfall vorbereitet ist. Gerade KMU denken oft, dass sie zu klein sind und zu unbedeutend, um für einen Cyber-Angriff interessant zu sein. Verschiedene Cyber-Attacken auf Hotels, Altersheime oder sogar Copyshops beweisen jedoch das Gegenteil: Im Grundsatz ist kein Unternehmen, egal welcher Branche angehörig, vor Cyber-Attacken gefeit.

Versicherbarkeit verbessern

Um den Schutz vor Cyber-Risiken in der Schweiz zu stärken, arbeitet die Versicherungsindustrie sowohl mit verschiedenen Wirtschafts- und IT-Verbänden als auch eng mit den Bundesbehörden zusammen. Die Versicherer haben hierzu auch einen Massnahmenkatalog erarbeitet. Eine der zentralen Massnahmen, die Bund und Versicherer demzufolge in Angriff nehmen sollten, ist die Sensibilisierung der Öffentlichkeit und insbesondere der KMU für die durch Cyber-Risiken ausgehenden Gefahren. Die Einführung von niederschwelligen Mindeststandards in Bezug auf die Cyber-Sicherheit würde auch die Versicherbarkeit der Risiken verbessern. Die Mindeststandards sollten prinzipienbasiert sein und dürfen Unternehmen nicht übermässig belasten. Dazu zählen zum Beispiel die regelmässige Aktualisierung von Antivirenschutz und Firewalls oder die Pflicht zu regelmässigen Backups. Um dem Mangel an Daten und Erfahrungswerten im Bereich Cyber-Risiken zu begegnen, schlagen die Versicherer vor, eine Meldestelle für Cyber-Vorfälle zu prüfen.

Die Privatversicherer unterstützen die «Nationale Strategie zum Schutz vor Cyber-Risiken 2018-2022» des Bundesrats. Sie unterstreicht die Notwendigkeit der Zusammenarbeit von Staat, Gesellschaft und Wirtschaft, um den Herausforderungen durch Cyber-Bedrohungen begegnen und um die Versicherbarkeit bei Cyber-Vorfällen verbessern zu können. ■

KMU brauchen mehr Verständnis für IT-Risiken

KMU unterschätzen die Gefahr aus dem Cyberraum häufig. Dabei ist es einfacher und günstiger, zu agieren, als zu reagieren – also auf IT-Sicherheit zu setzen, statt bloss reaktiv zu handeln.

von Stefan Kühnis

Professionalisierte Angreifer

«Cyber-Angriffe zielen zunehmend auf die Vertraulichkeit von Daten», sagt Malz. «Die Angreifer wollen in ein System eindringen, Daten entwenden und unbemerkt das System wieder verlassen – entweder auf Bestellung oder um die Daten danach zum Verkauf anzubieten.» Diese Angreifer haben es primär auf Geschäftsgeheimnisse oder Kundendaten abgesehen. Andere möchten das Bankkonto des Opfers plündern oder dessen Infrastruktur für weitere Angriffe missbrauchen. Bei DDos-Attacken (Distributed Denial of Service) oder Ransomware wiederum geht es vor allem um Erpressung.

Wer die Angreifer sind, weiss man selten. «Aber wir sehen deutlich, dass sich diese Kreise professionalisieren. Ausserdem finden vermehrt spezifische Angriffe statt», sagt Malz. «Ein Trojaner wird so angepasst, dass der Virenscanner ihn nicht entdeckt und er auf das anzugreifende System ausgerichtet ist. Immer häufiger wird er kein zweites Mal wiederverwendet.»

Arié Malz
Leiter des Sekretariats der Expertengruppe zur Zukunft der Datenbearbeitung und Datensicherheit beim Bund

«Cyber-Angriffe zielen zunehmend auf die Vertraulichkeit von Daten.»

KMU brauchen einen Grundschutz

Bereits durch den Aufbau einer minimalen digitalen Umgebung, zum Beispiel durch ein simples Online-Bestellsystem, wird ein Unternehmen angreifbar. Deshalb braucht es einen IT-Grundschutz, der es den Angreifern bereits viel schwerer macht und an dem die Expertengruppe derzeit arbeitet. Er soll eine Orientierungshilfe sein, wie man die IT-Sicherheit im eigenen Unternehmen pragmatisch und zielgerichtet gestalten kann. Setzt man diesen Grundschutz um, hat man schon viel erreicht. Denn: Mehr IT-Sicherheit bedeutet nicht nur Kosten, sondern eine Investition in die Zukunft und in das Vertrauen der Geschäftspartner. Jedes Unternehmen, das einmal betroffen war, wünscht sich, dass es präventiv gehandelt hätte. «Reaktives Handeln verursacht langfristig den grösseren Schaden und die höheren Kosten», sagt Arié Malz. ■

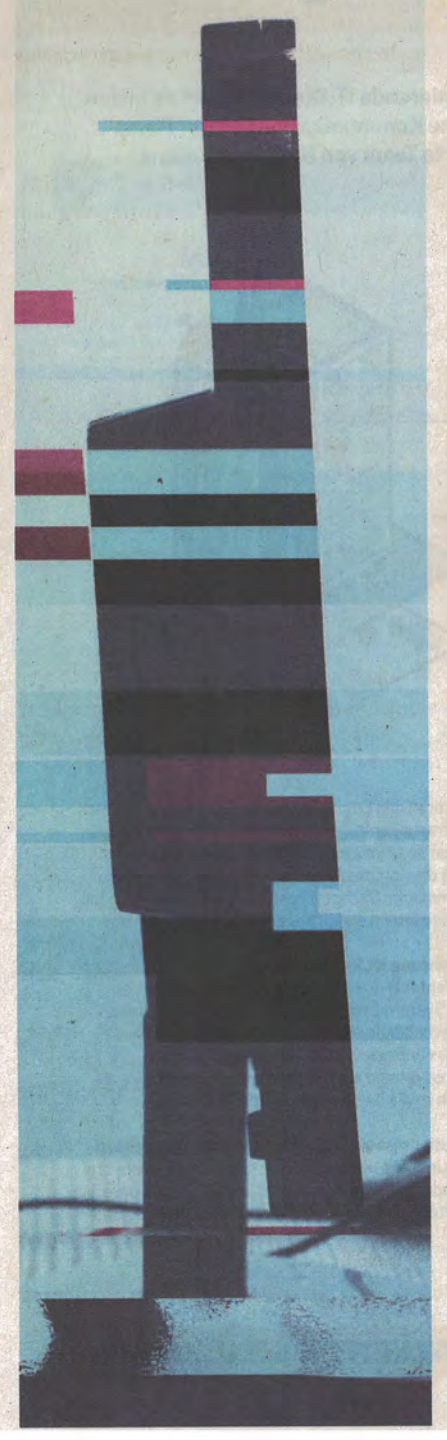
UMFRAGE

In Zusammenarbeit mit Fachverbänden (ICT Switzerland, ISSS, Schweizer Versicherungsverband) und weiteren Stellen im Bund, führte die Expertengruppe Ende 2017 eine repräsentative Umfrage unter KMU aus allen Branchen durch.

14 %
aller Geschäftsleiter haben demnach nicht das Gefühl, einer grossen Gefahr aus dem Cyberraum ausgesetzt zu sein.

58 %
denken, dass sie sehr gut davor geschützt sind.

35 %
wurden bereits einmal erfolgreich angegriffen.



«Jedes Unternehmen kann jederzeit Opfer von Cyberkriminalität werden»

Im Gegensatz zu Grossunternehmen sind sich viele KMU der Gefahr und Tragweite eines Cyberangriffes nicht vollumfänglich bewusst.

von Anna Birkenmeier

Peter Hacker
Cyber Sicherheit & Crypto-Technologie Experte und Keynote Speaker

Peter Hacker – weltweit einer der führenden Experten zu Cybercrime, Cybersecurity und Kryptotechnologie sagt: «Es ist schwierig bis praktisch unmöglich, einen Cyberangriff zu verhindern. Deshalb sollte der Fokus auf Risikominimierung, integriertem Risikomanagement und individuellen Lösungsansätzen liegen.»

Cybersicherheit sollte heute eine absolut fundamentale Bedeutung für Unternehmen haben. Die Herausforderung und die Verantwortung sind eindeutig auf Geschäftsleitungsebene anzusiedeln, und zwar nicht nur wegen potenzieller Vorstands- und Vertragshaftungen. «Wenn man sich den Wert eines Unternehmens anschaut, besteht der oft zwischen 80 und 95 Prozent aus immateriellen Gütern wie zum Beispiel Patenten, Daten, Reputation eines Unternehmens, Brand, Kunden- und Lieferantenbeziehungen oder R&D-Wissen von Mitarbeitern in Bezug auf Werteketten», sagt Peter Hacker. Hauptziel und Fokus eines Cyberkriminellen sind nun genau diese immateriellen Werte. Deshalb muss ihnen Priorität und hoher Schutz gelten. Schätzungen zufolge wurde in der Schweiz schon eines von drei KMU gehackt oder Ziel eines Cyberangriffs. Dazu Peter Hacker: «Cyberkriminelle wissen sehr gut, dass KMU weder über genügende Verteidigungsmittel verfügen, noch individualisierte Strategien haben und oft nur unkoordiniert über den Eigentümer angegangen werden. Dadurch mangelt es häufig an einem guten Risikomanagement, oder es liegt gar nicht vor.»

Es drohen massive Bussen

Das Thema IT-Sicherheit wird in zu vielen KMU denn noch immer als eine nicht unbedingt notwendige Budgetposition beziehungsweise reiner Kostenblock angesehen. Mit der neuen EU-Datenschutz-Grundverordnung, der DSGVO, die am 25. Mai 2018 in Kraft trat, wird sich das nun schlagartig ändern. «Bei einem fahrlässigen Umgang mit Personendaten drohen massive Bussen, und zwar bis zu vier Prozent des weltweiten Umsatzes oder 20 Millionen Euro, je nachdem, welcher Betrag höher ist und nach der Art Verfehlung. Schweizer KMU werden jetzt zum Umdenken gezwungen», ist der Experte überzeugt. Die DSGVO ist zwar eine EU-Verordnung, ihre Reichweite ist jedoch global.

Individualisierte Lösungen sind zentral!

Fundamental ist, dass sich das Unternehmen eine Lösung schafft, die individualisiert ist. «Jedes Unternehmen hat differenzierte Werte, die für Cyberkriminelle interessant sind. Diese Werte muss man kennen, um sie schützen zu können», so Peter Hacker. Die Risiken müssen also identifiziert, quantifiziert und kontrolliert werden, um dann in Lösungsstrukturen hineingepackt zu werden. «Es reicht nicht, irgendein Sicherheitskonzept zu kopieren, sondern man muss eine individuelle Strategie, IT-Sicherheit und ein individuelles Risiko-Management mit möglichem Risikotransfer (zum Beispiel in der Form von Cyber-Versicherung) erarbeiten und testen.» Schwachpunkte und Sicherheitslücken lassen sich besser mit dem regelmässigen Simulieren (Redteaming) eines konkreten Cyberangriffs identifizieren.

«Schwachpunkte und Sicherheitslücken lassen sich besser mit **Redteaming** eines konkreten Cyberangriffs identifizieren.»

«Früher oder später trifft es jeden»

Dass ein Angriff früher oder später fast jedes KMU treffen wird, ist, laut Hacker, sehr wahrscheinlich. Die Frage sei vielmehr, wann dies passieren wird und wie das Unternehmen darauf vorbereitet ist. Wichtig ist, dass ein Angriff immer ernst genommen wird und dass man sich der Konsequenzen, die ein solcher zur Folge haben kann, bewusst ist. «Häufig wird der Fehler gemacht, dass das Thema zu lange verschwiegen beziehungsweise vertuscht wird. Der Prozess, wann und vor allem auch was informiert wird, muss weiter individualisiert sein. Die DSGVO bietet hier einen sehr soliden Anfang. In einem nächsten Schritt müssen auch die internationalen Strafbehörden näher zusammenwachsen. Allzu oft endet die Verfolgung heute noch an der Grenze eines Landes.» ■

Was ist zu beachten für sicheres Cloud-Computing?

Um Cloud-Services sicher zu nutzen, sind ein paar Punkte zu beachten. Es lohnt sich, darüber nachzudenken!

von Umberto Annino

Cloud-Computing, auch als «Cloud-Services» bezeichnet - also Computer-Leistungen aus dem Internet (das mit dem Begriff «Cloud» ersetzt wurde) -, stand lange unter dem pauschalen Verdacht, inhärent unsicher zu sein. Ist das wirklich so, und was sollte man als Leistungsbezüger beachten, damit sichere Cloud-Services genutzt werden können?

Ein sogenannter «Cloud-Service-Provider», kurz CSP, ist letztlich ein Unternehmen, das Computer-Leistungen sozusagen «zur Miete» anbietet. Der Bezug der Leistungen erfolgt dabei über einen Arbeitsplatz-Computer, der am Internet angeschlossen ist. Die bekanntesten Anbieter im internationalen Geschäft sind Microsoft, Google, Amazon - es gibt darüber hinaus unzählige kleinere Anbieter, die ihre Leistungen als Cloud-Service anbieten.

Ganz generell: Bei der Nutzung von Cloud-Services erfolgt die Bereitstellung der Dienstleistung, und damit der Betrieb der dazu benötigten Computer, nicht mehr durch den Leistungsbezüger selber. Damit gibt der Leistungsbezüger die Kontrolle über die «Maschine» ab, und er muss für die Leistung dem CSP vertrauen. Selbstverständlich wird dies vertraglich geregelt, wobei hier eine wichtige Unterscheidung zum sogenannten «Outsourcing» zu machen ist: Bei Cloud-Services handelt es sich nicht um individuelle Verträge zwischen Anbieter und Bezüger, sondern typischerweise um standardisierte, modularisierte Angebote, die über «allgemeine Geschäftsbedingungen» geregelt sind. Entsprechend lohnt es sich, diese Bestimmungen genau zu studieren, um zu wissen, worauf man sich einlässt. Insbesondere Datenschutz und Sicherheit sind im Grund-Angebot möglicherweise nur minimal abgedeckt und müssen durch zusätzliche Dienstleistungen und einen höheren Preis bezogen werden.

Angebot an Cloud-Services und Merkmale zur Sicherheit

Im Wesentlichen lassen sich drei Dienstleistungs-Typen aus der Cloud beziehen: Speicherkapazität - zur Ablage von Daten, zur Erweiterung des eigenen Speicherplatzes, zum einfachen Teilen mit Dritten, zur gemeinsamen Bearbeitung oder auch für Langzeit-Aufbewahrung. Rechenleistung, meist in Form von Software - zur Erweiterung der bestehenden Computerkapazität oder bereits durch Nutzung von Software, die in der Cloud betrieben wird; typischerweise im Servicemodell «Software as a Service - SaaS». Netzwerk-Kapazität beziehungsweise Übertragungsleistung - Cloud-Services zeichnen sich unter anderem durch eine hoch-kapazitative Anbindung an das Internet aus, entsprechend können diese hohen Netzwerk-Leistungen zur Übermittlung von (grösseren) Datenmengen genutzt werden.

Je «tiefer» das Servicemodell, desto mehr Leistungen müssen durch den Dienstleistungsbezüger erbracht werden.

Umberto Annino
Präsident ISSS – Information Security Society Switzerland, Senior Information Security Officer

Bei «Infrastructure as a Service» wird lediglich die Hardware gemietet - Betriebssystem und Anwendungssoftware (insbesondere deren Aktualisierung) müssen durch den Bezüger abgedeckt werden. Bei «Platform as a Service» sind die Angebote oft sehr unterschiedlich, je nach Anbieter werden bestimmte (sicherheitsbezogene) Dienstleistungen ins Angebotspaket integriert oder eben nicht. Das «Rundumsorglos-Paket» ist meistens «Software as a Service», wobei auch hier die verschiedenen Qualitätsstufen unterschieden werden müssen - Sicherheit sollte nicht vorausgesetzt und impliziert werden, sondern konkret verlangt und mit dem Anbieter vereinbart werden.

Werden personenbezogene Daten in Cloud-Services verarbeitet, so müssen die datenschutz-rechtlichen Bestimmungen eingehalten werden. Sowohl das schweizerische wie auch das europäische Datenschutzgesetz sehen Einschränkungen in der Übertragung und Bearbeitung von personenbezogenen Daten ausserhalb der Schweiz beziehungsweise ausserhalb von Europa vor. Vor allem die grossen, internationalen Anbieter von Cloud-Services betreiben ihre Systeme global - eine geografische Limitierung der Bearbeitung der Daten zum Beispiel auf Europa kostet zusätzlich. Wenn die Daten nur innerhalb der Schweiz bearbeitet werden sollen, wird das Feld der möglichen Anbieter zusätzlich verkleinert.

Cloud-Services werden oft mit mobilen Endgeräten konsumiert - Notebook im Normalfall, immer öfter auch Smartphone und Tablet. Bei der Sicherheit dieser mobilen Geräte, die bei der Nutzung von Cloud-Services entsprechend für geschäftliche Zwecke eingesetzt werden, sind minimale Sicherheitsmassnahmen umzusetzen:

- Einrichten einer starken Zugriffskontrolle mit einem ausreichend langen, nicht erratbaren Passwort. Die Nutzung von biometrischen Zugriffskontrollen wie Fingerabdruck oder Gesichtserkennung bietet je nach Gerät ebenfalls Sicherheit, ein komplexes Passwort ist für einen Angreifer in den meisten Fällen aber noch schwieriger zu beschaffen.
- Besonders wichtig ist die sogenannte «Zwei-Faktor-Authentifizierung» für Anwendungen und Apps - insbesondere für die Cloud-Services. Eine unberechtigte Nutzung kann damit wirksam abgewehrt werden. Achtung bei Wechsel des Mobilgerätes: Stellen Sie sicher, dass Sie die Authentifizierungs-Apps auf das neue Gerät zügeln, bevor Sie das alte Gerät ausser Betrieb nehmen.
- Verschlüsselung des Datenspeichers beziehungsweise des Geräts: Bei einem Diebstahl wird mit dieser Massnahme, in Kombination mit der starken Zugriffskontrolle, eine Nutzung der Daten wirksam verhindert. ■

Sehr nützliche Hilfsmittel zum Thema Sicherheit im Cloud-Computing bietet das deutsche BSI (Bundesamt für Sicherheit in der Informationstechnik) mit der Anleitung «Sichere Nutzung von Cloud-Diensten». Auch der eidgenössische Datenschutzbeauftragte hat Empfehlungen und Hinweise zum Thema Datenschutz und Cloud-Services bereitgestellt. Die «Cloud Security Alliance CSA» stellt ausführliche Ressourcen im Themenbereich Cloud-Computing und Sicherheit zur Verfügung.

BSI www.bsi.bund.de/DE/Themen/DigitaleGesellschaft/CloudComputing/CloudComputing_node.html

EDOEB www.edoeb.admin.ch/edoeb/de/home/datenschutz/Internet_und_Computer/cloud-computing.html

CSA cloudsecurityalliance.org

Let's talk about Cyber Security

Reden ist gut - Handeln ist besser! Wir haben vier Experten befragt, welche Lösungsmöglichkeiten heute zur Verfügung stehen und was zu beachten ist.

Daniel Berning
Stv. Geschäftsführer HEAD IT Solutions GmbH

Warum sind massgeschneiderte Datensicherheitslösungen so wichtig für Unternehmungen?

Es existiert kein perfektes Konzept für eine allgemeine Datensicherheitslösung. Jedes Unternehmen hat andere Arten von Daten und auch die Verarbeitungsart ist von Unternehmen zu Unternehmen unterschiedlich. Deshalb analysieren wir bei HEAD IT Solutions in einem ersten Schritt die Daten und klassifizieren sie, um die richtige Vorgehensweise zu bestimmen. Handelt es sich um unternehmenskritische und -relevante Daten? Müssen sie hochverfügbar sein? Wie schnell muss der Zugriff sein? Dabei spielen Vertraulichkeit, Integrität und Verfügbarkeit der Daten die Hauptrollen.

Welche Vorteile bringen Virtualisierungen für Unternehmen?

Man sagt, dass der Mensch nur circa zehn Prozent seines Gehirns nutzt. In einer rein physischen Serverumgebung ist dies ähnlich, da man die vorhandenen Ressourcen nicht optimal nutzt. Mit der Virtualisierung kann die Hardware viel effizienter genutzt werden, da auf einem Server mehrere virtuelle Maschinen parallel laufen. Die Stromrechnung wird tiefer ausfallen und hochverfügbare Systeme können dadurch gewährleistet werden. Das Unternehmen spart also Zeit, Platz und Geld und steigert gleichzeitig die Produktivität.

Wie kann man eine sichere IT-Infrastruktur gewährleisten?

Das Sicherheitskonzept der IT-Infrastruktur muss stets dynamisch bleiben. Die Gefahren wachsen und verändern sich laufend. So muss auch Ihre Infrastruktur auf aktuellem Stand bleiben. Deshalb ist es für HEAD IT wichtig, stets proaktiv zu bleiben. Zur Grundausstattung für ein KMU gehören sicherlich eine gut eingerichtete Firewall, ein Antivirusprogramm, eine funktionierende Datensicherung sowie der korrekte Einsatz und Umgang mit Passwörtern. Nebst den technischen Aspekten ist auch eine Sensibilisierung der Mitarbeiter enorm wichtig. Auch Zugriffsrechte und Verantwortlichkeiten müssen geregelt sein. ■

Raffael Luthiger
Geschäftsführer Huanga IT Solutions AG

Schweizer Rechenzentren oder ausländische Rechenzentren – wo sind meine Daten sicher?

Bei dieser Frage gibt es verschiedene Gesichtspunkte zu betrachten. Wenn es einem vor allem um die Erreichbarkeit der Daten geht, dann gibt es keine grossen Unterschiede zwischen den verschiedenen Anbietern, da alle ähnliche Produkte einsetzen für den Betrieb der Infrastruktur. Wichtiger wird die Thematik dann, wenn man Daten hat, welche nicht von Personen ausserhalb der Schweiz eingesehen werden dürfen (zum Beispiel Bankdaten oder Krankendaten).

Welche Prozesse können durch Cloud Computing optimiert werden?

Beim typischen Cloud Computing werden die Bereitstellungsprozesse der Anbieter optimiert und standardisiert. Am meisten profitieren dabei die Anbieter von Software, welche im Zusammenspiel mit dem Cloud-Anbieter die Installation/Ausbreitung der Software automatisieren können. Dies kommt dann dem Kunden zugute, da dieser schneller und stabiler seine gewünschte Software bereitgestellt bekommt. Firmen mit grösseren IT-Abteilungen können auch interne Clouds aufbauen und so IT-interne Prozesse optimieren.

Auf was soll man bei der Wahl des Cloud-Anbieters achten?

Es gibt heutzutage viele Cloudanbieter auf dem Markt. Als Basis bieten alle Anbieter virtuelle Server an. Wichtiger ist darum, welche Services die Anbieter auf der Cloud-Infrastruktur drauf anbieten. Gewisse Anbieter stellen individuelle Pakete zusammen, andere haben nur standardisierte Produkte. Bei den Anbietern mit standardisierten Produkten gibt es eine Spanne von 10 bis 2000 Produkten. Es ist darum sinnvoll, diese zusätzlichen Produkte zuerst genauer anzuschauen, bevor man einen Entscheid fällt. ■

Thomas Bergmann
Gründer DIGIRATIS - Schweizer Netzwerk der Digitalen Elite

Herr Bergmann, wie kann man sich vor Cyberattacken schützen?

Das lässt sich leider nicht so einfach beantworten. Der einzige 100-Prozent-Schutz vor Cyberangriffen wäre, das Internet nicht zu nutzen. Ein Leben und Arbeiten ohne Internet ist heute natürlich kaum mehr machbar. Ich rate deshalb zur gesunden Vorsicht im Umgang mit dem World Wide Web. Die grösste Schwachstelle ist nach wie vor der Nutzer selber.

Zu einem umfassenden Schutz können einerseits technische Massnahmen beitragen, andererseits ist das Verhalten des Benutzers von entscheidender Bedeutung. Das gilt auch für Unternehmen. Die Sensibilisierung der Mitarbeitenden bezüglich Cyberschutz ist zentral!

Aus Ihrer Erfahrung: Sind KMU ausreichend gegen Cyberattacken geschützt?

Wie man anhand zahlreicher Beispiele sieht, können Cyberangriffe auch grosse, vermeintlich gut gesicherte Unternehmen treffen. Sicherheitslücken gibt es immer.

Eine neue Umfrage des GFS Zürich zeigt, dass die Schweizer KMU eine relativ hohe Schutzlosigkeit gegenüber der Cyberkriminalität aufweisen und 36 Prozent der KMU bereits von Schadsoftware wie Viren oder Trojanern betroffen waren.

Welche Sicherheitstipps haben Sie für KMU?

Es lohnt sich, in die Sicherheit zu investieren! Daher ist es ratsam, eine externe IT-Firma mit der Installation und Betreibung der PCs zu beauftragen. Gleichzeitig gibt es nicht die eine Lösung - der beste Schutz ist ein Puzzle aus verschiedenen Initiativen: Mitarbeitende sensibilisieren, Daten verschlüsseln, Personal Firewall, Software-Updates, Antiviren-Software installieren. Auf der Website der Melde- und Analysestelle Informationssicherung Melani kann man sich über aktuelle Viren und Würmer schlaumachen. Wichtige Informationen und Lernwerkstätten zum Thema Cyber Security findet man beim Digital Summit für KMU am 28. und 29.8.2018 an der Messe Zürich. ■

Michael Sieber
Vice President Sales & Marketing, QuoVadis Trustlink Schweiz AG, a WISeKey company

Ihr Kerngeschäft ist die Prüfung und Ausstellung von digitalen Identitäten. Weshalb sind digitale Identitäten im Rahmen des Cyberschutzes unerlässlich?

Eine sichere und zuverlässige Identifizierung im Internet ist die Vertrauensbasis jeder Online-Handlung. Nutzer/innen möchten sich zweifelsfrei darauf verlassen können, dass ihre digitale Kommunikation, insbesondere mit sensiblem Inhalt, auch tatsächlich mit dem «richtigen» Empfänger geschieht. Wir prüfen die Identität von Personen, die Echtheit von Angaben von Unternehmen und Maschinen und bestätigen dies mit digitalen Zertifikaten höchster Güte. Durch den Einsatz digitaler Zertifikate schützen sich Unternehmen und Ihre Kunden nicht nur, sie verbessern dadurch auch die Erkennbarkeit und das Benutzererlebnis ihrer eigenen Marke im Internet. Darüber hinaus können Unternehmen dadurch ihre traditionellen und analogen Prozesse, zum Beispiel Unterschriftsprozesse, rechtlich verbindlich digitalisieren und damit signifikante Effizienzvorteile gewinnen.

Wo ist der Einsatz von digitalen Zertifikaten sinnvoll?

Digitale Zertifikate finden ihren Einsatz entlang der gesamten Digitalisierungsstrategie. Sie werden beispielsweise in der Webseiten-Verschlüsselung eingesetzt, womit die Echtheit der Unternehmenswebseite für den Besucher bestätigt wird. Ein anderer häufiger Anwendungsbereich ist die Signierung und Verschlüsselung des E-Mail Verkehrs. Gerade in Zeiten des «Phishings» sind Kunden sensibel und möchten sicherstellen, dass ihre E-Mail-Kommunikation tatsächlich mit dem Gegenüber stattfindet dessen Anschein es hat. Einen weiteren grossen Einsatzbereich sehen wir im Rahmen der Digitalisierung von analogen Unterschriftsprozessen durch elektronische Signaturen, welche durch digitale Zertifikate ermöglicht werden. Unabhängig ob dieser Prozess intern (z. B. HR) oder extern (z. B. Online Kundengewinnung einer Bank) ist, können heute mit einer rechtsgültigen elektronischen Signatur diese Abläufe effizienter, sicherer und für den Endkunden attraktiver gestaltet werden.

Was empfehlen Sie KMU mit begrenzten Ressourcen gegen Cyberrisiken?

Es sollte versucht werden, mit den investierten Ressourcen nicht nur Cyberrisiken vorzubeugen, sondern gleichzeitig auch Wertschöpfung zu ermöglichen, womit ein ROI auf die Investition erzeugt werden kann. Sei es durch die Schaffung eines sicheren neuen digitalen Absatzkanals (z. B. Digital Onboarding für Banken) oder durch Kostenersparnisse aufgrund optimierter intern oder externe Prozesse. ■