VON **BARBARA STEININGER**

Das Beste für Daten? Sichere Käfighaltung!

Die Digitalisierung macht viele **INNOVATIONEN** überhaupt erst möglich, eröffnet aber auch Einfallstore für ungebetene Gäste, wenn Security und sichere Datenhaltung nicht beachtet werden.

RECHENZENTRUM. Seit Ausbruch der Pandemie und forciert auch durch neue Gefährdungslagen werden die Standorte und Betreiber stärker hinterfragt.

FOTO: DEUTSCHE TELEKOM AG

Seine Leute gesund durch die Pandemie und motiviert durch hybride Arbeitswelten bringen, Produkte und Dienstleistungen trotz fragiler Lieferketten und steigender Rohstoffpreise auf den Markt liefern und nun auch noch mit schwer kalkulierbaren Auswirkungen eines Krieges rechnen müssen, das sind gewaltige Herausforderungen. Selten waren Unternehmer und Manager mit ihren Fähigkeiten als Krisenmanager stärker gefordert. Und daneben muss das eigene Geschäft auch noch ethischer und grüner werden.

Bei all diesen großen Aufgaben erwiesen sich die Werkzeuge der Digitalisierung als sehr hilfreich, mitunter sogar „lebensrettend" für Mensch und Geschäft. In der Pandemie wurden die Standards für Teamarbeit neu geschrieben, die Telekomnetze und Rechenzentren liefen als kritische Infrastruktur stabil und zuverlässig.

Peter Lenz, Geschäftsführer von T-Systems in Österreich und der Schweiz, spricht gar von „einer Sternstunde für die IT" (siehe Interview ab Seite 72).

Wie durchgängig und zugleich fragil die digitale Globalisierung ist, offenbaren die massiven Verwerfungen der letzten Wochen – seit dem russischen Angriff auf die Ukraine. Die Digitalisierung eröffnet, so sie unkontrolliert und ungeschützt passiert, auch Flanken, die zum Problem werden können: auch für Unternehmen und Organisationen, die mit dem Krieg nichts zu tun haben.

Welche Konsequenzen die Russland-Sanktionen für die Technologiekonzerne – vom Telekomausrüster bis zum Chiplieferanten fahren große Namen der Industrie ihr Geschäft herunter – haben, ist seriöserweise noch nicht abschätzbar. Betroffen sind vor allem auch die lokalen Niederlassungen ausländischer Konzerne, die deswegen nicht nur in Lieferschwierigkeiten geraten, sondern ihre Rechenzentrumsstandorte verlieren können. SAP bietet ihren Kunden derzeit an, Daten aus den russischen Rechenzentren kostenlos auf andere Clouds „umzuziehen".

Mit dem Konflikt ändert sich auch im Cybersecurity-Bereich die Gefährdungslage. Ukrainische, russische und andere Gruppen sind online aktiv ins Kriegsgeschehen involviert. Neben Propagandagefechten werden mit Überlastungsangriffen (DDoS-Attacken) Server lahmgelegt, aber auch Websites gehackt und mit anderen Inhalten versehen. Der österreichische Securityexperte Robert Herscovici von der Firma TCSS glaubt, dass viele Entwicklungen derzeit noch nicht absehbar sind: „Cybermäßig stehen wir an einer absoluten Zeitenwende. Wir stehen erst am Anfang. Noch laufen sich alle warm." Das Hackerkollektiv Anonymous positioniert sich in dem Krieg auf ukrainischer Seite und erklärte Russland und Unternehmen, die nicht klar Position beziehen, öffentlichkeitswirksam den Krieg. ►

CYBERANGRIFF
Ein Phänomen in Zahlen

12 % der heimischen Unternehmen mit mehr als 50 Beschäftigten geben an, dass sie fast täglich Ransomware-Attacken haben, neun Prozent mehrmals im Monat. Das ergab der jüngste Cybersecurity Report von Deloitte und SORA.

67 % würden bei einem Vorfall zuerst den IT-Dienstleister kontaktieren, nur 38 Prozent würden Polizei und 25 Prozent die Datenschutzbehörde rufen (Ergebnisse aus der selben Umfrage). Die Kunden würden nur 14 Prozent kontaktieren. Das kollektive Ziel: öffentliche Blößen zu vermeiden.

20 -mal pro Sekunde versuchten Erpresser im letzten Jahr, ihre Schadsoftsoftware in die Systeme zu schleusen, hat der Dienstleister Atlas VPN gemessen.

623 Millionen Ransomware-Angriffe wurden 2021 weltweit registriert – 105 Prozent mehr als im Jahr davor. Die meisten Attacken werden auf US-Unternehmen unternommen, auf Platz zwei folgt Deutschland, auf Platz drei Großbritannien, ermittelt Security-Dienstleister SonicWall in seinem Cyber Threat Report.

► Im Gefechtsnebel sind die Unterschiede zwischen Drohgebärden und konkreten Taten, etwa dem Angriff auf die deutsche Rosneft-Tochter, nicht immer gleich auszumachen.

KRIMINELLES TAGESGESCHÄFT. Bedrohlich ist die Lage auch abseits des Krieges, denn die Cybererpressung durch Ransomware-Banden bleibt extrem häufig. Dass die Erpresser allein das Lösegeld im Blick haben, gilt nicht als ausgemacht. Es gibt häufig Schnittmengen zur Cyberspionage, wo im Hintergrund staatliche Angreifer bestimmte Ziele verfolgen – und das wird den Opfern oft erst im Nachhinein klar, wie Rik Boddeus, Attaché der niederländischen Botschaft in Wien, auf einem Security-Kongress unlängst berichtete: „Wir Niederländer mussten erst lernen, dass es nicht in allen Belangen immer gut ist, eine offene Gesellschaft zu sein."

2011 war die niederländische Kleinfirma Diginotar, die Sicherheitszertifikate für Websites ausstellte, ausgerechnet über ihren IT-Dienstleister, der eine Sicherheitssoftware nicht rechtzeitig eingespielt hatte, Opfer eines Hacks geworden – mit weitreichenden Folgen: Über Diginotar wurden Sicherheitszertifikate ausgestellt, die mit Schadcode präpariert waren und zu Spionagezwecken genutzt wurden.

Der GAU in Holland führte zu jahrelangen Schockwellen im Netz und laut Boddeus dazu, dass die Behörden die lokale Unternehmenslandschaft komplett neu bewerteten. „Es sind nicht immer nur die großen, sichtbaren Unternehmen, die relevant sind. Oft sind auch Klein- oder Kleinstfirmen strategisch wichtig für die nationale Sicherheit", sagt Boddeus. Die niederländische Cybersecurity-Strategie wurde neu geschrieben und schließt heute auch KMU ein.

Ippolito Forni, Analyst bei Eclectic-IQ, studiert die Bedrohungslagen seit Jahrzehnten und beschreibt die jüngsten Entwicklungen: „Erpresser sehen sich oft Wochen und Monate unbemerkt in einem Firmennetzwerk um. Sie wollen ihre Opfer verstehen, wissen, wo die Kronjuwelen sind und wie hoch sie ihre Forderungen taxieren können." Die Moden und Methoden werden laufend angepasst: War vor der Pandemie häufig „Big Game Hunting" zu beobachten, also die Erpressung großer und mutmaßlich lukrativer Unternehmen und Organisationen, zeichnet sich seit 2020 eine Entwicklung der „Double Extortion" ab, eine perfide Form von Zweitverwertung. Forni: „Wir beobachten nicht nur die Erpressung von Lösegeld. Im Nachgang werden die gestohlenen Daten oft auch online angeboten und verkauft."

In Deutschland wird der jährliche Schaden durch Diebstahl, Spionage und Sabotage auf über 220 Milliarden Euro taxiert. Selbst wenn Österreich weniger als ein Zehntel dessen haben sollte, ist das ein immenser Schaden. Die Dunkelziffer der erpressten Unternehmen ist auch in Österreich hoch, nur ein Bruchteil wird den Ermittlungsbehörden gemeldet. Securityexperten beobachten, dass die Bedrohungslage gern unterschätzt wird. Ist der Wissensstand um die Problematik zwar höher als früher, wird die individuelle Lage gern verklärt, nach dem Motto: Österreich ist ein kleines Land, das eigene Unternehmen zu unwichtig, um „interessant" zu sein. Ein Trugschluss, dem sich österreichische Unternehmer noch immer gerne hingeben.

„Die Awareness ist in den Ländern mit starken Geheimdiensten traditionell stärker ausgeprägt, in Europa etwa in Großbritannien und Frankreich," bestätigt auch Claudine Vartian, Managing Partner der Kanzlei DLA Piper Weiss-Tessbach, die schon seit Jahren eine eigene Cybersecurity-Einsatzgruppe hat, die dem globalen Kanzleiverbund zur Verfügung steht und mehr als 1.000 Einsätze weltweit begleitet.

SICHERE INFRASTRUKTUR. Immer mehr Unternehmen und staatliche Organisationen versuchen, in der Datenhaltung mehr Unabhängigkeit von US-Anbietern zu erreichen. Ein Konzept dabei ist, die Infrastruktur der Amerikaner zu nutzen, sie aber technisch unter die Verwaltung lokaler Treuhänder zu stellen. In der EU werden Cloud-Projekte derzeit stark gefördert.

CYBERKRIMINELLE. Die Erpressung gehört zum einträglichsten kriminellen Geschäft, Banden haben eine „beeindruckende" Wertschöpfungskette aufgebaut. Auch hier wird unmittelbar auf Entwicklungen in der Wirtschaft reagiert: Cyberexperten der Allianz Versicherung rechnen damit, dass Angriffe auf globale Lieferketten der „nächste Trend" sind.

HOMEOFFICE. Drei von vier Führungspersonen (konkret 77 Prozent in Unternehmen mit mehr als 50 Beschäftigten), gingen in einer Deloitte-SORA-Umfrage davon aus, dass die Bedrohung durch Cyberrisiken im Homeoffice „deutlich" oder „eher größer" ist als bei Arbeit im Büro. Die Beschäftigten selbst beurteilten sich mit 55 Prozent etwas weniger gefährdet.

„Wir beobachten nicht nur die Erpressung von Lösegeld. Die gestohlenen Daten werden oft online angeboten und verkauft."

IPPOLITO FORNI
ECLECTIC IQ

FOTOS: DEUTSCHE TELEKOM AG, ISTOCKPHOTO (2), BOP MULDER PHOTOGRAPHY 2016

Neben den forensischen Aufräumarbeiten sind die juristischen Fallstricke nicht zu unterschätzen, weiß die Juristin: „Die Gesetzeslagen für den Verlust von Kunden- oder Mitarbeiterdaten sind weltweit unterschiedlich. Empfindliche Bußgelder und Klagen können drohen."

Die Kanzlei war 2016 selbst Opfer einer Ransomware-Attacke und konnte mithilfe britischer und amerikanischer Beratungsfirmen die Spuren zurückverfolgen, die die Angreifer auf Hunderten Rechnern hinterlassen hatten. Die Malware war über einen unsicheren Rechner der ukrainischen Gehaltsabrechnungsfirma ins System gekommen. Nach zehn Tagen waren die Systeme wieder hergestellt, Klientendaten kamen nicht abhanden.

SICHERE CLOUDS. Die Pandemie und zuletzt die Kriegsgeschehnisse haben die Lieferkettenproblematik auch in der Beschaffung digitaler Dienstleistungen offenbart. Geschäftsführer und IT-Verantwortliche müssen sich jetzt auch mit digitalen Lieferengpässen beschäftigen und klopfen ihre Sourcing-Strategien grundsätzlich ab.

Die Datenverarbeitung und -haltung muss dabei nicht nur effizient und skalierbar sein, sie muss auch sicher und grün sein. Standorte und Betrieb von Rechenzentren werden unter diesen Aspekten neu bewertet – und eine Entwicklung scheint sich nachhaltig abzuzeichnen: Europa soll im Wettbewerb mit den US-amerikanischen Anbietern gestärkt werden. Zum einen sollen nach dem „Airbus-Modell" länderübergreifende Cloud-Infrastrukturen in Europa aufgebaut, zum anderen die außereuropäischen Anbieter zu neuen Konzessionen verpflichtet werden.

Mehr europäische Souveränität auch in der Datenwirtschaft ist politisch ein klar deklariertes Ziel. Die deutsche Regierung hat unlängst eine Dreiviertelmilliarde Euro für die Unterstützung solcher Cloud-Initiativen freigegeben, um Industrie und Mittelstand hier autonomer zu machen und den Unternehmen mehr Auswahl an die Hand zu geben als Big Tech aus den USA. T

TO-DO-LISTE
Reagieren auf Cyberattacken

AWARENESS. Bewusstseinsbildung und Risikoeinschätzung in eigener Sache sind die beste Vorbereitung: Elementar ist hier die Definition der für den Betrieb sensibelsten und kritischsten Daten („Kronjuwelen") und das Erstellen von Sicherungskonzepte dafür. Gern unterschätzt, aber mithin das lohnendste Investment sind aufgeklärte Mitarbeiter, die regelmäßig sensibilisiert werden.

NOTFALLPLÄNE. Wer im Krisenfall zu verständigen ist (Telefonnummern aller internen und externen Experten auf Papier dokumentieren!) und wer zum Krisenteam gehört, muss im Vorfeld festgelegt sein. Wichtig: Die „Rettungskette" ab und zu durchspielen, um Routine zu bekommen. Echte Angriffe kommen immer zur Unzeit, und garantiert nicht zur Bürozeit.

VERHANDLUNGEN. Wer kein funktionierendes Backup hat, das eingespielt werden kann, wird sich auf Verhandlungen einlassen müssen, sollte das aber mithilfe von Experten tun. Wichtig: Fachleute wie Cybersecurity-Experten oder Anwälte bereits im Vorfeld screenen bzw. beauftragen. Zudem müssen alle Schritte dokumentiert werden, um diese rechtlich – und im Fall einer Versicherung – nachweisen zu können.

AUFRÄUMARBEITEN. Es kann Tage, mitunter sogar Wochen dauern, bis ein reibungsloser Betrieb wieder hergestellt werden kann. Die Systeme müssen komplett untersucht und neu aufgesetzt werden, um sicherzustellen, dass die Angreifer sich nicht unbemerkt im Netzwerk zurückgezogen haben.