CYBERSECURITY

Spionage und Erpressung im Netz: Wenn Daten entführt werden

Cyberkriminalität kostet die Schweiz jährlich dreistellige Millionenbeträge. Datenraub und Cyber-Erpressung bedrohen Unternehmen in der Existenz. Es ist Zeit, Abwehrstrategien genauer zu betrachten.

TEXT: FRANK WAGNER

Systemblockade auf dem Rechner, kein Zugriff mehr auf wichtige Dateien – nur noch ein Fenster mit der Lösegeldforderung. Erst im August traf es die auf Augenheilkunde und ästhetische Medizin spezialisierten Pallas Kliniken. Kriminelle hatten per sogenannter Ransomware wichtige Dateien der Firmengruppe verschlüsselt und forderten nun Lösegeld (englisch: ransom). Auch wenn Kundendaten offenbar verschont blieben, entstand doch ein erheblicher Schaden. Der ebenfalls betroffene Schweizer Vergleichsdienst Comparis zahlte schliesslich sogar an seine Erpresser, der Druck war offenbar zu gross. Solch schwere Cyberattacken, aber auch andere Formen von Phishing, Malware, Spyware und Computerviren sind eine ständige Bedrohung, gerade für Unternehmen. Gemäss aktuellen Marktforschungsstudien wurde bereits jedes vierte KMU bereits Opfer eines Angriffs. Nach Berechnungen der Marktforschungsfirma Comparitech beliefen sich die wirtschaftlichen Schäden durch Cyberattacken allein in der Schweiz zuletzt auf 728 Millionen US-Dollar jährlich, Tendenz steigend. Weltweit liegt der Wert bei 318 Milliarden US-Dollar.

KOMPETENZZENTRUM DES BUNDES

Seit 2012 gibt es eine Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS). Verantwortlich für deren koordinierte Umsetzung ist das Nationale Zentrum für Cybersicherheit (National Cyber Security Centre, NCSC). Das NCSC erhält seit Ende 2020 wöchentlich eine dreistellige Anzahl freiwilliger Meldungen; der bisherige Peak lag bei 822 Vorfällen Anfang Februar. Alarmierende Zahlen, zumal die Schweizer Wirtschaft nach Meinung vieler Experten trotz Firewalls, verschlüsselter Verbindungen und Ähnlichem gegen diese Bedrohungen nicht allzu gut gerüstet scheint.

NACHHOLBEDARF BEI ABWEHRSTRATEGIEN

Laut einer Google-Online-Umfrage in der DACH-Region aus 2019 waren 22 Prozent der Schweizer Internetnutzer bereits Opfer von Viren- oder Malware-Angriffen, aber nur zehn Prozent der deutschen. Der europäische Durchschnitt lag bei 16 Prozent. Carlos Casián, Cyber-Risk-Spezialist der Allianz Suisse warnt: «Die besten IT-Sicherheitsvorkehrungen helfen nichts, wenn sie über die Mitarbeitenden umgangen werden.» Casián ist gemeinsam mit Carlo Pugnetti Autor einer aktuellen Studie der Zürcher Hochschule für Angewandte Wissenschaften (ZHAW): «Cyberrisiken und Schweizer KMU». Danach setzten die Täter auf Unachtsamkeit: Ein Phishing-Mail, das beispielsweise einen Anhang oder einen Link enthält, werde immer noch viel zu oft geöffnet beziehungsweise angeklickt. Unbemerkt wird so Schadsoftware installiert.

«CYBERANGRIFFE WERDEN IMMER HÄUFIGER UND RAFFINIERTER»

CYBERVERTEIDIGUNG VERSUS EXTERNES ARBEITEN

Das internationale Marktforschungs- und Beratungsunternehmen ISG stellt in seiner aktuellen Studie «Cyber Security – Solutions and Services. Switzerland 2021» fest: «Aktuell bedeutet die Coronakrise auch weiterhin eine Herausforderung für die IT-Sicherheit, da mit der verstärkten Homeoffice-Nutzung und der dadurch bedingten externen Anbindung der Mitarbeiter die IT-Systeme leichter angreifbar sind.» Diese Herausforderung werde langfristig bestehen bleiben, da auch nach der Pandemie voraussichtlich nicht alle Arbeitsplätze wieder in die Unternehmen zurückverlagert würden. Ein vergleichbares zusätzliches Risiko für die Cybersicherheit sehen Beobachter auch in dem Trend, immer mehr Aufgaben an externe Firmen auszulagern.

VERTEIDIGUNGSSYSTEME AUF AUGENHÖHE

Die bestehenden Vorschriften der Cybersecurity müssen also genau befolgt und stetig weiterentwickelt werden. Cyberkriminelle werden zunehmend schneller neue, raffiniertere und komplexere Wege finden, Verteidigungssysteme zu überwinden. Auch wenn es keine absolute Sicherheit geben kann und spezielle Versicherungen vielfach unverzichtbar werden dürften: Einige oft erstaunlich simple Methoden können dennoch sehr effizient vor Cyberattacken schützen, solange sie nur konsequent umgesetzt werden. Die Websites des NCSC oder der entsprechenden Versicherer geben hier stets aktuelle Tipps für Unternehmen, Institutionen und Privatleute.

UNTERNEHMENSBEITRAG – INTERVIEW

«So bleiben die Einfalltore für Hacker dicht»

Wie können sich KMU effizient gegen Cyber-Attacken und finanzielle Schäden schützen? Die Lösung: der neue Massnahmenkatalog, die Swiss Cyber Defence DNA. Thomas Liechti von MOUNT10 stellt ihn vor.

IM INTERVIEW
Thomas Liechti
CEO
MOUNT10 AG
E: info@mount10.ch
www.mount10.ch

Herr Liechti, im vergangenen Halbjahr registrierte der Bund 85 Prozent mehr Cyberattacken. Worauf ist dieser extreme Anstieg zurückzuführen?

Nicht die Firmen sind unsicherer geworden. Auch die Awareness ist in den vergangenen Jahren gestiegen. Man kann also nur mutmassen: Die einzige mir logisch erscheinende Erklärung ist, dass es anscheinend genügend Firmen gibt, die Lösegeld für ihre Daten bezahlen und damit den Hackern wieder mehr Mittel für neue Angriffe geben. Es muss also ein wirklich grosses Business rund um Schutzgeldzahlungen existieren, dass die Anzahl der Attacken so sehr nach oben schnellen.

Welche Auswirkungen hat dies für die betroffenen Unternehmen? Was wird Ihnen berichtet?

Gerade diejenigen Firmen, die vorher bereits in einer schwierigen Situation waren und dann durch einen Cyberangriff überrascht wurden, sind auf diese Weise in eine noch stärkere Schieflage geraten – mit der Folge, dass nun einige von ihnen nicht mehr am Markt vertreten sind. Das ist leider bereits mehrfach passiert. Besonders tragisch ist dies angesichts der hunderten Arbeitsplätze, welche davon betroffen sind.

Wo muss der Hebel zuerst angesetzt werden?

Wenn es etwas gibt, was essenziell und überlebenswichtig ist, dann ist dies ein robustes Backup. Es braucht ein Sicherheitsnetz, welches im Fall der Fälle tragen muss. Zwar gibt es keine 100-prozentige Sicherheit, jedoch müssen die Daten unveränderbar an irgendeinem sicheren Ort noch vorhanden sein.

Damit es zu diesen Angriffen gar nicht erst kommt, haben Sie für KMU einen Best Practice Leitfaden zusammengestellt …

Ja richtig, grundsätzlich ist die Initiative von MOUNT10 ausgegangen. Letztlich erstellt haben wir die Swiss Cyber Defence DNA aber zusammen mit verschiedenen sehr gewichtigen Playern, wie Microsoft, Trend Micro, HPE, Cisco oder Swisscom. Als eine Non-Profit-Initiative haben wir einen Flyer gestaltet, welcher in guter, einfacher und verständlicher Sprache erklärt, wie man sich effizient gegen Gefahren der Cyber-Kriminalität schützen kann.

Welche Massnahmen sind das?

Diese reichen vom unveränderbaren Backup über den aktuellen Schutz vor Schadsoftware, wie Virenscanner und Firewall, bis hin zur Segmentierung und Absicherung von Netzwerken. Zudem geht es darum, Hard- und Software aktuell zu halten. Ziel ist es aber auch, mittels des Flyers einen Notfallplan im Unternehmen zu erstellen und Notfallprozesse zu definieren.

«WER SICH AN DEN DNA-LEITFADEN HÄLT, WIRD ZUMINDEST NICHT TÖDLICH GETROFFEN»

Oft rennen Unternehmen ihren Angreifern hinterher. Ist es mit diesen Massnahmen möglich, einen Schritt voraus zu sein?

Wir sprechen hier von einem Wettrüsten. Unser Paket ist momentan in einem sehr guten Zustand. Wer sich an diesen Leitfaden hält, wird zumindest nicht tödlich getroffen. Aber es wird in Zukunft weitere Schritte brauchen. Nur so werden wir uns neuen Angriffsszenarien stellen können. Fakt ist: Es gibt kein einziges Mittel, das immer vor einem Hacker schützt.

Schlussendlich sind häufig die Mitarbeitenden die Schwachstellen. Auch sie machen Unternehmen verwundbar, etwa indem sie auf Links in E-Mails klicken, dem grössten Einfallstor von Cyberattacken. Dieses Verhalten kann man nicht komplett unterbinden – eine Schwachstelle, die es immer geben wird.

Wie können Unternehmen ihre Mitarbeitenden noch wachsamer machen?

Es ist eine Gratwanderung zwischen Sensibilisierung und Überdruss. Ein bis zweimal im Jahr sollten die Mitarbeitenden auf diese Gefahren angesprochen werden. Noch häufiger erachte ich als nicht sinnvoll, da dies das Gegenteil bewirken kann.

Raten Sie Unternehmen, Cyberattacken zu versichern?

Es gibt mit Sicherheit Gründe, die für den Abschluss einer Versicherung sprechen. Jedoch kann es nur das Ziel sein, einen finanziellen Schaden abzusichern. Es gibt keine Versicherung die das Überleben oder die Daten schützt oder auch garantiert, diese wieder zurückzubekommen.

Inwieweit stehen Sie Ihren Kunden in der Cyberabwehr noch zur Seite?

Wir, die Trägerschaft, unterstützen unsere Kunden beim Finden des geeigneten Umsetzungspartners. Letztendlich entscheidet aber der Kunde, mit wem er welche Massnahmen umsetzen möchte. Ziel unserer gemeinsamen Initiative ist es, den Nutzen für die KMU, den Schutz vor Erpressung, in den Vordergrund zu stellen.

WEITERE INFORMATIONEN UNTER:
www.kmuschutz.ch

UNTERNEHMENSBEITRAG

Wenn die IT-Sicherheit ausgelagert ist

Für viele Firmen in unserer Region ist es eine grosse Herausforderung, intern genügend IT-Fachwissen bereitzustellen, um ausreichend gegen Cyber-Angriffe geschützt zu sein.

Für Unternehmungen in Regionen ausserhalb der Ballungszentren ist es sehr schwierig, spezifische IT-Fachkräfte zu finden und deren Kosten im Rahmen einer Festanstellung zu tragen. Zudem müssen sich IT-Sicherheitsexperten stets weiterbilden, um auf dem neuesten Stand zu bleiben, was zudem durch die Tatsache erschwert wird, dass sie meist nicht Teil eines grösseren Teams sind und dadurch kein Wissenstransfer stattfindet. Dies sind wesentliche Gründe, wieso heutzutage nicht nur zur Beantwortung verschiedenster Fragestellungen der IT-Sicherheit Beratungsdienstleistungen für einen bestimmten Zeitraum eingekauft, sondern das Thema IT gänzlich ausgelagert wird.

ZUM AUTOR
Christopher Oehri
Executive Director, Advisory IT & Digitalisation
Grant Thornton AG
Claridenstrasse 35 · 8002 Zürich
T: +41 (0)43 960 71 71
E: info@ch.gt.com
grantthornton.ch

Wird die Entscheidung getroffen, IT-Dienstleistungen einzukaufen, stellt sich die Frage, ob der gewählte Anbieter die versprochenen Dienstleistungen in der geforderten Qualität erbringen kann. Um eine angemessene Sicherheit zu gewährleisten, stellen Dienstleistungsanbieter ihren Kunden daher jährlich Prüfberichte zum Beispiel nach den Standards ISAE 3402/3000 zur Verfügung. Solche Prüfberichte geben Auskunft darüber, ob der ausgewählte Anbieter die vertraglich vereinbarten Leistungskriterien erfüllt und dienen gleichzeitig dazu, Anteilseigner oder Aufsichtsorgane mit Informationen hinsichtlich betrieblicher Sicherheit zu versorgen.

Während vor einigen Jahren solche Prüfberichte primär in der Finanzindustrie auf Verlangen von Aufsichtsbehörden erstellt wurden, so ist es heute üblich, dass sehr viele Dienstleistungserbringer mit der Erstellung solcher Berichte nach aussen aufzeigen können, dass sie über ein funktionierendes internes Kontrollsystem verfügen, das die wesentlichen Aspekte der IT-Sicherheit berücksichtigt.

Grant Thornton Schweiz/Liechtenstein unterstützt Sie in allen Themen rund um Ihre IT-Sicherheit!

Grant Thornton

IMPRESSUM

Projektleitung:
Daniel Ronner, dr@xm-solutions.com;
Philipp Rohr, pr@xm-solutions.com

Redaktion:
Mark Krüger, Tobias Lemser, Frank Wagner

V.i.s.d.P.: Nadine Effert

Chief Operating Officer:
Erik Ulrich, eu@xm-solutions.com

Fotos:
depositphotos.com;
Quaritsch Photography - unsplash.com;
freepic, Kiranshastry - flaticon.com und die teilnehmenden Unternehmen

Druck:
DZZ Druckzentrum Zürich AG

Für weitere Informationen wenden Sie sich bitte an:

E: info@xm-solutions.com, T: +41 (0)44 514 22 42

Xmedia Solutions AG
Neustadtstrasse 7
CH – 6003 Luzern

Xmedia Solutions hat sich auf crossmediale Publikationen spezialisiert, welche in Tageszeitungen und auf Online-Portalen veröffentlicht werden.

Inhalte von Unternehmensbeiträgen, Interviews und Gastbeiträgen geben die Meinung der beteiligten Unternehmen wieder.

Die Redaktion ist für die Richtigkeit der Beiträge nicht verantwortlich. Die rechtliche Haftung liegt bei den jeweiligen Unternehmen.

Xmediasolutions

Mehr Informationen unter:
www.xmedia-solutions.com

UNTERNEHMENSBEITRAG – INTERVIEW

«Hybride Arbeitsplätze haben spezielle Ansprüche»

Arbeiten sowohl im Büro als auch im Homeoffice könnte die Zukunft für viele Mitarbeitende sein. Damit dies technisch funktioniert, braucht es das entsprechende Equipment. Doch worauf kommt es dabei an?

Herr Prasovic, seit Pandemiebeginn arbeiten noch immer viele Mitarbeitende von zu Hause. Wird die alte Normalität bald zurückkehren?

Nach mehr als einem Jahr Coronakrise beginnt die Präsenzkultur in Unternehmen zu bröckeln. Hybride Arbeitsplätze haben in dieser Zeit für viele Firmen ihren Wert bewiesen. Mehreren Studien zufolge möchte demnach der grösste Teil der Befragten mindestens zwei Tage von zu Hause arbeiten. Ich bezweifle, dass das «alte Normal» zurückkehren wird. Ganz im Gegenteil: Wir befinden uns in einer neuen Phase der «New-Work-Ära». Nun liegt es an der Führung vieler Unternehmen zur Steigerung der eigenen Attraktivität, hybride Arbeitsplätze zu ermöglichen. Funktionierende, digitale Lösungen sind hierfür die Grundvoraussetzung. Je digitaler die Interaktion, desto wichtiger ist die Gestaltung und das Design der ICT-Umgebung.

Wie sollte ein perfekter hybrider Arbeitsplatz aussehen?

Dies hängt davon ab, ob es etwa ganze Teams oder wenige Mitarbeitende betrifft und ob die Beschäftigten nur noch zu persönlichen Meetings erscheinen oder ganze Teams in zeitlichen Abständen Präsenzpflicht erhalten. Hybride Arbeitsplätze haben den Vorteil, diese nahezu vollständig remote organisieren zu können, sodass die Mitarbeitenden in der Lage sind, ortsunabhängig zu arbeiten. Arbeitgeber wiederum können bestehende Bürostrukturen neugestalten und dank der Flexibilität an Attraktivität gewinnen. Jedoch ist der hybride Arbeitsplatz nicht mit dem Vollzeit-Homeoffice zu verwechseln, sondern soll die Work-Life-Balance fördern.

solutions.9 steht für Cloud-Infrastrukturen. Was braucht es für ein reibungsloses Arbeiten in der Cloud?

Heute versteht man unter einer Cloud einen Verbund mehrerer Server in Form eines online verfügbaren Rechenzentrums. Um auf die Cloud zugreifen zu können, benötigt man nicht nur einen guten Internetprovider. Bei einer Cloud-Only Lösung müssen auch Faktoren wie Agilität, Flexibilität und die richtige Kenngrösse berücksichtigt

«SICHERHEIT BRAUCHT EINEN KOMPETENTEN PARTNER»

werden. Mit dem richtigen IT-Partner erhält man eine stabile Cloud, indem das reibungslose Arbeiten gewährleistet ist. Zumal dauerhaft Kosten gesenkt sowie die Qualität und Verlässlichkeit der eignen IT erhöht werden können, was letztlich konkurrenzfähig macht.

Was ist der grosse Vorteil an einem Pay-as-you-go-Modell?

Dieser liegt darin, dass die Infrastruktur punktuell skalierbar ist. Sprich, werden für Projekte mehr Rechenleistung, Speicherkapazität oder Memory benötigt, können diese für den entsprechenden Projektzeitraum auf den Tag genau bereitgestellt werden. Dies verschwendet keine Ressourcen, spart Hardwarekosten ein und ist zudem ökologisch sinnvoll.

Wie können Sie eine ununterbrochene Datenverfügbarkeit sicherstellen?

Unsere Rechenzentren werden an zwei geografisch getrennten Standorten betrieben, sodass sie hinsichtlich Stromversorgung, Klimatisierung und Netzanbindung vollständig voneinander getrennt und unabhängig laufen. Durch Synchronisation und Spiegelung der Daten wird wiederum eine ununterbrochene Datenverfügbarkeit sichergestellt.

Und in Sachen Datensicherheit? Welche Lösungen bieten Sie an?

Sicherheit braucht einen kompetenten Partner. Dank innovativen Lösungen, Künstlicher Intelligenz und erfahrenen Spezialisten im Team ist es uns mit dem Produkt security.9 möglich, Unternehmen bestmöglich für die Zukunft zu schützen. Von der klassischen Firewall über E-Mail-Security bis hin zum Malware- und Ransomware-Schutz, decken wir sämtliche Services in der IT-Security ab. Dabei gilt es, immer den Spagat zwischen Chancen und Risiken zu meistern. IT-Security sollte Bestandteil jeder IT-Strategie sein und nicht nur als «Nice-to-have» angesehen werden.

Was ist zu tun, um auch von zu Hause sicher arbeiten zu können?

Cyber-Security hat auch zu Hause höchste Priorität. Ein gesichertes VPN bildet dabei die Achillesverse. Zusätzlich lässt sich mittels Multi-Faktor-Authentifizierung, kurz MFA, das Homeoffice noch sicherer gestalten. Ein weiteres Muss sind Endpoint Protection, Policy Enforcement und Monitoring sowie Updates am Betriebssystem oder Anwendungsupdates. Nicht zuletzt sind Security Awareness-Trainings zentral. So werden die Mitarbeitenden auf die Gefahren aufmerksam gemacht, welche etwa durch Phishing-Mails oder Social-Engineering entstehen können.

IM INTERVIEW
Haris Prasovic
Solution Architect & Co-Founder
solutions.9 GmbH
Zürich und Rapperswil-Jona
E: info@solutions9.ch
www.solutions9.ch

solutions.9