«Wie ein Einbrecher, der die Wohnung zertrümmert, aber nichts klaut.»
Markus Wechsler über den Hacker, der seine Metzgerei angriff.

Metzger Wechsler und die Hacker

Cyberkriminelle kosten die Weltwirtschaft Milliarden. Ihre Opfer suchen sie sich überall.

Hannes von Wyl
Florian Kalotay

Markus Wechsler ist ein kräftiger Mann. Man spürt das an seinem Händedruck, mit dem er in seiner Metzgerei im luzernischen Nebikon begrüsst. Wechsler hatte die einstige Dorfmetzg vor acht Jahren übernommen und daraus in akribischer Arbeit einen Betrieb mit vier Filialen und 50 Angestellten aufgebaut.

An einem Donnerstag im letzten Oktober aber ist Markus Wechsler ratlos. Als er um 4.30 Uhr in die Produktionsstätte kommt, geht nichts mehr. Die Auszeichnungswaage, mit der das abgepackte Fleisch vor der Auslieferung an die Filialen und Dorfläden etikettiert wird, kennt keine Preise mehr. Die Lieferscheine, auf dem Computer abgespeichert: weg.

«Dabei sollten wir die Ware um 7 Uhr ausliefern», sagt Wechsler im Pausenraum der Metzgerei, auf dem Tisch vor sich Würste, Brot, Senf, Kaffee. «Aber wir wussten nicht einmal, wie teuer das Nierstück sein soll.» Also ruft der Nebiker Herrn Zimmer an, seinen Vertrauten für alle Computerbelange. Der IT-Spezialist merkt schnell, was das Problem ist: Der Server mit den Geschäftsdaten wurde gehackt, eine Schadsoftware hat die Festplatten verschlüsselt. Auch die Fleischwaagen sind mit dem System verbunden und darum ausgefallen.

Nach ein paar Stunden läuft alles wieder, Wechsler kann um 10 Uhr seine Koteletts und Würste ausliefern. Aber die Lieferscheine, Bestellmengen, Arbeitsrapporte der letzten zwei Wochen sind weg. So lange liegt die letzte Datensicherung zurück. Der Metzger und sein Team müssen alle Daten nach Feierabend nachtragen, über 100 Stunden Zusatzaufwand. «Wir mussten unsere Buchhalterin über Wochen jeden Tag mit Schoggi versorgen, sonst wäre sie uns davongelaufen», sagt Wechsler nur halb im Witz. Kosten des Vorfalls: rund 20 000 Franken.

Tatsächlich werden Cyberattacken für Unternehmen schnell teuer. Im Jahr 2018 schätzten Analysten des Sicherheitspezialisten McAfee die globalen Kosten durch Internetkriminalität auf knapp 600 Milliarden Dollar. Für die nächsten fünf Jahre berechnete die Beratungsfirma Accenture Mehrkosten und Umsatzverluste durch Cyberangriffe von rund 5,2 Billionen Dollar. Das entspricht rund einem Prozent der globalen Wirtschaftsleistung in diesem Zeitraum – Tendenz steigend.

40 Prozent der KMU wurden Opfer von Attacken

Hierzulande beziffert der Schweizerische Versicherungsverband den wirtschaftlichen Schaden auf fast 10 Milliarden Franken pro Jahr. Die Schätzung beruht jedoch auf Zahlen von 2014 und dürfte heute deutlich höher liegen. Dabei sind nicht nur die grossen Banken und Pharmakonzerne betroffen, bei denen man Cyberattacken vermuten würde. Sondern tausende kleine und mittlere Unternehmen (KMU), wie eine Studie des Schweizer IT-Branchenverband ICT Switzerland Ende 2017 aufzeigte. Demnach wurden rund 40 Prozent aller befragten KMU schon Opfer von Viren, Trojanern oder Cybererpressung. Das sind hochgerechnet über 230 000 Betriebe.

«Ich hätte nie gedacht, dass es uns erwischt», sagt Metzger Wechsler. «Andere: ja. Man liest ja viel über solche Dinge in der Zeitung. Aber eine Dorfmetzg?» So denken viele. Einen Tag lahmgelegt zu sein, das halten gemäss der KMU-Studie nur zehn Prozent der >

Gewerbler für eine grosse oder sehr grosse Gefahr. Und nur gerade jeder Fünfundzwanzigste rechnet damit, einen existenzbedrohenden Cyberangriff zu erleben. «Bestimmte KMU haben nach wie vor Aufholbedarf bezüglich Sensibilisierung.» Das sagt Max Klaus, stellvertretender Leiter der Melde- und Analysestelle Informationssicherung (Melani) und damit einer der obersten Cyber-Verantwortlichen des Bundes. Melani ist Anlaufstelle für private Internetnutzer und KMU und hat den Auftrag, die kritischen Infrastrukturen der Schweiz vor Angriffen zu bewahren.

Kleinen und mittleren Unternehmen fehle oft das nötige Personal und die Infrastruktur, um ihre Daten zu schützen, sagt Klaus. Wo grosse Konzerne ihre eigenen IT-Abteilungen unterhalten, sind kleine Betriebe oft auf externe Dienstleister angewiesen. Das bedeutet Zusatzkosten, die viele Firmen scheuen. Nur jedes fünfte befragte Unternehmen hat laut der KMU-Studie Software installiert, die Cyberattacken erkennen kann. «Dabei unterscheiden die meisten Angriffsformen nicht zwischen bestimmten Sektoren oder Unternehmensgrössen», sagt Klaus. Die meisten Unternehmen und staatlichen Behörden seien also den gleichen Bedrohungen ausgesetzt.

Die Gefahr gilt auch für Privatpersonen. Jeder sechste Erwachsene mit einem internetfähigen Gerät hat bereits durch einen Cyberangriff finanziellen Schaden erlitten, aufwändige Reparaturarbeiten durchführen müssen oder grossen emotionalen Stress durchlebt. Das zeigt eine Umfrage von ICT Switzerland vom Februar dieses Jahres.

Im Bewerbungsschreiben war ein Trojaner

Die Methoden, mit denen Cyberkriminelle ihre Opfer angehen, sind dabei genau so vielfältig wie die Ziele, die sie damit verfolgen. Bei Metzger Wechsler gelang es dem Angreifer, über eine ungeschützte Stelle des Routers – das Gerät, das einen Computer mit dem Internet verbindet – einen Trojaner einzuschleusen. Die Schadsoftware verschlüsselte alle Dateien und machte sie für Wechsler unlesbar. «Verschlüsselungstrojaner gehören zu den verbreitetsten Schadprogrammen», sagt Ivan Bütler von der Compass Security AG. Er kennt die Tricks der Hacker ganz genau – denn er ist selber einer. Allerdings einer von den Guten. «Penetration Testing» nennt sich das, was Bütler anbietet: Er versucht im Auftrag von Unternehmen, in deren Systeme einzudringen, um Sicherheitslücken aufzudecken. Details über seine Kunden und deren Sicherheitsvorkehrungen darf Bütler keine nennen. Diskretion ist Teil des Geschäfts. Also erzählt er, wie er für eine SRF-Sendung die Weihnachtsbeleuchtung

> «Als Samichlaus und Schmutzli verkleidet sind wir in den Empfangsbereich des zuständigen Energieunternehmens getreten.»

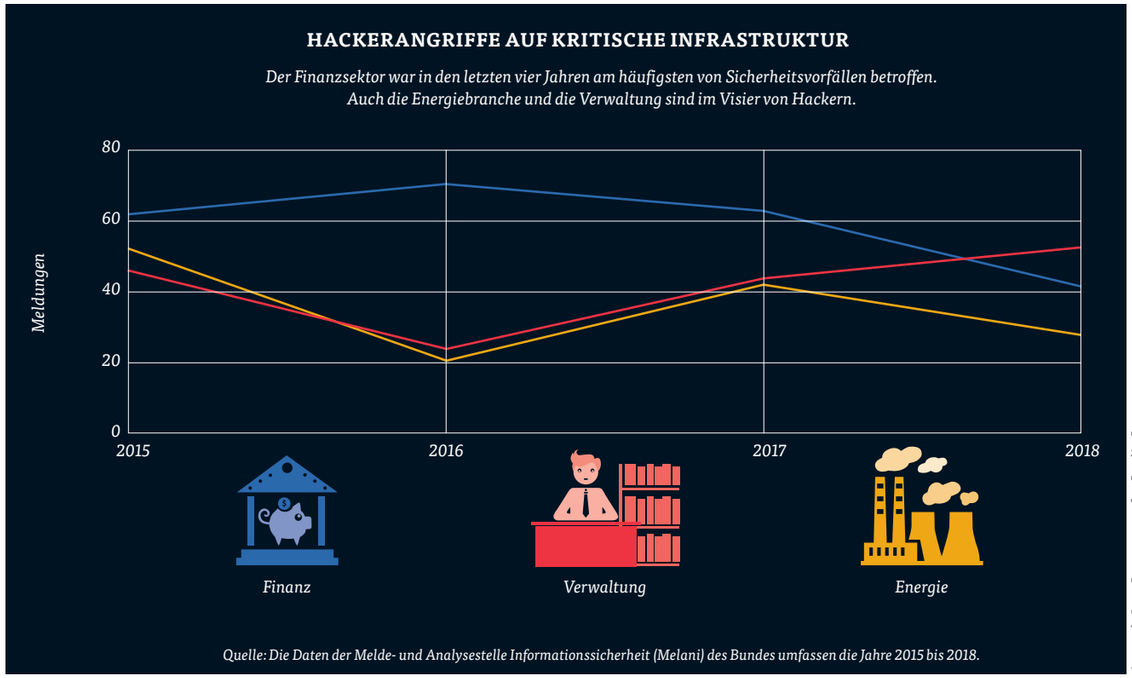
von Liestal BL ausschalten sollte. «Wir haben uns als Samichlaus und Schmutzli verkleidet. So sind wir in den Empfangsbereich des zuständigen Energieunternehmens getreten.» Der Chef habe für alle Mitarbeitenden einen Chlaussack spendiert, sagten sie der Rezeptionistin. «Alles nur ein Ablenkungsmanöver.» Hinter Bütler und seinem Teamkollegen schlich sich ein Drucktechniker ins Gebäude – ebenfalls einer von Bütlers Leuten. Dieser gelangte mit seiner Verkleidung problemlos in die Geschäftsräumlichkeiten. In einem Sitzungszimmer fand er einen ungeschützten Computer. «Der Rest war ein Kinderspiel», sagt Bütler mit einem Lächeln.

«Social Engineering» nennt sich das: Die Umgehung von Sicherheitsvorkehrungen über sozialen Kontakt. «Üblicherweise läuft das virtuell ab», sagt Bütler. Etwa über ein fingiertes Bewerbungsschreiben. So geschehen bei einem Hotelier in der Region Zürich. An einem Abend im letzten November erhielt sein Betriebsleiter ein Bewerbungs-E-Mail und öffnete es umgehend, da das Hotel mit einem Inserat neue Mitarbeitende suchte. «Es war in astreinem Deutsch und wie ein standardmässiges Bewerbungsschreiben verfasst», sagt der Hotelier. Im angehängten Lebenslauf befand sich ein Trojaner, der Doppelklick auf das Word-Dokument aktivierte die Schadsoftware. «Zum Glück waren keine sensiblen Daten betroffen, nur Putzpläne und die Bankettplanung.»

Manchmal wollen die Angreifer mit solchen Aktionen einfach nur Schaden anrichten. Wie bei Metzger Wechsler: «Das war wie ein Einbrecher, der die Wohnung zertrümmert, aber nichts klaut.» Oft stecken hinter Cyberangriffen aber finanzielle Interessen. Auch da kommen oft Verschlüsselungstrojaner zum Einsatz. Nach erfolgter Verschlüsselung melden sich die Angreifer beim Opfer und fordern Lösegeld für die unlesbar gemachten Daten. Meist soll das Geld in der Kryptowährung Bitcoin bezahlt werden. Dabei bleibt der Empfänger des Geldes anonym, was die Strafverfolgung erschwert.

Ins öffentliche Bewusstsein rückte diese «Ransomware» genannte Methode erstmals im Mai 2017, >

Daniel Nussbaumer, Leiter der Abteilung Cybercrime der Kantonspolizei Zürich, kämpft mit seinem Team gegen Internetkriminalität.



Artwork: Jürg Sturzenegger für Studio Sturzenegger

als der Trojaner «Wannacry» weltweit über 230 000 Computer infizierte und Lösegeldzahlungen verlangte. In Grossbritannien waren Spitäler lahmgelegt, in Deutschland Bahnanzeigetafeln betroffen, in Spanien der nationale Telekomanbieter. Die Schweiz kam mit einem blauen Auge davon, hierzulande waren nur gerade 200 Rechner betroffen. Vorausgesetzt, man hatte seine Daten auf einem sicheren Träger gespeichert, konnte man die Lösegeldzahlung mit einer Löschung und Neuinstallation des Systems umgehen.

Grosse Bedrohung durch E-Banking-Trojaner

Weitaus raffinierter sind Schadprogramme, die vom Nutzer unbemerkt Zahlungsverbindungen ins Visier nehmen: die E-Banking-Trojaner. Die Schadprogramme leiten die Verbindung des Nutzers zur Bank über einen Server der Cyberkriminellen. So können die Angreifer Login-Daten abgreifen und erhalten damit Zugriff auf die Konten der Betroffenen. «Für das private Portemonnaie sind E-Banking-Trojaner im Moment die grösste Cyberbedrohung», sagt IT-Spezialist Bütler.

Auch Max Klaus von der Bundesstelle Melani sieht Angriffe auf E-Banking-Verbindungen als grosse Gefahr für die Nutzer. «Die Attacken verlaufen wellenförmig», sagt Klaus. Die jüngste Angriffswelle sei erst vor wenigen Wochen erfolgt.

Die Meldungen über Cyberattacken auf kritische Infrastruktur, die Melani sammelt, zeigt denn auch: Der Schweizer Finanzplatz ist im Vergleich zum Gesundheitswesen oder zur Energiebranche überdurchschnittlich betroffen. «Die meisten Angreifer wollen mit ihrem Tun Geld verdienen», sagt Klaus. Dazu würden sich Phishing-E-Mails gegen E-Banking-Kunden geradezu anbieten: «Diese Angriffe sind relativ einfach durchzuführen und können finanziell lukrativ sein.» Cyberkriminelle nutzen dabei eine besonders perfide Form von Social Engineering. Die Schadsoftware ist in E-Mails versteckt, die angeblich von vertrauenswürdigen Quellen stammt: von der Schweizerischen Post, der SBB, der Swiss Airline – und sogar von der Kantonspolizei Zürich.

Ob er das persönlich nehme? Daniel Nussbaumer, Leiter der Abteilung Cybercrime der Kapo Zürich, lacht. «Natürlich haben wir keine Freude, wenn unser Name für kriminelle Aktivitäten missbraucht wird», sagt er. «Aber wir sind genauso wenig davor gefeit wie

«Obwohl die Sicherheit ständig verbessert wird, steigt die Verwundbarkeit durch die zunehmende Verbreitung von vernetzten Geräten exponentiell.»

andere grosse Unternehmen.» Nussbaumer empfängt in einem kahlen Büro im Hauptsitz des kantonalen Polizeikorps zum Gespräch. Die Atmosphäre in der ehemaligen Militärkaserne an der Sihl will so gar nicht zur modernen Tätigkeit seines Teams passen. Nur der Handvenen-Scanner am Eingangstor zum Gelände verrät, dass hier Polizeiarbeit auf High-Tech trifft.

Spionagevorwürfe gegen Huawei

Die Cybercrime-Abteilung umfasst 15 Polizisten und 30 IT-Forensiker, die je nach Fall in spezifischen Task Forces zusammenarbeiten. «Wir kombinieren klassische Ermittlungstätigkeiten mit den Methoden der Computer-Forensik», sagt Nussbaumer. Der Polizist ermittelt im realen, der IT-Spezialist im virtuellen Leben. Doch Cyber-Ermittlungen sind aufwändig und ressourcenintensiv. «Das Internet bietet Kriminellen die Möglichkeit, anonym und in vielen Ländern gleichzeitig aktiv zu sein», sagt der ehemalige Staatsanwalt für Wirtschaftsdelikte.

Das macht die Ermittlung der Täterschaft schwierig. Umleitungen über verschiedene Server und Zugriff über verborgene Teile des Internets ermöglicht es Cyberkriminellen, ihre Herkunft zu verschleiern. Dennoch gibt es Hinweise, woher viele der Angriffe kommen. «Hacker aus Russland verfolgen oft monetäre Interessen und benutzen Ransomware», sagt Experte Ivan Bütler. Aus Brasilien kämen Wellen von E-Mails, die E-Banking-Trojaner und andere Schadsoftware verbreiteten. Nordkorea, China und die USA seien Hauptakteure in der Wirtschaftsspionage. Zwischen den letzten beiden Ländern tobt seit Trumps Präsidentschaft ein Handelskrieg, der auch den Cyberbereich erfasst hat.

So warnt der amerikanische Geheimdienst davor, Komponenten des chinesischen Herstellers Huawei für die nächste Mobilfunkgeneration einzusetzen. Sie würden der chinesischen Regierung als Einfallstor zur Spionage im Westen dienen. Auch die Nummer zwei der Schweizer Telekombranche, Sunrise, setzt für den Aufbau des 5G-Netzes auf Huawei-Geräte. Der Schweizer Nachrichtendienst NDB erstattete im April dem Bundesrat Bericht über die Gefahr durch Huawei. Chef Jean-Philippe Gaudin soll laut Medienberichten keine Beweise für Spionageaktivitäten via 5G-Technologie des chinesischen Herstellers festgestellt haben.

Foto: Qilai Shen/Bloomberg/Getty Images

Huawei-Gründer Ren Zhengfrei: Die USA stellten seinen Konzern unter Spionageverdacht.

Ivan Bütler ist dennoch überzeugt, dass die grossen Netzausrüster bei ihren Geräten Hintertüren verbauen. Das gelte für chinesische und amerikanische Hersteller gleichermassen. «Vor den Enthüllungen von Edward Snowden hätte man mich einen Verschwörungstheoretiker geschimpft.» Jetzt wisse man aber, welch enormen Aufwand die staatlichen Geheimdienste betreiben, um auch übers Internet private oder sogar geheime Informationen zu beschaffen. «Wir befinden uns in einem eigentlichen Cyber-Wettrüsten», sagt Bütler. Nur sei der Hunger der Gesellschaft nach dem enormen Potenzial von Technologie so gross, dass Sicherheitsbedenken eine geringe Rolle spielten. «Und obwohl die Sicherheit ständig verbessert wird, steigt die Verwundbarkeit durch die zunehmende Verbreitung von vernetzten Geräten exponentiell.»

Metzger Wechsler in Nebikon zumindest macht sich heute mehr Gedanken über die Sicherheit seiner Daten. Nach dem Vorfall im Oktober hatte er in ein automatisches Backup-System investiert, damit alle Bestellungen und Lieferscheine täglich gesichert werden. So kann er bei einem erneuten Angriff alle nötigen Daten einfach wiederherstellen. Nun erhält Wechsler jeden Tag ein E-Mail als Bestätigung für die erfolgreiche Datensicherung. «Das beruhigt. So einen Stress brauche ich nicht mehr.»