«Die Vertraulichkeit der Kundendaten hat höchste Priorität»

Die Methoden von Cyberkriminellen werden immer ausgefeilter. Ob Private, Behörden oder Firmen: Alle können ins Visier von Hackern und Betrügern geraten. Was tut die Bank WIR, um sich und die Daten ihrer Kunden zu schützen?

Das Internet hat neue Formen von Diebstahl, Erpressung oder Sabotage entstehen lassen. Einen Überblick über die Formen der Cyberkriminalität gibt zum Beispiel die Website der schweizerischen Kriminalprävention (skppsc.ch). Das Nationale Zentrum für Cybersicherheit NCSC (ncsc.admin.ch) ist eine Anlaufstelle für Private, Firmen, Behörden und IT-Spezialisten. Das Zentrum macht auf aktuelle Bedrohungen aufmerksam, nimmt Meldungen zu Cybervorfällen entgegen und zeigt auf, wie mit Sicherheitsmassnahmen und Verhaltensregeln viele Cyberrisiken vermieden werden können.

In Zürich ist dieses Jahr in Anwesenheit von Bundesrat Ueli Maurer und Vertretern von rund 80 Banken und Versicherungen der vom NCSC konzipierte Verein Swiss Financial Sector Cyber Security Center – kurz Swiss FS-CSC – gegründet worden. Es handelt sich dabei um die erste spezifische «Branchenlösung» im Kampf gegen Cyberkriminalität. Eines der Ziele: Die Resilienz der Schweizer Finanzindustrie gegenüber Cyberkriminalität weiter zu erhöhen. In der Expertengruppe «Krisenmanagement» der Swiss FS-CSC vertreten ist Michael Ankelin, Chief Information Security Officer der Bank WIR. Als Erfahrungsschatz bringt Ankelin den erfolgreichen Schutz einiger grösserer Schweizer Banken und Versicherungen während eines massiven Angriffs bei einem Outsourcing-Unternehmen sowie Zertifizierungen im Bereich Business Continuity Management und Informationssicherheit ein. Von diesem Engagement profitieren kann natürlich auch die Bank WIR: Durch die aktive Mitarbeit von Michael Ankelin im Swiss Financial FS-CSC erhält die Bank Zugang zu Produkten und Dienstleistungen mit spezifischem Mehrwert für den Finanzsektor, die über die Angebote des NCSC hinausgehen.

Auch das Netzwerk ist wichtiger Bestandteil. «Wir erhalten Unterstützung und Informationen bei systemischen Cyberkrisen und -vorfällen, profitieren vom Austausch und den Lernmöglichkeiten unter Banken und Versicherungen und können uns mit Cyberexpertinnen und -experten von anderen Finanzmarktakteuren und Schweizer Behörden vernetzen», erklärt Michael Ankelin, «die Eidgenössische Finanzmarktaufsicht Finma wird zudem das Swiss FS-CSC beratend unterstützen.»

Wo verorten Sie das grösste operationelle Risiko für die Bank WIR?

Michael Ankelin: Insbesondere die Bedrohungen durch Cyberangriffe, z. B. mit Ransomware, haben in den letzten Monaten massiv zugenommen, weshalb auch wir unsere vielfältigen Massnahmen zur Erhöhung der Resilienz verstärkt haben. Neben den kriminellen Akteuren, die sich immer professioneller und in richtigen Firmenstrukturen organisieren, sind jedoch auch durch den Krieg in der Ukraine – und den damit verbundenen Beteiligungen an den wirtschaftlichen Sanktionen gegen Russland – die Gefahren durch fremdstaatliche bzw. politische Aktivisten gestiegen.

Bild: iStock

Seit Mitte Jahr besteht in der Bank WIR die Möglichkeit, je nach Aufgabenbereich bis zu 50% der Arbeitszeit im Homeoffice zu verbringen. Hat das Ihre Arbeit erschwert?
Statistiken zeigen, dass Cyberkriminelle sehr gezielt Angriffspunkte im Bereich des Homeoffice suchen. Deshalb schützen wir uns natürlich verstärkt in diesem Umfeld mit Massnahmen wie z. B. Anomalien-Erkennungen oder Virenschutz. Da für uns die Vertraulichkeit der Kundendaten die höchste Priorität hat, müssen wir selbstverständlich im Sinne des Datenschutzes auch ein noch grösseres Augenmerk auf angemessene organisatorische Massnahmen legen.

Die Mitarbeitenden jeder Firma gelten als Einfallstor z. B. für Phishing. Was tut die Bank WIR, um ihre Mitarbeitenden zu sensibilisieren?
Die Mitarbeitenden der Bank WIR werden regelmässig durch E-Learnings und praktische Übungen u. a. auch zu diesen Informationssicherheitsthemen geschult.

Wie ist die Bank WIR auf einen Ernstfall vorbereitet?
Wir verlassen uns nicht nur auf unsere sehr gut dokumentierten Notfallprozesse, sondern führen auch im Rahmen des Business Continuity Managements Simulationen von Hackerangriffen durch, in denen wir nicht nur unsere Mitarbeitenden in der IT, sondern auch den Krisenstab und das Management mit einbeziehen.

Die Bank WIR verfolgt eine Cloud-First-Strategie. Was ist darunter zu verstehen und wie sicher sind Clouds?
Bei neuen IT-Infrastrukturen, Plattformen oder Anwendungen prüfen wir zunächst, ob diese auch in der Cloud betrieben werden könnten. Hierzu führen wir Risikoanalysen durch, in denen wir zunächst überprüfen, ob der Cloud Anbieter prinzipiell alle Anforderungen zur Datensicherheit und zum Datenschutz erfüllen kann. Der Massstab sind hier u. a. die Anforderungen der Finanzmarktaufsicht FINMA und der geltenden Datenschutzgesetze. Sind diese erfüllt, prüfen wir den jeweiligen Service, der in die Cloud ausgelagert werden soll.
Mit einem sehr gut qualifizierten Betriebsteam, klar definierten Prozessen sowie Rollen und Verantwortlichkeiten und nicht zuletzt einem durchdachten Architekturkonzept, können Cloud-Infrastrukturen sicher betrieben werden. Die Zeiten, in denen On-Premise-Lösungen im eigenen Rechenzentrum mehr Sicherheit und einen höheren Datenschutz geboten haben, sind in vielen Bereichen bereits vorbei. Cloud-Infrastrukturen bieten heute schon sehr ausgereifte Tools zur Sicherstellung der Compliance und eine sehr hohe Betriebsstabilität. Aber es gibt auch Unternehmen, die wieder eine «back-to-earth»-Strategie verfolgen und den Schritt in die Cloud bereut haben. Oftmals sind das Cloud-Projekte, die zu wenig durchdacht und überhastet umgesetzt wurden. Die Bank WIR agiert hier eher konservativ und in wohl überlegten kleineren Schritten, um ein sicheres Fundament für unsere Zukunft zu erstellen, auf dem wir dann sehr agil neue Produkte entsprechend sicher und nachhaltig anbieten können.

Sind Sie selbst auch schon in eine Phishing-Falle getappt?
Nein, bisher zum Glück nicht. Aber auch ich muss sowohl im beruflichen als auch privaten Umfeld sehr aufmerksam

agieren; die Angriffe werden immer ausgefeilter und schwerer erkennbar.

Zum Team von Michael Ankelin gehört Umut Yilmaz. Neben seiner beruflichen Tätigkeit als Information Security Officer bei der Bank WIR engagiert er sich als Vizepräsident der Liberal-Demokratischen Partei Basel-West. In letzterer Eigenschaft gehört er zu den Autoren der Motion «Stärkung der Cybersicherheit für staatliche Verwaltungen, Firmen und Private in Basel-Stadt», die vom Basler Grossen Rat Anfang Juni angenommen wurde. Anstoss für die Motion gab einerseits die zunehmende Bedrohungslage im Cyberraum, andererseits das – nach Dafürhalten der Motionäre – unzureichende Engagement der Politik auf dem Gebiet Cybersicherheit. Eine Hauptforderung der Motion ist die Schaffung eines kantonalen Kompetenzzentrums für Cybersicherheit – wie man sie schon in Zürich, Schwyz, St. Gallen und Baselland kennt. «Das macht als Ergänzung zur NCSC gerade für Basel Sinn», sagt Umut Yilmaz, «denn Basel ist als Finanzplatz, als bedeutender Standort der Life-Sciences-Industrie und als Güterumschlagsplatz ein attraktives Ziel für Cyberkriminelle.»
Würde die Kompetenzstelle geschaffen, so diente sie als Anlaufstelle für Opfer von Cyberkriminalität und würde erste Hilfsmassnahmen anbieten sowie Sensibilisierungskampagnen durchführen. Die Sammlung und Analyse von Cybervorfällen erlaubte es zudem, die jeweilige Bedrohungslage besser einzuschätzen und so den Unternehmen und der ganzen Bevölkerung eine zusätzliche Sicherheit zu bieten.

Wie beurteilen Sie die gegenwärtige Bedrohungslage?

Umut Yilmaz: Die gegenwärtige allgemeine Bedrohungslage im Cyberraum ist sehr angespannt und auch für die Schweiz erhöht. Die Professionalisierung der Hackerbanden, der Ukraine-Konflikt und das fehlende Sicherheitsbewusstsein sind hierbei zentrale Faktoren. Auch die Statistiken des Nationalen Zentrums für Cybersicherheit NCSC bestätigen die massive Zunahme von Cybervorfällen. Im Jahr 2021 konnte man gegenüber 2020 eine Verdoppelung der Fälle feststellen, und bereits jetzt zählt man für dieses Jahr mehr Vorfälle als letztes Jahr. Obwohl die Schweiz nicht das primäre Angriffsziel von Russland ist, könnte sich die Bedrohungslage durch Spill-over-Effekte, die durch die Angriffe auf die Infrastruktur von anderen europäischen Staaten auch auf die Schweiz überschwappen, weiter verschärfen.

Gibt es Branchen, die besonders gefährdet sind?
Wenn man die diversen Cyberangriffe der letzten Wochen und Monate unter die Lupe nimmt, sieht man, dass Firmen unabhängig von ihrer Branchentätigkeit angegriffen werden. Die Opferliste erstreckt sich über kantonale Verwaltungen, Autohändler, Spitäler, Banken und Versicherungen, Hochschulen oder auch Industriefirmen. Im besonderen Fokus der Hacker stehen KMU und kritische Einrichtungen wie z. B. Spitäler, da sich deren IT-Infrastrukturen oft als grösstes Tummelfeld für die Hacker anbieten.

Spielt die Grösse eines KMU eine Rolle für die Attraktivität bei Hackern?
Natürlich sind Firmen mit einer grösseren Bilanzsumme attraktiver für Angreifer. Die Attraktivität wird jedoch noch mehr von den jeweiligen Daten bestimmt, die eine Firma verarbeitet. Dabei werden die Schwachstellen von IT-Infrastrukturen präzis geplant oder zufällig identifiziert und ausgenutzt. Wenn dann die Möglichkeit für einen Hacker besteht, eine technische oder organisatorische Schwachstelle auszunutzen und Lösegeld zu erpressen, passiert das unabhängig von der Firmengrösse, da man sich primär finanziell bereichern will.

Es wird geschätzt, dass jedes Dritte KMU in der Schweiz schon Opfer eines Hackerangriffs wurde. Täuscht der Eindruck, dass man im Vergleich dazu doch eher selten von erfolgreichen Angriffen hört?
Die Dunkelziffer ist viel höher einzustufen, da gegenwärtig – abgesehen von FINMA-regulierten Unternehmen – keine Meldepflicht von Cybervorfällen besteht. Aus Angst vor Imageschaden gehen viele angegriffene Firmen nicht vor die Presse. Die Politik in Bern diskutiert zurzeit über eine Art Meldepflicht bei kritischen Infrastrukturen, die auch Bussen vorsieht.

Wie schützt man sich am besten als KMU oder als Privatperson?
Eine allgemeine Patentlösung gibt es nicht, da die Anforderungen und die IT-Infrastrukturen der Firmen sich unterscheiden. Es gibt jedoch gewisse technische Grundschutzmassnahmen, welche die Hürde für einen Cyberangriff massiv erhöhen können. Hierzu zählen Offline-Back-ups, Firewallsysteme, Anti-Malware-Schutz, Einspielung von Updates, komplexe Passwörter und insbesondere die Absicherung von exponierten (externen) Zugriffen via Multi-Faktor-Authentifizierung. Nebst den technischen Massnahmen sind wiederkehrende Sensibilisierungs- und Trainingsmassnahmen der Mitarbeitenden essenziell, da in vielen Fällen das Durchdringen in das Firmennetzwerk über eine E-Mail mit schädlichen Links oder Anhängen erfolgt. Hier empfehle ich allen – auch privaten – Benutzern, mit dem Mauszeiger über den Link zu fahren (ohne ihn anzuklicken!) und zu prüfen, wohin der Link in der E-Mail tatsächlich führt.

Wenn «es» passiert ist und man z. B. Erpressern ausgeliefert ist, wie soll man sich verhalten?

Ganz wichtig ist es, für diesen Moment vorbereitet zu sein, indem man Drehbücher skizziert und Notfallprozesse z. B. für einen Ransomware-Fall wiederkehrend trainiert. So kann man im Ernstfall bedachter handeln und weiss, welche Schritte durch wen als Erstes einzuleiten sind. Hat man die Expertise nicht im Haus, sollte man sich Unterstützung z. B. bei externen Spezialisten oder der Anlaufstelle der NCSC holen. Einer Lösegeldforderung sollte man weder als KMU noch als Privatperson nachkommen, da man keine Garantien hat, dass die Daten tatsächlich wieder freigegeben werden.

Was kann der Staat für Firmen und Privatpersonen machen?
Der Staat bzw. die kantonalen Behörden können als Erstanlaufstelle bei einem Cyberangriff die Opfer mit ihrer Expertise unterstützen und beraten. Die Empfehlung von präventiven Schutzmassnahmen und die Darstellung der aktuellen Bedrohungslage können KMU und Privatpersonen ebenfalls unterstützen, um ihre Resilienz zu erhöhen. Im Juni dieses Jahres hat der Grosse Rat von Basel eine von mir mitverfasste Motion angenommen, welche u. a. die Schaffung eines zentralen Cybercrime-Kompetenzzentrums fordert, um primär KMU und Private mit gezielten Massnahmen stärker zu unterstützen. Der Ball liegt jetzt beim Regierungsrat.

Wieso ist es so schwierig, Cyberkriminelle zu packen?
Weil die professionell organisierten Hackerbanden ihre Spuren in den meisten Fällen sehr gut verwischen können und meistens im Ausland sitzen. Durch technische Mittel können sie ihre Identitäten verbergen und leiten die Kommunikation durch viele verschiedene Länder um. Jedoch konnten in der jüngsten Vergangenheit durch die internationale Zusammenarbeit von verschiedenen Behörden grössere Hackerbanden zerschlagen und verhaftet werden. Einen Freischein nicht geschnappt zu werden, hat man als Cyberkrimineller also nicht.

Ist es von Nutzen, wenn Sie als Cybersecurity-Experte über Hackerwissen und -qualitäten verfügen?
Das kann enorm hilfreich sein. Um einen Dieb zu fassen, hilft es ja auch der Polizei, wenn sie wie ein Dieb denkt. Denn wenn man die Angriffsvektoren kennt, kann man auch spezifische Abwehrmassnahmen ableiten und umsetzen. Leider ist die Rekrutierung von guten Cybersicherheitsspezialisten aufgrund des Fachkräftemangels enorm schwierig. Die Schweizer Armee, das NCSC, aber auch private Sicherheitsfirmen kämpfen mit diesem Problem. Die Politik ist auch hier stark gefordert und sollte mit frühzeitigen Massnahmen intervenieren, insbesondere im Bildungswesen. So könnte dieses Problem mittelfristig entschärft werden.

● *Interviews: Daniel Flury*

s-u-p-e-r.ch

Cyberangriffe per E-Mail oder Messenger-Nachrichten nehmen zu. Um die Aufmerksamkeit der Bevölkerung zu fördern, haben das Nationale Zentrum für Cybersicherheit NCSC und die Schweizerische Kriminalprävention SKP gemeinsam mit den kantonalen und städtischen Polizeikorps die nationale Sensibilisierungskampagne s-u-p-e-r.ch zum Thema Cybersicherheit gestartet.

Cyberangriffe erfolgen oftmals per E-Mail oder Nachricht über einen Messenger-Dienst. Cyberkriminelle versuchen potenzielle Opfer in die Falle zu locken, indem sie grosse Gewinne versprechen, ein Erbe eines Unbekannten in Aussicht stellen oder vorgeben, dass der Computer gehackt worden sei. Nicht immer ist der Betrug offensichtlich, denn die Angreifer werden immer geschickter. Häufig verwenden sie psychologische Tricks wie Angst und Zeitdruck oder nutzen die Hektik und Zerstreutheit der Empfängerinnen und Empfänger aus.

Schneller Klick, grosser Schaden
Eine scheinbar harmlose Aktion, wie der Klick auf einen Link oder das Öffnen eines Anhangs, kann zu grossem Schaden führen. Manchmal werden die Kreditkartendaten abgefragt und anschliessend missbraucht. Oder es wird eine Schadsoftware installiert und die Daten werden verschlüsselt und gestohlen. Sowohl für Unternehmen wie auch für Private kann dies existenzbedrohend sein. Die Ermittlungen gestalten sich oft schwierig, da die Kriminellen in der Regel aus dem Ausland operieren.

Abwehr durch Aufmerksamkeit
Mit der nötigen Aufmerksamkeit kann eine betrügerische Nachricht schnell erkannt und Schaden verhindert werden. Es gibt verschiedene Hinweise und Vorgehensarten, die auf einen Cyberangriff hindeuten. Seit Anfang September sensibilisieren das Nationale Zentrum für Cybersicherheit NCSC und die Schweizerische Kriminalprävention SKP gemeinsam mit den kantonalen und städtischen Polizeikorps die Schweizer Bevölkerung für die Erkennung betrügerischer Nachrichten. Auf der Kampagnen-Website s-u-p-e-r.ch werden die wichtigsten Informationen vermittelt. Die Merkmale betrügerischer Nachrichten werden anhand konkreter Beispiele veranschaulicht. Mit einem Quiz lassen sich die erworbenen Fähigkeiten überprüfen. Die Sensibilisierungskampagne dauert bis am 16. Oktober 2022.