«Ein Ende unserer Vertrauensgesellschaft wäre sehr bedauerlich»

In unserem Schwerpunkt-Interview spricht der Schweizer Sicherheitsexperte Christian Folini über Cyberattacken im KI-Zeitalter, minimale Sicherheitsstandards und die Frage, ob auch unsere Abhängigkeit von US-Techgiganten ein Risiko darstellt.

› Das Gespräch führten Pascal Huber und Marco Ratschiller, Fotos: Simon Schwieters

Herr Folini, wer die Medien verfolgt, gewinnt den Eindruck, digitale Kriminalität sei allgegenwärtig. Wie sieht die Realität für Schweizer KMU aus?
Grundsätzlich: Wir sind daran, Gesellschaft, Staat und Wirtschaft zu digitalisieren. Auch KMU funktionieren immer digitaler und damit werden sie immer stärker den Gefahren ausgesetzt. Die Zahlen nehmen also nur schon deshalb zu, weil der Digitalisierungprozess noch längst nicht abgeschlossen ist. Die Angriffsfläche wird schlicht laufend grösser. Wo früher, in der analogen Welt, Waren und Dienstleistungen grösstenteils physisch vor Ort geschaffen wurden, steht heute ein Unternehmen mit seiner ganzen Produktionsstrasse mehr oder weniger vollständig im Netz. Egal, welches Verbrechen begangen wird, es hat heute fast immer eine Cyber-Komponente.

Das erklärt aber vermutlich noch nicht alles?
Nein, zwei weitere Aspekte sind von Bedeutung. Zum einen nehmen auch die Kompetenzen im Umgang mit der Problematik zu. Dies trifft sowohl auf die Nutzer als auch auf die Behörden zu. Vor zehn Jahren wurde man auf vielen Polizeiposten noch mit grossen Augen angeschaut, wenn man ein digitales Verbrechen zur Anzeige bringen wollte. Das hat sich glücklicherweise stark geändert. Einen weiteren Aspekt sehe ich durchaus kritisch: Die Branche operiert sehr gerne mit grossen Zahlen. Swisscom-CEO Christoph Aeschlimann behauptete letztes Jahr in einem Interview mit der NZZ, seine Firma verzeichne monatlich 200 Millionen Cyberangriffe. Nun, diese Zahl ist entweder viel zu klein, wenn man jedes einzelne IP-Päckchen zählt, oder viel zu gross, wenn gezielt gestartete Aktionen gemeint sind. Die Zahl sollte wohl vor allem beeindrucken. Die Branche braucht gewissermassen so eindrückliche Werte: Sicherheit ist ja auch ein Geschäftsmodell.

Also ist jenseits der Schlagzeilen alles halb so wild?
Das dann doch eher nicht. Für einige cyberkriminelle Strategien wie etwa den Bereich der Ransomware-Angriffe gehe ich zwar davon aus, dass die Aktivitäten langsam ein Plateau erreicht haben. Worauf aber jetzt wirklich jedes KMU allergrösste Aufmerksamkeit richten muss, sind sogenannte Deepfakes, also manipulierte Aufnahmen. Die neusten KI-Modelle fälschen Stimmen, Bilder, Videos fraglos täuschend echt. Und das macht Deepfakes gerade für KMU besonders gefährlich. Besonders dann, wenn Prozesse oft nicht exakt definiert sind oder das Vier-Augen-Prinzip nicht sakrosankt ist. Was tut der Angestellte, wenn kurz vor Feierabend der vermeintliche Chef aus den Ferien anruft und eine dringende Überweisung verlangt?

Er macht vermutlich genau das, was ihm aufgetragen wird …
Ohne Vier-Augen-Prinzip droht genau das. Und da ist ja nicht nur die täuschend echte Stimme allein. KI ist Kriminellen auch zunehmend behilflich, die Schwachstellen der Firma zu analysieren. Es werden Profile des Chefs oder von Kaderleuten erstellt. Deren Hobbys, Interessen und Pläne werden ermittelt. Es sind diese Informationen, welche den Deepfakes fatale Glaubwürdigkeit verleihen. Was früher eine aufwendige Recherche nötig machte, erledigt heute ein Computer von A bis Z. Damit lassen sich Angriffe skalieren. Noch bis vor Kurzem war dazu jemand nötig, der Deutsch liest, spricht und versteht; jemand, der sich in der spezifischen KMU-Welt auskennt. Doch diese Arbeit haben inzwischen digitale Helfer übernommen.

Jüngst machte die US-Firma Anthropic damit Schlagzeilen, dass ihr neustes KI-Modell «Claude

Mythos» potenziell so mächtig und gefährlich sei, dass es nur noch ausgewählte Kunden überhaupt erhalten sollen. Droht uns der Kontrollverlust?
Der Angreifer ist immer der Treiber, auf den es zu reagieren gilt. Das war schon immer so. Richtig gefährlich wird es, wenn der Angreifer zu weit voraus ist. Deshalb ist es für Unternehmen so wichtig, am Ball zu bleiben. Bis vor Kurzem wurde – gerade hier in der Schweiz – noch gerne über ungelenke Phishing-Versuche gelacht: Holprige Formulierungen, unzulängliches Deutsch, handwerkliche Fehler. Jetzt erhältst du einen Telefonanruf mit KI-generierter Stimme in perfektem Schweizerdeutsch. Du hast kaum noch eine Chance, den Betrug zu erkennen. Das ist neu – und macht es brisant.

«Bis vor Kurzem wurde noch über Phishing-Mails voller Fehler gelacht. Jetzt spricht KI Schweizerdeutsch.»

Hat Sie das Tempo der Entwicklung überrascht?
Tatsächlich gingen selbst Experten lange davon aus, dass die Kapitalintensität der Branche der qualitativen Verbesserung der KI-Modelle gewisse Grenzen setzt. Dass es ab einem gewissen Zeitpunkt darum gehen würde, auf dem bis dahin erreichten – durchaus beeindruckenden – Intelligenzniveau vor allem die Kosten zu senken. Das ist bisher aber nicht geschehen. Input und Output, also Investitionen und Ergebnisse, nahmen weiter zu. Selbst wenn es in der KI-Branche zu Marktbereinigungen und Konkursen kommen dürfte, wird der heute verfügbare Stand der KI wohl nicht wieder verschwinden.

Müssen wir künftig also allem und jedem misstrauen?
Die Schweiz ist eine Vertrauensgesellschaft. Vertrauen ist ein wichtiger Kitt. Dies gilt gerade auch in unserer Unternehmenskultur. Es wäre ein riesiger Verlust, wenn uns das abhanden käme.

Wie lässt sich das konkret verhindern?
Wer Zahlungen nur mit dem bereits erwähnten Vier-Augen-Prinzip vornimmt und die Prozesse klar definiert, kommt schon relativ weit. Keine einzige Zahlung geht raus, die nicht von zwei Personen autorisiert wurde. Diese Regel gilt ohne Ausnahme, auch für Chefs und Vorgesetzte. Auch wenn es Freitag 18 Uhr ist, respektive gerade dann. Es wird keine Überweisung mehr veranlasst, wenn das zweite Augenpaar schon im Feierabend oder in den Ferien ist.

Schon früher hiess es: Doppelt genäht hält besser.
Die Entsprechung in der digitalen Welt heisst 2-Faktor-Authentifizierung. Das ist die zweite zentrale Sicherheitsmassnahme, die einfach jedes KMU verinnerlicht haben muss. Selbst das bringt nicht die absolute Sicherheit, sorgt aber für markant höhere Hürden bei Angriffsversuchen. Denn so muss man eine Zielperson dazu bringen, neben dem Passwort via PC auch noch einen Handy-Code übers Smartphone preiszugeben.

Stellt grundsätzlich der Mensch oder die Technik das grössere Risiko dar?
Eine gute Frage. Das Tragische ist, dass im Zuge der Digitalisierung viel Verantwortung zum Kunden hin verschoben worden ist. Wir werden gezwungen, unser Banking online abzuwickeln. Wenn es jemandem gelingt, unser Konto leer zu räumen, sind die Geschäftsbedingungen der Bank so formuliert, dass wir so gut wie sicher selbst schuld sind – und der Bank einen Fehler nachweisen müssen. Für Menschen, die diesen virtuellen Schalter nicht wollen, ist überhaupt keine Alternative mehr vorgesehen.

Sehen Sie da regulatorischen Handlungsbedarf?
Ehrlich gesagt, wundere ich mich vielmehr, weshalb der Markt das nicht regelt. Dass keine Bank einen Wettbewerbsvorteil darin sieht, rechtlich weniger Verantwortung auf den Kunden abzuwälzen. Ein Grund ist sicher, dass die meisten Institute sich im Schadensfall einigermassen kulant zeigen. Bis auf die Fälle, bei denen Betrugsopfer auch wirklich sämtliche roten Ampeln überfahren haben. Wer Monat für Monat einen fünfstelligen Betrag an einen Scam-Account überweist, ist dann irgendwann auch wirklich selbst schuld.

Wenn ich heute Opfer eines Cyberangriffs werde: Ist das mehr statistischer Zufall oder gezielte Attacke?
Das ist unterschiedlich. Spam geht grundsätzlich flächendeckend raus und schafft es immer mal wieder durch den Filter. Wer auf so etwas klickt, dürfte auch für künftige Versuche interessant sein. Insgesamt nimmt die Systematik zu: Mit meinem ausländisch klingenden Nachnamen erhalte ich markant mehr Scam-Anrufe als die «Meiers» und «Müllers» um mich herum. Wenn ich Zeit habe, mache ich mir – auch aus beruflichem Interesse – gerne einen Spass daraus, Scam-Anrufer möglichst lange in der Leitung zu halten und ihre Masche auszutesten.

Wie sieht es bei Ransomware-Angriffen aus?
Man geht davon aus, dass heute sehr zielgenau operiert wird. Nur ein paar Strassen entfernt gab es ein gestandenes Informatikunternehmen mit rund 70 Mitarbeitern. Vor zwei Jahren ist es in die Ransomware-Falle getappt. Trotz Cyberversicherung gibt es das Unternehmen heute nicht mehr. Primär, weil zu viel Zeit benötigt wurde, um bei allen Kunden die Informatik wieder zum Laufen zu bringen, und die Regressforderungen nicht beglichen werden konnten. Besonders gefährdet sind Firmen, die zu klein sind für eine aufwendige IT-Sicherheitsarchitektur, aber wirtschaftlich interessant genug, um erpresst zu werden.

Ist bekannt, wie hoch der Anteil der Firmen ist, die bei einem Ransomware-Angriff bezahlen?

Christian Folini empfing die KMU-Magazin-Redaktoren Marco Ratschiller und Pascal Huber in seinem Garten.

Es kommt vor, dass Firmen in Abstimmung mit Experten oder Versicherungen zahlen. Und irgendwie ist es doch verständlich, den Geldhahn zu öffnen, wenn die Existenz von Dutzenden Arbeitsplätzen auf dem Spiel steht.

Ist eine Cyberversicherung überhaupt sinnvoll?
Auch wenn sich – wie im vorhin erwähnten Beispiel – der Reputationsschaden nicht versichern lässt, ist eine Versicherung sicher dennoch eine gute Sache. Denn nebst der finanziellen Absicherung hat man im Schadensfall zumindest schon einmal eine professionelle Ansprechperson, welche die Expertise einbringt, die man sich als KMU selbst oft nicht leisten kann.

Damit es nicht so weit kommt: Was muss ich tun, wenn sich der Verdacht auf einen Angriff erhärtet?
Ganz wichtig: Sofort den Stecker ziehen! Das hat absolut Vorrang. Noch besteht die Möglichkeit, dass nicht sämtliche Daten verschlüsselt oder gestohlen wurden. Für ein KMU wird es kaum möglich sein, im Vorfeld des Angriffs reale und vermeintliche Warnsignale zu erkennen. Man kann nicht jedes Mal die ganze Firma vom Netz nehmen, wenn das Internet wieder einmal seltsam langsam ist. Dennoch gilt: Sofort Stecker raus, sobald sich ein Verdacht erhärtet. Der zweite Schritt lautet dann bereits: Echte Profis an die Sache lassen. Schon oft ist es vorgekommen, dass ein Unternehmen alles schlimmer gemacht hat, weil es unvorsichtig mit Back-ups hantierte, die ebenfalls schon Schadcode enthielten.

Sprechen wir doch noch etwas mehr über die Prävention anstelle der nachträglichen Intervention.
Ich empfehle jedem KMU, den IKT-Minimalstandard umzusetzen. Diese Empfehlungen des Bundesamts für wirtschaftliche Landesversorgung bieten eine vernünftige, praktikable Basis für den Schutz der vorhandenen Informations- und Kommunikationstechnologien. Ebenfalls empfehlenswert ist die Website cybernavi.ch, welche für unterschiedliche Betriebsgrössen und Branchen die angemessenen Schutzmassnahmen rund um Cybersecurity aufzeigt.

Kurz gesagt, was gehört zum Minimalstandard?
Natürlich gehört die schon erwähnte 2-Faktor-Authentifizierung dazu. Machen Sie Software-Updates und regelmässige Back-ups. Der Vorteil von Empfehlungslisten, wie bei den IKT-Minimalstandards, liegt darin, dass man schwarz auf weiss und Punkt für Punkt seine Sicherheitsmassnahmen durchchecken kann. Natürlich hilft es auch bei einem Versicherungsabschluss, auf diese eingehaltenen Standards zu verweisen.

Gibt es eine Faustregel, wie viel eine Firma in die eigene Sicherheit investieren soll?
Am besten betrachtet man seine Firma von oben nach unten. Was sind die wichtigsten Bereiche der Firma? Womit verdient sie ihr Geld? Wie viel fliesst in die Informatik? Und dann empfehle ich als Faustregel, zehn Prozent des Informatikbudgets in die Sicherheit zu investieren. Hat man zehn Personen in der In-

Folini ist Mitglied der nationalen Cybersicherheitskommission.

formatik, sollte sich eine davon ausschliesslich um Security kümmern. Habe ich eine kleinere Abteilung, empfiehlt es sich sehr, externe Fachleute zu engagieren, die auch Schwachstellen erkennen, welche der interne Mitarbeiter, der die Software oder den Drucker installiert, leicht übersehen kann.

«Als Faustregel empfiehlt sich, zehn Prozent des Informatikbudgets in die Sicherheit zu investieren.»

Wie kann man allgemein jene Mitarbeiter schulen, die nicht in der Informatikabteilung arbeiten?
Offen gesagt bin ich Awareness-Skeptiker. Ich bezweifle, dass man Menschen umerziehen kann. Man kann Mitarbeiter sicher dazu bringen, eine 2-Faktor-Authentifizierung zu machen. Aber Mitarbeitern zu sagen: Seid vorsichtig, klickt keine Links, öffnet keine Anhänge – das ergibt einfach keinen Sinn. Denn genau das ist ihr Job: E-Mails öffnen und beantworten. Ausserdem erwischt es ja nicht nur den «normalen» Mitarbeiter. Mir ist folgender Fall eines Verwaltungsrates eines deutschen Milliardenkonzerns bekannt: Alles begann mit einem Linkedin-Kontakt, der sich nach einem Referat des Verwaltungsrates ergab. Der Kontakt zur jungen, attraktiven und auch wissbegierigen Frau wurde über ein Jahr gepflegt und intensiviert, ehe der Verwaltungsrat von ihr die entscheidende Mailanfrage erhielt: Er solle sich doch bitte rasch ihr Konzept aus seinem Fachbereich ansehen, das sie in wenigen Stunden abgeben müsse. Und dann folgte dieser eine teure Klick zu viel. Für diesen Scam war ein ganzes Jahr kriminelle Aufbauarbeit nötig. Doch künftig wird die KI diese Vorarbeit leisten und bequem melden, wenn das Opfer Vertrauen gefasst hat und reif für einen Angriff ist.

Vertrauensbasis ist ein gutes Stichwort, um noch auf ein anderes Thema zu sprechen zu kommen. Mit Trumps zweiter Amtszeit – Stichwort Zollstreit – wurde ja die Forderung lauter, die Abhängigkeit von US-Firmen zu überwinden.
Wir kaufen unsere Software heute zu einem guten Teil in den USA. Das ist Geld, das wir nicht in die eigene Volkswirtschaft investieren. In Schleswig-Holstein hat man errechnet, dass jeder Euro, der lizenztechnisch in die USA fliesst, auch dort bleibt. Wird derselbe Euro in ein deutsches Unternehmen investiert, kommt er oft drei- bis vierfach zurück. Die jüngsten politischen Verwerfungen haben uns bewusst gemacht, dass jenseits der Nischen, die eigene Softwareunternehmen besetzen, ein Marktpotenzial vorhanden ist, das nicht realisiert wird. Denn: Das Know-how in Europa und der Schweiz wäre absolut vorhanden. Aber wie heisst es so schön: Der beste Moment, einen Baum zu pflanzen, war vor 20 Jahren, der zweitbeste Zeitpunkt ist heute. Von dem her ist die verstärkte Diskussion über mehr digitale Souveränität natürlich sehr zu begrüssen.

Braucht es den Staat, damit den Worten Taten folgen?
Wir machen in der Schweiz keine Industriepolitik, wenn es nicht um Landwirtschaft und Tourismus geht. In der Regel müssen sich alle Branchen selbst helfen. Aber man könnte durchaus bessere Rahmenbedingungen schaffen, fernab von irgendwelchen Subventionen. Die Open-Source-Firmen in der Schweiz wären nur schon zufrieden, mit gleich langen Spiessen antreten zu können: Sie wollen keine Subventionen, aber öffentliche, WTO-konforme Ausschreibungen. Mit den Freihändern bei der Büroautomation, also Vergaben ohne Ausschreibung, muss Schluss sein.

Sind valable Alternativen überhaupt vorhanden?
Da landen wir wieder beim Baum, den man besser schon vor 20 Jahren gepflanzt hätte. Doch wer nicht endlich pflanzt, wird auch in zehn Jahren nur davon reden. Eine vollständige Autarkie werden wir im Digitalen genauso wenig erreichen wie in der Landwirtschaft. Die Schweiz wird auch künftig nur in einzelnen Nischen eigene Chips herstellen. Es wäre aber schon viel gewonnen, wenn es im Softwarebereich einen echten Markt gäbe. Es braucht ein heterogenes System, welches das Klumpenrisiko reduziert, dass ein launischer US-Präsident uns jederzeit den Stecker ziehen könnte.

Wobei auch schon die Drohung allein wirkt.
Was der Bund meiner Meinung nach inzwischen auch richtig erkannt hat und deshalb nach Alternativen sucht. Klar ist: Es kann nicht mehr so weitergehen. Wenn wir nur schon sehen, wie US-Firmen an der Preisschraube drehen, weil für ihre Kun-

den der Lock-in Tatsache ist. Kantone und Städte, die von Office 365 abhängig sind, müssen für die Lizenzen Jahr für Jahr massive Preisaufschläge hinnehmen.

Muss die Frage der digitalen Souveränität eigentlich eine nationale Antwort bekommen – oder reicht auch eine europäische Perspektive?
Der Diskurs läuft national und europäisch parallel. Wir werden die amerikanischen Anbieter weder kurz- noch mittelfristig ganz ersetzen. Aber es wäre ja schon schön, wenn ein Drittel des Geldes nicht nach Übersee abfliessen würde, sondern in Europa und der Schweiz verbliebe. Hinzu kommt, dass alleine die Existenz ernsthafter Konkurrenz grossen Wert hätte. Die amerikanischen Anbieter würden dadurch gezwungen, ihre Preise zu senken.

«Der beste Moment, um einen Baum zu pflanzen, war vor 20 Jahren. Der zweitbeste ist jetzt. Die Metapher gilt auch für die digitale Souveränität.»

Ist es überhaupt realistisch, von Office365 wegzukommen, wenn man die Komplexität und die Vernetzung der Anwendungen berücksichtigt?
Hier stelle ich die Gegenfrage, was man denn von all den Funktionen auch wirklich benötigt. Oft ist das doch erstaunlich überschaubar. Es mangelt wirklich nicht an Alternativen, um den Bereich klassischer Büroanwendungen abzudecken. Aber was nun einmal anfällt, sind die Transitionskosten.

Kosten, die ein KMU davon abhalten, zum Beispiel von Windows auf Linux zu wechseln …
… aber oft nur deshalb, weil das Ganze nicht wirklich durchgerechnet wird. Lohnt es sich wirklich, eine ganze Firma auf Windows zu halten, weil vielleicht drei Spezialmaschinen ausschliesslich mit Windows laufen? Während das Gros der Belegschaft die Microsoft-Plattform nur hochfährt, um den Tag in plattformunabhängigen Browser-Applikationen zu verbringen. Lohnt es sich da wirklich, die Linzenzkosten zu berappen?

Viele stecken also in der Bequemlichkeitsfalle: Microsoft bietet schön alles aus einer Hand.
Auch dieses Bundle-Argument spricht nicht mehr wirklich gegen Open-Source-Lösungen. In Deutschland bietet das «Zentrum für Digitale Souveränität der Öffentlichen Verwaltung» die Kollaborationssoftware «openDesk» an. Diese ist eine Alternative zu Microsoft 365. Frankreich verfolgt derzeit einen völlig anderen Ansatz und entwickelt KI-unterstützt etwas komplett Neues. Noch ist offen, ob beides zum Fliegen kommt, aber im Idealfall haben wir in Zukunft echten Wettbewerb und Auswahlmöglichkeiten.

Die beiden Initiativen in Deutschland und Frankreich werden teils aber auch kritisch gesehen.
Tatsächlich gibt es Experten, die denken, dass Europa nicht versuchen soll, die USA dort zu schlagen, wo das kaum möglich ist. Aber: Bei KI-Sicherheit fangen wir alle ganz neu an. Hier besteht eine reale Chance für Europa und die Schweiz, etwas zu bewegen und in einem neuen Feld unverzichtbar zu werden.

Mit Blick auf all die Entwicklungen: Soll ein KMU einen Systemwechsel nicht noch etwas vertagen?
Es ist tatsächlich eine Frage des Timings und der Prioritäten. Vieles ist im Wandel. Oft lässt sich nicht alles gleichzeitig finanzieren. Was ich zudem beobachte: Man schaut darauf, was der Bund nun macht. Ihm kommt eine Leuchtturmfunktion zu. Es ist gut denkbar, dass sich hier noch Lösungen entwickeln, die auch für andere Arbeitgeber interessant sein werden.

Eine Frage zum Schluss: Wenn Sie morgen die Verantwortung für ein typisches KMU übernehmen würden: Was wären Ihre ersten drei sicherheitstechnischen Massnahmen?
Ich würde sicher einmal alles analysieren und grob inventarisieren, was ich antreffe. Was funktioniert wie? Was ist wirklich wichtig? Als Zweites gilt es einen Notfallplan zu definieren, den alle kennen und mit kühlem Kopf anwenden können: Stichwort «sofort Stecker ziehen». Und danach ginge ich umgehend daran, zusammen mit einem geeigneten Partner den erwähnten IKT-Minimalstandard umzusetzen. «

Porträt

Christian Folini
Security Engineer

Dr. Christian Folini ist Sicherheitsexperte und Open-Source-Enthusiast mit 20 Jahren Erfahrung im Bereich Anwendungssicherheit. Zudem ist er Programmleiter der Konferenz «Swiss Cyber Storm» und Mitglied des Steuerungsausschusses der Nationalen Cyberstrategie.

Kontakt

christian.folini@netnea.com
www.netnea.com