EINE PUBLIKATION VON SMART MEDIA

SEP '22

FOKUS SICHERHEIT

smart media agency

Passwortsicherheit
Worauf zu achten ist

Kommunikation
Private 5G-Netze bieten Schutz

Unternehmens-sicherheit
Nachhaltige Sicherheit fördern

Interview

Florian Schütz

Delegierter des Bundes für Cybersicherheit

«Cybersicherheit muss auf Geschäftsleitungsebene thematisiert werden.»

Lesen Sie mehr auf fokus.swiss

Arié Malz & Angelo Mathis

Cyber-Risikomanagement statt Cyber-Sicherheit

Schlagzeilen über Hackerangriffe sind so alltäglich geworden, dass sie nur noch bedingt unsere Aufmerksamkeit fesseln. Die Gewöhnung täuscht darüber hinweg, dass die Cyberrisiken und das Schadensausmass zunehmen. Daten werden gestohlen, verändert, erpresst. Eine Vielzahl von betrügerischen Angriffsmethoden wie Phishing kommen zum Einsatz. Hochrechnungen gehen davon aus, dass die Cyberkriminalität längst mehr Geld umsetzt als der weltweite Drogenhandel. Viel mediale Aufmerksamkeit erhielten in letzter Zeit Ransomware-Angriffe: Der Angreifer kompromittiert dabei ein System, verschlüsselt alle Daten und erpresst für deren Entschlüsselung ein Lösegeld.

Weitaus schwerwiegender ist aber die Tendenz zum Datendiebstahl: Der Angreifer schleicht sich ins System und kopiert heimlich alle Daten. Oft bemerkt das Opfer erst sehr viel später, wenn überhaupt, dass es angegriffen worden ist. Wir sehen zunehmend, dass beide Angriffsformen kombiniert werden: Die Ransomware dient dazu, vom eigentlichen Angriff, der Datenentwendung, abzulenken.

Staaten, kritische Infrastrukturen, Unternehmen aller Grössen und Privatpersonen sind das Ziel dieser Angriffe. Im Cyberraum kann jedes Unternehmen Opfer eines Angriffs werden: Wenn nicht direkt, dann durch seine Zulieferer oder Kunden. Diese Entwicklung ist nicht zuletzt das Resultat einer zunehmenden Professionalisierung und Arbeitsteilung bei den Angreifern. Dank «Cyber-Attack as a Service» finden selbst technisch unbedarfte Akteure ausgeklügelte und massgeschneiderte Dienstleistungen im Darknet, um einen Cyberangriff auszuführen. Die Angebotsvielfalt ist eindrücklich: Für 20 Dollar pro Stunde kann man bereits schlagkräftige Infrastrukturen mieten.

Arié Malz
ISSS Co-Präsident

Angelo Mathis
ISSS Vorstandsmitglied

Mittlerweile ist viel Cyber-Awareness da, oft auch eine Grundhygiene an IT-Sicherheitsmassnahmen. Angesichts immer raffinierterer Angriffe reicht dies jedoch je länger, desto weniger aus. So stellt sich die Frage: Was ist zu tun? Und vor allem: Was davon ist verhältnismässig und bezahlbar?

Kein Unternehmen kann sich dem Konkurrenzkampf im Bereich der Innovation durch Digitalisierung entziehen. Die Folge ist eine zunehmend grössere Cyberangriffsfläche. Standardisiertere, einfachere, cloud-basierte und vor allem kostengünstige Hard-Software haben diese Entwicklung befeuert.

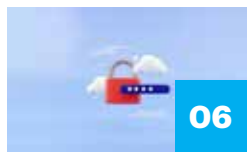
Die IT-Sicherheit dagegen hat nicht Schritt halten können: Sie ist weniger standardisiert, weniger automatisiert und entsprechend teuer. Diese IT-Sicherheitslücke wurde nicht geschlossen, sondern gleichsam als vermeintliche Dividende der Digitalisierung einkassiert. In die Sprache des Risikomanagements übersetzt wurde das ganze IT-Risiko als «Restrisiko» stehen gelassen.

Mehr IT-Risikomanagement tut deshalb Not. Dabei darf nicht vergessen gehen: Die viel zitierte IT- Sicherheit gibt es nicht, nur die Möglichkeit, IT-Risiken gezielt zu reduzieren. IT-Nutzer müssen ein ausgewogenes Verhältnis finden zwischen der Investition in spezifische IT-Sicherheitsmassnahmen und denjenigen Geschäftsrisiken, die durch den Einsatz von IT verursacht werden. Diese IT-Risiken sind als Teil der operationellen Risiken zu verwalten. Was unter die Risikoakzeptanz fällt und was nicht, ist sorgfältig abzuwägen.

Dazu braucht es auch mehr Informationsaustausch. Wir müssen eine partizipative Sicherheit schaffen, in der die Opfer von Cyberangriffen ihre Erfahrungen und ihr Wissen teilen. So können wir gemeinsam weitere Angriffe vereiteln. Der Mut der Betroffenen, den Hackerangriff nicht zu verheimlichen, sondern offen zu kommunizieren, muss auf ein positives Umfeld stossen. Nicht die Opfer sind zu beschämen, sondern die Täter. Sie sind die Bösen!

„Kein Unternehmen kann sich dem Konkurrenzkampf im Bereich der Innovation durch Digitalisierung entziehen.

Text **Arié Malz, ISSS Co-Präsident**
Angelo Mathis, ISSS Vorstandsmitglied



LESEN SIE MEHR.

FOKUS SICHERHEIT.

PROJEKTLEITUNG
LORRAINE ACAR
COUNTRY MANAGER
PASCAL BUCK
PRODUKTIONSLEITUNG
MIRIAM DIBSDALE
LAYOUT
ANJA CAVELTI
TEXT
JESSICA PETZ, VANESSA BULLIARD, RÜDIGER SCHMIDT-SODINGEN
TITELBILD
ISTOCKPHOTO
DISTRIBUTIONSKANAL
TAGES-ANZEIGER
DRUCKEREI
gedruckt in der schweiz
DZZ DRUCKZENTRUM AG

SMART MEDIA AGENCY.

GERBERGASSE 5, 8001 ZÜRICH, SCHWEIZ
TEL +41 44 258 86 00
INFO@SMARTMEDIAAGENCY.CH
REDAKTION@SMARTMEDIAAGENCY.CH

FOKUS.SWISS

Viel Spass beim Lesen!
Lorraine Acar
Senior Project Manager

Wer reale Ergebnisse möchte, muss ein reales Angriffsszenario durchlaufen

Niemand kann die Schwachstellen eines IT-Systems besser ausfindig machen als Hacker. Genau diese Tatsache nutzt man bei Bug Bounty Switzerland: Durch das Verpflichten sogenannter «ethischer Hacker» unterzieht die Firma IT-Infrastrukturen gezielten Stresstests. Daraus entstehen wertvolle Learnings hinsichtlich Cybersecurity. Doch die Vision von Bug Bounty Switzerland reicht noch viel weiter.

Interview mit den Gründern von Bug Bounty Switzerland: Sandro Nafzger (CEO), Florian Badertscher (CTO) und Lukas Heppler (CPO)

Sandro Nafzger, Florian Badertscher, Lukas Heppler – worum geht es bei Bug-Bounty-Programmen genau?
Sandro Nafzger: Der Begriff «Bug Bounty» beschreibt einen Ansatz, der sich international bereits als Best Practice für das Eruieren von Schwachstellen in IT-Systemen etabliert hat. Dabei handelt es sich um nicht weniger als einen Paradigmenwechsel: Es geht nicht mehr darum zu beweisen, wie sicher man ist, sondern um einen gekonnten Umgang mit der zunehmenden Verletzlichkeit sowie dem Aufbau von neuen Handlungsfähigkeiten. Durch die Zusammenarbeit mit externen Security Researcherinnen sowie «ethischen Hackern» passiert genau das – und es können reale und oft verborgene Schwachstellen in der digitalen Infrastruktur von Unternehmen und Organisationen identifiziert werden. Daraus lassen sich dann praxistaugliche Optimierungsmassnahmen ableiten. Es geht also darum, proaktiv Fehler zu finden und diese als Chance zu verstehen. Wir von Bug Bounty Switzerland nehmen in diesem Feld eine Pionierrolle in der Schweiz ein und wollen in dieser Funktion mehr Awareness für die Vorzüge des Ansatzes schaffen – und ihn hierzulande möglichst umfassend etablieren.

Können Sie diese Vorzüge benennen?
Florian Badertscher: Firmen sämtlicher Branchen und Grössen kommen um die Digitalisierung nicht herum, wenn sie agil, innovativ und wettbewerbsfähig bleiben möchten. Ein höherer Digitalisierungsgrad macht Organisationen aber auch potenziell anfälliger für Cyberattacken, denn digitale Systeme weisen mit hoher Wahrscheinlichkeit irgendwann in ihrem Lebenszyklus Schwachstellen auf. Wie unsere Erfahrung zeigt, gibt es keine echte Alternative zum Bug-Bounty-Ansatz, wenn es darum geht, diese Schwachstellen zu finden und sich gegen reale Gefahrenszenarien zu wappnen. Wir arbeiten mit ethischen Hackern zusammen. Diese Fachleute suchen gezielt nach Schwachstellen in IT-Systemen und unterziehen die digitale Infrastruktur einem realistischen Stresstest. Für das Finden und Aufzeigen solcher Schwachstellen werden sie dann entlöhnt. Auf diese Weise bringen wir das Thema «Cybersecurity» von einer eher abstrakten Ebene auf eine äusserst konkrete hinunter – was in der Folge zu wirklich praxistauglichen Massnahmen führt. Wir kreieren Fakten, keine Theorien und Hypothesen. Damit dieser kollaborative Ansatz funktionieren kann, muss aber ein Kulturwandel stattfinden: IT-Sicherheit kann heute nicht mehr «im stillen Kämmerchen» vorangetrieben werden, sondern vielmehr proaktiv und transparent als Zusammenarbeit mit externen Expertinnen und Experten.

Lukas Heppler: Das wiederum führt zu einer neuen Lernkultur, die nicht darauf abzielt, Fehler zu verstecken oder auszublenden, sondern deren Entdeckung als etwas Positives zu sehen. Wir von Bug Bounty Switzerland unterstützen Organisationen aller Art dabei, diesen Wandel einzuleiten und davon zu profitieren. Die Nachfrage nach dieser Expertise sowie den entsprechenden Dienstleistungen ist offenkundig: 2020 haben wir das Unternehmen als Nebenprojekt gegründet. Heute beschäftigen wir bereits 15 Mitarbeitende und wachsen stetig. Nicht nur Grossfirmen setzen auf unser Konzept, sondern auch kommunale, kantonale sowie nationale Behörden. Die Betreiber von kritischen Infrastrukturen lassen unsere Fachleute ebenfalls auf die Jagd nach Fehlern in ihrem System gehen. Zudem sind wir strategischer Partner des Nationalen Zentrums für Cybersicherheit (NCSC). Unsere Aufgabe besteht daraus, die Bug-Bounty-Plattform zu betreiben und unsere Expertise in der Zusammenarbeit mit ethischen Hackern einzubringen, damit möglichst rasch für die gesamte Bundesverwaltung Bug-Bounty-Programme betrieben werden können.

Aktuelle Studien zeigen, dass die Anzahl von Cyberattacken insgesamt zunimmt. Worauf ist dies zurückzuführen?
Florian Badertscher: Jedes komplexe IT-System weist irgendwo und irgendwann eine Schwachstelle auf. Perfektion ist in diesem Zusammenhang eine Illusion. Und leider gibt es heute immer mehr bösartige Akteure, die sich solche Schwachstellen zunutze machen. Denn das wird zunehmend lukrativer, je mehr die Organisationen von IT-Systemen abhängig sind.

Wie beurteilen Sie die «Readyness» von Schweizer Unternehmen hinsichtlich Cybersecurity?
Florian Badertscher: Der Grad an «Readyness» variiert stark. Grundsätzlich lässt sich aber sagen, dass wir bei praktisch allen Firmen und Organisationen Schwachstellen finden, egal aus welcher Branche ein Unternehmen stammt oder ob es ein kleiner oder grosser Betrieb ist. Dies zeigt unserer Ansicht nach auf, wo die Problem liegen: Schwachstellen zu finden, ist mit der richtigen Methode gut möglich und man kann dabei auf die Unterstützung von ethischen Hackern und Security Researcherinnen zählen. Die identifizierten Schwachstellen aber schnell und nachhaltig zu beheben, das ist schwierig und setzt technische Fähigkeiten, Agilität sowie eine reibungslos funktionierende Zusammenarbeit von allen Involvierten voraus, darunter Outsourcing-Partner und Lieferanten. Die Fähigkeit, mit Schwachstellen gut umgehen zu können, ist in der Schweiz unterentwickelt. Mit Bug-Bounty-Programmen wird neben dem Finden von Schwachstellen genau dies gefördert. Die Programme dienen somit als Training für den notwendigen «Schwachstellen-Muskel» und können diesen ohne Überlastung schrittweise aufbauen.

Vielen Unternehmerinnen und Unternehmern ist das wahre Gefährdungspotenzial aus dem Netz oft gar nicht bewusst. Wie schafft der «Reality Check» von Bug Bounty hier Abhilfe?
Lukas Heppler: Wir bieten mit unserem «Reality Check» einen unkomplizierten und schnellen Einstieg in die Zusammenarbeit mit ethischen Hackern. Der «Reality Check» ist ein zeitlich limitiertes, komplett durch uns gemanagtes Bug-Bounty-Programm, bei dem die Hacker versuchen, Lücken in der virtuellen Verteidigung des Kundenunternehmens zu finden. Dieser «Stresstest» kann innerhalb von 24 Stunden gestartet werden. Das ermöglicht eine ebenso rasche wie realistische Risikoeinschätzung. Im Vorfeld gibt es ein Gespräch mit den Kundinnen und Kunden, welches eine erste Orientierung über den digitalen Footprint des Betriebs gibt. Diese Informationen dienen uns als Basis, um die «Spielregeln» für die Hacker zu definieren. Selbstverständlich sind die Tests so angelegt, dass das Business einer Firma stets weiterläuft und es zu keinerlei Beeinträchtigungen vom Betrieb kommt.

Wie viele Hacker lassen Sie jeweils auf ein System los?
Florian Badertscher: Manchmal reicht eine Handvoll, manchmal sind es etwas grössere Gruppen. Essenziell ist aber nicht nur die Anzahl der Angreifenden, sondern auch deren Expertise, Motivation und aktuelle Verfügbarkeit: Wir achten darauf, dass wir Leute auswählen, die bestens vertraut sind mit der jeweiligen Technologie, die wir testen. Alle involvierten Personen sind dabei an absolute Geheimhaltung gebunden.

Wie lange dauert ein Stresstest im Durchschnitt?
Sandro Nafzger: Das ist stark von der individuellen Ausgangslage einer Organisation abhängig. Unser «Reality Check» dauert in der Regel ca. zwei Wochen. Meist finden wir die ersten Sicherheitslücken bereits nach wenigen Stunden und müssen auch öfter einen Test bereits nach wenigen Tagen beenden, da das Budget für die Belohnungen an die ethischen Hacker ausgeschöpft ist. Es gibt auch seltene Fälle, in denen sich die Hacker quasi «die Zähne ausbeissen». Bei solchen Systemen wurde von Beginn weg alles richtig gemacht. Hier brauchen wir etwas mehr Zeit, um kritische Schwachstellen zu finden. Nach dem «Reality Check» entscheiden sich die meisten Kunden dann für ein kontinuierliches Bug-Bounty-Programm. Dazu gibt es heute einfach keine echte Alternative. Es gibt Sicherheitslücken, die nur durch ein Bug Bounty Programm gefunden werden.

Was hat es mit der Plattform von Bug Bounty Switzerland auf sich?
Sandro Nafzger: Wir entwickeln und betreiben die erste Kollaborationsplattform der Schweiz für Bug-Bounty-Programme. Dadurch bringen wir die Welt der Unternehmen und Behörden mit der Sphäre der ethischen Hacker zusammen. Wir vereinen also Kundinnen und Kunden mit den passenden ethischen Hackern und Security Researcherinnen. Die Plattform hilft, diesen Ansatz möglichst vielen Organisationen zugänglich zu machen und das Testen unter realen Bedingungen auch im KMU-Bereich zu etablieren. Unsere Vision besteht darin, dass wir bis 2025 eine umfassende Plattform für die Zusammenarbeit mit ethischen Hackern und den Umgang mit Schwachstellen jeder Schweizer Organisation zugänglich machen können.

Lukas Heppler: Uns schwebt eine Art virtueller Schutzschild vor, den wir über die Schweiz legen können. Das wäre ein wesentlicher Beitrag für die digitale Transformation der Schweiz. Unsere Plattform dient dabei als Basis für ein Ökosystem und agiert als Drehscheibe zwischen allen relevanten Akteuren.

Florian Badertscher: Um dorthin zu gelangen, investieren wir viel in die kontinuierliche Weiterentwicklung unserer SaaS-Plattform (Software as a Service). Damit das Bug-Bounty-Prinzip für die Schweiz flächendeckend und erfolgreich zum Einsatz kommen kann, müssen wir es auf die Ansprüche unserer KMU-Landschaft anpassen. Dafür benötigen wir Innovation und Vernetzung, zum Beispiel in Form von Kollaborationsprojekten mit Hochschulen. Auch in diese Richtung sind wir aktiv und forschen an der Methode Bug Bounty selbst. Zusammenfassend wollen wir mit unserer Plattform und unserem Ökosystem die Zusammenarbeit im Feld der Cybersecurity auf eine neue Ebene anheben.

Dafür benötigen Sie auch die Gunst der breiten Öffentlichkeit.
Sandro Nafzger: Absolut, das Thema «Public Trust» wird zu einem zentralen Erfolgsfaktor in der digitalen Welt: Es genügt nicht mehr, einfach ein funktionierendes und sicheres IT-System zu bauen – man muss auch die Akzeptanz und das Vertrauen der Öffentlichkeit dafür gewinnen. Eine wesentliche Grundvoraussetzung dafür stellt ein kontinuierlicher und transparenter Diskurs zum Stand der Sicherheit und möglichen Verbesserungen dar. Dieser wird in Zukunft entscheidend sein, um Vertrauen in digitale Angebote zu sichern. Gerade im E-Government Umfeld wird «Public Trust» besonders erfolgsentscheidend werden. Diese Entwicklung wollen wir mit unserem Schweizer Ökosystem bestmöglich unterstützen und fördern. Damit die Schweiz auch im digitalen Zeitalter weltklasse ist.

Die Bug-Bounty-Gründer (v.l.n.r.) Florian Badertscher, Lukas Heppler und Sandro Nafzger wollen die Schweiz zu einem sicheren Cyberspace machen.

Über Bug Bounty Switzerland

Die digitale Transformation kann ohne eine kontinuierliche, kollaborative und transparente Verbesserung der Informationssicherheit nicht gelingen. Darum arbeitet das 2020 gegründete Unternehmen Bug Bounty Switzerland am Ausbau des Schweizer Ökosystems für die Zusammenarbeit mit unabhängigen Security Researcherinnen und ethischen Hackern. Die Firma stellt mit ihrer Plattform die Grundlage dafür zur Verfügung, arbeitet mit ihren Kundinnen und Kunden an einem ganzheitlichen Schwachstellenmanagement, der Befähigung der ganzen Organisation und dem Aufbau von Public Trust. Auf diese Weise wird kollaborativ ein neuer Standard für Cybersecurity in der Schweiz geschaffen. Ganz nach dem Motto: «Gemeinsam für eine sichere Schweiz».

Weitere Informationen finden Sie unter **www.bugbounty.ch**

BUG BOUNTY SWITZERLAND

Gefahr von Cyberangriffen auf vernetzte Medizinprodukte

Von Cyberangriffen sind heutzutage viele Schweizer Unternehmen betroffen. Dies ist unter anderem darauf zurückzuführen, dass das weltweite Internet-of-Things-Netzwerk (IoT) immer dichter wird. Gleichzeitig werden die Cyberattacken professioneller und ausgeklügelter und tangieren mittlerweile sämtliche Branchen – auch das Gesundheitswesen.

Cyberangriffe können jede Organisation treffen. Gerade im Umfeld von kritischen Infrastrukturen wie medizinischen Einrichtungen muss dabei mit gravierenden Konsequenzen gerechnet werden. Vermehrt geraten vernetzte Medizinprodukte in den Fokus der Hacker:innen. Doch was sind eigentlich vernetzte Medizinprodukte und welchen Schaden können Hacker:innen im Medizinbereich anrichten?

Was sind vernetzte Medizinprodukte?

Das Gesundheitswesen wird zunehmend durch das Internet der Dinge (IoT) durchdrungen. Durch die Vernetzung von medizin- und labortechnischen Produkten und Anwendungen haben sich Möglichkeiten ergeben, von denen man vor Jahren nur träumen konnte. Heutzutage ist es mithilfe von IoT beispielsweise möglich, Prozesse in medizinischen Einrichtungen zu optimieren und die Behandlung sowie die Lebensqualität von Patient:innen erheblich zu verbessern. So lassen sich der Zustand von Patient:innen dank der IoT-Technologie durchgängig überwachen und kritische Veränderungen rechtzeitig erkennen. Die erhöhte Datenqualität führt schliesslich zu einem verbesserten Behandlungserfolg.

Ein Beispiel für die zahlreichen Vorteile von IoT in der Medizin ist das Remote Patient Monitoring (RPM). RPM-Technologien werden eingesetzt, um beispielsweise hochinfektiöse, chronisch erkrankte oder in der Mobilität eingeschränkte Patientinnen und Patienten in Echtzeit von der Ferne aus zu überwachen.

Schwachpunkte von IoT

Wo Digitalisierung auf das Gesundheitswesen trifft und somit gravierenden Einfluss auf das Leben von Menschen hat, gilt es besondere Sicherheitsbedürfnisse zu berücksichtigen. Allerdings: «Vernetzte Medizinprodukte und die daraus resultierenden Datenflüsse sind mit hohen Cyberrisiken verbunden, wenn sie nicht ausreichend geschützt werden», gibt Reto Amstad, Senior Security Consultant bei der CyOne Security, zu bedenken. Dies hat verschiedene Ursachen: So sind Medizinprodukte selber attraktive Angriffsziele, da sie ständig eingeschaltet, immer online und oft schlecht gewartet sind und zudem häufig nur geringen Security-Standards genügen. Amstad betont, dass bei der Entwicklung von IoT-Anwendungen häufig Sicherheitsaspekte vernachlässigt werden und Geräte vernetzt werden, die ursprünglich nicht dafür entwickelt worden sind. Ebenfalls führen unsichere Hardwaredesigns und Schwachstellen in der Software zu gravierenden Sicherheitsmängeln.

Zudem können IoT-Anwendungen gemäss Amstad nicht isoliert betrachtet werden. Denn sie sind stets Teil eines komplexen IoT-Ökosystems mit einer Vielzahl von Geräten, Schnittstellen und Zonenübergängen. Über die vielschichtigen Angriffsflächen im IoT-Ökosystem können sich potenzielle Cyberkriminelle Zugriff auf das System verschaffen – typischerweise über den schwächsten Punkt im Gesamtsystem.

Amstad betont, dass die Schnittstellen und Zonenübergänge sicher authentifiziert, gemanagt und überwacht werden müssen. Gleichzeitig ist es zentral für die Sicherheit, dass die vernetzten Medizinprodukte mit sicherheitsrelevanten Updates, Patches oder neuer Firmware ausgestattet werden können. Eine resistente Verschlüsselung ist dabei die Grundvoraussetzung für die Sicherstellung des Datenschutzes sowie der Integrität der übertragenen Daten.

Die Sicherheit beginnt beim Hersteller

Sowohl der Hersteller als auch der Betreiber von IoT-Anwendungen sind punkto Sicherheit in der Verantwortung. Hersteller müssen die Sicherheit der Geräte bereits bei der Entwicklung berücksichtigen. Das Nachrüsten von fehlenden Sicherheitskomponenten ist meist mit hohen Kosten verbunden. Betreiber von IoT-Anwendungen – beispielsweise ein Spital oder Labor – sollten ihrerseits von den Herstellern detaillierte Angaben bezüglich der Sicherheitsaspekte Konnektivität, sicheres IoT-Produkt, sichere Integration und Datenhaltung einfordern und prüfen.

Sicherheitsfunktionen in Medizintechnikprodukten

Vernetzte Medizinprodukte werden meist mit dem Ziel entwickelt, die Versorgung und Lebensqualität der Patient:innen zu verbessern und die Prozesse zu optimieren. Um dieses Ziel zu erreichen, und das enorme Potenzial auszuschöpfen, welches das IoT in der Medizintechnik bietet, ist der Fokus auf die Sicherheit unabdingbar. Gemäss Amstad ist dabei das «Security by Design»-Prinzip zentral. Der Ansatz verfolgt die Prämisse, dass die notwendigen Sicherheitsmassnahmen vor allem innerhalb eines medizintechnischen Produkts, insbesondere in dessen Hard- und Software, umgesetzt werden. Wichtige Cyber Security-Aspekte sind hierbei eine sichere Identifikation des Geräts, unveränderbare Log-Informationen, sichere Update-Prozesse sowie Tamper Protection. Amstad sagt: «Es ist erfolgsentscheidend, dass diesen Sicherheitsaspekten schon früh in der Entwicklungsphase Rechnung getragen wird.»

Text **Jessica Petz**

«Jede Firma benötigt dringend einen ‹Plan B›»

Die Digitalisierung eröffnet Unternehmen aller Branchen und Grössen ungeahnte Chancen. Doch mit der zunehmenden Abhängigkeit von Online-Services und Automatisierung entstehen auch neue Gefahren: Die Anzahl der Hacker-Angriffe nehmen zu und sind für betroffene Unternehmen oft existenzbedrohend. Wir wollten von einem Experten wissen, welche Lösungsansätze es gibt.

Interview mit Urs Küderli, Partner, Leiter Cybersecurity und Privacy, PwC Schweiz

Urs Küderli

Urs Küderli, das Thema «Cybercrime» gewinnt immer mehr an Relevanz: Aktuelle Erhebungen, unter anderem zwei Studien von PwC, zeigen, dass die Gefährdung aus dem Netz zunimmt. Wie beurteilen Sie die Lage?
Es trifft in der Tat zu, dass die Anzahl der Angriffe ansteigt und auch die Art und Weise, wie diese erfolgen, immer facettenreicher und vor allem professioneller wird. Längst ist die Grösse eines Unternehmens nicht mehr als einziger Faktor ausschlaggebend dafür, ob man ein attraktives Ziel für Hacker:innen darstellt oder nicht. Auch ist das Gefährdungsrisiko eines Unternehmens nicht mehr nur abhängig von der Exposition: Banken gehörten lange zu den präferierten Opfern, da es dort potenziell Geld direkt zu holen gab, aber heute ist jedes Unternehmen im Fokus, so auch Industrie-, Retail- und KMU-Betriebe. Gerade auch Firmen im Pharmabereich sind anfällig, insbesondere für Spionage-Angriffe. Eine weitere Veränderung: Cybercrime ist heute deutlich «lauter» als früher. Bis vor Kurzem wurden Cyberangriffe von betroffenen Unternehmen teilweise gar nicht registriert und erst spät entdeckt. In den letzten zweieinhalb Jahren hat sich hier ein Wandel vollzogen. Sogenannte massive «Ransomware-Angriffe», bei denen Unternehmen durch die breite Verschlüsselung ihrer Systeme daran gehindert werden, ihrer Arbeit nachzukommen und damit erpresst werden, bestimmen das Bild. Zusätzlich werden vertrauliche Daten gestohlen, was die Firmen noch erpressbarer macht. Das sind Angriffe, die Firmen aufrütteln und Schlagzeilen generieren – auch weil sie hohe Schäden verursachen. Betroffene Firmen können durch derartige Attacken für Tage oder Wochen in die technologische Steinzeit zurückgeworfen werden. Etliche Betriebe kämpfen noch Jahre nach dem Angriff mit Folgen der Attacke.

Was geschieht in einem solchen Worst-Case?
Es sind sehr grundlegende Fragen, die in solchen Situationen schlagartig an Relevanz gewinnen: Wer ist verantwortlich für die weiteren Schritte? Wie sollen die Massnahmen aussehen, wie ermöglichen wir so schnell wie möglich einen Betrieb? Haben wir Backups, die nicht verschlüsselt wurden, wie spielen wir diese zurück? Im Falle von solchen massiven Ransomware-Angriffen werden ganze IT-Landschaften blockiert und dann ein Lösegeld per Bitcoin gefordert. Da stellt sich für viele Firmen die Frage, ob sie Lösegeld zahlen sollen – und wo sie eigentlich Bitcoin herbekommen. Der Stresspegel ist in einer solchen Extremsituation hoch, denn das Schadensspektrum reicht – je nach Fall – von 50 bis 150 Millionen Franken an direktem Schaden. Denn die betroffenen Firmen benötigen mindestens sieben bis zehn Tage, um in einen geordneten Betrieb zurückkehren zu können.

Wer sind die Angreifenden, die solche Cyberattacken verüben?
Das Spektrum reicht von Schüler:innen, die sich einen Spass daraus machen, eine Website lahmzulegen, bis hin zu staatlich geförderten Organisationen. Den Grossteil machen allerdings kriminelle Organisationen aus, für die Cybercrime zum Businessmodell geworden ist. Dabei handelt es sich überwiegend um kleine Unternehmen, die auf spezifische Aspekte von Cybercrime spezialisiert sind, wie Phishing, Social Engineering oder physische Attacken. Dadurch hat sich in diesem Feld eine regelrechte Ökonomie etabliert: Es gibt spezialisierte Gruppen, die in Firmen eindringen und diesen Zugriff dann weiterverkaufen – etwa an Kriminelle, die einer Organisation dann vertrauliche Firmen-Datensätze entwenden und diese weitervertreiben. Der Abnehmer bereitet die Daten anschliessend für die Übergabe an die nächsten Akteure auf, welche zum Schluss die Verschlüsselung sowie die Erpressung des geschädigten Unternehmens einleiten. Da gemäss aktuellen Erhebungen rund 70 Prozent der betroffenen Firmen das Lösegeld bezahlen, um ihre Systeme wieder entschlüsseln zu können, handelt es sich dabei um ein lukratives Business.

Stehen Unternehmen also auf verlorenem Posten angesichts der professionellen Angreifenden?
Es ist teilweise ein ungleicher Kampf, doch wer sich der Gefahren aus dem Netz bewusst ist, kann sich absichern. Genau dabei unterstützen wir vom Bereich Cybersecurity bei PwC Schweiz unsere Kundschaft. Wir fokussieren uns auf zwei essenzielle Aspekte: Zum einen geht es darum, Firmen auf mögliche Angriffe vorzubereiten und sie für den Ernstfall zu wappnen. Dafür konzentrieren wir uns stark auf das individuelle Bedrohungsszenario eines Unternehmens sowie auf dessen Möglichkeiten und Fähigkeiten. Wir helfen Firmen, sich auf den Krisenfall vorzubereiten, um schnellstmöglich reagieren und somit baldmöglichst den Betrieb wieder aufnehmen zu können. Zum anderen unterstützen wir unsere Kunden im Krisenmanagement in rechtlichen und technischen Aspekten, bei der Forensik, im Datenschutz sowie beim Wiederaufbau, sollte dieser Ernstfall eintreten. Die Summe dieser Massnahmen hilft Firmen dabei, resilienter gegen Angriffe zu werden – oder im Angriffsfall den Schaden zu minimieren.

Wie schätzen Sie die durchschnittliche digitale Resilienz von Schweizer Unternehmen ein?
Viele Betriebe haben ihre «Hausaufgaben» gemacht und sind heute deutlich besser geschützt, als dies noch vor einigen Jahren der Fall war. Doch die Angreifer:innen bleiben nicht stehen, sondern passen sich an: Oft ist es einfacher, einen kleinen Betrieb anzugreifen, der Teil der Lieferkette einer grösseren Unternehmung ist. Die meisten Firmen haben heute verschiedene Partner und Zulieferer, die nicht selten über privilegierten Zugriff auf Systeme und Daten verfügen. Das macht diese Firmen zu idealen Gateways für Kriminelle. Hinzu kommt, dass Produkte und Dienstleistungen, die von Dritten bezogen werden, ausserhalb der eigenen Kontrolle liegen. Um zu verhindern, dass sich Angreifer:innen über diese Partner Zugang zum eigenen System verschaffen, kann und sollte man nachfragen, welche Sicherheitsmassnahmen und -Zertifizierungen vorliegen. Zu viele Unternehmen haben wenig bis gar kein Verständnis für die IT und Software-Risiken in ihrer Lieferkette. Am Ursprung erfolgreicher Angriffe stehen aber noch immer oft Phishingmails und ungenügend gewartete Systeme.

Wo kann man ansetzen?
Grundsätzlich beginnt dies bei der Aufklärung und dem Schaffen von Verständnis, aber essenziell ist auch das Etablieren einer offenen Fehlerkultur. Wenn jemand in der Firma zum Beispiel eine Phishingmail öffnet und den Fehler bemerkt, kann es entscheidend sein, dass er oder sie den Fall sofort meldet. Dann kann man nämlich reagieren und den potenziellen Schaden eingrenzen. Ist eine solche Kultur nicht vorhanden, werden derartige Fehltritte vielleicht nicht oder erst spät kommuniziert – was den möglichen Folgeschaden erhöht.

Cybersecurity ist also ein komplexes Handlungsfeld, das sowohl technische Faktoren als auch Aspekte der Führung und Kommunikation umfasst. Wie läuft ein Mandat ab, wenn Unternehmen bei PwC diesbezüglich Unterstützung suchen?
Zuerst müssen wir natürlich unterscheiden, ob es sich beim Mandat um die Vorbereitung auf einen möglichen Angriff handelt oder ob dieser bereits geschehen ist. Ist Letzteres der Fall, begleiten wir die Kundschaft sehr eng durch den «Krisenmodus». Auf der technischen Ebene arbeiten wir dann zum Beispiel daran, sicherzustellen, dass nicht das gesamte System verschlüsselt wird. Ist es dafür bereits zu spät, fokussieren wir uns darauf, das Unternehmen so schnell wie möglich zurück zu einem funktionierenden System zu verhelfen. Das kann einen Neu- oder Teilneubau der IT-Umgebung voraussetzen. Gleichzeitig unterstützen wir das Management bei der Krisenorganisation und helfen auch bei der Kommunikation nach innen und aussen. Das oberste Ziel besteht immer darin, die Situation so schnell wie möglich wieder in den Griff zu bekommen. Einfacher – und deutlich weniger stressig – ist es, wenn wir proaktiv einbezogen werden, und nicht erst im Ernstfall.

Wo liegt dann der Fokus?
Wir erhöhen die Resilienz gezielt. Dazu führen wir unter anderem Assessments durch, um herauszufinden, wo das Unternehmen steht, etwa mit Krisensimulationen. Diese sind sehr nahe an realen Fällen angelegt und dienen der Erkennung von Schwachstellen. Gemeinsam mit dem Unternehmen erarbeiten unsere Fachleute dann Massnahmen, um diese blinden Flecken zu beheben. Ganz wichtig: Wir helfen unseren Kundinnen und Kunden dabei, einen «Plan B» auszuarbeiten. Wer nämlich im Ernstfall trotz Verschlüsselung von Daten und Systemen in der Lage ist, handlungsfähig zu bleiben, ist unweigerlich im Vorteil. Das kann etwa bedeuteten, alternative Systeme zu nutzen oder sogar eine gewisse Zeit lang auf Papier und Stift zurückzugreifen.

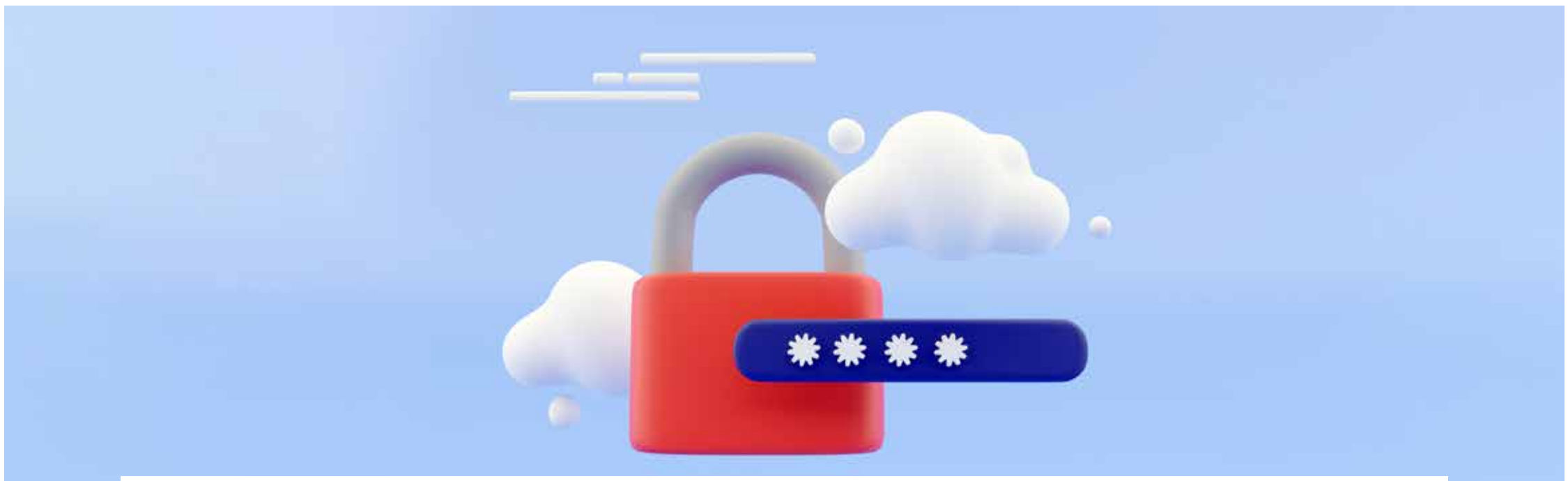
Wie wird sich Cybersecurity in Zukunft entwickeln?
Unsere Studien haben eine weitere Zunahme von Gefährdungen und Angriffen im virtuellen Raum gezeigt. Diese Tendenz bleibt ungebrochen, denn Cybercrime ist lukrativ und die Risiken sind vergleichsweise gering. Insgesamt hinken Unternehmen den kriminellen Organisationen hinterher. Aus diesem Grund muss es uns gelingen, möglichst viele Betriebe für das Thema «Cybersecurity» zu sensibilisieren und sie bei der Vorbereitung auf einen Angriff zu unterstützen.

Zum Schluss: Sollte man als Opfer eines Ransomware-Angriffs das Lösegeld zahlen, um den Schlüssel für die verschlüsselten Daten zu erhalten?
Wir empfehlen in der Regel, dies nicht zu tun. Diesen Entscheid muss letztlich jedes Unternehmen für sich fällen. Das Entrichten des Lösegelds ist längst kein Garant dafür, dass man einen funktionierenden Schlüssel erhält beziehungsweise die Daten in jedem Fall entschlüsselt werden können. Zudem muss man sich der rechtlichen Konsequenzen bewusst sein, etwa wenn man Geld an Akteure zahlt, die von sanktionierten Staaten aus operieren. Schlussendlich darf man nicht vergessen, dass man zwar in den meisten Fällen den Zugriff auf die Daten zurückerhält, aber die Umgebung ist noch immer infiziert, die Angreifer:innen im System und die Schwachstellen weiter vorhanden. Die Investition in die Reinigung der Umgebung, Beseitigung von Schwachstellen und mehr ist also trotzdem notwendig. Rechtzeitige Investitionen in einen guten «Plan B» sind auf jeden Fall die bessere Lösung.

Mehr Informationen zu den verschiedenen Cybersecurity-Lösungen von PwC Schweiz finden Sie hier:

Über PwC

PwC Schweiz ist das führende Prüfungs- und Beratungsunternehmen in der Schweiz. Der Zweck von PwC ist es, das Vertrauen in der Gesellschaft aufzubauen und wichtige Probleme zu lösen. Das Netzwerk von Firmen ist in 155 Ländern tätig und beschäftigt über 327000 Mitarbeitende. Diese setzen sich dafür ein, in den Bereichen Wirtschaftsprüfung, Beratung und Steuern erstklassige Dienstleistungen zu erbringen. PwC Schweiz hat über 3380 Mitarbeitende und Partner an 14 verschiedenen Standorten in der Schweiz sowie einem im Fürstentum Liechtenstein.



Wie der digitale Sesam geschlossen bleibt

Die private und unternehmerische Sicherheit fängt beim Passwort an. Insbesondere in Unternehmen sind die Passwörter von Mitarbeitenden ein Problem. Denn das menschliche Hirn ist kein Computer. In der Folge werden häufig kurze, simple Zeichenabfolgen gewählt, die bei Brute-Force-Attacken schnell geknackt werden können.

Nicht nur Betriebe schreiten mit der Automatisierung und Digitalisierung mit, Cyberkriminelle entwickeln sich genauso in diese Richtung. Auch sie nutzen automatisierte Vorgänge und AI, um effizient und in schneller Abfolge die üblichen Schwachstellen zu attackieren. Phishingmails und Brute-Force-Angriffe bieten den Hacker:innen die Möglichkeit, unzählige Ziele zügig abzuklappern. Der Einsatz von Algorithmen für kriminelle Absichten ist in diesem Jahr auf einem Rekordhoch. Neben der regelmässigen Schulung von Mitarbeitenden bezüglich verdächtigen E-Mails ist vor allem auch die Regelung von starken Passwörtern essenziell.

Was macht ein Passwort unsicher?

Wir leben in einer Welt der Passwörter. Privat und auf der Arbeit müssen wir uns mit massenweisen Zugangscodes herumschlagen. Einige Dienste und Websites verlangen, dass gewisse Sicherheitsanforderungen erfüllt werden. Andere enthalten wiederum keine Vorgaben. Fachkundige warnen jedoch vor den folgenden schlechten Eigenschaften eines Passworts.

Passwortmenge: Leider ist es gang und gäbe, für unterschiedliche Dienste dieselben oder ähnliche Passwörter zu verwenden. Die Gefahr hierbei ist, dass wenn Hacker:innen eines der Logins knacken, schnell auch Zugang zu den anderen finden werden. Um solch einen Vorfall zu vermeiden, sollte man für jede Website und Applikation ein einzigartiges Passwort festlegen.

Länge: Noch vor Komplexität ist die Zeichenanzahl ein wichtiges Sicherheitsmerkmal. Mit jedem Charakter mehr dauert auch die automatische Auswertung länger. Empfohlen wird aus diesem Grund, mindestens 8 bis 16 oder mehr Zeichen zu verwenden.

Wortwahl: Viele Menschen greifen auf bekannte Wortkombinationen zurück, um sich die Passwörter merken zu können. Tatsächlich nutzen Cyberkriminelle Wörterbücher als Grundlage, um bei Brute-Force-Angriffen Kennwörter zu knacken. Deshalb verzichtet man besser auf Worte, die auch so im Duden erscheinen, optimalerweise kann man die Zeichenabfolge gar nicht aussprechen.

Persönlicher Bezug: Genauso wenig sollten persönliche Informationen wie Geburtstage, Haustiere, Adressen und dergleichen in die Logins integriert werden. Durch Social Engineering können Cyberkriminelle an diese Bezüge herankommen und ein Eindringen erleichtern.

Muster: Schematische Zeichenabfolgen sollten nicht Teil eines Passwortes sein. Zum Beispiel verringern zusammenhängende Zahlen oder dasselbe Zeichen mehrere Male hintereinander die Komplexität erheblich. Dazu gehören ausserdem Buchstabenfolgen, wie sie auf der Tastatur zu finden sind, beispielsweise das bekannte «qwertz».

Sonderzeichen: Grundsätzlich sind Sonderzeichen eine gute Idee und werden auch von Sicherheitsexpert:innen empfohlen. Allerdings erhöhen sie die Sicherheit nicht, wenn sie als Ersatz für ähnlich aussehende Buchstaben oder Zahlen verwendet werden. Tatsächlich ist zum Beispiel «pa$$wort» kaum schwieriger zu knacken als «passwort», insbesondere wenn Brute-Force-Methoden zum Einsatz kommen.

Plain-Text: Bei den vielen Passwörtern ist die Versuchung hoch, sich diese irgendwo zu notieren, um sie nicht zu vergessen. Dennoch sollten sie nicht im Plain-Text abgespeichert oder auf einem Zettel aufgeschrieben werden. Auch sollten Logins nicht weitergegeben werden. Selbst die IT-Abteilung darf die persönlichen Zugänge der Mitarbeitenden nicht kennen.

Wie kann man sichere Passwörter erstellen?

Die oben genannten Punkte zu vermeiden, scheint in der Theorie einfach, in der Praxis finden Studien aber immer wieder, dass sich ein grosser Teil nicht daran hält. Egal wie simpel oder komplex die Tipps sind, Menschen wählen den Weg des geringsten Widerstands oder in diesem Falle: des geringsten Erinnerungsaufwands. Trotzdem gibt es einige Erfahrungswerte, aus denen man Best Practices extrapolieren kann.

Passphrasen: Eine Vorgehensweise, um ein sicheres Passwort zu erstellen, ist, sich eine einfach zu merkende Phrase auszudenken. Zum Beispiel: «Im Bett darf ich keine Chips essen? Nur weil 2019 alles voller Krümel war!» Daraus entsteht das Passwort «IBdikCe?Nw2019avKw!». Ein guter Weg, um die häufigsten Fallen zu vermeiden und es sich trotzdem merken zu können.

Multifaktor-Authentifizierung: Auf der technischen Seite kann man ebenfalls einiges bewirken. Falls vorhanden, sollte die Zwei- oder Multifaktor-Authentifizierung aktiviert werden. Egal ob zusätzlicher Fingerabdruck, SMS-Code oder Bestätigung per App, die Zwischenschritte erhöhen die Sicherheit enorm.

Versuchsbegrenzung: Für Unternehmen ist es sinnvoll, eine Versuchsbegrenzung für Logins festzulegen. Nach einigen Anläufen sollte der Account für eine gewisse Dauer gesperrt bleiben. Auf diese Weise nimmt man Brute-Force-Angriffen den Wind aus den Segeln und man erhält Zeit zu reagieren, auch bei kurzen Sperrzeiten.

Passwortwechsel, ja oder nein?

Unter Sicherheitsexpert:innen tobt in den letzten Jahren ein Kampf darüber, ob Passwörter gezwungenermassen in regelmässigen Abständen gewechselt werden sollten. Das Nationale Zentrum für Cybersicherheit NCSC führt dies als optionale Empfehlung auf. Für Aufsehen sorgte das deutsche Bundesamt für Sicherheit in der Informationstechnik BSI, als es 2020 die Empfehlung zum erzwungenen Passwortwechsel revidierte und es als potenziell schädlich einstufte. Nur bei Hinweisen auf eine Kompromittierung eines Accounts sollten alle Passwörter konsequent geändert werden. Das amerikanische National Institute of Standards and Technology NIST war die Ursache für den Kurswechsel. Laut dem Institut kann ein erzwungener Passwortwechsel insofern schädlich sein, da Menschen ihre Logins nur geringfügig ändern oder einfach wählen, da sie sich es andernfalls nicht merken können. Dennoch sind sie der Auffassung, dass für bestimmte Dienste in gewissen Unternehmen ein Zwang Sinn ergibt. Schlussendlich zählt die Stärke des Passworts, nicht wann es definiert wurde.

Automatisierte Governance stärkt Kollaboration und verhindert Sicherheitsfallen

Zu den gängigen Office-Programmen hat sich durch die Pandemie und New Work ein neues Tool etabliert: Microsoft Teams. Durch das schnelle Tempo der Einführung wurde die Governance vernachlässigt. Das Resultat ist ein Kontrollverlust, der zu unkoordiniertem Wildwuchs führen kann. Ein Umstand, der nicht nur eine produktive Zusammenarbeit behindert, sondern auch ein Sicherheitsrisiko darstellt. «Teamarin» für Microsoft Teams kann hier Abhilfe schaffen.

Für viele Unternehmen hat sich MS Teams als leistungsstarkes Produktivitätstool und als Plattform für moderne Kollaboration entwickelt. Denn seine Funktionen fördern neue Arten der Zusammenarbeit. Jedoch führt die tiefe Integration von MS Teams in Microsoft 365 und Azure Active Directory (AD) zu Herausforderungen für IT- und Compliance-Abteilungen, denen die Rolle des Ordnungshüters übertragen wird. Die Regulation von Inhalten und deren Ausbreitung muss zwar Teil der Sicherheitsstrategie sein, um das Unternehmen vor dem Risiko des Datenmissbrauchs zu schützen. Doch wie kann eine solche Steuerung aussehen, damit sowohl Effizienz als auch Sicherheit gewährleistet sind?

Risikofaktor Unübersichtlichkeit

Die Einführung von Tools wie MS Teams sollte durchdacht mit Governance-Richtlinien erfolgen, damit die vereinfachte und erhöhte Kollaboration nicht mit einem gesteigerten Sicherheitsrisiko einhergeht. Der überstürzte Einsatz ohne klar definierte Richtlinien, Anleitungen und Durchsetzung kann auf ein Durcheinander an Accounts und Arbeitsbereichen auf MS Teams hinauslaufen. Irrtümlicherweise könnten mehrere Teams für denselben Zweck erstellt worden sein, denn ohne Steuerung ist es nur allzu leicht, viele neue Teams und Channels aufzusetzen.

Das gegenteilige Extrem sollte aber auch vermieden werden. Übermässige Restriktionen können die Akzeptanz von MS Teams negativ beeinflussen, sodass die Vorteile in den Hintergrund rücken. Wenn alle Anfragen über eine Ordnungsstelle laufen und die Bereitstellung eines neuen Teams ein langwieriger und komplizierter Prozess ist, werden die Mitarbeitenden diese nicht nutzen und sich selbst Abhilfe schaffen. So entsteht eine Schatten-IT, die ebenfalls eine organisatorische Herausforderung darstellt, die sicherheitsrelevante Aspekte untergräbt.

Gefährlicher Wildwuchs

Die entstandene Unübersichtlichkeit ist einerseits ein Problem für die reibungslose Zusammenarbeit im Unternehmen, sowie andererseits auch ein potenzielles Einfallstor für Cyberkriminelle. Durch das Fehlen von Governance und eines Lifecycle-Managements von Kollaborationstools entsteht – ohne sich dessen bewusst zu sein – ein Berg von in Vergessenheit geratenen Teams. Diese beanspruchen Speicherkapazitäten und erhöhen den Wartungsaufwand. Die verwaisten Teams und Channels, in welchen externe Nutzer:innen involviert sind, sowie die Schwierigkeiten bei der Identifizierung unbekannter öffentlich freigegebener Inhalte, können zu Datenlecks führen, wenn diese nicht konform archiviert oder gelöscht werden. In einer zunehmend vernetzten Welt betrifft dieses Problem das gesamte Microsoft-Ökosystem.

Problemlösung durch automatisiertes Provisioning

uniQconsulting hat selbst mit dieser Herausforderung gekämpft und nun eine Lösung entwickelt. Die App «Teamarin» wurde für MS Teams entwickelt, um die Arbeitsumgebung der Mitarbeitenden intuitiv zu gestalten, Kollaboration einfach zu ermöglichen und trotzdem die Sicherheit nicht ausser Acht zu lassen. Die Provisioning- und Lifecycle-Lösung gewährleistet eine kontrollierte Art der Teambildung, bei der Governance-Anforderungen wie Namenskonventionen und Berechtigungsvorgaben automatisiert angewendet und einfach geklont werden können. Die richtlinienkonformen Templates können spezifisch auf das Unternehmen angepasst werden, um die Konformität, Compliance und Sicherheit individuell sicherzustellen. Der automatisierte Prozess verbessert selbstorganisierte Arbeitsmodelle: Mitarbeitende sollen so selbst Teams und Channels erstellen, Daten sicher teilen und Gäste einladen können, ohne von Richtlinien oder langwierigen Genehmigungsprozessen ausgebremst zu werden. Zudem wird auch die Archivierung geregelt, indem relevante Inhalte gesichert und entsprechend archiviert sowie die Zugriffsrechte von Gästen bereinigt werden.

Integration mit Mehrwert

Die App «Teamarin» ermöglicht eine durchgehende Integration von MS Teams, sodass Mitarbeitende intuitiv handeln, effizient vorgehen und sicher kollaborieren können. Jedoch profitieren nicht nur Unternehmen und deren Belegschaft. Sämtliche Applikationen aus dem Hause uniQconsulting tragen eine Adaption der Funktion und eines Tieres der roten Liste der IUCN als Produktname. Der Name «Teamarin» ist inspiriert durch den «Golden-headed Lion Tamarin». Das Goldkopflöwenäffchen lebt mit seiner löwenartigen Mähne im brasilianischen Staat Minas Gerais und ist stark bedroht. uniQconsulting spendet zwei Prozent jeder Subscription-Gebühr an eine Tier- und Artenschutzorganisation, um die weltweite biologische Vielfalt zu stärken.

Dr. Alfred J. Beerli
CEO uniQconsulting

Interview mit Dr. Alfred J. Beerli, CEO uniQconsulting

Herr Beerli, worauf führen Sie die Herausforderungen hinsichtlich digitaler Zusammenarbeit zurück?
Während der Coronapandemie mussten Unternehmen schlagartig reagieren, um Mitarbeitenden Homeoffice zu ermöglichen. Viele Firmen nutzten dazu die zahlreichen Funktionalitäten von Microsoft 365 und Teams. Nebst den Tools mussten Mitarbeitende sich abrupt mit neuen Arbeitsweisen befassen. Nach wie vor fehlen deshalb Prozesse, wer, wie, wann, welche Teams und Channels eröffnen darf. Daraus entstanden individuelle Nutzungsmuster und eine unübersichtliche Datenablage ohne Regelwerk.

Inwiefern verhindert dies die volle Nutzung aller Potenziale von MS Teams?
Zum einen werden die vielseitigen Möglichkeiten von MS Teams oft direkt über die Berechtigungsstufe zensiert. Zum anderen muss diese Frage aus einem erweiterten Blickwinkel beleuchtet werden. MS Teams ist eine vollumfängliche Kollaborationsplattform für die interdisziplinäre Zusammenarbeit bei Projekten und Innovationen. Dies fordert neue Arbeitsweisen und Methoden. Viele der Unternehmensstrukturen sind aber noch entlang einer funktionalen Organisationsstruktur aufgebaut. Die Zusammenarbeit wird dadurch behindert. Hat dieser Wandel einmal stattgefunden und das Unternehmen sich den neuen Arbeitsweisen angepasst, kann das Wissen einfacher durch die Organisation fliessen und die Funktionen von MS Teams werden entsprechend besser genutzt.

Was ist für Mitarbeitende bei der Nutzung von MS Teams wichtig?
Sie müssen das Tool einfach und schnell nutzen können, ohne sich mit Guidelines, Richtlinien oder Einschränkungen zu befassen. Für das Management ist essenziell zu verstehen, dass Kollaboration nicht nur aus Chats und Videokonferenzen besteht, sondern dass sich weitere Wege der Zusammenarbeit öffnen. Alle Mitarbeitenden können von gegenseitigem Wissensaustausch profitieren und so ihr Know-how erhöhen.

Welche Vorteile ergeben sich businessseitig?
In einem Unternehmen ist dieser Gedankenaustausch ein fundamentales Element für Innovationen. Das gilt nicht nur intern, sondern auch extern: Die Kollaboration mit der Kundschaft ist genauso wichtig. Wer klar und transparent zusammenarbeitet und kommuniziert, wird immer im Vorteil sein.

Wie kann «Teamarin» diesen Kollaborationsgedanken stärken?
Die App ermöglicht Mitarbeitenden, nach Bedarf Teams und Channels zu erstellen, ohne sich dabei um die Governance und Sicherheit kümmern zu müssen. Die unternehmensspezifischen Richtlinien sind bereits in den jeweiligen Templates abgebildet. Diese können im Hintergrund jederzeit angepasst werden, sollten neue Anforderungen aus dem Business entstehen oder neue Tools zur Verfügung stehen.

Die IT-Abteilung wird insofern entlastet, dass sie die Rolle des Ordnungshüters automatisiert. Weitere Funktionen wie das standardisierte Housekeeping sichern das Lifecycle-Management von ungenutzten Teams und Channels, um die Datenmenge und die Gastzugriffe im Blick zu behalten. Dadurch schliesst «Teamarin» eine Sicherheitslücke, die Cyberkriminelle als Einfallstor nutzen können.

Wie erhöht «Teamarin» die drei Aspekte der Nachhaltigkeit?
Auf der sozialen Ebene erhalten die Mitarbeitenden die Möglichkeit, mit der Kundschaft oder intern in funktionsübergreifenden Arbeitsgruppen zusammenzuarbeiten. Gleichzeitig wird auf der ökonomischen Ebene der Betrieb entlastet und Kosten eingespart. «Teamarin» trägt zudem die ökologischen Aspekte einer neu auflebenden Kultur mit. Mit dem Namen und der dahinter liegenden Idee der Sinnhaftigkeit können sich sowohl unsere Mitarbeitenden als auch unsere Kundschaft eingehender identifizieren. Alle Apps der neuen Kompetenzmarke uniQinu tragen daher als Markenbild eine Visualisierung einer bedrohten Tierart aus der roten Liste der IUCN. Der jeweilige Produktname wird aus dem Namen der Art und der Funktion der App gebildet.

Individuelle Standardisierung durch «Teamarin»

Templating und Kloning: Teamarin sorgt für Effizienz und Konformität gemäss unternehmensspezifischen Vorgaben, Richtlinien und Berechtigungsstufen. Das Klonen von bestehenden Teams und Private-Channels inklusive Microsoft Apps wird durch Teamarin möglich.

Mitgliederverwaltung und Management: Teamarin ermöglicht die Benutzerverwaltung sowohl über einzelne User:innen als auch AD-Gruppen.

Lifecycle-Management und Housekeeping: Teamarin regelt und automatisiert den Prozess, wie Teams beantragt, genehmigt, angelegt, verwaltet und archiviert werden. Relevante Inhalte werden gesichert und Gästezugriffe bereinigt.

Gästezugriff und externes Sharing: Einfacher Datenaustausch und Kollaboration erfolgt automatisiert durch die Abbildung von Unternehmensrichtlinien.

IT-Betrieb und Logging: Die Mitarbeitenden werden befähigt, selbstorganisiert Teams nach Bedarf zu erstellen bei gleichzeitiger Entlastung der IT-Abteilung.

Weitere Informationen unter
uniQconsulting.ch

teamarin
UNIQ consulting

Nur wer die Welt der Hacker versteht, kann effektiven Schutz bieten

Bei Hackerangriffen handelt es sich längst nicht mehr um Einzelfälle, die von Individuen verübt werden. Vielmehr agieren Cyberkriminelle heute organisiert und professionell. Die Fachleute der Infoguard AG kennen sich mit den Wirkmechanismen der Angreifer bestens aus – und sind dank langjährigem Sicherheits-Know-how sowie modernster Technik in der Lage, Firmenkunden effizient zu schützen – vor, während und nach einem Angriff.

Interview mit CEO Thomas Meier und Mathias Fuchs, Vice President Investigation & Intelligence, Infoguard AG

Thomas Meier
CEO

Mathias Fuchs
Vice President Investigation & Intelligence

Thomas Meier, Mathias Fuchs, wie schätzen Sie die aktuelle Bedrohungslage für Unternehmen ein?
Mathias Fuchs: Interessanterweise war es in diesem Sommer überraschend ruhig an der Cyberfront. Während man beim Ausbruch des Kriegs in der Ukraine noch davon ausging, dass die Anzahl der Attacken aus dem Netz zunehmen würde, war eher das Gegenteil der Fall. Ransomware-Angriffe, sprich die Verschlüsselung von Unternehmensdaten und -systemen, nahmen über den Sommer hinweg ab. Allerdings ist diese ruhige Phase nun vorbei: Am vergangenen Wochenende haben wir gleich mehrere Cases registriert. Diese Ab- und Zunahme eröffnet uns spannende Einblicke in die Ökonomie der Cyberangreifer: Diese funktioniert ähnlich saisonal wie die «normale» Wirtschaft.

Warum nahm die Anzahl der Attacken gerade zum Ukraine-Krieg hin ab?
Mathias Fuchs: Wir beschäftigen uns sehr ausgiebig mit dem Thema Cyberkriminalität und sind entsprechend nahe am Geschehen. Wir wissen daher, dass viele der Teams, die Ransomware-Angriffe durchführen, sich sowohl aus ukrainischen als auch aus russischen Leuten zusammensetzen. Der Krieg stellte auch für sie einen Konfliktgrund dar und führte teilweise gar dazu, dass sie sich zersplitterten und gegenseitig unterminierten.

Thomas Meier: Wenn wir uns aber jetzt das aktuelle Volumen an Angriffen betrachten, stellen wir ein extrem hohes Wachstum fest. Während wir vor einigen Jahren vielleicht 40 Fälle von Ransomware-Attacken pro Jahr betreuten, hat sich deren Anzahl per 2021 mit 125 Cases mehr als verdreifacht.

Wo stehen wir aktuell in diesem Jahr?
Thomas Meier: Bisher haben wir 110 Cases verzeichnet. Allerdings muss man diese Zahlen ein Stück weit relativieren: Infoguard ist mittlerweile in der gesamten DACH-Region tätig, wodurch wir es natürlich mit mehr Vorfällen zu tun bekommen, als wenn wir weiterhin primär in der Schweiz operierten. Als kompetente Anlaufstelle für Incident-Response konnten wir uns dank unserer weitreichenden Erfahrung sowie ausgewiesenen Expertise sehr gut etablieren und positionieren. Das ist wichtig, da sowohl die schiere Anzahl als auch die Aggressivität der Ransomware-Attacken zunimmt und die Gefährder zunehmend professioneller agieren.

Welche präventiven Massnahmen kann man Unternehmen empfehlen?
Mathias Fuchs: Die Gefahrenquelle Nummer eins für Unternehmen stellt nach wie vor das Handling von externen Zugriffsmöglichkeiten dar. Jedes Mal, wenn ich einer Person oder Organisation Zugang zu meinem System erlaube, kann dies zu einer potenziellen Sicherheitslücke werden. Aus diesem Grund ist es essenziell, eine echte Multifaktor-Autorisierung zu aktivieren. Dies muss heute in jedem Betrieb zum Pflichtprogramm gehören.

Thomas Meier: Dann gibt es leider immer wieder Computersoftware-Schwachstellen, welche von extern angreifbar sind. Um solche Schwachstellen zu schliessen, ist das regelmässige Durchführen von Updates enorm wichtig. Zudem gibt es noch sogenannte «Zero-Days». Dabei handelt es sich um Schwachstellen, die sowohl den Userinnen und Usern als auch den Anbietenden unbekannt sind und von Angreifern gezielt ausgenutzt werden können. Des Weiteren lohnt es sich, wenn wir von präventiven Massnahmen sprechen, frühzeitig auch die Partnerschaft mit einem Unternehmen zu etablieren, das auf das Handling von Sicherheits-Incidents spezialisiert ist. Wir von Infoguard überprüfen zum Beispiel die getroffenen Schutzmassnahmen unserer Kundenfirmen und führen entsprechende Audits sowie gezielte Penetrationstests durch. Bei der «Attack-Simulation» agiert ein Angriffsteam von uns wie eine Hacker-Organisation und führt Cyberangriffe in der vollen Bandbreite durch – natürlich ohne die Systeme zu schädigen. Basierend auf den Erkenntnissen der verschiedenen Massnahmen erstellen wir dann eine ausführliche Roadmap zur weiteren Verbesserung der Cybersicherheit.

Wenn es zu einem Incident gekommen ist – wie geht man vor und wie kann Infoguard seine Kundschaft unterstützen?
Thomas Meier: Unser Unternehmen besteht seit mehr als 20 Jahren und von Anfang an war «Security» unsere DNA. Dementsprechend haben wir Cyber Security umfassend aufgebaut. Einen Teil davon bildet der Bereich «Prevention», der die bereits umrissenen Schutzmassnahmen umfasst. Zudem haben wir sehr früh Detect- und Response-Infrastrukturen sowie die entsprechenden Prozesse und das Expertenteam aufgebaut. Heute kommt man nicht mehr darum herum, sich für einen konkreten Schadensfall zu wappnen. Und gerade, wenn es um das Reagieren und das richtige Vorgehen bei sicherheitsrelevanten Incidents geht, sind wir bei Infoguard führend. Unsere Klientel setzt sich daher aus eher grösseren Unternehmen zusammen, die in sämtlichen Branchen tätig sind. Die Bandbreite reicht von Banken und Versicherungen über Industrieunternehmen aller Art. Auch Energieunternehmen, Spitäler sowie die Chemie- und Pharmabranche decken wir ab, ebenso Dienste der Öffentlichen Hand.

Was kann man sich unter dem Cyber Defence Center von Infoguard vorstellen?
Thomas Meier: Dabei handelt es sich um eine zentrale Plattform, über die wir sämtliche SOC-Dienstleistungen (Security Operation Center) für unsere Kundschaft verfügbar machen. Dadurch können sich unsere Cyber-Defence-Expert:innen 24 Stunden am Tag sowie sieben Tage die Woche der Sicherheit unserer Kundschaft widmen. Rund 200 Fachleute sind hierfür im Einsatz, um eine 360-Grad-Abdeckung bezüglich Cybersicherheit bieten zu können. Und wir gehen noch einen Schritt weiter: Kürzlich bauten wir ein brandneues SOC, welches mehr als 550 Quadratmeter umfasst. In diesen Räumlichkeiten arbeiten Analyst:innen Hand in Hand mit unseren Incident-Response-Teams und Plattformentwickler:innen zusammen. Auf diese Weise bündeln und konzentrieren wir unser Sicherheits-Know-how zusätzlich. Und davon profitieren natürlich unsere Kundenunternehmen.

Mathias Fuchs: Typischerweise begleiten wir unsere Kundschaft hinsichtlich Cyber Security von A bis Z. Im Angriffsfall unterstützen wir also den Krisenstab und führen schnellstmöglich forensische Arbeiten durch. Auf diese Weise eruieren wir unter anderem, wie die Angreifer ins System gelangt sind und wie sie sich darin konkret bewegen. Zudem prüfen wir, welche Daten exfiltriert wurden. Ferner können wir jederzeit spezialisierte Anwältinnen und Anwälte hinzuziehen, um potenzielle juristische Folgen ebenfalls direkt zu adressieren. Das entspricht unserem Anspruch, alles sicherheitsrelevanten Dienstleistungen aus einer Hand erbringen zu können.

Mathias Fuchs: Im Gegensatz zu vielen anderen Sicherheitsdienstleistern besteht unser wesentlicher Fokus darin, den finanziellen Schaden eines Cyberangriffs möglichst gering zu halten. Wir möchten also den Cashflow einer Firma aufrechterhalten und entlang der unternehmerischen Wertschöpfungskette des Kunden retten, was noch zu retten ist. Zu diesem Zweck ist eine schnelle Reaktion unumgänglich, weswegen das Cyber Defence Center eine so zentrale Rolle spielt.

Und was geschieht, wenn nichts oder kaum noch etwas zu retten ist?
Mathias Fuchs: Wir verfügen über ausreichend Erfahrung, um die meisten Unternehmen zu befähigen, einen sicheren Minimalbetrieb aufzunehmen. Dadurch können sie ihrer Geschäftstätigkeit partiell nachkommen und dann auch zeitnah wieder voll produktiv werden. Im Übrigen gehört auch die Verhandlung mit den Angreifern zu unserer Dienstleistung, etwa bei Ransomware-Attacken, die stets mit einer Lösegeldforderung einhergehen. Dieser Dialog dient dazu, uns sowie dem Kundenunternehmen Zeit zu verschaffen, die Arbeitsweise der Cyberkriminellen besser zu verstehen – und im Idealfall Zwietracht zwischen den gegnerischen Akteuren zu säen. Die Kombination aus Expertise sowie schneller Reaktion führt dazu, dass unsere Kundschaft in den allerseltensten Fällen die Erpresser bezahlen muss.

Wie wird sich die Bedrohungslage aus dem Netz Ihrer Meinung nach künftig verändern?
Thomas Meier: Das Verbrechen ist immer da, wo auch das Geld ist. Die Motivation der Angreifer wird sich also nicht grundlegend verändern in Zukunft. Die Frage ist, wie bald die IT-Infrastruktur einen so hohen Sicherheitsstandard erreicht, dass sie die Gefährder dazu zwingt, aufzustocken und noch professioneller zu agieren. Denn obschon sich bereits eine regelrechte «Hacker-Ökonomie» gebildet hat, gibt es noch Potenzial nach oben. Dessen muss man sich bewusst sein – und sich entsprechend vorbereiten.

Mathias Fuchs: Wir werden einen Sprung in der Qualifikation der Angreifenden sehen. Das ist insofern kritisch, als dass die Angriffsfläche nicht kleiner wird, sondern sich vielmehr vergrössert: Das Internet der Dinge sowie der vermehrte Sicherheitsbedarf bei OT (Betriebstechnologie kritischer Infrastrukturen) werden unseren Alltag immer stärker durchdringen. Wir bereiten uns darauf vor, indem wir uns heute schon auf Technologien fokussieren, die noch nicht breit eingesetzt werden. Das wird sich in Zukunft ändern – und dafür wollen wir bereit sein.

Über die Infoguard AG

Die Infoguard AG ist spezialisiert auf umfassende Cyber Security. Ihre rund 200 Sicherheitsexpert:innen sorgen tagtäglich für die Cyber Security bei über 400 Kunden in der Schweiz, Deutschland und Österreich. Zu den Kompetenzen zählen massgeschneiderte Dienstleistungen im Bereich der Sicherheitsberatung und Security Audits sowie in der Architektur und Integration führender Netzwerk- und Security-Lösungen. Cloud-, Managed- und Cyber Defence Services erbringt der Schweizer Cyber-Security-Experte aus dem ISO 27001 zertifizierten Infoguard Cyber Defence Center in der Schweiz, welches im September 2022 auf die doppelte Fläche vergrössert und personell ausgebaut wurde. Infoguard hat ihren Hauptsitz in Baar/Zug sowie eine Niederlassung in Bern. Zudem ist Infoguard ISO/IEC 27001:2013 zertifiziert und Mitglied bei FIRST (Global Forum of Incident Response and Security Teams).

Weitere Informationen unter
www.infoguard.ch

InfoGuard
SWISS CYBER SECURITY

Wie sicher sind digitale Zutrittssysteme?

Zutrittssysteme müssen höchste Sicherheitsanforderungen erfüllen. Sie steuern, wer zu welcher Zeit und für welchen Ort eine Zugangsberechtigung erhält. Sie gewährleisten den Schutz für Gebäude, Mitarbeitende, Güter und Daten. Beat Aeschimann, der seit über 20 Jahren in der Sicherheitsindustrie tätig ist, erklärt, wie sicher solche Systeme sind.

Beat Aeschiman

Welche Sicherheitsbedürfnisse muss ein digitales Zutrittssystem erfüllen?
Sicherheit ist etwas sehr Individuelles. Für Menschen, Firmen und Gebäude gibt es ganz unterschiedliche Anforderungen hinsichtlich Sicherheit und Zutritt. Was beispielsweise für eine Bank die perfekte Lösung in Sachen Zutritt darstellt, kann in einem Krankenhaus oder Handwerksbetrieb den täglichen Ablauf behindern.

Grundsätzlich werden digitale Zutrittssysteme als Cloud- oder On-Premises-Lösung angeboten. Letztere setzen eine gewisse IT-Infrastruktur wie Server oder ein Rechenzentrum und entsprechendes IT-Know-how voraus. Cloud-Lösungen hingegen bieten den Vorteil, dass sie mit geringerem Initialaufwand betrieben werden können.

Beide Systeme haben ihre Vor- und Nachteile und werden unterschiedlichen Sicherheitsanforderungen gerecht. Machbarkeit, Kosten und Risiken müssen individuell bestimmt und abgewogen werden. Das Zutrittssystem regelt immer, wer wann und wo Zutritt erhält, aber nicht, unter welchen Bedingungen und wie der Zutritt vergeben wird.

Haben die Sicherheitsanforderungen in den letzten Jahren zugenommen?
Die Zahl und die Kosten von Cyberangriffen sind in den letzten Jahren kontinuierlich gestiegen. Dementsprechend haben die Anforderungen an die Sicherheit zugenommen, auch bei den Zutrittssystemen. Das äusserst sich unter anderem in neuen Vorgaben und Gesetzen. Nehmen wir als Beispiel den Datenschutz. Auch wir als Entwickler von Zutrittssystemen müssen diese Richtlinien erfüllen.

Für die Entwicklung unserer Hard- und Softwares eruieren wir im Austausch mit unseren Kundinnen und Kunden aktuelle Sicherheitsanforderungen und berücksichtigen sie bei zukünftigen Entwicklungen. Ein gutes Beispiel dafür ist der digitale Schlüssel auf dem Smartphone. Ziel war es, eine digitale und sichere Lösung zu bieten. Das haben wir mit Mobile Access erreicht, indem wir sowohl den digitalen Schlüssel als auch die Übertragung verschlüsseln.

Was unternimmt dormakaba für die Sicherheit digitaler Zutrittssysteme?
dormakaba greift hier verschieden Strategien auf, da auch Cyberangriffe unterschiedliche Stellen angreifen. Ein wichtiger Faktor ist dabei der enge Austausch mit Kunden sowie die Sensibilisierung aller Beteiligten. Penetrationstests, Security-Audits, Updates und Zertifizierungen sind weitere wichtige Faktoren. Wir sehen Sicherheit nicht als gegebenen Zustand. Unsere Aufgabe ist es, Sicherheit jeden Tag kritisch zu prüfen und wenn notwendig zu verbessern.

Zur Person

Beat Aeschimann ist seit über 20 Jahren in der Sicherheitsindustrie tätig, Sicherheitsberater für Zutritts- und Türtechnik sowie Mitglied der Geschäftsleitung der dormakaba Schweiz AG.

Zutrittsverwaltung für Liegenschaften

resivo ist ein zukunftsweisendes, cloudbasiertes Zutrittsmanagementsystem. Es bietet Verwaltungen sowie Menschen, die Häuser besitzen oder zur Miete wohnen, wesentliche Vorteile gegenüber herkömmlichen mechanischen Schliesssystemen. Der Zutritt erfolgt digital mit Badge, Schlüsselanhänger oder Smartphone. Verlorene oder gestohlene Schlüssel bilden kein Sicherheitsrisiko mehr und Wohnungsübergaben werden einfacher und smart. Die einzigartige Hoheitstrennung des Systems ermöglicht eine zuverlässige Trennung. Mietende bestimmen so selbst, wer wann Zutritt zur Wohnung erhält – auch aus der Ferne. Mit resivo eröffnet sich eine neue Dimension der Gebäudenutzung voller Vorteile.
resivo.dormakaba.com

dormakaba Schweiz AG
www.dormakaba.ch
info.ch@dormakaba.com

dormakaba

Private 5G-Netze als Schlüssel für sichere Kommunikation

Angesichts einer Zunahme von E-Mail-Bedrohungen um über 100 Prozent sind immer mehr Unternehmen bereit, mit externen Partnern zusammenzuarbeiten. Eine Studie zeigt zudem, dass verbesserte Security- und Datenschutzfunktionen etwa das Hauptmotiv für den Ausbau privater 5G-Netze darstellen.

Immer mehr Betreiber von vernetzten Produktionsanlagen, Krankenhäusern oder anderen «smarten» Infrastrukturen sind auf der Suche nach Alternativen zu öffentlichen 5G-Netzwerken und erhoffen sich durch private 5G-Netze eine bessere Abdeckung sowie Kontrolle, niedrige Latenzzeiten und ein höheres Sicherheitsniveau. Solche Umgebungen weisen jedoch eine Reihe an Sicherheitsanforderungen auf, die herkömmliche IT- und OT-Umgebungen nicht haben. Allen voran gilt die Offenlegung von Daten, die über das private Funknetz übertragen werden, als die grösste Herausforderung, wie eine Studie von Trend Micro, einem der weltweit führenden Anbieter von Cybersicherheitslösungen, zeigt. Dazu wurden 400 Entscheidungsträger für Informationssicherheit aus 400 Unternehmen in den USA, Deutschland, Grossbritannien und Spanien befragt.

Grosse Erwartungen an die 5G-Security

Weitere relevante Angriffsvektoren sind Software-Schwachstellen in Betriebssystemen, Konfigurationsfehler, Schwachstellen in der Netzwerkausrüstung, Geräteschwachstellen in Ran- und Core-Netzwerken sowie die Kompromittierung des angeschlossenen Netzwerks. «Private 5G-Netzwerke sind unübersichtlich: Zwei Drittel der Befragten geben an, die Technologie zukünftig in irgendeiner Form einsetzen zu wollen», sagt Eric Hanselman, Chefanalyst bei 451 Research, einem Teil von S&P Global Market Intelligence. «Das Modell der geteilten Verantwortung in der Cloud bedeutet jedoch, dass Unternehmen dabei ihre eigenen Sicherheitsfunktionen aufbauen müssen. Dazu brauchen sie kompetente Partner, die sie auf diesem Weg unterstützen. Unternehmen haben grosse Erwartungen an die 5G-Security. Dabei wird es jedoch vor allem auf die Qualität ihrer Partnerschaften ankommen.»

Nur teilweise automatisierte Verbindungen

Eine weitere Herausforderung bei Security-Projekten wird sein, dass nur 23 Prozent der Befragten eine vollständige Integration von Private-5G-Security mit der bestehenden OT-Security erwartet. Nur etwas mehr als die Hälfte (55 Prozent) rechnet mit teilweise automatisierten Verbindungen mit bestehenden Sicherheitssystemen. Daraus lässt sich ableiten, dass Unternehmen zwar die Wichtigkeit von 5G-Sicherheit erkannt haben, jedoch die Zusammenarbeit unterschiedlicher Security-Teams noch nicht vollständig definiert haben. Dies lässt eine Silobildung befürchten.

Umfassendes Technologie-Bewusstsein

Angesichts der Komplexität solcher Projekte ist es nicht überraschend, dass mehr als die Hälfte (58 Prozent) der Befragten angeben, sie würden Risikobewertungen entweder gemeinsam mit Partnern durchführen oder die Aufgabe vollständig auslagern. 33 Prozent geben an, darüber hinaus mit einer dritten Partei zusammenzuarbeiten. Branchenspezifische Expertise in Sachen Security (24 Prozent) ist das wichtigste Kriterium für Unternehmen, die IT-Partner suchen. 19 Prozent geben ausserdem an, mit bereits bestehenden Partnern zusammenarbeiten zu wollen. «Wir sehen das Management von Sicherheitsrisiken als einen der wichtigsten Treiber für das Geschäft. Deswegen wollen wir sicherstellen, dass Unternehmen ein umfassendes Bewusstsein über die Technologie erhalten, die hinter IT, OT und Kommunikationstechnik wie privaten 5G-Netzwerken steht», erklärt Udo Schneider, IoT Security Evangelist bei Trend Micro.

Erstes privates 5G-Netzwerk der Schweiz

Die stürmsfs ag, eines der modernsten Stahl- und Metall-Service-Center Europas, hat das erste private 5G-Netzwerk in der Schweiz in Betrieb genommen. Für den Aufbau und Betrieb arbeitete die Firma unter anderem mit dem Kommunikationsnetzausrüster Nokia zusammen. Das Schweizer Unternehmen Dätwyler verantwortet die Implementierung der gesamten technischen Infrastruktur vor Ort – von der Verkabelung bis hin zur verbauten Antennentechnik. Intel unterstützt diese Entwicklung mit Schlüsseltechnologien für Konnektivität und IoT-Edge-Computing, wie es auf der Firmenhomepage heisst.

Smart Manufacturing

Die 5G-Technologie wird den Weg der stürmsfs in Richtung Smart Manufacturing ebnen: Über diesen besonders leistungsfähigen Funkstandard sollen künftig alle relevanten Assets der Fertigung miteinander vernetzt werden. Als Software kommt dabei die Open-Source-Lösung IndustryFusion zum Einsatz. «IndustryFusion ist von Grund auf als herstellerübergreifende Vernetzungslösung gedacht, die eine interoperable Verknüpfung von Maschine, Fabrik und Cloud-Plattformen schafft. Die einfache Implementierung ist zentraler Bestandteil der Lösung und befähigt Unternehmen jeder Grösse Fertigung & Produkte intelligent zu digitalisieren und die Vorteile einer fortschreitenden Digitalisierung zu nutzen», sagt Igor Mikulina, Präsident der IndustryFusion Foundation, die ihren Sitz in St. Gallen hat.

Sichere Datenverarbeitung vor Ort in Echtzeit

Die Vernetzung von Fertigungstechnik, Robotik und beweglichen Assets im Rahmen von Campus-Mobilfunknetzen ist eine wichtige Voraussetzung für einen höheren Automatisierungsgrad, Produktivitätssteigerungen und damit letztlich für Industrie 4.0: «Die Nokia Digital Automation Cloud (DAC) ist eine industrietaugliche Campuslösung und Plattform für die Digitalisierung. stürmsfs ist damit ein wichtiger Schritt zur Smart Factory gelungen», erläutert Patrick Langelaan, Vice President für den Enterprise-Markt in Südeuropa bei Nokia. «Die DAC-Bereitstellung bietet eine zuverlässige Konnektivität mit hoher Bandbreite und geringer Latenz für Sensoren, Maschinen, Fahrzeuge und andere Geräte. Gleichzeitig wird sichergestellt, dass alle Daten im Unternehmen verbleiben und vor Ort in Echtzeit verarbeitet werden.» Dadurch behält die stürmsfs ag auch die volle Kontrolle über sein Produktions-Know-how – ein klarer Vorteil gerade auch puncto sichere Kommunikation.

«Der Ernstfall ist nur eine Frage der Zeit»

Cyberangriffe auf Firmen nehmen zu und gleichzeitig agieren Hacker immer gezielter und professioneller. Die Kooperation zwischen BearingPoint und Arco IT erhöht die Chancengleichheit für Unternehmen: Denn dank der kombinierten Fach-, Markt- sowie Technik-Expertise der beiden Firmen profitiert die Kundschaft auf mehreren Ebenen. «Fokus» wollte mehr erfahren.

Interview mit Matthias Roeser, Partner BearingPoint AG und Bertram Dunskus, CEO Arco IT GmbH

Matthias Roeser
Partner BearingPoint

Bertram Dunskus
CEO Arco IT

Matthias Roeser, Bertram Dunskus, Cyberangriffe auf Unternehmen und damit das Thema «Cybersecurity» sind derzeit in den Medien äusserst präsent. Berechtigterweise?
Matthias Roeser: Ohne Zweifel. Aktuelle Erhebungen zeigen, dass die Anzahl der Attacken steigt und das Gefährdungspotenzial immens hoch ist: Offizielle Zahlen sprechen davon, dass rund 60 Prozent der Unternehmen von Attacken betroffen sind – wobei ich die effektive Zahl noch deutlich höher einschätze. Zudem stellen wir vermehrt fest, dass der erlittene Schaden nicht mehr im Unternehmen versteckt werden kann: Dies unter anderem, weil häufig die Supply Chain eines Unternehmens betroffen ist und die Attacke dementsprechend weite Kreise zieht. Je nach Ausgangslage und Tragweite des Vorfalls schalten sich dann auch die Polizei und Staatsanwaltschaft ein.

Bertram Dunskus: Alle Anbieter von Sicherheitslösungen beobachten, dass die Nachfrage enorm gestiegen ist. Bei Arco schoss ab 2019 die Nachfrage in die Höhe, also sogar vor der Covid-Krise, was uns dazu veranlasst hat, unsere Dienstleistungen sukzessive auszubauen. Insbesondere die Zunahme von Ransomware-Angriffen stellt einen essenziellen Treiber dieser Entwicklung dar. Aus diesem Grund ist die Partnerschaft zwischen uns von der Arco IT und BearingPoint so wichtig: Auf diese Weise können wir unsere Kompetenzen für unsere Kundschaft bündeln und einen Service anbieten, der grösser ist als die Summe seiner Teile.

Bevor wir auf die konkreten Vorzüge dieser Partnerschaft eingehen: Können Sie uns die potenziellen Folgen eines Cyberangriffs aufzeigen?
Bertram Dunskus: Wenn wir zunächst nur ein einzelnes Unternehmen anschauen, ist es zum Beispiel der Ausfall von ganzen Geschäftsbereichen, der verheerende Folgen haben kann. Wenn etwa die IT eines Fertigungsbetriebs angegriffen wird und in der Folge die Produktions-Geräte stillstehen, entsteht praktisch sofort finanzieller Verlust. Das Bereinigen und Wiederherstellen der IT produziert auch erhebliche Kosten. Wenn wir aber das Unternehmen im Kontext seiner Geschäftspartner anschauen, offenbart sich ein zusätzliches, systemisches Problem: Durch die stark verknüpfte Supply Chain sind auch deren Aktivitäten betroffen. Und die Digitalisierung der Abläufe hat dazu geführt, dass die Angriffe oft auch Auswirkungen auf die IT-Systeme der Lieferanten und Kunden haben. Darum kommt schnell ein Schaden zusammen, der zehn- oder gar einhundertmal höher ausfällt als die Lösegeldforderung der Cyberkriminellen.

Matthias Roeser: Wir stellen immer wieder fest, dass Unternehmen, die ins Visier von Cyberkriminellen geraten sind, sich niemals hätten vorstellen können, wie weitreichend die Schäden dieser Angriffe sind – für sie selbst, ihre Kundinnen und Kunden sowie ihre Partnerunternehmen. Insbesondere das Feld der KMU weist in Sachen Cybersicherheit noch einen hohen Nachholbedarf auf. Das ist problematisch, da die Gegenseite heutzutage hochprofessionell aufgestellt ist – Cybercrime ist zum lukrativen Business geworden und funktioniert wie eine gut geölte Maschinerie. Dementsprechend kommen auch kleine und mittelgrosse Unternehmen nicht um ein professionelles Sicherheits-Set-up herum.

Welche Möglichkeiten haben Unternehmen denn, um sich gegen Angriffe zu wappnen?
Bertram Dunskus: Ein essenzieller erster Schritt besteht darin, die eigenen Risiken sachlich und strukturiert zu beurteilen. Glücklicherweise ist die Awareness für Cyber-Risiken in den letzten Jahren angestiegen. Wenn es um das Thema «Ransomware» geht, steht jedes Unternehmen in der Verantwortung, sich zu schützen. Das ist sehr schwierig im Alleingang, die Zusammenarbeit mit Sicherheits-Dienstleistern und Versicherungen ist daher sehr zu empfehlen.

Matthias Roeser: Gerade letzter Punkt ist für Firmen aller Branchen und Grössen sehr spannend: Nicht nur kann das Abschliessen einer Cyber-Versicherung einen Betrieb vor den gröbsten Schäden schützen, sie hilft auch bei der proaktiven Vorbereitung.

Inwiefern helfen die Versicherungen?
Matthias Roeser: In den meisten Fällen fordert der Versicherer das Einhalten von sicherheitsrelevanten Mindeststandards ein. Dadurch wird eine Firma quasi «gezwungen», Lücken in ihrem System zu adressieren. Mittlerweile wurde die Wichtigkeit des Ransomware-Themas auch politisch erkannt: Aktuell ist eine Parlamentsvorlage hängig, die eine Meldepflicht von Cyberangriffen umfasst. Das würde zu einem besseren Austausch sowie mehr Transparenz führen, was eine Grundvoraussetzung darstellt, um der zunehmend professioneller agierenden Gegenseite Paroli zu bieten.

Wie kann die Partnerschaft von BearingPoint und Arco IT dazu beitragen, Firmen gegen Cybercrime zu schützen?
Bertram Dunskus: BearingPoint und Arco IT kooperieren mit dem Ziel, sowohl die Management-Beratung abzudecken als auch das technische Know-how und die Security-Services anzubieten – und dadurch unserer Kundschaft eine «360-Grad-Abdeckung» ihrer Cybersicherheits-Bedürfnisse zu liefern.

Matthias Roeser: BearingPoint ist seit jeher der Go-to-Place für Organisationen, wenn es um die strategische Digitalisierung und damit um die sinnvolle Auswahl sowie erfolgreiche Implementierung neuer Tools und Technologien geht. Wir sind uns aber durchaus bewusst, dass im Rahmen der digitalen Transformation die Themenvielfalt unserer Kundschaft immer grösser wird. Mit Arco IT haben wir einen fokussierten Partner gefunden, der optimal vernetzt ist und qualitativ hochwertige Sicherheits-Expertise in ebenso erstklassige Lösungen umwandeln kann. Damit schaffen wir gemeinsam einen enormen Mehrwert für unsere Kundschaft.

Bertram Dunskus: Nebst dem technischen Fachwissen können wir durch die Bündelung unserer Kompetenzen auch einen Wandel im strategischen Denken anregen: Denn zusätzlich zum Schutz vor Cyberangriffen müssen Firmen unbedingt ein Krisenmanagement mit der Geschäftsführung etablieren. Nur so können sie im Ernstfall die Schäden minimieren, indem sie zielführend mit den Kunden und Mitarbeitenden, der Presse, Anwälten, Datenschutzbeauftragen und der Polizei kommunizieren.

Sie regen also bei den Kundenunternehmen auch ein kulturelles Umdenken an.
Matthias Roeser: In der Tat. Und dieser Change muss ganz oben seinen Anfang nehmen: Cyber-Risiken müssen ein Top-Thema im Verwaltungsrat sein, dieser steht in der Verantwortung. Das Thema ist auch darum so wichtig, weil sich die Situation für Unternehmen nicht entspannen wird, im Gegenteil: Sobald Hacker nicht mehr mit Angriffen auf die Ukraine und Partner beschäftigt sind, verlagern sich die Angriffe auf kommerzielle Ziele.

Bertram Dunskus: Darum müssen Unternehmen ihre Resilienz erhöhen – dabei können wir sie ideal unterstützen. Unsere Kundschaft schätzt die Kombination aus Business-Erfahrung und technischen Fähigkeiten, mit der optimierte und kostengünstige Strategien und Services für die Verbesserung der Cybersicherheit erhalten.

Wie läuft ein Mandat typischerweise ab?
Bertram Dunskus: Je früher wir von einer Firma beigezogen werden, desto besser. Idealerweise beginnen wir mit einem Security-Assessment. Dabei bewerten wir den Sicherheits-Status des Kundenbetriebs und helfen, eine Strategie zum Aufbau geeigneter Schutzmechanismen sowie konkreter Massnahmen für den Ernstfall zu definieren. Wenn die Strategie abgestimmt ist, unterstützen wir bei der Umsetzung, die in mehreren Phasen, oft über ein bis drei Jahre, abläuft.

Matthias Roeser: Die IT-Sicherheit ist heutzutage dermassen wichtig, dass die genannten Punkte zum Standardumfang unserer Beratung gehören. BearingPoints Anspruch besteht darin, Firmen dabei zu unterstützen, sich durch moderne Technologien neue Potenziale zu erschliessen. Da muss die Sicherheitsthematik dringend miteinbezogen werden, deswegen kooperieren wir mit Arco IT.

Welche primäre Handlungsempfehlung haben Sie für Geschäftsführerinnen und Geschäftsführer hinsichtlich IT-Sicherheit?
Matthias Roeser: Wenn ich mich auf eine einzige Handlungsempfehlung beschränken müsste, würde ich sagen: Sprechen Sie mit Ihrer Versicherung über die Möglichkeit, Cyber-Risiken zu versichern. Wie gesagt, profitiert man so von einer möglichen Schadensdeckung und wird vonseiten Versicherung Inputs erhalten, die wertvoll für das Absichern der eigenen IT-Systeme sein können.

Bertram Dunskus: Ich erachte es als enorm wichtig, eine systematische Bestandsaufnahme vorzunehmen. Dabei geht es um die Beantwortung von Fragen wie: Welche Ressourcen hat mein Betrieb? Wo sind die Lücken? Wer ist im Ernstfall verantwortlich? Und kann mein Geschäft weiterlaufen, wenn Teile davon verschlüsselt und damit auf Eis gelegt werden? Diese Bestandsaufnahme zu veranlassen ist Aufgabe eines jeden Verwaltungsrats, ebenso wie die Investition in Lösungen und Fachberatung zu ermöglichen, um bestehende Schwächen zu adressieren.

Über BearingPoint und Arco IT

BearingPoint ist eine unabhängige Management- und Technologieberatung mit europäischen Wurzeln und globaler Reichweite. Zu BearingPoints Kunden in über 70 Ländern gehören viele der weltweit führenden Unternehmen und Organisationen. Seit 2022 besteht eine Partnerschaft mit Arco IT.

Die Arco IT GmbH, mit Sitz in Zürich, unterstützt ihre Kunden seit 10 Jahren, eine IT Security aufzubauen, die auf ihre strategischen Ziele abgestimmt ist. Dazu liefert sie Security Assessments, CISO Beratung, Awareness Trainings und 24x7 Managed Detection and Response.

Durch die Kombination der Expertise der beiden Unternehmen können wir die ideale Präventions-Strategie sowie Massnahmen für den Ernstfall entwickeln.

Weitere Informationen unter
bearingpoint.com und **arco-it.ch**

BearingPoint®

arco
IT SECURITY SERVICES

«Cyberkriminalität wird immer aktuell bleiben»

Mit zunehmender Digitalisierung erhöht sich auch das Risiko für digitale Verbrechen. Das Nationale Zentrum für Cybersicherheit setzt sich für einen sicheren Cyberspace ein und macht die Bevölkerung mithilfe der aktuellen SUPER-Kampagne auf die Gefahren im Internet aufmerksam. Florian Schütz, Delegierter des Bundes für Cybersicherheit, im Gespräch mit «Fokus».

Interview **Vanessa Bulliard** Bild **KEYSTONE-SDA/Gaëtan Bally**

Florian Schütz, Sie sind Leiter des Nationalen Zentrums für Cybersicherheit. Was ist das Ziel des NCSCs?
Das Nationale Zentrum für Cybersicherheit ist das Kompetenzzentrum des Bundes für Cybersicherheit und damit die erste Anlaufstelle für Wirtschaft, Verwaltung, Bildungseinrichtungen und Bevölkerung bei Cyberfragen. Es ist für die koordinierte Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken verantwortlich. Das Hauptziel der NCS-Strategie und somit des NCSC ist die Erhöhung der Schweizer Resilienz gegen Cybervorfälle.

Weshalb braucht es das NCSC?
Die Cybersicherheit ist ein Thema, dessen Bedeutung in Zukunft weiter zunehmen wird. Der Schutz vor Cyberrisiken ist eine gemeinsame Verantwortung von Wirtschaft, Gesellschaft und Staat. Dies bedeutet zunächst, dass alle Akteur:innen für ihre eigene Sicherheit verantwortlich sind. Der Bund muss in erster Linie Rahmenbedingungen schaffen, damit sich Unternehmen selbst besser schützen können. Um die Bevölkerung, Wirtschaft, Bildungseinrichtungen und Verwaltung beim Schutz vor Cyberrisiken zu unterstützen und die Sicherheit der eigenen Systeme zu verbessern, hat der Bundesrat 2020 das Nationale Zentrum für Cybersicherheit geschaffen.

Hacker:innen sind nichts Neues. Was hat sich jedoch in letzter Zeit bezüglich Cyberattacken geändert?
Cyberkriminelle sind sehr innovativ und bringen immer neue Angriffsszenarien und -vektoren hervor. Versuchen sie, über den Faktor Mensch in ein System zu gelangen, wenden sie häufig aktuelle Themen und psychologische Tricks an, um ihre Angriffsversuche geschickt zu tarnen. Um technische Hürden einfach überwinden zu können, bedienen sich Cyberkriminelle oft des Darknets. Dort gibt es beispielsweise digitale Marktplätze, wo Zugangsdaten und Schwachstellen gehandelt werden. Interessierte Kriminelle können gegen entsprechendes finanzielles Entgelt Werkzeuge zur Ausnutzung dieser Sicherheitslücken kaufen. Das NCSC berichtet wöchentlich in seinen Rückblicken auf der Website über neue Angriffsmethoden.

In der Medienmitteilung vom 5. September erklären Sie, dass Cyberangriffe per E-Mail oder Messenger-Dienste zunehmen. Weshalb sind diese beliebte Ziele von Hacker:innen?
Die meisten Nutzer:innen von elektronischen Geräten erhalten jeden Tag viele Nachrichten – egal ob via E-Mail oder Messenger-Dienste. Jede dieser Mitteilungen sollte mit Sorgfalt gelesen und geprüft werden. Im Alltag wird dieses vorsichtige Verhalten aber oft durch fehlende Kenntnis, hohe Arbeitsbelastung oder Sorgen im Privatleben eingeschränkt. Dies wissen auch Cyberkriminelle und nutzen deshalb den Nachrichteneingang als Angriffsvektor im Massengeschäft. Denn selbst wenn nur ein kleiner Prozentsatz der Nutzer:innen auf die betrügerische Masche hereinfällt, lohnt sich das Geschäft für Cyberkriminelle.

Sie schreiben auf Ihrer Webseite, dass ein falscher Klick grossen Schaden verursachen kann. Was genau sind die Folgen?
Je nach Angriffsart sind die Folgen unterschiedlich. In den meisten Fällen werden Daten gestohlen, oder es entsteht ein finanzieller Schaden. Beispielsweise kann durch einen falschen Klick eine Schadsoftware auf dem Computer installiert und die Daten verschlüsselt werden. So kann man danach erpresst werden. Oder es kann sein, dass ein teures Abo abgeschlossen wird, aus dem man nur mühsam wieder herausfindet.

Bei Cyberangriffen denken viele: «Mich trifft es eh nicht.» Was sagen Sie dazu?
Die Menschen gehen grundsätzlich davon aus, da sie vermeintlich denken «nicht interessant zu sein». Oft sind sie sich nicht der Motivation und Möglichkeiten der Gegenseite bewusst und wissen nicht, was sie aufs Spiel setzen, wenn sie sich falsch oder bequem verhalten. Gerade mit der aktuellen SUPER-Kampagne wollen wir hier Aufklärung betreiben und die Nutzer:innen sensibilisieren.

Welche Massnahmen sollten Einzelpersonen treffen, um sich gegen Cyberattacken zu schützen?
Es gibt fünf zentrale Schritte, welche auf der Webseite *S-U-P-E-R.ch* beschrieben werden:

- *Sichern* Sie Ihre Daten regelmässig auf mindestens zwei Medien;
- *Updaten* Sie Ihr System, Ihre Programme und Apps regelmässig mit der neusten Version;
- *Prüfen* Sie bei Ihrem Gerät, ob es gegen Schadsoftware geschützt ist (Antivirus, Firewall usw.);
- *Einloggen* Loggen Sie sich nur mit starken Passwörtern ein. Jedes Mal ein anderes verwenden;
- *Reduzieren* Sie Betrugsrisiken im digitalen Raum mit einer gesunden Portion Misstrauen. Wahren Sie Privatsphäre und Datenschutz auch online. Erhalten Sie eine Nachricht, denken Sie, bevor Sie klicken.

Was sollten Unternehmen tun?
Cybersicherheit ist Chefsache! Es muss auf Geschäftsleitungsebene thematisiert werden und ein Risikomanagement bezüglich Cybervorfällen muss in jedem Unternehmen etabliert sein. Die Finanzierung der wichtigsten Massnahmen muss festgelegt und deren Umsetzung geregelt werden. Die damit verbundenen Investitionen scheinen gross, aber es muss nicht alles auf einmal gemacht werden. Priorisieren Sie! Eine Aufgabe, die die erste Priorität haben sollte, ist auf jeden Fall das Up-to-date-Halten der Systeme. Die meisten erfolgreichen, für Firmen verheerende Ransomware-Angriffe nutzen bekannte Schwachstellen aus – für die es Patches gibt.

Wie machen Sie die Bevölkerung auf potenzielle Cyberrisiken aufmerksam?
Einer unserer wichtigsten Kanäle ist die NCSC-Webseite. Auf dieser veröffentlichen wir Warnungen, Handlungsanleitungen und Checklisten für Cyberbedrohungen. Auch kann dem NCSC dort ein Cybervorfall oder eine Schwachstelle über ein Meldeformular gemeldet werden und man kann auf Wunsch Hilfestellungen zur Bewältigung erhalten. Neben unserer Webseite informieren wir regelmässig auf Social Media.

Zudem startete am 5. September bereits zum zweiten Mal eine nationale Sensibilisierungskampagne zum Thema Cybersicherheit. Diese bis zum 16. Oktober dauernde Kampagne wird vom Nationalen Zentrum für Cybersicherheit und der Schweizerische Kriminalprävention (SKP) gemeinsam mit den kantonalen und städtischen Polizeikorps durchgeführt.

Wie genau ist die Kampagne aufgebaut?
Das zentrale Element der Kampagne ist die Website *S-U-P-E-R.ch*. In diesem Jahr wird auf den Buchstaben «R wie Reduzieren» eingegangen. Der Fokus liegt dabei auf dem Risiko des Nachrichteneingangs. Es wird auf die Themen Phishing sowie die damit verbundenen verschiedenen Betrugsformen eingegangen. Ein Betrugsquiz und unterhaltsame Geschichten der Websters runden das Angebot auf der Webseite ab. Neben der Webseite wird auf den verschiedenen Social-Media-Kanälen oder auf Plakaten mittels Kernbotschaften auf die Thematik hingewiesen.

Die Kampagne erfolgt in Zusammenarbeit mit der Schweizerischen Kriminalprävention. Welche Vorteile ergeben sich daraus?
Eine wichtige gemeinsame Aufgabe der Schweizerischen Kriminalprävention und des Nationalen Zentrums für Cybersicherheit ist die Sensibilisierung und Aufklärung der Bevölkerung über Gefahren und Risiken im Internet sowie das Aufzeigen der damit einhergehenden Präventionsmöglichkeiten. Das Ziel ist die Vermittlung grundlegender Kenntnisse, mit denen sich Nutzer.innen von Computern und Smartphones in Eigenverantwortung vor Internetkriminalität schützen können. Um dieses Ziel möglichst effizient und ressourcenschonend erreichen zu können, sind das NCSC und die SKP eine präzise definierte Kooperation für die gemeinsamen SUPER-Sensibilisierungskampagnen eingegangen. Mit dieser Zusammenarbeit werden Fachwissen erweitert, Kräfte gebündelt und die potenzielle Reichweite der Kampagnen maximiert.

Eine Kampagne allein wird die Cyberkriminalität nicht aufhalten können. Was braucht es noch?
Mit der Digitalisierung und dem gesellschaftlichen Wandel werden sich auch die Bedrohungen verändern. Aber die Cyberkriminalität wird immer aktuell bleiben. Daher ist es wichtig, dass das Problem immer wieder thematisiert wird, sich alle bewusst werden, dass sie mit ihrem Verhalten viel zur Cybersicherheit beitragen und entsprechende Massnahmen ergreifen können. Aber nicht nur der Mensch ist hier gefragt, sondern auch die Entwickler:innen neuer Produkte. Cybersicherheit sollte im Innovationsprozess schon früh mitgedacht werden.

> **«Der Schutz vor Cyberrisiken ist eine gemeinsame Verantwortung von Wirtschaft, Gesellschaft und Staat.**

> **«Cybersicherheit sollte im Innovationsprozess schon früh mitgedacht werden.**

Informationssicherheit hat eine zentrale juristische Komponente

Die Digitalisierung und die steigende Anzahl an Cyberattacken auf Unternehmen und Behörden werfen neue rechtliche Fragen auf. «Fokus» sprach mit zwei Experten von Walder Wyss über die juristischen Aspekte von Cybersecurity.

Interview mit Jürg Schneider und David Vasella, Rechtsanwälte und Partner bei Walder Wyss

David Vasella
Dr. iur., Rechtsanwalt
Partner

Jürg Schneider
Dr. iur., Rechtsanwalt
Partner

Jürg Schneider, David Vasella, die Anzahl an Cyberattacken nimmt zu. Welche Gründe und welche Folgen hat das, auch aus rechtlicher Sicht?
David Vasella: Es trifft zu, dass mehr Vorfälle geschehen und dass sich Unternehmen und Behörden generell vermehrt mit dem Thema IT-Security auseinandersetzen. Das hat auch damit zu tun, dass Cyberattacken vermehrt mediale Aufmerksamkeit erfahren. Grundsätzlich ist die steigende Anzahl der Angriffe auf eine wachsende Gruppe an Personen zurückzuführen, die Cyberangriffe und besonders Ransomangriffe als Industrie betreiben. Es wird sehr professionell und arbeitsteilig gehandelt. Das erhöht die Effektivität und die Gefahr. Gleichzeitig wird die IT-Infrastruktur von Unternehmen immer komplexer und ist für die jeweiligen Firmen oft kaum mehr beherrschbar. Und als dritter Faktor kommt die Digitalisierung hinzu: Wir produzieren immer mehr Daten und sind immer stärker von digitalen Prozessen abhängig. Alle diese Aspekte sorgen in Kombination dafür, dass sich Cybercrime mehr lohnt. Der Gesetzgeber reagiert auf diese Entwicklung mit zunehmender Regulierung: So wird etwa das Datenschutzrecht verschärft, oder es werden kritische Infrastrukturen geregelt.

Welche Folgen hat diese Entwicklung für KMU?
David Vasella: Dort rückt die Frage in den Fokus, wer eigentlich die Verantwortung für die IT-Sicherheit einer Organisation trägt. Aus juristischer Sicht ist es zuerst der Verwaltungsrat. Dieser haftet für das Nichteinhalten von Sicherheitsbestimmungen, sofern er die entsprechenden Aufgaben nicht delegiert oder nicht beaufsichtigt. Betrachtet man das Thema im rechtlichen Kontext, müssen also Fragen des Risk Managements geklärt werden, und es müssen Strukturen geschaffen werden, die Risiken entdecken und möglichst minimieren. Zu diesem Zweck benötigt auch der Verwaltungsrat eine Minimalkompetenz hinsichtlich Cybersicherheit. Er muss Fragen adressieren können, wie etwa: Welche Assets müssen wir prioritär schützen? Welche Personen oder Stellen sind dafür zuständig? Und was geschieht im Falle eines Angriffs? Das ist enorm wichtig, weil Behörden im Fall eines Breachs nachfragen, welche Massnahmen zum Schutz der Daten und Infrastrukturen ergriffen wurden. Wer keine valable Antwort auf diese Frage bereithält, kommt in Erklärungsnot.

Wie verhindert man bei Walder Wyss, dass ein solcher Fall für die Kundschaft eintritt?
Jürg Schneider: Es sind zwei wesentliche Bereiche, in denen wir hierzu tätig werden. Zum einen unterstützen wir Unternehmen proaktiv dabei, sich auf potenzielle sicherheitsrelevante Vorfälle vorzubereiten. Zum Beispiel verfassen wir entsprechende Policies und definieren Richtlinien und Handlungsanweisungen bei Sicherheitsvorfällen. Zum anderen werden wir beigezogen, wenn eine Attacke bereits stattgefunden hat und dies im Unternehmen oder innerhalb einer Firmengruppe Ramifikationen haben könnte. In derartigen Fällen decken wir die juristische Seite ab. Da geht es unter anderem um Informationspflichten. Zudem setzen wir unseren Fokus gemeinsam mit dem Kundenunternehmen auf die Frage, wie man solchen Ereignissen künftig vorbeugen kann. Natürlich: Im idealen Szenario werden wir präventiv hinzugezogen. Glücklicherweise stellen wir dies bei Walder Wyss auch vermehrt fest, was unter anderem auch auf das revidierte Datenschutzrecht zurückzuführen ist. Denn dieses ahndet das Nichteinhalten von Sicherheitsbestimmungen nicht nur zivilrechtlich, sondern kann potenziell auch strafrechtliche Konsequenzen zur Folge haben. Darum hat sich auch bei den KMU mittlerweile die Awareness bezüglich Cybersecurity erhöht.

Welche Branchen sind Ihres Erachtens besonders gefährdet?
David Vasella: Das Gefährdungspotenzial ist weniger von der Branche als vielmehr von der Grösse eines Betriebs und von der Position in der Wertschöpfungskette abhängig. Für Angreifer interessant sind zum Beispiel grössere KMU, die über relevante Daten verfügen. Angreifer recherchieren im Vorfeld einer Attacke minutiös, welche Firmen vulnerabel sind und über welche finanziellen Mittel diese verfügen. Schliesslich müssen sie zum Beispiel im Falle eines Ransomware-Angriffs das Lösegeld in einer Höhe ansetzen, die für den erpressten Betrieb noch tragbar und kommerziell sinnvoll ist.

Ein spannendes Stichwort: Sollte man bei einem Ransomware-Angriff das Lösegeld bezahlen oder nicht?
David Vasella: Wir raten nicht dazu, Lösegeld zu bezahlen, aber letztlich muss das jedes Unternehmen für sich selbst entscheiden. Natürlich wäre es aus ethischer und strategischer Sicht besser, Lösegeldforderungen zurückzuweisen. Doch es ist nachvollziehbar, wenn Firmen in einer Notlage mit dem Gedanken spielen, dies zu tun, um ihre Operationalität rasch wiederherzustellen.

Immer mehr Versicherungsanbieter bringen Cyber-Versicherungen auf den Markt. Als wie sinnvoll erachten Sie diese?
Jürg Schneider: Eine solche Versicherung kann ein gutes Hilfsmittel für Firmen darstellen. Man sollte prüfen, welche Aspekte und Vorkommnisse tatsächlich abgedeckt werden, um die passenden Versicherungslösungen für das eigene Unternehmen zu wählen. Manche Leistungen werden vielleicht bereits von bestehenden Versicherungen abgedeckt. Manchmal wird der Abschluss einer solchen Versicherung auch vorausgesetzt, etwa von Zulieferern von grösseren Unternehmen.

Sie haben das Thema «Datenschutz» bereits angesprochen. Im nächsten Jahr tritt hierzulande das neue Datenschutzgesetz in Kraft. Welche Folgen hat dies für Unternehmen?
Jürg Schneider: Mit dem neuen Datenschutzgesetz zieht die Schweiz mit Europa gleich. Dort trat bereits im Jahr 2018 mit der DSGVO (Datenschutzgrundverordnung der EU) eine Verordnung in Kraft, die den besseren Schutz von Personendaten bezweckt. Schweizer Unternehmen, die bereits DSGVO-konform sind, müssen angesichts der neuen Schweizer Gesetzgebung nur wenige Anpassungen vornehmen. Viele KMU haben sich aber noch nicht damit auseinandergesetzt. Gerade für Unternehmen, die in europäischen Ländern agieren, ist es wichtig, beiden Gesetzgebungen nachzukommen. Es bleibt nun noch genau ein Jahr, bis das neue Datenschutzgesetz der Schweiz in Kraft tritt. Da es eine gewisse Zeit sowie einiges an Aufwand bedeuten kann, diesbezüglich Compliance zu gewährleisten, sollten sich Unternehmen spätestens jetzt an die Umsetzung machen.

David Vasella: Für die meisten Unternehmen bringt die Gesetzänderung Anpassungen mit sich. Darum muss man sich kümmern. Grund zur Panik besteht aber nicht. Die Umsetzung sollte mit einem gewissen Pragmatismus erfolgen. Wir gehen auch nicht davon aus, dass man hohe strafrechtliche Bussen aussprechen wird – zumindest nicht in Bagatellfällen. Darum: Keine Panik ist angezeigt, aber man muss sich jetzt mit dem Ganzen beschäftigen.

„ Das Gefährdungspotenzial ist weniger von der Branche als vielmehr von der Grösse eines Betriebs und von der Position in der Wertschöpfungskette abhängig.

Über Walder Wyss

Wachstum und Nähe sind die zentralen Erfolgsfaktoren der Walder Wyss AG. Die Kanzlei wurde im Jahr 1972 in Zürich gegründet und wächst seither kontinuierlich. Heute unterhält Walder Wyss zusätzliche Standorte in Genf, Basel, Bern, Lausanne und Lugano und beschäftigt rund 250 Anwältinnen und Anwälte. Die Expertinnen und Experten des Unternehmens arbeiten standortübergreifend, sprechen verschiedene Sprachen und betreuen nationale und internationale Kunden in allen Sprachregionen der Schweiz.

Weitere Informationen finden Sie unter
www.walderwyss.com

walderwyss rechtsanwälte

E-Mails vor unbefugtem Zugriff schützen

Im Zeitalter der digitalen Kommunikation versenden Unternehmen täglich Dutzende, wenn nicht gar Hunderte von E-Mails. Und obschon viele Firmen sensible Daten und Inhalte auf dem digitalen Postweg versenden, schützen sie ihre Sendungen kaum bis gar nicht. Dabei wäre das nicht nur äusserst wichtig – sondern auch einfach umsetzbar.

Interview mit Stefan Klein, Gründer und Managing Director von SEPPmail

Stefan Klein, Cybercrime und damit das Bedürfnis nach Cybersecurity nehmen zu. Für viele Firmen ist noch immer das Thema «E-Mail» eine Achillesferse.
Das ist leider korrekt, der Anstieg von Hackerangriffen lässt sich nicht von der Hand weisen. Dabei spielt die E-Mail-Sicherheit eine zentrale Rolle – und das nicht erst seit gestern. Die Idee, E-Mails mit sensiblen Inhalten ohne grossen Aufwand zu verschlüsseln, hatte ich schon vor 25 Jahren. Während meiner Studienzeit erbrachte ich für Anwaltskanzleien verschiedene IT-Dienstleistungen. Da diese auch Mandantinnen und Mandanten im Ausland betreuten, sollte der E-Mailverkehr verschlüsselt werden. Das Vorgehen war dazumal aber noch sehr komplex und umständlich, weswegen ich damals gemeinsam mit einem Bekannten entschied, diese Sicherheitsdienstleistung zu optimieren und alle notwendigen Services aus einer Hand anzubieten. Dieser Grundsatz bildet noch immer den Kern von SEPPmail. Die Technologie ist in der Zwischenzeit natürlich deutlich raffinierter geworden: So ermöglichen wir etwa nicht mehr «nur» die Verschlüsselungen von E-Mails, sondern bieten unter anderem auch das Signieren von Nachrichten an. Seit Neustem ermöglichen wir Nachrichtensicherheit und -Compliance auch über unsere Cloudlösung. An unserem ursprünglichen Grundsatz hat sich hingegen nichts verändert: Damals wie heute unterstützen wir unsere Kundschaft dabei, ihre Nachrichten vor unbefugten Dritten zu schützen. Und wie aktuelle Statistiken bezüglich Cybercrime zeigen, ist das wichtiger als je zuvor.

Welche Unternehmen und Branchen profitieren besonders von einer verschlüsselten E-Mailkorrespondenz?
In einer zunehmend digitalisierten Gesellschaft und Wirtschaftswelt profitieren natürlich Firmen aller Branchen und Grössen davon. Dementsprechend bedienen wir eine Kundschaft, die sich quer über sämtliche Branchen erstreckt. Ein grosser Teil der Unternehmen, die unsere Dienstleistungen in Anspruch nehmen, ist in der Gesundheitsbranche angesiedelt. Der sogenannte HIN-Mailgateway ist dort überall anzutreffen. Mittlerweile haben wir uns aber auch im Finanz- und Bankenbereich stark etabliert – zu unserem Kundenstamm gehören grosse Player, darunter

> **Der Anstieg von Hackerangriffen lässt sich nicht von der Hand weisen.**

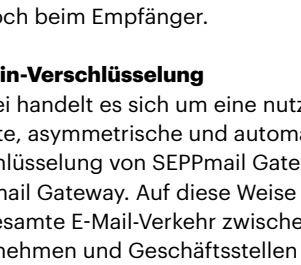
verschiedene Kantonalbanken. Auch kantonale Ämter und Behörden haben erkannt, wie zentral das Thema «E-Mail-Sicherheit» ist und ziehen uns dafür bei.

Es ist noch nicht lange her, da herrschte unter vielen Schweizer KMU die Ansicht, dass Cybersecurity ein Thema ist, dass nur «die Grossen» betrifft. Wie sieht das in Sachen E-Mail-Verschlüsselung aus?
Die Erkenntnis, dass sich auch kleine und mittelgrosse Unternehmen vor Angriffen aus dem Netz schützen müssen, setzt sich immer mehr durch. Auf das Argument «eine E-Mail-Verschlüsselung brauchen wir nicht», entgegne ich dann jeweils, dass man doch einfach mal einen Blick in den «Gesendet-Ordner» des eigenen Office-Mailaccounts werfen sollte. Sind da tatsächlich keinerlei Nachrichten drin, die man vor unbefugter Einsicht schützen möchte? Wahrscheinlich nicht. Diese Argumentation ist für die meisten Leute gut nachzuvollziehen.

Wie können Unternehmen am besten vorgehen, um Ihre E-Mail-Korrespondenz sicherer zu gestalten – wie sieht ein Mandatsablauf mit SEPPmail aus?
Wir arbeiten schweizweit mit mehr als 100 Partnerbetrieben, die unsere Lösungen und Technologien für Firmenkunden implementieren. Diese führen die Unternehmen durch den Beratungsprozess, eruieren ihre Bedürfnisse sowie Möglichkeiten und führen das Onboarding durch. Wir erbringen ab diesem Zeitpunkt den technischen Support. Darauf legen wir enormen Wert, schliesslich haben wir den Anspruch, unserer Kundschaft immer schnell und unkompliziert zur Seite zu stehen, wenn es zu einem Vorfall kommt.

Um die Sicherheit im E-Mail-Verkehr zu gewährleisten, müssen Sie technologisch immer am Puls der Zeit bleiben. Wie schwierig ist das, angesichts des aktuellen Fachkräftemangels?
Wir befinden uns in der glücklichen Lage, dass wir uns auf eine langjährige und äusserst treue Belegschaft verlassen können. Unsere Fluktuationsrate ist niedrig und wir geben uns grösste Mühe, den Bedürfnissen unserer Mitarbeitenden nachzukommen. Ein Schlüsselelement ist die Chance zur Weiterentwicklung: Wer sich hervortun und Verantwortung übernehmen möchte, erhält bei uns die Gelegenheit dazu. Für unsere neuen Cloudservices konnten wir glücklicherweise ein ganzes Team übernehmen, das in diesem Bereich absolut versiert ist. Insbesondere der in der Cloud mitangebotene Antispam- und Antimalwaredienst ist daher sehr gut.

> **Die Erkenntnis, dass sich auch KMUs vor Angriffen aus dem Netz schützen müssen, setzt sich immer mehr durch.**



Wie werden E-Mails eigentlich verschlüsselt?
SEPPmail bietet verschiedene innovative Ansätze, um die Sicherheit der digitalen Kommunikation zu gewährleisten. Ein Kernelement stellt dabei die sogenannte «asymmetrische» Verschlüsselung dar. Damit wird ein Verschlüsselungsverfahren beschrieben, bei dem nicht ein einziger Schlüssel, sondern ein Schlüsselpaar zum Einsatz kommt, bestehend aus einem öffentlichen sowie einem privaten Schlüssel. Dadurch wird die Sicherheit erhöht und – das richtige Schlüsselmanagement vorausgesetzt – die Handhabung der Lösung vereinfacht.

GINA-Verschlüsselung
Dieses patentierte Verfahren ermöglicht die verschlüsselte Übermittlung von E-Mails an Empfänger, die keine Verschlüsselungssoftware einsetzen und keinen Schlüssel besitzen. GINA verschlüsselt nach den neusten und sicheren Public-Key-Standards und benötigt keine Softwareinstallation – weder beim Sender noch beim Empfänger.

Domain-Verschlüsselung
Hierbei handelt es sich um eine nutzertransparente, asymmetrische und automatische Verschlüsselung von SEPPmail Gateway zu SEPPmail Gateway. Auf diese Weise lässt sich der gesamte E-Mail-Verkehr zwischen zwei Unternehmen und Geschäftsstellen ohne Zutun der Absender und Empfänger sichern. Dieses «E-Mail-VPN» benutzen heute schon deutlich mehr als 10 000 Domänen in der DACH-Region.

OPENPGP-Verschlüsselung
Bei OpenPGP handelt es sich um ein asymmetrisches Verschlüsselungsverfahren für ein- und ausgehende E-Mails, basierend auf den Normen RFC 4880 und RFC 3156. Dabei werden die öffentlichen Schlüssel zentral auf das Gateway geladen, woraufhin die Verschlüsselung transparent und automatisch im Hintergrund erfolgt – ohne Zutun der User.

S/MIME-Verschlüsselung
Dieses asymmetrische Verschlüsselungs-/Signaturverfahren für ein- und ausgehende E-Mails beruht auf Norm RFC 5751. Sie basiert auf persönlichen S/MIME-Zertifikaten, deren Vertraulichkeit und Integrität von öffentlichen Stellen, den sogenannten Certification Authorities (CAs), bestätigt werden.

TLS-Verschlüsselung
Im Gegensatz zu den vorgängig beschriebenen Verschlüsselungsverfahren handelt es sich bei der TLS-Verschlüsselung nicht um eine inhaltliche, sondern «lediglich» um eine Transportverschlüsselung. Diese endet am nächsten angesprochenen E-Mail-Server, der nicht zwingend der finale E-Mail-Server des Empfängers sein muss. Vor diesem Hintergrund kann auf Basis des TLS-Verfahrens keine durchgängige Verschlüsselung bis zum Zielserver garantiert werden.

Über SEPPmail

Das Unternehmen setzt sich dafür ein, dass via E-Mail übermittelte Inhalte sowie die Identität der jeweiligen Absender zuverlässig geschützt werden – ohne technische und administrative Hürden für Sender oder Empfänger. Der Schlüssel dazu liegt in den wegweisenden Secure-E-Mail-Gateway-Lösungen zur Verschlüsselung von E-Mail-Nachrichten sowie zur Authentifizierung der Absender. Diese werden von unzähligen Firmen und Institutionen genutzt, darunter Unternehmen aus Branchen wie Industrie, Forschung und Entwicklung, Medizin, Energie, Finanz- und Versicherungswesen, öffentliche Verwaltung, Pharma und Recht.

Weitere Informationen unter
www.seppmail.com

SEPPMAIL

«Es lohnt sich nicht, sich in Sicherheit zu wähnen»

KMUs werden vermehrt Opfer von Erpressungen durch Cyberkriminelle. Dabei reichen bereits einfache Massnahmen aus, um sich davor zu schützen und auch bei einem erfolgreichen Angriff mit minimalen Schäden aus der Situation hervorzukommen. Marcel Zumbühl, CISO der Schweizerischen Post, spricht über die Gefahren und wie die «Swiss Cyber Defence DNA» KMUs unterstützt.

Marcel Zumbühl
CISO
Schweizerische Post

Herr Marcel Zumbühl, die Cybergefahren sind so sichtbar wie noch nie. Stellen sie auch für KMUs bereits ein alltägliches Risiko dar?
Mit der zunehmenden Digitalisierung kleiner und mittlerer Unternehmen rücken diese natürlich genauso ins Zentrum der Aufmerksamkeit. Kriminelle gehen den Weg des geringsten Widerstands. Wenn sie vermuten, dass ein KMU schlecht geschützt ist, werden sie einen Angriffsversuch unternehmen. Da die meisten Firmen in der Schweiz KMUs sind, sind die meisten Attacken gegen sie gerichtet. Das heisst, ein KMU muss über eine robuste Cybersecurity verfügen, um nicht zum Ziel zu werden.

Welche Branchen stehen der erheblichsten Bedrohung gegenüber?
Es handelt sich um ein organisiertes Verbrechen. Professionell und geplant unternehmen die Kriminellen Fischzüge durch verschiedene Branchen hindurch. Unter Druck stehende Sektoren liegen vielleicht im Mittelpunkt solcher Angriffe, weil sie tendenziell undeutlicher reagieren können. Zum Beispiel war die Gesundheitsbranche während der Coronakrise stark belastet. Die Cyberkriminellen sehen sich den Markt genau an.

Welche Ziele stecken hinter den Cyberattacken?
Diese können bei den verschiedenen Gruppen unterschiedlich sein. Bei der grossen Mehrheit handelt es sich aber um ein monetäres Interesse. Ein oft gesehenes Muster ist, dass sie eindringen, die Daten verschlüsseln und das Unternehmen erpressen. Ein weiteres Vorgehen ist der Datendiebstahl, um auf dem Schwarzmarkt Geld zu verdienen.

Wo liegen die gefährlichsten Stolperfallen, in der Technologie oder beim Menschen?
An beiden Orten bestehen Gefahren. Mensch und Maschine müssen zusammenspielen, um Angriffsflächen zu minimieren. Technologie stellt einen potenziellen Einstieg dar, beispielsweise durch Überlastungsangriffe wie Denial of Service. Menschen sind genauso ein Einfallstor, wenn sie über Phishingmails dazu verleitet werden, einen Link zu einem Schadcode anzuklicken. Bei der Post setzen wir auf drei Achsen: Mensch, Maschine und Geschäft. Deswegen verfolgen wir in der Zusammenarbeit eine partizipative Sicherheit, um die Kette von der Kundschaft zum Unternehmen und den Lieferanten zu schützen.

Mit den Ressourcen der KMUs ist es schwierig, von einer Fachperson Risikoanalysen durch- und Massnahmen einführen zu lassen. Was sind die Empfehlungen in einem solchen Fall?
Der Massnahmenkatalog der «Swiss Cyber Defence DNA» zeigt, dass man mit einfachen Mitteln ein gutes Mass an Sicherheit erreichen kann. Nicht in jedem Fall muss eine eigene Sicherheitsabteilung aufgebaut werden. Die Initiative führt auf, welche lokalen Partner zur Seite stehen können.

Sie sprechen den Leitfaden der «Swiss Cyber Defence DNA» an. Was beinhaltet dieser?
Die Massnahmen zielen sowohl auf den Menschen als auch auf die Maschine ab. Im Bereich des Menschen gibt es grundsätzliche Fragen zu klären wie: Wer hat welche Zugriffe? Wie sind die Mitarbeitenden geschult? Wie sieht die Reaktion auf einen Angriff mit allfälliger Erpressung aus? Wo kann man sich Hilfe holen? Die Empfehlung hierbei ist, niemals auf eine Erpressung einzugehen oder mit Kriminellen zu verhandeln, sondern direkt auf die Behörden zuzugehen.

Maschinenseitig gilt, ein gutes Back-up anzulegen sowie einen Antivirenschutz einzurichten. Die wohl einfachste Massnahme ist, immer mit den Aktualisierungen mitzugehen und Soft- und Hardware inklusive Handy auf dem neuesten Stand zu halten. Zusätzlich kann man über einen Partner eine Sicherheitsüberwachung einrichten, sodass man bei einem Vorfall rechtzeitig alarmiert wird und reagieren kann.

Es lohnt sich aber niemals, sich in Sicherheit zu wähnen. Es ist erschreckend, wie viele Unternehmen es trifft. Wenn man gut vorbereitet ist, kann man solche Angriffe jedoch überstehen. Beispiele aus dem letzten Jahr zeigen, dass man durch transparente Dialoge mit der Belegschaft, Kundschaft und der Öffentlichkeit mit einer besseren Reputation aus der Situation kommen kann.

Weshalb hat sich die Schweizerische Post der Trägerschaft der Initiative angeschlossen?
Wir standen schon zuvor in losem Austausch mit der «Swiss Cyber Defence DNA». Sie passt zur Art und Weise, wie wir über Sicherheit denken. Denn Sicherheit ist ein kontinuierlicher Prozess, den man am besten mit einem partizipativen Approach umsetzt. Das ist genau der Weg, den wir insgesamt für eine hohe Cybersecurity in der Schweiz gehen müssen. Zu diesem Ziel möchten wir auch unsere Expertise weitervermitteln, um jene zu unterstützen, die sich dem Thema annehmen.

Weitere Informationen sind unter *kmuschutz.ch* auf Englisch, Deutsch, Französisch und Italienisch ohne Angabe von Firmendaten einsehbar.

„ Es ist erschreckend, wie viele Unternehmen es trifft.

Marcel Zumbühl ist Chief Information Security Officer der Schweizerischen Post mit rund 65 000 Mitarbeitenden. Er ist Mitglied der Geschäftsleitung Informatik der Post und Verwaltungsrat von Hacknowledge SA, ein Tochterunternehmen der Post, das managed Security Operations anbietet.

Neben seiner Arbeit ist er Dozent an der ETHZ und der HSLU und Co-Präsident von Information Security Society Switzerland (ISSS). ISSS ist der führende Fachverband in der Schweiz für ICT-Sicherheit, welchem heute mehr als 1100 Security Professionals und an Security Interessierte aus Wirtschaft, Verwaltung und Wissenschaft angehören.

Stufen zur Sicherheitskultur

Die Sicherheit gilt als essenzieller Wertebestandteil einer demokratischen Gesellschaft. So möchte man politisch, militärisch, ökonomisch, sozial, rechtlich und technisch ein möglichst hohes Sicherheitsniveau erlangen. Immer wichtiger wird da auch die Unternehmenssicherheit, die sich sogar zertifizieren lässt.

Grundsätzlich kann jedes Individuum und rational handelnde Wesen selbst bestimmen, wie es sich verhält. Doch die Gesellschaft, Arbeitgeber und der Umwelt geben Rahmenbedingungen, Anforderungen und Normen vor, an denen man sich orientieren sollte, um Sanktionen zu vermeiden. Sicherheitskultur bedeutet, die Sicherheit in das tägliche Handeln Aller aktiv einzubinden, vollumfänglich zu gewährleisten sowie dauerhaft aufrechtzuerhalten.

> **Um den hohen Ansprüchen heute und in Zukunft gerecht zu werden, braucht es eine Sicherheitskultur, die von allen gelebt wird.**

Nachhaltige Sicherheitskultur

Die Verantwortung für eine nachhaltige und etablierte Sicherheitskultur ist eine zentrale Aufgabe des Managements. Sie muss jedoch vor allem von den Beschäftigten selbst gelebt werden. Diverse Sicherheitsanforderungen wie etwa die Einführung einer Verpflichtung zum Sichtbartragen von Ausweisen, der Beachtung von Zutrittsbeschränkungen oder der Einhaltung von Besucherregelungen üben immer auch einen gewissen Anpassungsdruck auf die Unternehmenskultur aus. Ein wesentlicher Wertebestandteil einer Unternehmenspolitik sollte daher die Ablehnung unternehmensschädigenden Verhaltens sein, was wiederum auch in die Sicherheitskultur übergeht.

Safety Culture Ladder (SCL)

In diesem Jahr hat Swissgrid das erste Safety Culture Ladder (SCL) Zertifizierungsaudit erfolgreich bestanden. Als nationale Netzgesellschaft hat die Gewährleistung der Sicherheit von Menschen, Anlagen und Umwelt bei Swissgrid höchste Priorität, wie es auf der Firmenhomepage heisst. Um den hohen Ansprüchen heute und in Zukunft gerecht zu werden, braucht es eine Sicherheitskultur, die von allen gelebt wird. Mit der Einführung der Safety Culture Methode (SCL) und dem erfolgreich absolvierten Zertifizierungsaudit hat Swissgrid mit dem ausgestellten Zertifikat einen wichtigen Meilenstein erreicht.

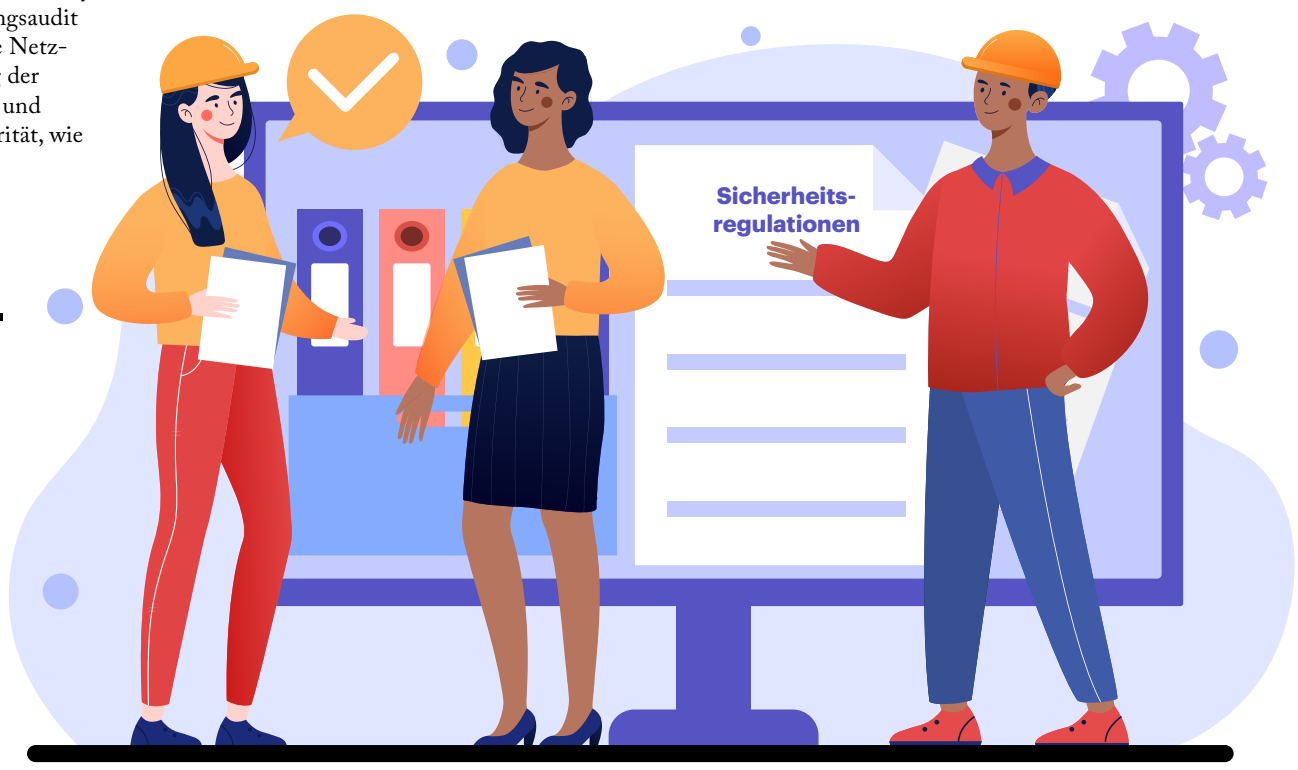
Fünf Stufen zum Zertifikat

Im März 2022 fand erstmals ein Zertifizierungsaudit nach der SCL-Methodik statt. Dabei wurde die Sicherheitskultur anhand eines fünfstufigen Reifegradmodells durch eine unabhängige Prüfstelle beurteilt und bewertet. Im Zentrum stand die Frage nach der Priorität von Arbeitssicherheit und Gesundheit im Unternehmen, und: inwiefern sich dies im Bewusstsein und Verhalten der Beteiligten widerspiegelt.

Menschen statt Dokumente

Während des mehrtägigen Audits standen die Menschen und ihr Sicherheitsverhalten im Mittelpunkt. Die Auditoren verschafften sich im Dialog mit Führungskräften und Mitarbeitenden aus allen Organisationsbereichen sowie Dienstleistern ein Bild von davon, wie Sicherheit bei Swissgrid gelebt wird. Das Besondere am Audit: Die Auditoren verzichteten konsequent darauf, Dokumente zu prüfen und legten den Fokus auf die tatsächliche Umsetzung in die Praxis – erklärt und geschildert in den Worten der interviewten Personen.

> **Die Verantwortung für Sicherheitskultur ist eine zentrale Aufgabe des Managements.**



Ein kontinuierlicher Prozess

Die angestrebte Stufe 3, welche den Fokus auf vorhandene Sicherheitsregeln und deren Einhaltung legt, wurde von der Zertifizierungsstelle im Mai bestätigt. Dieses Ergebnis motiviert Swissgrid, im Bereich Sicherheit noch mehr Fahrt aufzunehmen. Sowohl Mitarbeitende als auch Dienstleister sollen das Thema Sicherheit zukünftig noch proaktiver angehen, mit dem gemeinsamen Ziel, die Arbeit jeder einzelnen Person tagtäglich noch sicherer zu gestalten. Sicherheit ist ein kontinuierlicher Prozess. Eine Sicherheitskultur muss entsprechend systematisch und nachhaltig weiterentwickelt werden. Dazu wird Swissgrid die Empfehlungen der Audit-Gesellschaft prüfen und entsprechende Massnahmen einleiten. Der Fortschritt der Weiterentwicklung wird in den nächsten zwei Jahren mit einem Re-Zertifizierungsaudit überprüft.

Einbezug von Dienstleistern

Mit einem integralen Sicherheitsansatz bezieht Swissgrid Mitarbeitende und Dienstleister bei der Entwicklung der Sicherheitskultur mit ein, um so das Sicherheitsbewusstsein bei allen zu stärken. Die Dienstleister spielen eine wichtige Rolle, denn nur in enger Zusammenarbeit ist eine sichere und zuverlässige Stromversorgung möglich. Swissgrid fordert seit Januar 2022 im Rahmen von neuen Beschaffungen die Einführung der SCL bei denjenigen Dienstleistern ein, bei deren Tätigkeiten im Auftrag von Swissgrid die Arbeitssicherheit eine zentrale Rolle spielt. Dies leistet einen wichtigen Beitrag für die Förderung eines gemeinsamen Sicherheitsverständnisses.

Safety Culture Ladder

Die Safety Culture Ladder (SCL) basiert auf einem fünfstufigen Reifegradmodell und ist eine zertifizierungsfähige Methode zur Weiterentwicklung der Sicherheitskultur von Organisationen unterschiedlichster Branchen, in denen die körperliche Sicherheit (Arbeitssicherheit und Gesundheitsschutz) erhöhten Risiken ausgesetzt ist. Der Fokus der SCL liegt auf der gelebten Arbeitssicherheit mit dem Ziel, das Sicherheitsbewusstsein aller Führungskräfte, Mitarbeitenden und Vertragspartner (Dienstleister) fortlaufend zu fördern. Obwohl die SCL in erster Linie für die Weiterentwicklung der Arbeitssicherheit konzipiert wurde, lässt sich das Grundprinzip in allen sicherheitsrelevanten Bereichen anwenden. Die Weiterentwicklung der Sicherheitskultur erfolgt entlang der fünf Stufen: Je ausgeprägter die Sicherheitskultur einer Organisation, umso höher die Stufe.

Mehr Infos: **safetycultureladder.com/de**

Kann die Schweiz in der globalen Cybersicherheit eine Führungsrolle übernehmen?

Neutralität, politische Stabilität und Rechtssicherheit – all dies garantiert die Schweiz. Das IT-Unternehmen ELCA mit Sitz in Lausanne und Niederlassungen in Genf, Zürich, Bern und Basel ist überzeugt: Die Schweiz erfüllt alle Voraussetzungen, um sich als globales Zentrum für Cybersicherheit zu behaupten.

Nicht nur für ihre Käseproduktion oder Uhrenindustrie geniesst die Schweiz weltweit einen hervorragenden Ruf, sondern auch als Wirtschaftsplatz für sichere, seriöse und zuverlässige Geld- und Versicherungsgeschäfte. Im Allgemeinen steht das Land in puncto Sicherheit an der Weltspitze. Vermögenswerte aus aller Welt befinden sich in der Schweiz. Das Vertrauen in das hiesige Rechtssystem und dessen stabile Wirtschaft ist gross. Und wie sieht es in Bezug auf die globale Cybersicherheit aus? ELCA Informatik, Schweizer IT-Unternehmen mit Sitz in Lausanne und mit über 50 Jahren Erfahrung, macht sich für mehr Cybersicherheit in der Schweiz stark. Die Tochtergesellschaft ELCA Security fokussiert sich auf Cybersecurity und ist überzeugt: Helvetia kann eine Führungsrolle in der globalen Cybersicherheit übernehmen.

Schweiz: der perfekte Standort

Die Welt ist im Griff des digitalen Wandels. Diese Transformation birgt Gefahren, wobei die Schweiz einen sicheren Hafen darstellt und ihre politische Stabilität sich auch in der digitalen Transformation als Vorteil erweist. Das Label «Swiss Made» gilt bei Sicherheitslösungen als Garant. Das dem Schweizer Standort entgegengebrachte Vertrauen ist nicht selten grösser als jenes in die amerikanischen oder anderen europäischen Märkte. Alles spricht dafür, diese Vorteile auch beim Aufbau und der Stärkung des Marktes für Cybersicherheit zu nutzen.

Kostenpunkt

Was Beratungsleistungen und Dienstleistungskosten betrifft, ist die Schweiz teurer als die meisten anderen Länder. Allerdings machen die Qualität und die Unabhängigkeit der Schweizer Dienste den Unterschied aus. Dieses Gut ist schwer zu finden. Für Unternehmen ist das Stärken der eigenen Cybersicherheit heute von grösster Dringlichkeit. Und ausserdem eine wichtige und lohnende Investition in die Zukunft. Das Ausblenden von Bedürfnissen in Bezug auf Cybersicherheit kommt Unternehmen bei erfolgreichen Angriffen deutlich teurer. Prävention und stetige Kontrollen schaffen Sicherheit und gewährleisten diese langfristig.

Genf als zukünftige Haupstadt für Cybersecurity

Bereits Microsoft-Vorsitzender Brad Smith identifizierte das Potenzial der Schweiz. Seit einigen Jahren setzt er sich für eine «Digitale Genfer Konvention» ein. Diese soll dazu dienen, das Zusammenleben im digitalen Raum zu regulieren. Zudem gründete Smith das «CyberPeace Institute» im Jahre 2019. Die Genfer Organisation setzt sich für die Rechte und Sicherheit der Menschen in der digitalen Welt ein. Dabei arbeitet sie gemeinsam mit Unternehmen weltweit – ELCA Informatik AG mit eingeschlossen sowie mit deren Expert:innen. Die Tatsache, dass alle wichtigen UNO-Organisationen sowie unzählige Nichtregierungsorganisationen ihren Sitz in Genf haben, spricht ebenfalls für den Standort Schweiz.

Die Schweizer Lösung Senthorus

Mit der Gründung des Joint Venture «Senthorus» mit Sitz in Genf stellt ELCA Security sicher, dass die zusammengeführten Kompetenzen und Dienste den weltweiten Vergleich nicht zu scheuen brauchen. Hierbei arbeitet ELCA mit dem führenden Anbieter für Cyberabwehr BlueVoyant zusammen. Qualität und Fachkompetenz, ergänzt durch international erprobte und moderne Cyberlösungen. Ziel ist es, hiesigen Unternehmen ein massgeschneidertes Angebot zu bieten und so von den Vorteilen des Schweizer Standortes zu profitieren. In Anbetracht der steigenden Anzahl an Cyberattacken ist dies ein wichtiges Angebot für Unternehmen und den Wirtschaftsplatz Schweiz.

> **Cybersicherheit ist eine wichtige und lohnende Investition in die Zukunft.**

«Wir wollen Schweizer Unternehmen gegen Cyberattacken schützen»

ELCA ist ein etablierter IT-Anbieter in der Schweiz. Fabrice Guye, Strategieleiter bei ELCA Security und General Manager von Senthorus, erklärt die Bedeutung von Nähe und Unabhängigkeit bei Cybersicherheit im Gespräch mit «Fokus».

Fabrice Guye
Strategieleiter ELCA Security, General Manager von Senthorus

Fabrice Guye, ELCA Security hat Cybersicherheit in der Schweiz zum Ziel. Was bedeutet es für Unternehmen, die eigene Cybersecurity zu stärken?
Die Stärkung der Cybersicherheit bedeutet, das Risiko von Cyberattacken zu reduzieren. Unternehmen müssen sich schützen. Schützenswert sind nicht nur monetäre Güter, sondern auch die Reputation der Firma. Zudem kann geistiges Eigentum von Mitarbeitenden ebenfalls gefährdet sein. Die Zeiten, in denen der Kauf einer marktführenden Sicherheitslösung ausreichte, sind vorbei.

Welche grundlegenden Cybersicherheitsmassnahmen sollten Unternehmen treffen?
Zunächst müssen sich Firmen ihrer eigenen Risiken bewusst sein, um den Fokus auf den richtigen Bereich zu legen. Nur so lassen sich Entscheidungen, wie und wo investiert werden soll, treffen. Des Weiteren müssen Unternehmen ihre Infrastruktur und Vermögenswerte kennen. Dazu braucht es ein Up-to-value-Asset-Management, eine Zweifaktorauthentifizierung sowie eine Datenverschlüsselung. Selbstverständlich hilft es, Mitarbeitende bezüglich Cybersicherheit zu sensibilisieren und zu schulen.

Was ist das Ziel von Hacker:innen bei einem Cyberangriff auf Firmen?
Oftmals ist Geld das Ziel. Einerseits erreichen sie dies entweder direkt mit einer Lösegeldforderung, nachdem sie einen Teil oder die gesamte digitale Umgebung eines Unternehmens kontrollieren oder Daten gestohlen haben. Andererseits entwenden Hacker:innen teilweise Informationen für den späteren Gebrauch. Es gibt auch Fälle, bei denen Cyberkriminelle Menschenleben angreifen, indem sie Daten der Mitarbeitenden für den direkten Angriff benutzen. Vor einigen Jahren drangen Hacker:innen sogar in Krankenhäuser ein. Als Folge davon starben Menschen. Zum Glück sind solche Fälle jedoch selten.

Welches ist die grösste Schwachstelle von Firmen?
Die übliche Antwort wäre: der Mensch. Doch kommt es auch auf die Grösse und den Tätigkeitsbereich eines Unternehmens an. Selbstverständlich sind Menschen und mangelndes Sicherheitsbewusstsein ein Teil der Gleichung. Jedoch spielen viele andere Faktoren mit hinein, wie beispielsweise blindes Vertrauen in Dienste von Drittanbietern und ungesicherter Datenaustausch. Auch ein Risiko ist, die eigenen Schwachstellen nicht zu kennen und nicht zu wissen, was überhaupt geschützt werden muss.

ELCA gründete vor Kurzem das Joint Venture Senthorus mit dem Cyberabwehrunternehmen BlueVoyant. Weshalb wurde diese Partnerschaft eingegangen?
Die Idee von Senthorus ist, beste Technologie in der Schweiz zu betreiben und sich auf die lokalen IT-Kompetenzen und hiesigen Bedürfnisse zu stützen. Deshalb wählten wir eine Kooperation mit BlueVoyant, die für ihr Management und Service weltweit bekannt ist. Das ergänzt unsere Fachkompetenzen und Know-how mit weiteren modernen Technologien, Verfahren und Erfahrungen.

Was bedeutet die Partnerschaft für ELCA Security?
Die Zusammenarbeit ermöglicht das Abdecken des gesamten Spektrums von Kundenbedürfnissen. Wir verfügen bereits über Beratungsdienstleistungen und etablierte Lösungen wie Strategie, Zugangsverwaltung, Management von trustID sowie eine eigene eID und MFA-Lösung. Senthorus vervollständigt das Angebot mit einem kontrollierten Sicherheitsserviceangebot.

Weshalb wurde Senthorus gegründet?
Wir wollen Schweizer Unternehmen gegen Cyberattacken schützen. Senthorus bietet internationalen sowie lokalen Unternehmen moderne Technologie, garantierte Kontrolle über die eigenen Daten, einen Schweizer Standort sowie ein breites Serviceangebot. Wir decken die Bereiche Antizipation, Schutz und Verteidigung sowie auch Sanierung ab und stellen dabei die gesamte Kompetenz der ELCA-Gruppe zur Verfügung.

Das neue Security Operations Center (SOC) befindet sich in der Schweiz. Inwiefern profitieren Unternehmen von der Nähe?
Zwei SOCs sind in der Schweiz stationiert. Das erste ist bereits in Betrieb, das zweite befindet sich im Bau und wird noch vor Ende des Jahres betriebsbereit sein. Die Vorteile des Standorts sind vielfältig: Zunächst einmal ist die Schweiz an sich eine Garantie. Zudem ist die Möglichkeit, unsere Anlagen zu besuchen oder direkten Kundenkontakt zu haben, entscheidend. Deshalb ist es für uns selbstverständlich, unserer Schweizer Kundschaft nahe zu sein.

Weshalb ist es von Vorteil, wenn Daten von Unternehmen in der Schweiz bleiben und nicht international gehandelt werden?
Die Schweiz bringt Souveränität und Sicherheit mit sich. Jedoch ist neben dem Speicherort vor allem das Dateneigentum elementar. Transparenz ist hier von grosser Bedeutung. Senthorus garantiert Unternehmen einen vollständigen Überblick über die Aktivitäten und dass sie jederzeit Eigentümer:in ihrer Daten bleiben.

ELCA bzw. ELCA Security ist ein privates Unternehmen. Welche Rolle spielt Unabhängigkeit hierbei?
Unabhängigkeit ist im Beratungsgeschäft essenziell. Dies garantiert, dass unsere Leistungen und Tätigkeiten immer die beste Lösung für die Unternehmen sowie Kund:innen liefern.

Weitere Informationen:
www.elcasecurity.ch

> **Ein Risiko ist es, die eigenen Schwachstellen nicht zu kennen.**

Text & Interview **Vanessa Bulliard**

ELCASecurity

Senthorus

«Eine Panzertüre ist nutzlos, wenn man gleichzeitig das Fenster offenlässt»

Eine lückenlose IT-Sicherheit zu gewährleisten und im Schadensfall schnell und korrekt zu reagieren, liegt für viele Unternehmen ausserhalb der eigenen Möglichkeiten. Aus diesem Grund unterstützt Basevision seine Kundschaft nicht nur mit praxistauglichen technischen Tools – sondern steht ihnen auch bei der Formulierung einer nachhaltigen Security-Strategie inklusive der Prozesse und Ausbildung zur Seite. Das zahlt sich aus.

Thomas Kurth
CEO Basevision AG

Thomas Kurth, welches sind die dringlichsten Sicherheitsbedenken Ihrer Kundschaft?
Eigentlich kann man festhalten, dass diejenigen Firmen, die aktiv mit Fragen und Bedenken auf uns zukommen, bereits einen wichtigen Schritt in Richtung IT-Sicherheit gemacht haben: Sie sind sich nämlich der potenziellen Gefahr bewusst und wollen handeln. Leider ist diese wichtige Awareness noch längst nicht in allen Unternehmen verankert. Wir verfügen hierzulande über zahllose Betriebe, die in ihren Branchen und Sektoren führend sind und weltweit beachtete Innovationen hervorbringen. Doch viele dieser Firmen haben es verpasst, neben ihrem Kerngeschäft auch den Bereich IT-Sicherheit zu stärken. Immerhin: Die Anzahl der Unternehmen, die sich der potenziellen Gefahr aus dem Netz bewusst sind, steigt langsam, aber sicher an.

Welches Angriffsszenario ist derzeit das realistischste oder häufigste?
Aktuell sind die Ransomware-Angriffe in aller Munde. Bei dieser Art von Angriffen werden Teile oder sogar das gesamte IT-System verschlüsselt. Dadurch sind Unternehmen nicht mehr in der Lage, ihrer Arbeit nachzugehen. Kommt es zu einem solchen Vorfall, sind die meisten Unternehmen für eine längere Zeit teilweise oder komplett unfähig, ihrer Geschäftstätigkeit nachzugehen. Schnell werden die daraus entstehenden Umsatzeinbussen in Kombination mit hohen Fixausgaben, wie Lohnzahlungen, zu einem echten Liquiditätsproblem. Wir sprechen hier oft von gewaltigen Schadenssummen, die gerade für KMU rasch existenzgefährdend werden können.

Wie kann man das verhindern und wer ist dafür zuständig?
Die meisten Unternehmen beschäftigen IT-Mitarbeitende, die eigentlich wüssten, dass etwas zu tun wäre. Und manchen ist auch klar, was man unternehmen müsste. Häufig werden diese Mitarbeitenden aber dermassen vom Tagesgeschäft vereinnahmt, dass ihnen die Zeit und die Ressourcen fehlen, um sich sicherheitskritischen Fragen zu widmen. Dies zeigt, dass IT-Sicherheit eigentlich in den Aufgabenbereich der Geschäftsleitung gehört. Sie muss die benötigten Ressourcen bereitstellen sowie die notwendigen Massnahmen delegieren. Ganz wichtig: Es genügt nicht, einfach ein Sicherheitsprodukt zu erwerben und dann das Gefühl zu haben, man sei damit besser geschützt. Es braucht vielmehr ein tiefgreifendes Bewusstsein dafür, dass die Kombination von Technologie, Prozessen und Personal eingespielt sein muss.

Und wie schafft und schärft man ein solches Bewusstsein?
Dies erreicht man nur über breite Kampagnen auf allen Ebenen – von den Kunden zu den Mitarbeitenden bis hin zur Geschäftsleitung. Ich finde, das NCSC und Florian Schütz leisten hier einen extrem wertvollen Beitrag. Sobald man ein grundlegendes Bewusstsein erreicht hat, müssen Unternehmen ihr Personal aus- und weiterbilden und ihm klarmachen, warum ein sicherheitskonformes Verhalten essenziell ist. «Weiterbilden» bedeutet in diesem Zusammenhang nicht, dass man die Belegschaft im Rahmen eines einzelnen Seminars mit dem Thema konfrontiert, sondern dass man sich regelmässig damit beschäftigt. Nur so kultiviert man das notwendige Verständnis sowie Know-how und kann gleichzeitig dem Fachkräftemangel entgegenwirken. Aus diesem Grund haben wir in unserem Unternehmen die Basevision Academy ins Leben gerufen.

Worum handelt es sich dabei?
Nach der Gründung der Basevision AG im Jahre 2015 war es für uns zentral, Talente zu finden, um genügend Ressourcen für grosse Kundenprojekte aufbieten zu können. Doch das stellte sich aufgrund der digitalen Transformation als schwieriger heraus als gedacht: Technologien ändern sich ständig und jede Branche weist einen wachsenden Bedarf am IT-Fachpersonal auf. Kontinuierliche Anpassung und stetiges Lernen werden darum zu Schlüsselfaktoren für Erfolg. Um die besten Mitarbeitenden zu finden und in unserem Betrieb zu entwickeln, gründeten wir 2016 die Basevision Academy. Dadurch haben im Jahr 2021 unsere 35 Mitarbeitenden gemeinsam rund 4300 Stunden in Aus- und Weiterbildung investiert. Jedes Unternehmen sollte seine Leute auf dem neusten Stand halten. Dabei geht es nicht nur um das Verständnis für Technologie, sondern auch um das Wissen rund um übergeordnete Prozesse und Zuständigkeiten. Sie bilden die Basis für eine ganzheitliche Strategie.

Wie hilft die Basevision AG ihrer Kundschaft dabei, die zahlreichen Sicherheitsherausforderungen anzugehen?
Wir beginnen immer mit der Erstellung einer Roadmap. Diese schafft die notwendigen Voraussetzungen, um eine ebenso effektive wie nachhaltige Sicherheitsstrategie zu entwickeln, die wirklich zum Unternehmen passt. Die Roadmap basiert auf einer eingehenden Risikoanalyse: Welche Firmen-Assets muss man prioritär schützen? Welche Ressourcen stehen dem Unternehmen zur Verfügung? Diese und weitere Fragen stehen im Fokus. Bei der konkreten Umsetzung fangen wir meist mit dem Basisschutz an. Anschliessend definieren wir gemeinsam mit der Kundschaft die nächsten Schritte, Teilziele und Meilensteine. Dadurch lassen sich die notwendigen Ressourcen absehen und einplanen. Die Welt verändert sich schnell und auf Technologie trifft das sogar doppelt zu. Darum gehen wir das Thema «Sicherheit» Schritt für Schritt an und machen es so überschaubar.

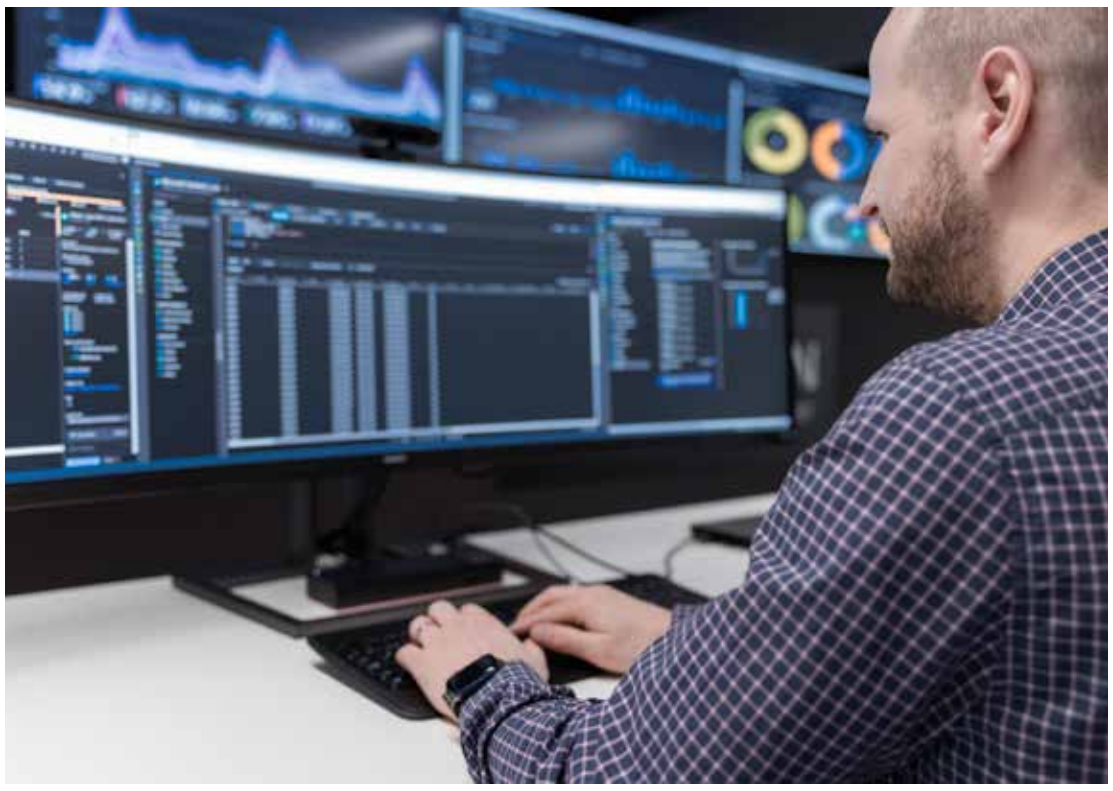
Auf welche technischen Tools setzen Sie dabei?
Viele Unternehmen führen in spezifischen Bereichen das passende Tool ein. Dieser «Best of Breed»-Ansatz ist aber nicht immer sinnvoll. Der Einsatz von vielen verschiedenen Top-Tools kann zu Datensilos führen und so neue Herausforderungen schaffen. Die Technologien müssen vielmehr aufeinander abgestimmt sein. Darum setzen wir auf die Microsoft-Technologien. Der Techgigant bietet ganzheitliche Lösungen, welche die ganze Angriffskette (Eintrittspunkte, Endpunkte, Identitäten, Clouds und IOT) abdecken. Unsere Roadmaps basieren auf integrierten Lösungen, die ihr Potenzial entfalten, wenn sie gemeinsam eingesetzt werden. Oder um es anders auszudrücken: Es nützt nichts, eine Panzertüre zu installieren, wenn man gleichzeitig die Fenster offenlässt. Und neben dem Schutz vor Angriffen, müssen wir auch Massnahmen und Prozesse definieren, die nach einer erfolgten Attacke greifen, um den Schaden möglichst gering zu halten.

Das Ganze hört sich nach einer enormen Herausforderung an.
Darum achten wir darauf, für jeden Kundenbetrieb eine individuelle Strategie zu entwickeln, welche die jeweiligen Prioritäten in der Roadmap festhält. Dadurch wird alles überschaubarer. Und mit den Microsoft Defender Suiten verfügen wir über ein ideales Produkt, welches zu einem guten Preis eine breite Abdeckung ermöglicht. Wir sind damit in der Lage, auf unsere vordefinierten Drehbücher zurückzugreifen und diese auf die Bedürfnisse der Kunden und deren Prozesse zu adaptieren. So entsteht eine Gesamtlösung «aus einem Guss», die flexibel anpass- und erweiterbar ist.

Wie kann aber der Schutz langfristig gewährleistet werden, wenn die Bedrohungsszenarien zunehmen?
Wie initial angetönt sind Produkte nur ein Baustein der Sicherheitsstrategie. Die Prozesse sowie das Personal sind genauso wichtig und werden leider oft vergessen, da diese auf den schönen Produktflyern der Hersteller fehlen und schlecht für ein Budget quantifizierbar gemacht werden können. Ideal ist es, wenn man sicherheitsrelevantes Wissen aufbauen kann und im eigenen Betrieb Leute beschäftigt, die dieser Aufgabe nachkommen. Das dürfte für die meisten Unternehmen aber schwierig umsetzbar sein, da man für eine 24/7-Abdeckung mindestens fünf Leute benötigt, die nicht für andere Projekte eingesetzt werden sollten.

Das ist finanziell kaum tragbar.
Korrekt. Darum kann die Auslagerung an ein externes SOC (Security Operation Center) eine ideale Alternative darstellen. Dadurch wird die interne IT entlastet und kann sich auf die Kernaufgaben konzentrieren. Wir bieten diese Dienstleistung von unserem Schweizer Standort aus an und belassen die Daten in der Infrastruktur der Kunden. Unser SOC ist ein zentrales Organisationsteam, das rund um die Uhr Sicherheitsvorfälle überwacht, untersucht und entsprechend auf diese reagiert. Dadurch unterstützen wir Unternehmen kontinuierlich dabei, ihre Vermögenswerte, Daten und Geschäftssysteme zu schützen.

Welche weiteren Sicherheitsthemen sehen Sie künftig auf Firmen zukommen?
Wir stellen einen Wandel von IT-Security fest: Früher war alles netzwerkbasiert. Heute wird vermehrt mit Cloud-Applikationen gearbeitet, was die Frage aufwirft, wie man in diesem neuen Setting einen durchgehenden Schutz aufbauen kann. Und auch das aufkommende «Internet der Dinge» wird uns vor viele neue Fragen stellen.



Über die Basevision AG

Das Basevision-Team macht die IT-Arbeitsplätze von Unternehmen fit für die Herausforderungen von heute und morgen, indem sie modern, flexibel und sicher gestaltet werden. Seit 2015 vertraut die Kundschaft auf die Kompetenzen der Basevision-Fachleute als Berater:innen, Integrator:innen und Coaches auf dem Weg zu modernen und sicheren IT-Arbeitsplätzen.

Weitere Informationen unter
basevision.ch

baseVISION
SECURE & MODERN ENDPOINT MANAGEMENT

Warum OT-Sicherheit essenziell ist, damit nicht plötzlich das Licht ausgeht

Wird das IT-System eines Unternehmens gehackt, drohen Produktionsausfälle, finanzielle Verluste sowie Reputationsschäden. Doch ist ein solcher Angriff auf eine Kritische Infrastruktur wie beispielsweise ein Kraftwerk erfolgreich, können davon weite Teile der Schweiz betroffen sein. Dies zu verhindern, ist die Aufgabe der Alsec Cyber Security Consulting AG.

Interview mit Reto Amsler und Markus Lenzin, Gründer der Alsec Cyber Security Consulting AG

Reto Amsler
Gründer Alsec Cyber Security Consulting AG

Markus Lenzin
Gründer Alsec Cyber Security Consulting AG

Reto Amsler, Markus Lenzin, was versteht man genau unter «Kritischen Infrastrukturen»?
Reto Amsler: In der Schweiz sind diese durch das Bundesamt für Bevölkerungsschutz genau definiert. Vereinfacht gesagt, handelt es sich bei Kritischen Infrastrukturen um Organisationen und Unternehmen verschiedener Sektoren, die zum Wohl der hiesigen Industrie oder der gesamten Schweizer Bevölkerung agieren. Konkret kann es sich dabei um Energieversorgungsunternehmen aller Art und Grösse handeln, welche Strom produzieren und diesen über die Netze bis an die Haushalte verteilen. Aber auch Spitäler gehören zu den Kritischen Infrastrukturen. Sie sind im Gegensatz zu anderen Unternehmen mit zusätzlichen Angriffsformen aus dem Cyberraum konfrontiert, zu denen auch Angriffe von staatlichen Akteuren zählen. Die Ausgangs- und Bedrohungslage ist also eine grundlegend andere. Dies war unter anderem in den Jahren 2015 und 2016 zu sehen, als erstmals durch einen Cyberangriff ein Blackout verursacht und somit aufgezeigt wurde, dass die Stromversorgung einer ganzen Region lahmgelegt werden kann.

Markus Lenzin: Wir sprechen in diesem Zusammenhang nicht von IT-, sondern von OT-Infrastrukturen. «OT» steht dabei als Kürzel für «Operational Technology», sprich für «Betriebstechnologie». Diese beschreibt die Verwendung von Hard- und Software zur Überwachung und Steuerung von physischen Prozessen, Geräten und Infrastrukturen. Das Problem: OT-Infrastrukturen kann man nicht auf die gleiche Weise schützen wie IT-Systeme.

Warum ist das nicht möglich?
Markus Lenzin: Im OT-Bereich sprechen wir von sogenannten «SCADA-Systemen». Diese dienen der Überwachung und Steuerung von technischen Prozessen. Konkret kann es sich dabei um die Steuerung einer Industrieanlage handeln. Anders als IT-Softwares, die man alle drei bis fünf Jahre generalüberholt und auswechselt, haben OT-Systeme einen deutlich längeren Lebenszyklus. Wir sprechen schnell mal von zehn bis 15 Jahren Betriebsdauer. Diese Steuerungsanlagen sind oft stark an die jeweiligen Produktionsprozesse gekoppelt. Sie auszuwechseln, würde einen enormen Aufwand bedeuten und im schlimmsten Fall die Versorgungssicherheit einschränken. Darum werden sie heute oft so belassen und nur rudimentär gepatched. Natürlich akkumulieren sich dadurch mit der Zeit Schwachstellen. Glücklicherweise sind die meisten OT-Systeme, anders als IT-Systeme, nicht direkt mit dem Internet verbunden. Doch es gibt andere Mittel und Wege, wie Cyberangreifer ihren Weg in diese Kritischen Infrastrukturen finden können. Ist ein solcher Breach erst einmal erfolgt, ist das System oft veraltet und stellt den Angreifenden nur kleine Hürden in den Weg. Wenn wir uns nun die Relevanz von Kritischen Infrastrukturen vor Augen führen, wird klar, welch enormes Schadenspotenzial sich hier eröffnet.

Was wird also in diesem Bereich unternommen?
Markus Lenzin: Der VSE (Verband Schweizerischer Elektrizitätsunternehmen) hat eine Branchenempfehlung zur OT-Sicherheit in der Strombranche herausgegeben. Wir von ALSEC sind primär in diesem Sektor tätig und wissen daher, dass die Umsetzung dieser Empfehlungen noch vielerorts am Anfang steht. Das hat auch damit zu tun, dass die Projekte zum einen sehr aufwendig sind und zum anderen die notwendigen Fachleute fehlen, um eine durchgehende Cybersicherheit zu gewährleisten.

Gibt es denn konkrete regulatorische Anforderungen im Bereich OT-Security?
Reto Amsler: Aktuell muss man das leider verneinen, zumindest für die Schweiz. In Deutschland beispielsweise existieren mit der KRITIS-Rechtsverordnung und dem IT-Sicherheitsgesetz Vorgaben für die Betreibenden von Kritischen Infrastrukturen. Hierzulande gibt es mittlerweile für den Energiesektor die besagte Branchenempfehlung, welche auf der Basis von bestehenden Standards, Best Practices sowie dem aktuellen Stand der Technik beruht, die letztlich aber nur das ist: eine Empfehlung. Das ist problematisch, da SCADA-Systeme oft schlüsselfertig von den Anbietern übernommen werden. Die Hauptanforderung von Kundenseite lautet: Das System muss primär verlässlich funktionieren. Auf das Thema «Security» legte man hingegen bisher viel zu wenig Wert, auch vonseiten der Hersteller, da der Kundendruck in den Ausschreibungen fehlte. Die Quintessenz lautet dementsprechend: Die Betreibenden von Kritischen Infrastrukturen müssen künftig höhere Anforderungen hinsichtlich Sicherheit stellen. «Security by Design» wäre hier anzustreben.

Gibt es ausreichend Know-how im Bereich OT-Security, um «Security by Design» zu etablieren?
Reto Amsler: Auch diese Frage muss man aktuell bedauerlicherweise verneinen. Das Grundproblem liegt darin, dass OT-Security nicht attraktiv scheint im Vergleich zu anderen Cybersecurity-Disziplinen. So wird zwar an den Fachhochschulen viel Know-how hinsichtlich Cybersecurity geschaffen, doch diese Expertise konzentriert sich vornehmlich auf den IT-Bereich. Industrielle Umgebungen hingegen sind weniger gefragt. Der Bereich OT- oder SCADA-Security kommt heute noch viel zu kurz. Das ist eine bedauerliche Entwicklung, denn der Bedarf an sicheren OT-Lösungen wird mit den ganzen Industrie-4.0-Themen noch zunehmen. Wie bereits angetönt, haben die ersten Blackouts in der Ukraine 2015 und 2016 klargemacht, wie gefährlich ein Cyberangriff auf Kritische Infrastrukturen sein kann.

Sind die Schweizer Stromnetze geschützt vor Cyberangriffen?
Markus Lenzin: Jein, weil sie derzeit mehrheitlich noch vom Internet abgekoppelt funktionieren. Doch es gibt andere Möglichkeiten, um in diese Systeme zu gelangen. Schadsoftware kann zum Beispiel durch USB-Sticks eingeschleppt werden. Oder wenn eine Person in den Ferien ihren Laptop im Internet verwendet und nach ihrer Rückkehr wieder ans System der Firma anhängt. Auf diese Weise finden Cyberkriminelle ihren Weg in die Anlagen von Kritischen Infrastrukturen. Das lässt sich also meistens auf menschliches Fehlverhalten sowie fehlende Awareness zurückführen. Hinzu kommt die Tatsache, dass unser Stromnetz mittel- bis langfristig noch mehr vernetzt sein wird. Smart Grids und Smart Meters sollen ein «intelligentes Stromnetz» schaffen, das unter anderem Energieschwankungen ausgleichen kann und so die Versorgungssicherheit erhöht. Durch diese Vernetzung nimmt aber auch der Gefährdungsgrad sprunghaft zu. Darum sollte man mit externen Fachleuten zusammenarbeiten und bereits jetzt die notwendigen Schritte einleiten, die zu einer erhöhten OT-Sicherheit beitragen.

Wie unterstützen Sie bei Alsec Cyber Security Ihre Kundschaft dabei?
Reto Amsler: Es gibt verschiedene Andockstellen, über die wir die Betreibenden von Kritischen Infrastrukturen mit unserer Erfahrung, unserem Fachwissen sowie unserem Technologieverständnis unterstützen. Eine essenzielle Aufgabe von uns besteht in der Schaffung von Awareness, Transparenz sowie klaren Zuständigkeiten. Denn oft ist im Unternehmen nicht festgelegt, wer für welche Aspekte von OT-Sicherheit verantwortlich ist. In den meisten «gewöhnlichen» Firmen liegt diese Kompetenz beim CISO, doch in Energieversorgungsunternehmen sind es meist die Expertinnen und Experten der Energietechnik, die den technischen Takt vorgeben. Und diesen geht es vor allem um die Aufrechterhaltung der Versorgungssicherheit. Der CISO hat darauf keinen oder wenig Einfluss. Solche organisatorischen Stolpersteine entfernen wir, indem wir Assessments durchführen und uns so einen Einblick in die Wirkmechanismen des Unternehmens verschaffen. Basierend auf diesen Learnings erstellen wir gemeinsam mit dem Kunden eine Strategie mit einem Massnahmenplan, welcher hilft, Bedrohungen frühzeitig zu erkennen – und entsprechende Massnahmen rechtzeitig zu implementieren.

Markus Lenzin: Nebst diesen präventiven Massnahmen stehen wir unserer Kundschaft auch zur Seite, wenn es darum geht, auf Angriffe zu reagieren. Das Incident Management stellt sicher, dass Attacken sofort erkannt und schnellstmöglich unschädlich gemacht werden. Ziel dabei ist immer das Aufrechterhalten des sicheren Betriebs einer Kritischen Infrastruktur. Dazu gehören auch flankierende Massnahmen wie die Netzwerksegmentierung: Auf diese Weise können die Anlagen weiterlaufen, während man andernorts die Gefährder unschädlich macht.

Was hat es mit Ihrem IT-/OT-Cyberlabor auf sich?
Reto Amsler: Dieses ist enorm wichtig, um den Akteuren der Energiebranche die Relevanz von OT-Sicherheit aufzuzeigen. Wir bieten ihnen in Zusammenarbeit mit der HSLU ein Praxislabor an, welches den aktuellen Cyber-Security-Vorgaben der Branche entspricht und alle aktuellen Technologien umfasst. Das Labor beinhaltet sechs Unterwerke mit Anbindung an ein zentrales Leitsystem, dem SCADA. Wir stellen dieses praxisorientierte Labor einem breiten Publikum für praktische Lösungen, Integration und Weiterbildung zur Verfügung und können es ebenfalls gut an andere Branchen adaptieren. So wird das relativ abstrakte Thema OT-Security im wahrsten Sinne des Wortes erfassbar und greifbar. Dieses wichtige Fachwissen weiterzugeben, ist eines unserer zentralen Anliegen. Aus diesem Grund bieten wir auch eigene oder gemeinsam mit dem VSE OT-Security-Kursreihen für technisches Personal und Führungskräfte mit einer anschliessenden Zertifizierung an.

Über die Alsec Cyber Security Consulting AG

Gegründet am 1. März 2019 von Markus Lenzin und Reto Amsler, fokussiert sich die Alsec Cyber Security Consulting AG auf die Erbringung von Cyber-Security-Dienstleistungen im Operational Technology (OT) Umfeld nach höchsten Standards. Die Kundschaft umfasst Organisationen und Unternehmen, die Kritische Infrastrukturen betreiben, deren Sicherheit integral unter den Aspekten Organisation, Technologie, Prozesse und Ausbildung betrachtet werden muss.

Weitere Informationen finden Sie unter **www.alsec.ch**

ALSEC protect critical infrastructure

Stellt Wirtschaftsspionage noch eine ernsthafte Gefahr dar?

«Swiss made» ist ein Siegel, das schon immer für gute Qualität und Status stand. Seit einigen Jahren ist es leider auch anfällig für Spion:innen, die mit verschiedenen Mitteln versuchen, Informationen von Unternehmen zu stehlen. Solche, die online Produkte anbieten, sind davon besonders betroffen, da die Informationen ihrer Produkte auf Servern liegen. Durch die Zugriffsberechtigung von Mitarbeitenden finden auch Kriminelle eine Tür zu den Daten.

Man sitzt morgens noch halb verschlafen am PC, öffnet den Mailserver und bekommt eine E-Mail mit der Info, dass das Arbeitskonto gesperrt ist und man in kürzester Zeit auf den beigefügten Link klicken muss, um es wieder freizuschalten. Man klickt diesen an und daraufhin sollte sich das Thema erledigt haben. Monate später tauchen ähnliche, aber viel billigere Produkte auf dem Markt auf, sodass Schweizer Firmen Absatzprobleme bekommen und im schlimmsten Fall ihr Unternehmen schliessen müssen. Nur das Anklicken des Links, gewährte Konkurrenzfirmen Zugriff auf den Firmenserver. Das ist ein klassischer Fall von Phishing-Mails, die heutzutage täglich zum Einsatz kommen, um an Informationen von Unternehmen zu gelangen.

Ausmass der Angriffe

Wirtschaftsspionage hat in den letzten Jahren, ohne dass man es mitbekommen hat, stark zugenommen. «Zudem sind die Urheber und deren Intentionen oft nur schwer zu eruieren und in vielen Fällen bleiben Angriffe gänzlich unbemerkt», so der Nachrichtendienst des Bundes (NDB). Viele Unternehmen melden diese Angriffe nicht, da sie hohe Reputationsschäden befürchten, wenn diese Informationen öffentlich gemacht werden. Laut NDB stehlen Cyberspion:innen üblicherweise Fabrikationsgeheimnisse, Patente sowie Informationen zu geplanten Fusionen, Übernahmen, Marktdurchdringung oder Investitionen. Sollten diese Informationen an die Öffentlichkeit gelangen, droht ein Glaubwürdigkeits- und Vertrauensverlust. Im schlimmsten Fall muss das Unternehmen schliessen, da es seine Kund:innen an das Konkurrenzunternehmen verliert.

Methoden der Auskundschaftung

Als grösstes Risiko für Unternehmen, Opfer von Wirtschaftsspionage zu werden, gelten die eigenen Mitarbeitenden. Sie haben direkten Zugriff auf alle Informationen und geniessen das volle Vertrauen des Unternehmens. Diese werden von Konkurrenzunternehmen mit hohen Summen bestochen, um wichtige Firmeninformationen zu verkaufen. Neben der Spionage durch Mitarbeiter:innen wurden in den letzten Jahren auch hochentwickelte elektronische Mittel eingesetzt, die das Abhören und Mitlesen elektronischer Übermittlungen ermöglichen. «Die Cyberbedrohung, welche die kritischen Infrastrukturen in der Schweiz derzeit hauptsächlich beschäftigt, ist Verschlüsselungsschadsoftware. Damit werden Daten unleserlich gemacht, um vom Besitzer, zum Beispiel einem Unternehmen, Geld zu erpressen», so der NDB.

Sicherheitslücken

Gründe für solche Angriffe sind Sicherheitslücken im Unternehmen. Da nicht viel Spionagefälle Berichterstattung finden, wiegen sich viele in Sicherheit und investieren kaum in IT-Sicherheit. Daher kommt ein mangelndes Problembewusstsein, welches zu Sicherheitslücken führt. Sowohl der interne als auch der externe Mailverkehr erfolgt meist unverschlüsselt. Dies erleichtert das Abgreifen von Daten sowie deren Missbrauch.

Ebenfalls gibt es nicht immer verbindliche Vorgaben für sichere Passwörter. Somit ist es für Hacker:innen ein Leichtes, diese zu knacken. Zusätzlich wird oft das Mitbringen von eigenen Datenträgern wie USB-Sticks toleriert. Dadurch können wichtige Informationen ausserhalb des Unternehmens getragen werden, wo meist eine noch niedrigere Sicherheit herrscht als im Unternehmen selbst.

Sicherheitsrisiko Homeoffice

Seit der Coronapandemie haben viele Arbeitgeber ihren Mitarbeitenden die Möglichkeit gegeben, im Homeoffice zu arbeiten. Doch dort lauern viele Risiken. Da Mitarbeiter:innen nicht im Unternehmensnetzwerk, sondern in ihren eigenen sind, ist keine Kontrolle durch das Unternehmen gewährleistet. Um die Sicherheit zu garantieren, muss ein sicheres Virtual Private Network (VPN) eingerichtet werden, damit sowohl das Unternehmensnetzwerk als auch das eigene gesichert sind. Vielen Unternehmen ist nicht bewusst, welches Sicherheitsrisiko damit einhergeht oder sie haben keine Kapazitäten, diese mit Laptops und Mobiltelefonen auszustatten. Dies führt dazu, dass diese nicht abgesichert sind, weil keine Unternehmenssoftware darauf installiert ist und somit keine Kontrolle über die Geräte herrscht. Die Einführung von Telearbeit oder deren Weiterführung muss aus der Perspektive der Sicherheit genau analysiert werden, um das Unternehmen nicht anfälliger für Cyberattacken zu hinterlassen.

Prävention

Um sich vor solchen Angriffen zu schützen, gibt es verschiedene Präventionsmöglichkeiten, die ein Unternehmen beachten muss. Viele scheuen sich aufgrund hoher Kosten davor, Sicherheitsbeauftragte einzustellen. Für grössere Unternehmen mit dem entsprechenden Budget ist dies jedoch die beste Option, um Spionagefälle frühzeitig zu erkennen und Gegenmassnahmen einzuleiten. Alternativ dazu können Schulungen durchgeführt werden, in denen Mitarbeitende auf die aktuellen Methoden der Kriminellen aufmerksam gemacht werden. Da interne Mitarbeitende selbst Spionage betreiben können, ist es wichtig, ein anonymes Meldesystem für Verdachtsfälle einzurichten. Denn finden die Kriminellen ein Einfallstor, ist Schadensbegrenzung die einzige Option. Vorbeugende Massnahmen sind der einzige Weg, den Worst-Case zu verhindern.

«Viele Unternehmen befinden sich noch im Dornröschenschlaf»

Die Digitalisierung führt dazu, dass immer mehr kritische Prozesse und Daten im Netz verfügbar sind. Alle Gefahren können allerdings nicht abgedeckt werden – deshalb ist ein professionelles Risikomanagement wichtig.

Interview mit Michael Schläpfer, Partner, CEO und Saner Çelebi, Partner, CCO

Michael Schläpfer
Partner, CEO

Saner Çelebi
Partner, CCO

In zwei, drei Sätzen: Was macht Ihre Firma genau; was ist Ihre Mission?
Secure Digital Business ist unsere Kernkompetenz. Wir verstehen es als unsere Mission, dass wir unsere Kunden dabei unterstützen, ihre digitalen Geschäftsmodelle sicher und kosteneffizient aufzubauen und zu betreiben. Viele Unternehmen nehmen Security als «Verhinderer» war, obwohl mit den heutigen technologischen Möglichkeiten sowohl die Sicherheit wie auch die Usability erhöht werden kann. In der heutigen digitalen Welt sind neue Technologien und Digitalisierung Chance und Risiko zugleich. Denn der Schlüssel für die Resilienz von innovativen Geschäftsmodellen liegt in der Sicherheit ihrer Geschäftsprozesse. Deshalb ist das Gesamtverständnis von Strategie, Architektur und Technologie entscheidend für den Geschäftserfolg. Wir kennen die Theorie und die Praxis der neuen Technologien und sind deshalb in der Lage, den Unternehmen massgeschneiderte Lösungen anzubieten.

Gemäss einer aktuellen Studie der gfs Zürich stufen zwei Drittel aller Schweizer KMU die IT-Sicherheit als wichtig ein. Aber nur 18 Prozent befürchten, selbst angegriffen zu werden. Ist das auch Ihre Erfahrung und was könnte der Grund dafür sein?
Das gilt nicht nur für Schweizer KMU. Wenige Tage nach dem aktuellen Sicherheitsvorfall bei Uber wurden Dutzende neue Stellen für Security-Rollen ausgeschrieben. Viele Unternehmen befinden sich immer noch im Dornröschenschlaf. Sie unterschätzen die Cyber-Gefahren. Dabei wäre es wichtig, das Gefahrenpotenzial fundiert und regelmässig zu analysieren, weil sich die Risikolandschaft ständig verändert – auch für die verschiedenen Branchen. Früher stand vor allem der Finanzsektor im Fokus, heute sind es zusätzlich die Betreiber von kritischen Infrastrukturen und im Allgemeinen Unternehmen mit einem kritischen digitalen Footprint. Gerade in wirtschaftlich schwierigen Zeiten wird die Security oft vernachlässigt.

Viele Industrien verstärken ihre Sicherheitsmassnahmen zu spät, oft erst nachdem durch einen erfolgreichen Angriff bereits ein hoher finanzieller Schaden oder Reputationsschaden entstanden ist. Unter dem Strich hat man die Chance verpasst, frühzeitig die Fähigkeiten aufzubauen, um den Schaden angemessen zu minimieren.

Die «Einschläge» kommen immer näher. Immer mehr Unternehmer und Unternehmerinnen kennen andere Firmen oder Lieferanten, die es getroffen hat und das Thema Cyberkriminalität wird auch von den Medien intensiver bearbeitet.

Wie wichtig ist die Benutzerfreundlichkeit und dass bei der Entwicklung und Umsetzung der Sicherheitsfunktionen die Benutzenden ins Zentrum gestellt werden, damit Akzeptanz und das Verständnis gewährleistet sind?
Die Benutzerfreundlichkeit ist ein sehr wesentlicher Aspekt. Es ist erwiesen, dass Benutzer, beziehungsweise Mitarbeitende, die Sicherheitsmassnahmen umgehen, wenn sie diese als hindernd oder zeitineffizient wahrnehmen und sie den Mehrwert nicht einsehen. Sie bauen Passwörter nach einer eigenen Logik auf, speichern die auf unsichere Weise oder sie nutzen Anwendungen, von denen die IT-Abteilung nichts weiss.

Deswegen ist es essenziell, den Sicherheitslevel und die Benutzerfreundlichkeit ausgewogen aufzubauen und möglichst benutzerfreundliche und praktikable Sicherheitsmassnahmen einzuführen. Nicht zu unterschätzen ist dabei die Sensibilisierung der Benutzer und Benutzerinnen beispielweise mit Awareness-Massnahmen.

Usability versus Security ist kein einfacher Spagat. Wenn Benutzer die Notwendigkeit von Sicherheitsmassnahmen sehen und diese auch benutzerfreundlich eingeführt werden, können Geschäftsprozesse resilienter aufgebaut werden. Im Endeffekt kann dies einen wesentlichen Wettbewerbsvorteil darstellen. Security muss also Usability nicht immer hindern. Es existieren Technologien, die beide Ziele erreichen können.

Also geht es darum, den Spagat zwischen optimaler Sicherheit und hoher Benutzerfreundlichkeit schaffen?
Die «bewusste Inkompetenz» ist wichtig. Der Kern der Cybersicherheit ist ein professionelles Risikomanagement. Eine objektive, aktuelle Sicht auf die eigenen Sicherheitsrisiken ist die Basis. Darauf aufbauend kann der Entscheid auch sein, ganz bewusst keine Sicherheitsmassnahmen einzuführen. Beispielsweise, wenn der Schaden eines Angriffs in als tragbar eingestuft wird. Oder die Analyse kann aufzeigen, dass eine Versicherung Sinn machen würde oder eine Investition in die Sicherheit. An diesem Punkt sind viele KMU aber noch nicht angekommen. Dabei liesse sich gerade auch bei KMU im Bereich Sicherheit Geld sparen oder effektiver einsetzen, wenn Sicherheitsrisiken objektiv beurteilt werden würden.

Die Analyse-Tools, die wir für Grossunternehmen entwickelt haben, können wir heruntergebrochen als Serviceangebot und als Webapplikation auch KMU anbieten. So ist eine pragmatische Risikoanalyse möglich, die auch für kleinere Betriebe finanziell tragbar ist.

Wir stellen den Trend fest, dass es aus Hackersicht einfacher ist, sich auf mehrere KMU zu konzentrieren, statt auf professionell geschützte Grosskonzerne. Gerade in der heutigen Zeit, in der auch Start-ups und Kleinstbetriebe durch die Möglichkeiten der Automatisierung schnell zu Global Players werden können. Aber auch lokale Kleinst- und Gewerbebetriebe sind gefährdet, wenn sich Hacker Zugriff auch die Maschinensteuerung, auf die Buchhaltung oder Kundendaten verschaffen. Das wäre oft ein existenzgefährdendes Desaster.

Kunden oder Kundinnen empfinden die Sicherheitsmassahmen beispielsweise von Banken oder Webshops mit Passwörtern, Code per SMS etc. eher als mühsam …
Das ist so – gerade Passwörter werden oft zum Sicherheitsproblem. Weil man sie sich nicht merken kann, schreibt man sie auf ein Post-it und klebt es an den Bildschirm … Aber gerade da liegt auch die Chance für die Firmen und Anbieter: Sicherheit so zu designen, dass sie von den Kundinnen und Kunden als Mehrwert empfunden wird. Das kann beispielsweise mit Awareness-Kampagnen gemacht werden, um den Kunden bewusst zu machen, dass ein Sicherheitsschritt eben wichtig ist und dafür das Geld auf der Bank oder die gespeicherten persönlichen Daten sicher sind. Das sind Beispiele, die die Gratwanderung betreffend Usability versus Security gut aufzeigen. Heute gibt es aber Technologien, die es erlauben, beides zu erreichen – beispielsweise einloggen ohne Passwort. Wenn es einem Unternehmen gelingt, den Kunden eine sichere Anmeldung ohne Passwörter anzubieten ist das natürlich ein riesiger Wettbewerbsvorteil.

Bieten Sie auf die Bedürfnisse der Kunden abgestimmte Sicherheitslösungen an?
Ja, wir haben in der Beratung wie auch in der Tool-Unterstützung sehr gute Erfahrungen mit einem gezielten, risikobasierten Ansatz gemacht – diese ist immer individuell auf die Bedürfnisse des Unternehmens abgestimmt, je nach Business und Branche. Geprüft wird vorab, welches Risiko einkalkuliert werden kann und auf welche reagiert werden muss. Im Vordergrund steht also immer das Erkennen der Risikoexposition des Unternehmens. Mit einer objektiven Risikobetrachtung kann man seine oft beschränkten Mittel gezielt einsetzen oder auch auf Massnahmen verzichten. Dafür gibt es Tools, um die Risiken systematisch zu erfassen, um dann zu entscheiden, welche Massnahmen getroffen werden sollen, abgestimmt auf die unterschiedlichen Geschäftsprozesse – und eben, welche Risiken das Unternehmen tragen kann. Dabei ist der Weg oftmals auch das Ziel – es geht nicht um einen perfekten, aufwändigen Risikomanagementprozess, sondern um das Verständnis und die Systematik. Mit unserer Expertise, langjähriger Erfahrung und eigenentwickelter Software-Lösung (fortControl) im Bereich risikobasiertem Security Management, befähigen wir unsere Kunden dazu, dass sie erkennen können, wo sie betreffend Sicherheit stehen und welche Massnahmen effizient und effektiv sind.

Welche Rolle spielt in diesen Szenarien der «Faktor Mensch»?
Der Faktor Mensch ist ein potenzielles Einfallstor, der aber auch als ein starker Schutzfaktor eingebettet werden kann. In der Risikoeinschätzung muss der Faktor Mensch klar berücksichtigt werden. Alle Massnahmen in einem Betrieb müssen auf diejenigen abgestimmt sein, die sich nicht um das Thema Sicherheit kümmern oder nicht sensibilisiert sind. Bis zu einem gewissen Punkt kann das mit Awareness-Kampagnen verbessert werden, in denen man auf die Gefahren hinweist und die Mitarbeitenden auf mögliche Cyberangriffe sensibilisiert. Auf der anderen Seite gibt es auch Technologien, die verhindern, dass Angreifer beispielsweise von Nachlässigkeiten profitieren können. Beispielsweise das «Zero Trust Security Model» mit seinem Paradigma «Never Trust, Always Verify». Dabei geht es nicht um Paranoia, sondern vielmehr darum, moderne Arbeits- (zum Beispiel Homeoffice) und Betriebsmodelle (zum Beispiel Cloud) sicher unterstützen zu können.

Sicherheit wird immer mehr zum Megatrend auf verschiedenen Ebenen. Wie sehen Sie die Zukunft der Cyber Security in und für Unternehmen, insbesondere auch für KMU?
Die Digitalisierung führt dazu, dass immer mehr kritische Prozesse und Services im Netz verfügbar sind – das führt unweigerlich dazu, dass die Cyberkriminalität weiter zunehmen wird. Die Sicherheitsanforderungen werden deshalb immer anspruchsvoller und müssen entsprechend angepasst werden.

Dazu kommt, dass die Nachfrage nach gut ausgebildeten Sicherheitsfachleuten das Angebot massiv übersteigen wird und deshalb Unternehmen jeder Grösse diese internen Stellen gar nicht mehr besetzen können. Das bedeutet, dass sie sich Gedanken darüber machen müssen, mit welchen Partnern sie in Zukunft zusammenarbeiten und welche Services sie dereinst nutzen wollen.

So wie sich die digitale Landschaft weiter schnell verändert und die Cyberkriminellen aufrüsten, werden auch die Unternehmen bessere und günstigere Sicherheitslösungen zu Verfügung haben. Oder eben auf kompetentes spezialisiertes Wissen von externen Firmen zugreifen können.

FortIT AG
Waldmannstrasse 10
8001 Zürich-Bellevue
info@fort-it.ch
+41 58 255 09 55

Weitere Informationen unter
www.fort-it.ch

FORT IT
SECURE DIGITAL BUSINESS

«Der Security-Mix muss stimmen – im richtigen Mass, zur richtigen Zeit»

Regelmässig werden immer mehr Unternehmen Opfer von Cyberattacken. Durch die zunehmende Digitalisierung und Abhängigkeit von einer einwandfrei funktionierenden IT werden die Schäden immer grösser. Dabei ist ein zuverlässiger Schutz rund um die Uhr möglich. Econis betreibt als lokaler Service Provider bei zahlreichen Schweizer Unternehmen eine erfolgreiche Gefahrenabwehr mit standardisierten und gleichzeitig zugeschnittenen Managed Services. CEO Beat Rascher und CISO Werner Stocker erklären, worauf es ankommt, um IT-Sicherheit schnell umzusetzen und langfristig zu gewährleisten.

Beat Rascher
CEO Econis AG

Werner Stocker
CISO Econis AG

Beat Rascher, Werner Stocker, worin bestehen die Herausforderungen, wenn ein Unternehmen seine IT schützen will?
Beat Rascher: Viele Unternehmen denken beim Schutz vor Cyberangriffen zuerst an Ransomware. Dieser Ansatz ist nicht falsch, er ist jedoch ein Entscheid aus dem Bauchgefühl heraus – oder aus dem, was gerade in den Medien als kritisch angeschaut wird. Das hinterlässt blinde Flecken, da Informationssicherheitsrisiken an vielen Orten lauern.

Werner Stocker: Die grösste Herausforderung für die Unternehmens-IT ist, die Informationssicherheit in seiner Gänze als Prozess im Griff zu haben. Damit gelangt man von reaktiver Sicherheit, wo nur auf Ereignisse reagiert wird, in eine proaktive Sicherheit. Mittel- und langfristig ist man so zusätzlich auf die sich verändernde Sicherheitslandschaft vorbereitet.

Wie sieht eine zuverlässige 360-Grad-Sicherheitsarchitektur aus?
Werner Stocker: Sicherheit ist ein Prozess und die Architektur wird in regelmässigen Zyklen an die sich verändernden Rahmenbedingungen angepasst. Hierfür ist ein sauberes Inventar aller wichtigen Geschäftsanwendungen und deren Daten notwendig, die sogenannten Assets. Diese Assets werden bezüglich deren Sensitivität eingestuft und anschliessend in ein strukturiertes Konzept integriert, um diese gemäss deren Sensitivität individuell zu schützen. Eine zuverlässige Sicherheitsarchitektur besteht darin, genau diesen Spagat aus individuellem Schutz und Wirtschaftlichkeit über wenige standardisierte, sich ergänzende Komponenten zu erreichen.

Sie setzen einen wichtigen Fokus auf das Business-Continuity-Management. Was gilt es hier zu beachten?
Beat Rascher: IT ist mittlerweile die Grundlage aller Geschäftsprozesse geworden. Das bedeutet auch, dass ein längerer Ausfall der IT die Existenz von Firmen gefährdet. Beim Business-Continuity-Management geht es darum, alle Vorfälle zu identifizieren, welche den IT-Betrieb gefährden können und entsprechende vorbereitende Massnahmen zu treffen. Dies hilft, um beispielsweise bei grösseren Ausfällen über ein Backup-Rechenzentrum den Betrieb wiederherzustellen oder rasch auf Cyberangriffe reagieren zu können, um Schäden zu minimieren. Oft wird jedoch aus Kosten- und Ressourcengründen auf regelmässige Tests verzichtet. Diese Tests sind jedoch wichtig, um über deren Resultate Optimierungsmassnahmen zur Verbesserung der betrieblichen Stabilität einzuleiten. Business-Continuity-Management ist deshalb eine lohnenswerte Investition in die Zukunft zur Sicherstellung des Geschäftsbetriebes.

Wie unterstützen Sie Ihre Kunden bei der Asset Security & Compliance?
Werner Stocker: Die Kernkompetenz der Econis ist die Sicherheit als Prozess gemäss der ISO/IEC 27001-Zertifizierung. Dies bedingt, dass die Sensitivität aller wichtigen Kundenanwendungen und deren Daten bezüglich Vertraulichkeit (wer darf was sehen), Integrität (bis zu welchem Zeitpunkt in der Vergangenheit dürfen Daten verloren gehen), Verbindlichkeit (wie viele Jahre sind Daten rechtlich relevant) und Verfügbarkeit (wie lange dürfen Daten und Prozesse maximal ausfallen) bekannt sind. Dies wird damit angereichert, welche Regulatorien oder branchenspezifischen Bestimmungen jeweils vorliegen. Econis begegnet dabei den Kunden auf Augenhöhe und begleitet sie proaktiv bei der Erfüllung des IT-Grundschutzes inklusive der notwendigen Datenschutzprozesse. Das geht über das Vorfallsmanagement auch bis in das Business Continuity Management hinein.

Ein wichtiger Punkt ist bei Ihnen die Datenklassifikation. Da zucken manche Unternehmen immer noch mit den Schultern, weil sie nicht wissen, wie sie konkret mit welchen Daten umgehen sollen. Wie können Sie hier helfen?
Beat Rascher: Econis führt Kunden ohne Datenklassifikation auf einfache Weise in dieses Thema ein und zeigt die Vorteile daraus auf. Dies geschieht über die jährlichen Review-Prozesse für die an Econis ausgelagerten Managed Services. Wenn ein Kunde bereits eine Datenklassifikation hat, wird diese einfach gemappt, damit beide Seiten vom selben sprechen und die richtigen Massnahmen ergreifen können.

Werner Stocker: Econis kann hierbei als Leading by Example nicht nur helfen, diese Datenklassifikation sauber zu definieren, sondern auch technisch umzusetzen. Es können neben den Geschäftsanwendungen und Daten auch unstrukturierte Daten wie beispielsweise E-Mail und Office eingestuft und mit Sicherheitsprozessen belegt werden. Beispielsweise kann so verhindert werden, dass sensible Daten die Firma verlassen. Wichtig ist, dass hier pragmatisch an die Sache herangegangen wird, nach dem Prinzip «so viel wie nötig». Mit Econis können sich Kunden auf ihre Kerngeschäfte konzentrieren und haben mehr Zeit für das Wesentliche.

Im Econis-Security-Monitoring wollen Sie Cyber Security sichtbar machen. Wie werden dabei Angriffe von aussen leichter oder schneller erkannt?
Werner Stocker: Systeme und Anwendungen protokollieren alle Tätigkeiten. Darin verstecken sich oft auch Angriffe oder unerwünschte Aktivitäten. Über eine zentrale Sammlung und Auswertung in einem Security Operation Center kann die berühmte Nadel im Heuhaufen sichtbar gemacht werden. Zusammen mit strukturierten Vorfallshandbüchern werden so Angriffe effizient eingedämmt und grössere Schäden verhindert. Ein Security Operation Center kann aber nicht nur monitoren, sondern in einer weiteren Ausbaustufe auch schwerwiegende Angriffe automatisiert abwehren und damit grössere Ausfälle oder Datenabflüsse verhindern.

Sie schauen sich im sogenannten Vulnerability Management auch an, wo genau in Soft- und Hardware-Komponenten Schwachstellen liegen. Wird in Unternehmen zu wenig ganzheitlich auf Sicherheit gesetzt?
Werner Stocker: Die Kunst des Vulnerability Managements ist es, zu wissen, welche Anwendungen und Komponenten im Einsatz sind und ob diese verwundbar sind gegenüber Angriffen. Man muss deshalb ein vollständiges Inventar aller Anwendungen haben und wissen, welche Schwachstellen auf diese wirken. Hierüber legt man dann einen risikooptimierten Prozess, um Probleme zu beheben. Dabei werden kritische Schwachstellen priorisiert und entsprechend rasch behoben. Häufig wissen Unternehmen gar nicht, wo sie verwundbar sind. Econis bietet das Vulnerability Management für alle seine Managed Services an und kann den Kunden auch bei selbst- oder fremdverwalteten Anwendungen beim Tracking und Reporting von Schwachstellen unterstützen. Dieser Prozess wird technisch unterstützt, um menschliche Fehler ausschliessen zu können.

Was können Sie zusätzlich in Ihren Cyber-Security-Workshops und -Trainings vermitteln?
Beat Rascher: Econis hat aufgrund seiner Zertifizierung einen umfassenden Sicherheitsprozess etabliert. Wir bieten einmalige oder wiederkehrende Sicherheits-Beurteilungen in zwei Stufen an. In der einfachen Form wird auf Cyber-Security fokussiert. In der umfassenderen Form erfolgt eine vollständige Analyse gemäss ISO/IEC27001 und 2. Hierbei berät Econis bei der Optimierung der Informationssicherheit, unabhängig von den eingesetzten Massnahmen. Wir können dazu auf einen jahrelangen Erfahrungsschatz über verschiedenste Branchen zurückgreifen. Auch hier gilt es, über einen pragmatischen Ansatz rasch eine Visibilität zu erreichen, damit der Kunde seine Ressourcen optimal und umfassend auf die wichtigen Themen fokussieren kann. Daneben bieten wir eine auf den Kunden abgestimmte fortlaufende Sensibilisierung der Mitarbeitenden an. Dies geschieht über ein Web-Based-Awareness-Training und kann die Effektivität über simulierte Phishing-Angriffe auch regelmässig überprüfen.

Weitere Informationen unter
www.econis.ch

Interview **Rüdiger Schmidt-Sodingen**

> **«Die Kernkompetenz der Econis ist die Sicherheit als Prozess gemäss der ISO/IEC 27001-Zertifizierung.**

ECONIS
IT with passion

Self-Sovereign Identity – Ökosystem digitaler Identitäten

Online können wir sein, wer oder was wir wollen. Doch wie stellt man sicher, dass eine Online-Identität der Wahrheit entspricht? Die Self-Sovereign Identity ist eine neue Art, in der digitalen Welt Vertrauen herzustellen – und geht weit über das derzeitige Verständnis von Identität hinaus.

Prinz, Model oder Milliardenerbin: Online können Menschen alles sein – und es ist schwierig, eine Onlineidentität offiziell zu prüfen. Das soll sich bald ändern. Was in der physischen Welt die Identitätskarte oder der Reisepass ist, soll in der virtuellen Welt die Self-Sovereign Identity (SSI) werden. Sie ermöglicht es, physische Identitätsnachweise in die digitale Welt zu übersetzen. Standardisiert und vertrauenswürdig, hochgradig fälschungssicher, verifizierbar – und nicht zuletzt datenschutzkonform.

Username und Passwort reichen nicht

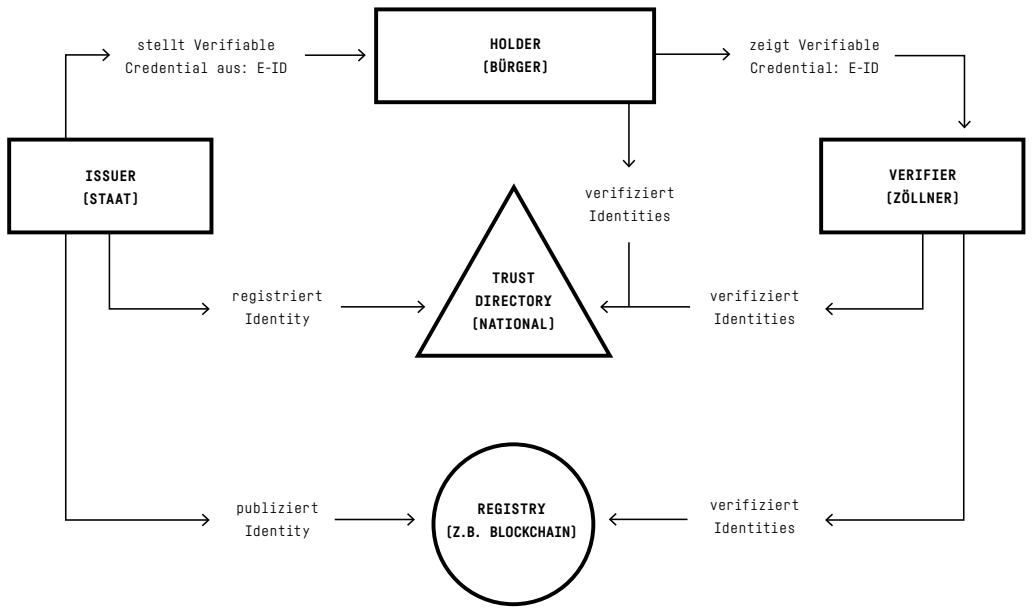
Wer sich heute bei einem Webdienst identifizieren muss, braucht dafür meistens einen Usernamen und ein Passwort. Die meisten Dienstanbieter nutzen ein lokales Identitätsmodell, um ihre User eindeutig zu identifizieren. Das hat viele Nachteile. Anbieter stehen in der Pflicht, diese Daten sicher zu verwalten – und erleiden bei einer Datenpanne finanziellen Schaden durch Folgekosten und Reputationsverlust. Nutzer:innen müssen die vielen verschiedenen Accounts und Passwörter verwalten, was mit Aufwand verbunden ist. Um hier Abhilfe zu schaffen, hat sich in den letzten Jahren die föderierte Identität etabliert: Nutzer:innen können sich mit dem Login eines anderen Dienstes wie Facebook oder Google identifizieren. Dieses Single Sign-on ist vor allem für Zugänge mit geringeren Sicherheitsanforderungen sinnvoll. Für Unternehmen, die auf eine stärkere Authentifizierung angewiesen sind, reicht das aber nicht aus. Hier ist eine dezentrale Identifikation wichtig.

Rechtliche Rahmenbedingungen schaffen

Die rechtlichen Rahmenbedingungen für international anerkannte, dezentralisierte Identitäten werden gerade erarbeitet. Nachdem das Schweizer Stimmvolk vergangenes Jahr die E-ID abgeschmettert hat, strebt der Schweizer Gesetzgeber eine selbstverwaltete Identität SSI an. Die Vernehmlassung zum neuen Gesetz soll Mitte 2022 eröffnet werden. Die EU hat ein Framework für eine europäische SSI erstellt, Pilotprojekte sind für die kommenden Jahre geplant. Auch Nordamerika geht diesen Weg: Die Standardisierungsorganisation W3C erarbeitet derzeit einen Standard für Self-Sovereign-Identitäten. Aus datenschutzrechtlicher Sicht ist die SSI eine gute Lösung: Sie funktioniert im Einklang mit den zurzeit verbreiteten Regelungen zur Verarbeitung personenbezogener Daten. Zudem erleichtert eine dezentrale Identifikation das Datenmanagement für Anbieter: Dank des Peer-to-Peer-Charakters der SSI sind grundsätzlich weniger Dienstleister in die Datenmanagementkette involviert. Und weil sie weniger sensible Daten speichern, haben Datenpannen weniger dramatische Folgen.

Nutzer:innen haben die Daten in der Hand

Die Dezentralisierung der SSI ist ein Paradigmenwechsel: Es sind nicht mehr die Anbieter, die Authentifizierungsdaten verwalten, sondern die Nutzer:innen selbst. Dazu speichern sie verifizierte Identitätsdaten – sogenannte Credentials – in einer Wallet auf dem Smartphone oder einem anderen Gerät. Vom Führerausweis über ein Zeugnis bis zur Social-Media-Historie sind diese Credentials weit breiter gefasst als die analoge Identitätskarte oder der Reisepass. Ein Issuer bezeugt die Richtigkeit der Credentials elektronisch – und die Anbieter, auf Neudeutsch Verifier, überprüfen sie ebenfalls auf elektronischem Weg. Welche Daten ein Verifier sieht, entscheiden die Besitzer:innen der Wallet: die Holder oder Nutzer:innen. Denn sie, und nur sie, haben die Hoheit über ihre Daten – ein Privileg, das auch mit Pflichten einhergeht. Wer beispielsweise seine Wallet verliert, der muss sich um Ersatz für alle Ausweise und Dokumente kümmern. Dafür entfallen komplizierte Login-Verfahren und die damit einhergehende Passwortverwaltung.



Das Konzept der Self-Sovereign-Identität illustriert am Beispiel der E-ID.

Catharina Dekker
Consultant, Ergon

„SSI revolutioniert unsere digitalen Interaktionen.

Das kann die SSI im Alltag

Eine SSI hat viele Vorteile. Finanzinstitute beispielsweise profitieren von der anerkannten digitalen E-ID: Statt in der Filiale vor Ort oder einem komplizierten Onlineidentifizierungsverfahren reicht es, wenn der:die Kund:in die Wallet zückt und die erforderlichen Credentials bereithält. Die Automiete wird dank der SSI ebenfalls einfacher, wenn das Kopieren von Identitätskarte und Führerausweis künftig entfällt. Womöglich können dann die Mieter:innen sogar direkt einsteigen und losfahren, weil dem smarten Auto der Fahrzeugschlüssel als Verifiable Credential (VC) direkt aus der Wallet vorgewiesen werden kann.

Auch digital zertifizierte Dokumente wie Zeugnisse oder Diplome erleichtern den digitalen Bewerbungsprozess – und potenzielle Arbeitgeber prüfen die Echtheit der Unterlagen automatisiert.

Um einen Jugend- oder Seniorenrabatt zu gewähren, muss das Alter der Person bekannt sein. Es besteht aber keine Notwendigkeit, einem Verkehrsbetrieb oder einem Museum das exakte Geburtsdatum offenzulegen. Wenn man dazu noch berücksichtigt, dass in der Schweiz 99,999 Prozent aller Personen durch den vollständigen Namen und das Geburtsdatum eindeutig identifiziert sind, dann wird klar, dass die Bearbeitung des Geburtsdatums aus Sicht des Datenschutzes besonders kritisch ist.

Im E-Commerce profitieren Händler dank SSI von einer sofortigen Bonitätsprüfung und einem schnellen Bezahlprozess. Und zwar mit einem Credential, das direkt mit der Bank der Käufer:innen verknüpft ist. Sichergehen können auch Käufer:innen, dass sie beim richtigen Online-Shop einkaufen und kein Geld verlieren – durch Überprüfung der Händler-Credentials.

Breit gefasster Identitätsbegriff

Credentials sind nicht zwingend auf Individuen begrenzt. Auch Unternehmen und Institutionen können eine SSI erhalten und diese in der Kommunikation mit Kund:innen und Lieferanten nutzen. Das kann zum Beispiel die neue Bankbeziehung für die Rechnungsstellung an Kund:innen oder der Handelsregisterauszug für Lieferanten und Partner sein. Es wäre sogar vorstellbar, dass autonome Fahrzeuge eine eigene Wallet bekommen, mit der sie dann gegenüber Mautstellen oder Werkstätten autark agieren könnten. Ihre «Identität» wäre in diesem Fall zum Beispiel an die Fahrzeugidentifikationsnummer gebunden.

Diese Beispiele zeigen, dass das Potenzial der SSI enorm ist. Löst der Staat das Henne-Ei-Problem der Einführung, so dürften sich immer mehr Use Cases auch wirtschaftlich rechnen. Zumal die Digitalisierung in Riesenschritten weiter voranschreitet. Das McKinsey Global Institute hat prognostiziert, dass im Jahr 2030 die Nutzung digitaler Identitäten in Industrieländern einen wirtschaftlichen Wert von drei Prozent des Bruttoinlandsprodukts freisetzt, in Schwellenländern sogar von sechs Prozent.

Lässt sich Vertrauen verwalten?

Bei allen Vorteilen, die eine Self-Sovereign Identity mit sich bringt, gibt es auch Herausforderungen. Wie stellt man zum Beispiel sicher, dass die Issuer wirklich vertrauenswürdig sind? Eine Lösung liegt im Aufbau vertrauenswürdiger Verzeichnisse. Hier können sich Issuer – beispielsweise eine Krankenkasse – prüfen lassen und erhalten einen Eintrag, den Verifier und Holder einsehen können. Für Behörden bietet sich ein staatliches Verzeichnis an. So wird Vertrauen quasi verwaltet. Ein anderes Problem liegt im Life-Cycle-Management der Credentials. Wie lassen sie sich in Zukunft rechtssicher aktualisieren? Was geschieht, wenn jemand seine Wallet verloren hat oder ein Credential mit Ablaufdatum versehen worden ist? Auch für diese Anforderungen gilt es, einen Weg zu finden, digitales Vertrauen zu schaffen.

Early Adopters profitieren

Auch wenn es noch offene Fragen gibt: Self-Sovereign Identity wird enorme wirtschaftliche Werte freisetzen. Wer schon jetzt erste Erfahrungen damit sammeln will, kann vorhandene Open-Source-Technologien nutzen. Mit einem gelungenen Proof of Concept erkennen Unternehmen die Möglichkeiten der neuen Technologie und können sie besser abschöpfen. Denn SSI ist viel mehr als ein digitales Portemonnaie: Sie führt den Begriff der Identität in Dimensionen, die sich heute noch nicht erahnen lassen. Wenn wir als Nutzer:innen unsere digitale Identität voll unter Kontrolle haben, verändert das auch unseren Umgang mit Privatsphäre im digitalen Raum. Wir können zwar keine Prinzen, Models oder Milliardenerbinnen mehr sein – aber unsere digitalen Beziehungen und Interaktionen werden eine neue Gestalt annehmen.

Michael Doujak
Product Manager Airlock, Ergon

„Die Frage ist nicht, ob SSI kommt. Sondern wann.

Mehr erfahren über die drei Arten von Digital Identities:

ergon.ch/ssi

Die verborgenen Kosten der Zwei-Faktor Authentifizierung

Aktuell verursachen Zwei-Faktor Authentisierung (2FA) Produkte ein 3-faches der Aufwände der Lizenzkosten für Unternehmen. Firmen brauchen einfache Cybersecurity Produkte, die für sie operativ nicht zu versteckten Kosten führen und für alle ihre unterschiedlichen Kunden einfach und sicher funktionieren. Ein Blick hinter die Authentifizierungs-Kulissen heute und der Zukunft.

Sandra Tobler
CEO & Co-Founder
Futurae Technologies AG

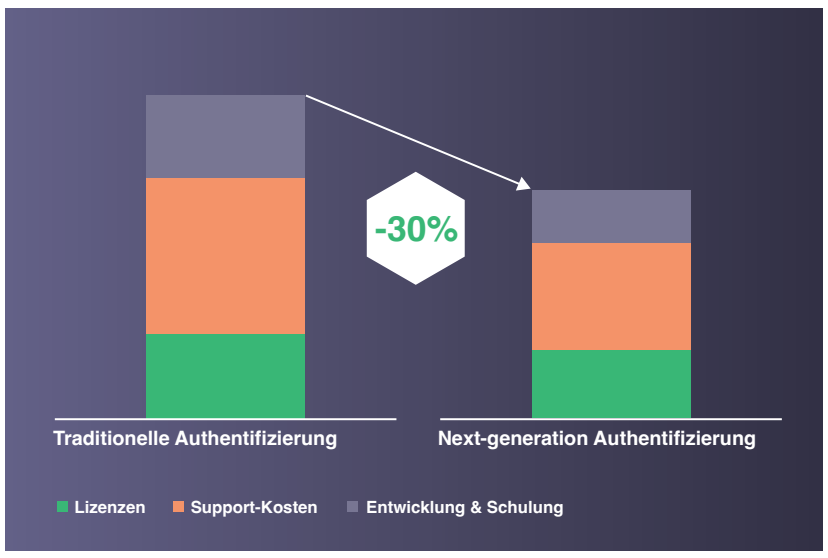
Heutzutage gilt das traditionelle Login auf Online-Dienste, bei dem Benutzername und Passwort, gefolgt von einem zweiten Faktor wie z.B. SMS eingegeben wird, als nicht zuverlässig und unsicher. Die Kosten für herkömmliche Login-Methoden steigen aufgrund der Lizenzverwaltung, Kundensupport-Kosten sowie Wartung und Schulungen laufend an. Immer mehr Menschen nutzen Online-Dienste in allen Bereichen des Lebens, Online-Shopping, Bürgerdienste oder Finanzdienstleistungen. Es ist daher wichtig digital-affinen Menschen als auch konservativen Nutzern mit unterschiedlichen Anforderungen an die Benutzerfreundlichkeit die Möglichkeit zu geben, auf diese Diensten sicher und auf einfache Weise zuzugreifen. Unternehmen müssen diesen steigenden Anforderungen an die Kundenerfahrung gerecht werden und Cybersicherheits-Lösungen wählen, die sicher und benutzerorientiert sind. Daher sollten die Systeme zur Benutzerauthentifizierung vereinheitlicht und für die verschiedenen demografischen, soziografischen Gruppen optimiert werden.

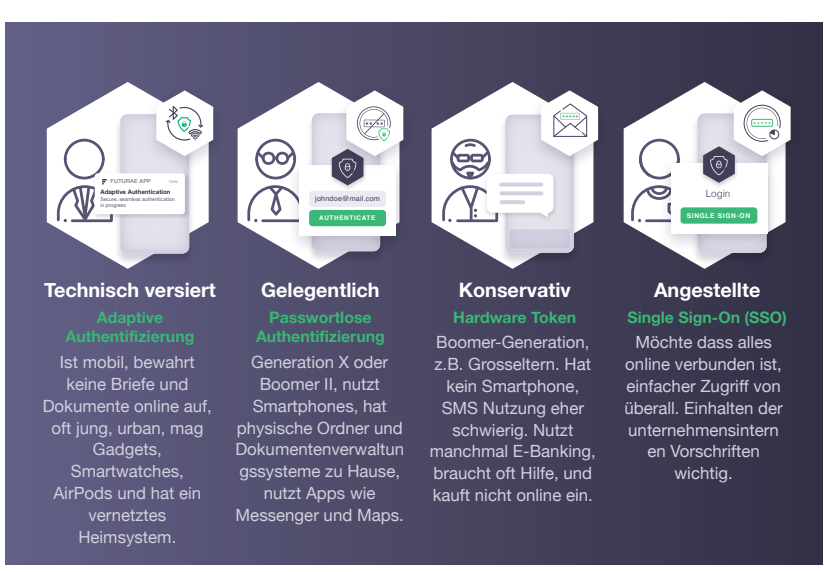
Die Verwendung von Passwörtern für die digitale Authentifizierung ist inzwischen etwa 40 Jahre alt und nicht mehr zeitgemäss. Erhöhte Sicherheit stand schon immer in einem negativen Verhältnis zur Benutzerfreundlichkeit, während die Kunden heute jedoch verlangen, dass das eine das andere nicht ausschliessen sollte.

Die nächste Generation des Logins beginnt jetzt.
Bei der einheitlichen digitalen Authentifizierung geht es darum, die Interaktionen zwischen Kunden und Unternehmen so nahtlos wie möglich zu gestalten. Um dies zu erreichen, wird es in der Zukunft der Authentifizierung keine Passwörter mehr geben, sondern etwas anderes wird diese Rolle übernehmen - dies könnten adaptive Authentifizierungssysteme oder passwortlose Anmeldungen sein. Die nächste Generation von Authentifizierungssystemen ist sicherer und benutzerfreundlicher als herkömmliche Logins. Es wird erwartet, dass solche Systeme auch kostengünstiger für Unternehmen und Verbraucher sind, da sie höhere Sicherheit mit besserer Benutzerfreundlichkeit verbinden.

Die adaptive Authentifizierung ist eine Art des Logins der nächsten Generation, die sich auf eine adaptive Risiko-Maschine stützt, um das mit dem Benutzer verbundene Risiko auf der Grundlage seines Kontexts, wie beispielsweise Profil, Gerät, Standort und Tageszeit, zu bewerten. Anschliessend wird entschieden, ob überhaupt ein Passwort oder eine andere Form der Authentifizierung verlangt werden soll. Immer mehr Unternehmen werden in eine adaptive Authentifizierung investieren, die den Kunden nicht dazu zwingt, sich zu viele Passwörter zu merken. Eine solche Lösung ist besonders für die technisch versierte Benutzergruppe geeignet, da sie die Reibungsverluste vollständig reduziert und gleichzeitig ein Höchstmass an Sicherheit bietet.

Die passwortlose Authentifizierung ist eine andere Art des Logins der nächsten Generation, bei der die Benutzer überhaupt keine Passwörter eingeben müssen. Sie authentisieren sich zum Beispiel mit den biometrischen Merkmalen ihres Smartphones, wie Fingerabdruckscanner oder Gesichtserkennungssoftware. Der Verzicht auf Passwörter löst vor allem die Reibungs- und Sicherheitsprobleme für Gelegenheitsnutzer.





Single Sign-On (SSO) ist eine Funktion, die vor allem bei Unternehmensanwendungen und -diensten zu finden ist und den Zugang zu verschiedenen Plattformen erleichtert, indem die Anmeldedaten eines Benutzers bei einem externen Anmeldedienst (wie Google, Facebook oder einem anderen Dienst) gespeichert werden. Auf diese Weise wird das Passwort beim externen Dienst registriert und nicht bei der App oder dem Dienst, der den digitalen Zugang anfordert. Dies ermöglicht ein transparentes Single Sign-On, das hohe Sicherheit mit hoher Benutzerakzeptanz verbindet. Gerade im Zusammenhang mit der Konsolidierung verschiedener Ökosysteme, die für Finanzdienstleister, aber auch für den Handel immer wichtiger werden, sind diese Funktionalitäten unerlässlich.

Moderne Authentifizierung allein nützt wenig, wenn sie nicht in Verbindung mit einem innovativen Identity- und Access Management (IAM) eingesetzt wird. Die Aufgabe eines IAM ist es, Benutzer und Authentifizierungsmittel zu verwalten, Identitäten zu authentifizieren und die entsprechenden Identitätsinformationen in geeigneter Form an die gewünschte Anwendung zu übermitteln. Glücklicherweise können moderne IAM-Systeme die Authentifizierung für verschiedene Benutzertypen leicht anpassen und integrieren. Mit dem Airlock Secure Access Hub beispielsweise kann die Authentifizierung von Anwendungen entkoppelt werden und so als intelligenter Identitätsschalter fungieren. Ein solches modernes IAM kann den Benutzerzugriff dynamisch auf unterschiedliche Weise steuern und bietet für alle Bedürfnisse die optimale Balance zwischen Sicherheit und Benutzerfreundlichkeit. Dabei können insbesondere die aktuelle Zugriffs-Situation, z.B. von der Arbeit, von zu Hause oder von unterwegs und die Historie eines Benutzers berücksichtigt werden. Logins der nächsten Generation wie adaptive oder passwortlose Authentifizierung und Single Sign-on können nahtlos implementiert werden so dass IAM allen oben genannten Benutzergruppen gerecht wird. Die Identität kann durch die Kombination von IAM mit der Web Application und API-Protection (WAAP) kontinuierlich und zeitabhängig auf das aktuell benötigte Risikoniveau geprüft werden und ermöglicht ein hohes Sicherheitsniveau bei geringstmöglicher Beeinträchtigung des Benutzers. Airlock IAM verwaltet beispielsweise Benutzer, die von aussen auf Anwendungen, APIs und Microservices zugreifen und ist entsprechend für grosse Benutzerzahlen skalierbar. Darüber hinaus bietet die cIAM-Lösung ein nahtloses Benutzererlebnis durch optimierte und integrierte Benutzeroberflächen für Onboarding und Self-Service. Der Umgang mit sozialen Identitäten (BYOI) und eine hohe Flexibilität im Authentifizierungsprozess sind weitere entscheidende Funktionen.

Kosten-Nutzen-Verhältnis von Login der nächsten Generation
Drei Hauptfaktoren sind in der Regel die Treiber für Unternehmen, ihre Cybersicherheitssysteme zu ändern, anzupassen oder aufzurüsten. Diese sind in der Regel 1) Regulierung (wie SCA, GDPR/DSGVO, PSD2 und mehr), 2) Kundenerfahrung durch Verbesserung der Customer Journey und 3) finanzielle Auswirkungen, wenn Kosten durch Betrug, Kundenverlust, Ransomware und andere cyberbezogene Angriffe entstehen. Untersuchungen haben gezeigt, dass die nächste Generation des Logins das Kundenerlebnis und die Sicherheit verbessert und die Authentifizierungslösungen für Unternehmen kostengünstiger macht. So sind herkömmliche Authentifizierungslösungen oft mit steigenden Helpdesk- und Lizenzverwaltungskosten verbunden und erfordern Schulungs- und Entwicklungskosten, um sie kontinuierlich zu verbessern oder an die ständigen Benutzeranforderungen anzupassen. Moderne Authentifizierungslösungen senken die Kosten, indem sie Reibungsverluste beseitigen und die Supportkosten reduzieren. Da sich das Authentifizierungssystem durch maschinelles Lernen und KI selbst verwaltet, werden auch Entwicklungs- und Schulungskosten erheblich reduziert. Der Business Case in der Grafik zeigt die erheblichen Vorteile - Ersparnisse von 30% - eines Wechsels zu modernen Authentifizierungslösungen.

Text **Sandra Tobler, CEO & Co-Founder Futurae Technologies AG**

AIRLOCK®
SECURE ACCESS HUB

Über Airlock
Der Airlock Secure Access Hub vereint die kritischen IT-Sicherheitsaspekte der Filterung und Authentisierung in einer abgestimmten Gesamtlösung, die in Sachen Usability Massstäbe setzt. Er deckt alle Funktionen für Applikations- und API-Sicherheit ab, einschliesslich eines cIAM mit integrierter Zwei-Faktor-Authentisierung.

Jetzt die passende 2FA wählen:
airlock.com/fragebogen

FUTURAE

Über Futurae
Das Schweizer Unternehmen Futurae entwickelt mit ihren Sicherheitsforschern der ETH Zürich eine Authentisierungs-Plattform, die extrem einfach zu implementieren und zu nutzen ist. Futurae ermöglicht es, jede web- und appbasierte Kundeninteraktion einfach und sicher zu authentifizieren. Jeden Monat verlassen sich Millionen von Nutzern von über 100 Banken und anderen Organisationen auf der ganzen Welt auf Futurae, um ihre Logins und Transaktionen zu sichern.

Weiter Informationen:
futurae.com/adaptive-authentication