EINE PUBLIKATION VON SMART MEDIA

FOKUS.

Cybersecurity

Dezember ’24

Marc Ruef

Der Cybersecurity-Experte schaut auf sein Leben zurück und wagt einen Blick in die Zukunft der Technologie.

Weitere Informationen auf Seite 8

Lesen Sie mehr auf
fokus.swiss

Florian Schütz

«Willkommen zu Fokus Cybersecurity»

In der heutigen digitalen Welt ist Cybersicherheit nicht nur ein technisches Thema, sondern eine strategische Notwendigkeit für jedes Unternehmen. Entscheidungsträger stehen vor der Herausforderung, sicherzustellen, dass ihre Organisationen gegen die ständig wachsenden Bedrohungen aus dem Cyberspace gewappnet sind.

Cyberangriffe sind vielfältig und die Vorgehensweise der Cyberkriminellen entwickelt sich ständig weiter. Von Phishing über Ransomware bis hin zu gezielten Angriffen auf kritische Infrastrukturen – die Bedrohungen sind real und allgegenwärtig. Dies bestätigt auch der Meldungseingang beim Bundesamt für Cybersicherheit (BACS), welches die Meldungen zu Cybervorfällen von der Bevölkerung und Unternehmen seit 2020 entgegennimmt und statistisch erfasst:

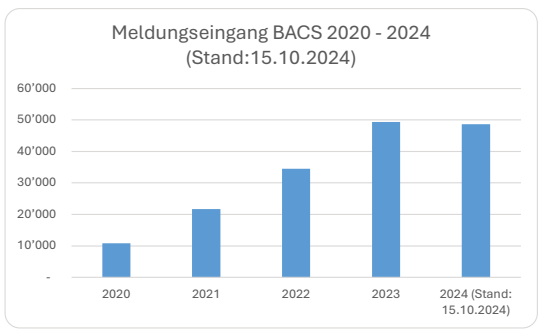


Abbildung 1: Meldungseingang im Bundesamt für Cybersicherheit 2020–2024 (Stand: 15.10.2024)

Die finanziellen Folgen eines Cyberangriffs können verheerende Ausmasse annehmen: Die Produktion steht für mehrere Tage still, Onlineshops können keine Umsätze mehr generieren. Daten wie Baupläne, Rezepturen usw. werden gestohlen und später beispielsweise im Darknet veröffentlicht, die Konkurrenz gelangt so an Betriebsgeheimnisse. Zusätzlich können Reputationsschäden entstehen, und die Kundinnen und Kunden verlieren unter Umständen das Vertrauen in das Unternehmen.

Betreffend Cybersicherheit stellen sich bei Organisationen zwei zentrale Fragen: «Ist mein Unternehmen ausreichend gegen Cyberangriffe geschützt?» und «Ist unsere IT-Abteilung auf dem neuesten Stand?»

Um die erste Frage zu beantworten, müssen verschiedene Aspekte berücksichtigt werden:

Zunächst sollte eine umfassende Risikoanalyse durchgeführt werden. Diese umfasst die Identifizierung und Bewertung potenzieller Bedrohungen sowie die Analyse von Schwachstellen in den Systemen. Dabei werden auch Restrisiken ermittelt, die von der Geschäftsleitung bewusst in Kauf genommen werden müssen.

Ein weiterer wichtiger Punkt sind klare und durchsetzbare Sicherheitsrichtlinien im Unternehmen.

Diese betreffen nicht nur Passwortlängen oder die Zwei-Faktoren-Authentifizierung, sondern auch Vorschriften zur Klassifizierung von Informationen, wie etwa «intern», «vertraulich» oder «geheim», sowie Regeln zum Umgang mit diesen Informationen. Es ist essenziell, diese Richtlinien regelmässig zu überprüfen und an neue Bedrohungen anzupassen.

Darüber hinaus sollte die Schulung und Sensibilisierung der Mitarbeitenden im Vordergrund stehen. Viele Cyberangriffe zielen zunächst auf die Mitarbeitenden ab, indem sie beispielsweise durch manipulierte E-Mails dazu gebracht werden, schädliche Anhänge zu öffnen. Um dem entgegenzuwirken, sind regelmässige Sensibilisierungsmassnahmen notwendig, damit die Mitarbeitenden aller Ebenen über die aktuellen Gefahren informiert und vorbereitet sind.

Auch technische Massnahmen spielen eine zentrale Rolle. Der Einsatz moderner Technologien und Tools zur Abwehr von Cyberangriffen wie z. B. Firewalls und Antivirenprogramme ist unerlässlich. Diese sollten stets auf dem neuesten Stand gehalten werden, ebenso wie alle auf den Geräten installierten Anwendungen und die eingesetzte Hardware. Regelmässige Datensicherungen sind ebenfalls ein wesentlicher Bestandteil der technischen Vorkehrungen, um im Notfall auf verlorene Daten zugreifen zu können.

Organisatorische Massnahmen ergänzen die technischen Vorkehrungen. Dazu gehört das Business Continuity Management (BCM), das sicherstellt, dass die Mitarbeitenden auch dann weiterarbeiten können, wenn die IT zeitweise ausfällt, sei es durch Stromausfälle oder technische Störungen. Das Krisenkommunikationskonzept legt fest, wer im Falle eines Cyberangriffs informiert werden soll, etwa die IT-Abteilung, die Geschäftsleitung, Mitarbeitende oder Kunden, und regelt zudem, wer die Kommunikation übernimmt. Zudem sollten alternative Kommunikationskanäle etabliert werden, falls herkömmliche Kanäle wie E-Mail oder Voice over IP ausfallen.

Ein Incident-Response-Plan schliesslich beschreibt, wie im Fall eines Cyberangriffs vorzugehen ist, um den Schaden zu minimieren und die Ausfallzeit der betroffenen Systeme zu reduzieren.

Bei der zweiten Frage, welche die zentrale Rolle der IT-Abteilung bei der Sicherstellung der Cybersicherheit betrifft, sind folgende Punkte zu berücksichtigen:

Zum einen ist die regelmässige Weiterbildung der IT-Mitarbeitenden von Bedeutung, da sich die Bedrohungslage ständig ändert. Es ist entscheidend, dass das Team auf dem neuesten Stand der Technik und der Best Practices bleibt. Zudem sollte die IT-Abteilung über ausreichende Ressourcen und Budget verfügen, da Cybersicherheit Investitionen in Technologie, Schulungen und Personal erfordert.

Eine effektive Cybersicherheitsstrategie setzt ausserdem eine gute Zusammenarbeit und Kommunikation innerhalb der IT-Abteilung sowie mit anderen Abteilungen voraus. Schliesslich sind proaktive Massnahmen wie regelmässige Sicherheitsüberprüfungen, Penetrationstests und die kontinuierliche Überwachung von Netzwerken und Systemen entscheidend, um Bedrohungen frühzeitig zu erkennen und abzuwehren.

Das Bundesamt für Cybersicherheit (BACS) ist das Kompetenzzentrum des Bundes für Cybersicherheit und damit erste Anlaufstelle für die Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen. Es unterstützt die Privatwirtschaft in verschiedenen Bereichen, insbesondere im Hinblick auf Cybersicherheit.

Das BACS entwickelt und veröffentlicht Sicherheitsrichtlinien und -standards, die Unternehmen bei der Implementierung robuster Sicherheitsmassnahmen unterstützen. Diese Richtlinien basieren auf den neuesten Forschungsergebnissen und internationalen Best Practices. Auf seiner Website (www.ncsc.admin.ch) hat das BACS zahlreiche kostenlose Factsheets und Checklisten veröffentlicht, die Ihnen helfen, Ihre Systeme noch resilienter gegen Cyberangriffe zu machen.

Das BACS fördert den Informationsaustausch und die Zusammenarbeit zwischen Unternehmen und anderen staatlichen Stellen. Durch den Aufbau von Netzwerken und Partnerschaften können Unternehmen von den Erfahrungen und dem Wissen anderer profitieren.

Text **Florian Schütz, Direktor des Bundesamts für Cybersicherheit BACS**

Lesen Sie mehr.

Fokus Cybersecurity.
Projektleitung
Nilujan Rajenthiran
Country Manager
Pascal Buck
Produktionsleitung
Adriana Clemente
Layout
Mathias Manner
Text
Dominik Frey, Heidi Leemann, Linda Carstensen, SMA, Tatiana Almeida, Valeria Cescato
Titelbild
iStockphoto/zmeel
Distributionskanal
Finanz und Wirtschaft
Druckerei
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!

Nilujan Rajenthiran
Project Manager

Gift für die Sicherheit: KI, die mächtige Waffe in den Händen von Cyberkriminellen

Dominik Frey
Co-Founder Swiss AI Experts

Künstliche Intelligenz (KI) revolutioniert nicht nur die Wirtschaft, sondern auch die Welt der Cyberkriminalität. KI eröffnet neue, perfidere und schnellere Angriffsmethoden, um Schweizer KMU ins Visier zu nehmen.

Böses Erwachen: Täuschend echte und blitzschnelle Angriffe

Der erste Tag im neuen Job. Marc ist stolz. Kurz vor Feierabend erreicht ihn eine E-Mail mit Absender des IT-Supports: Willkommen im Team, Marc! Dein Firmenaccount ist eingerichtet. Bitte logge dich mit deinem Passwort ein. Ein Link zum Firmen-Intranet ist beigefügt. Marc klickt, gibt sein Passwort ein. Nichts scheint verdächtig. Doch das böse Erwachen lässt nicht lange auf sich warten. Das Unternehmen ist gehackt, der finanzielle Schaden erheblich.

Wie kann ein solcher Angriff zeitnah und überzeugend durchgeführt werden? Es ist simpel: Marc kündigt seinen Jobantritt auf einer Business-Social-Media-Plattform an. Keine gute Idee, denn Hacker:innen nutzen solche scheinbar harmlosen Informationen, um gezielt Personen anzugreifen. Eine Mail-Adresse ist rasch abgeleitet, der Rest mit KI ein Kinderspiel.

Solche Angriffsszenarien waren bislang über einfache Webcrawler oder manuelles Suchen und Abgleichen möglich. Heute geht das vollautomatisiert, hochpräzise und in grossen Massen. Dank KI.

Warum KMUs besonders gefährdet sind

Durch Cybercrime-Trainings aufgeklärt, wähnen wir uns vermeintlich in Sicherheit. Doch die meisten von uns sind kaum darauf vorbereitet, wie KI die Cybercrime-Risiken potenziert und unser Verhalten überlistet. Schweizer KMU sind besonders gefährdet, da ihre Ressourcen oft begrenzt sind und KI-Know-how fehlt. Heute gilt: Wer nicht versteht, was KI kann und wie mächtig KI in den Händen Krimineller ist, ist in Sachen Cyberkriminalität schlecht aufgestellt.

KI-getriebener Cybercrime

Deepfakes: Realistische Fälschungen von Bildern, Videos und Audioaufnahmen können für Betrug oder Erpressung missbraucht werden.

«Echtzeit»-Phishing: KI analysiert das Verhalten von Nutzer:innen nahezu in Echtzeit und generiert innerhalb kürzester Zeit personalisierte Phishing-Nachrichten, die perfekt auf die jeweilige Situation zugeschnitten sind und von echten E-Mails kaum zu unterscheiden sind.

Social Engineering: Unser Verhalten wird mit gefälschten Webseiten und Social-Media-Profilen ausspioniert und manipuliert, um an sensible Daten zu gelangen.

Schadsoftware: KI kann komplexe Codes erstellen, die Sicherheitslücken ausnutzen und herkömmliche Antivirensoftware umgehen. Programmierkenntnisse sind dafür nicht mehr nötig.

Sicherheitslücken nutzen: KI kann Schwachstellen in Systemen schneller identifizieren und ausnutzen als je zuvor.

Was KMU jetzt tun müssen

KMU müssen verstehen, dass herkömmliche Cybersicherheitskonzepte nicht mehr greifen, denn die Angriffsmethoden entwickeln sich durch KI rasant weiter. Betroffen sind wir alle, denn der Mensch ist oft die Schwachstelle, wie auch Marcs wahre Geschichte eingangs zeigt.

KI-Schulung als Schlüssel zum Erfolg

KI-Awareness: Mitarbeitende über die Möglichkeiten von KI-Technologien aufklären, damit sie Angriffe besser erkennen können.

KI-Kompetenz aufbauen: Mitarbeitende in KI-Technologien und im sicheren Umgang mit Tools schulen. So können KMU die Vorteile von KI nutzen und gleichzeitig die Risiken minimieren.

Text **Dominik Frey, Heidi Leemann, Co-Founder Swiss AI Experts**

Ein Schutzschild, der die Cyberresilienz stärkt

Florian Badertscher
Co-Founder & CTO Bug Bounty Switzerland AG

Cyberresilienz entsteht dann, wenn man die Schwachstellen eines Systems findet und schliesst. Genau das tut Bug Bounty Switzerland für seine Kunden seit jeher – und setzt dafür auf die Mithilfe sogenannter «ethischer Hacker:innen». Nun hat man mit dem «Cyber Resilience Shield» ein brandneues Produkt lanciert, das diesen innovativen Sicherheitsansatz gezielt weiterentwickelt.

Herr Badertscher, das Unternehmen Bug Bounty Switzerland spielt in der Schweiz eine Pionierrolle hinsichtlich der Zusammenarbeit mit ethischen Hackerinnen und Hackern. Was muss man sich darunter vorstellen?
«Ethical Hacking» ist die Zusammenarbeit mit Hackerinnen, die ihre Fähigkeiten für gute Zwecke einsetzen. Ohne diese Zusammenarbeit ist es Unternehmen heute praktisch unmöglich, alle Schwachstellen in ihren Systemen zu finden. So ist beispielsweise ethisches Hacking eine Massnahme der Nationalen Cyberstrategie (NCS). Und trotzdem verzichten noch immer viele Unternehmen auf den Einsatz von sogenannten Bug-Bounty-Programmen – sei es, weil sie die Kooperation mit ethischen Hackern scheuen, wegen der Komplexität oder der schwierig zu planenden Kosten. Wir haben die Nutzung von Ethical Hacking über die Jahre perfektioniert und dabei gelernt, wie Bug-Bounty-Programme am effektivsten betrieben werden. Auf Basis dieses Know-hows haben wir ein innovatives Produkt entwickelt, das Ethical Hacking unter Nutzung der Daten aus bisherigen und laufenden Bug-Bounty-Programmen und mithilfe moderner KI-Technologie optimiert, der «Cyber Resilience Shield».

Wie darf man sich den «Cyber Resilience Shield» vorstellen?
Der «Cyber Resilience Shield» ist eine leistungsstarke, datengestützte, einfach zugängliche und skalierbare Lösung für die Steigerung der Widerstandskräfte von Unternehmen in der digitalen Welt. Der «Cyber Resilience Shield» schützt Unternehmen vor Cyberangriffen, indem er kritische Angriffspunkte identifiziert und vor deren Ausnutzung schliesst. Das System sorgt für kontinuierliche, gezielte Sicherheitstests, die sich auf die Schwachstellen mit dem grössten Bedrohungspotenzial konzentrieren. Durch eine schnelle Priorisierung identifizierter Problembereiche und klare Handlungsempfehlungen können Sicherheitslücken effizient adressiert werden – auch ausserhalb der betroffenen Organisation. Der «Cyber Resilience Shield» mobilisiert alle zur raschen Behebung benötigten Parteien.

Und wie funktioniert das? Wie stellen Sie sicher, dass der Schutzschild keine Lücken aufweist?
Die dem «Cyber Resilience Shield» zugrunde liegende Methodik basiert auf einem vierstufigen Ansatz des «Continuous Threat Exposure Managements», der auf ethisches Hacking abgestimmt wurde:

1 Identifikation und Überwachung der gesamten Angriffsfläche des Unternehmens, inklusive Brands, Cloud-Ressourcen, usw.

2 Aktivierung des adaptiven Schutzmechanismus, der gezielt die identifizierten Bedrohungen und Risiken adressiert. Dazu orchestriert der «Cyber Resilience Shield» auf smarte Weise laufend den Einsatz der ethischen Hackerinnen und Hacker.

3 Identifizierung und Priorisierung von Handlungsempfehlungen basierend auf ihrem tatsächlichen Bedrohungspotenzial. Zur Behebung der identifizierten Schwachstellen arbeitet Bug Bounty Switzerland bei Bedarf auch direkt mit involvierten Drittparteien und Behörden zusammen.

4 Transparente Berichterstattung und Benchmarking mit dem Cyber Resilience Score.

> «Unsere Kernkompetenz besteht seit jeher darin, die IT-Systeme unserer Kunden sicherer und die Organisationen selber resilienter gegenüber Cyberbedrohungen zu machen.
>
> – Florian Badertscher, CTO Bug Bounty Switzerland AG

Worum handelt es sich beim Cyber Resilience Score?
Der Cyber Resilience Score ermöglicht die Bewertung der Cyberresilienz einer Organisation und vereint verschiedene Dimensionen der präventiven Cybersicherheit in einem Wert. Dadurch erhalten Unternehmen einen klaren Überblick über die eigenen Fähigkeiten im Umgang mit Schwachstellen im Vergleich zu anderen Akteuren in der jeweiligen Branche. Der Cyber Resilience Score erlaubt ihnen, ihre Fortschritte nachzuverfolgen und jene Bereiche zu identifizieren, wo der grösste Handlungsbedarf besteht. Der Cyber Resilience Shield liefert Unternehmen aber nicht nur Daten, sondern auch detaillierte Berichte. Diese bieten insbesondere dem Management, Führungskräften und Verwaltungsräten wichtige Erkenntnisse, um die Cyberrisiken ihres Unternehmens besser zu verstehen und dessen Resilienz zu verbessern.

Was benötigen Organisationen, um diesen Schutzschild für sich einsetzen zu können?
Praktisch nichts – dank einem transparenten Preismodell und ohne die Notwendigkeit zusätzlicher Sicherheitsressourcen oder eigener Expertise, bietet der «Cyber Resilience Shield» umfassenden Schutz per Knopfdruck, der sich an die spezifischen Bedürfnisse jeder Organisation anpasst. Er ermöglicht einen schnellen Einstieg in eine kontinuierliche Verbesserung der Cybersicherheit und bietet gleichzeitig klare, umsetzbare Einblicke für die Geschäftsführung.

Informationen und Demo unter:
cyberresilienceshield.com

Über Bug Bounty Switzerland
Ethisches Hacking ist eine wichtige Massnahme der Nationalen Cyberstrategie (NCS). Bug Bounty Switzerland AG bietet Organisationen mit einer innovativen Lösung einfachen und sicheren Zugang zu Ethical Hacking und datengestützten Bug-Bounty-Programmen. Mit dem «Cyber Resilience Shield», einem virtuellen Schutzschild, der in kürzester Zeit auf Knopfdruck aktiviert werden kann und mithilfe von KI auf Basis laufend aktualisierter Daten den Einsatz ethischer Hacker:innen orchestriert, bietet das Unternehmen eine smarte Lösung zur Steigerung der Cyberresilienz von Organisationen. Bug Bounty Switzerland hat Zugriff auf über 15 000 ethische Hacker:innen und beschäftigt 20 Mitarbeitende an den Standorten Zürich, Luzern und Bern. Zu den Kunden zählen über 100 führende Organisationen aus dem In- und Ausland. Together for a resilient world.

bugbounty.ch

Cyber Resilience Shield

«Wir spielen in der Königsklasse der Komplexität»

Das Etablieren von Cyberresilienz ist für Organisationen aller Branchen und Grössen essenziell. Doch gerade im hochregulierten Finanzsektor liegt die Messlatte nochmals deutlich höher. at rete AG hilft den Akteuren dieses Sektors dabei, in Sachen Cybersecurity immer einen Schritt voraus zu sein. Davon profitieren auch Firmen anderer Branchen.

Christoph Pfister
Head of Cyber Security at rete AG

Herr Pfister, atrete erbringt unter anderem Beratungen und Dienstleistungen im Feld der Cybersecurity. Hier sind Sie insbesondere im Feld der Finanzdienstleister tätig. Welche Herausforderungen stellen sich für diese Branche?
Grundsätzlich sind alle Organisationen, die Daten verarbeiten, mit wichtigen Fragestellungen konfrontiert. Doch im Finanzmarkt sind die Anforderungen an die Sicherheit der Daten aufgrund ihrer sensiblen Natur besonders hoch. Organisationen in diesem Segment sind stark reguliert und müssen klare Vorgaben erfüllen. Das Einhalten von Cybersecurity-Aspekten ist daher ein absolutes Muss, was, anders als in vielen anderen Sektoren, auch strengstens kontrolliert wird. Wir verfügen in dieser Branche über eine breite Erfahrung und sind daher mit den besonderen Ansprüchen des Finanzwesens vertraut. Unsere Expertise, etwa im Feld von Regulatory Compliance oder Cloud-Security, zeichnet uns ebenso aus wie die Fähigkeit, Kenntnisse von branchenspezifischen Bedürfnissen mit technischem Know-how zu kombinieren. Natürlich machen unsere Consultants dieses Know-how auch anderen Kunden und Branchen zugänglich. In sämtlichen Fällen achten wir auf einen pragmatischen Hands-on-Approach.

Warum ist ein solcher Ansatz so wichtig?
Echte Cybersecurity entsteht nur dann, wenn man die Mitarbeitenden einer Organisation mit an Bord holen kann. Dafür ist es unerlässlich, alle Hierarchiestufen zu erreichen, von den IT-Spezialisten bis zum Verwaltungsrat. Genau darin liegt unsere Stärke und dadurch sind wir in der Lage, erfolgreiche Projekte für finanzmarkt-regulierte Institute wie Banken und Versicherungen zu realisieren. Dieses Segment ist die «Königsklasse der Komplexität», was anderen Kunden, etwa im Gesundheitswesen, der Industrie oder der öffentlichen Verwaltung, ebenfalls zugutekommt.

> «Echte Cybersecurity entsteht nur dann, wenn man die Mitarbeitenden einer Organisation mit an Bord holen kann. Dafür ist es unerlässlich, alle Hierarchiestufen zu erreichen, von den IT-Spezialisten bis zum Verwaltungsrat.
>
> – Christoph Pfister, Head of Cyber Security at rete AG

Welche technologischen Aspekte bestimmen die aktuelle Sicherheitsdebatte?
Cloud-Security, Identitätsmanagement und Netzwerksicherheit sind hier absolut wesentlich. Gleichzeitig ist gerade die Cloud auch für die Digitalisierung zentral und stellt zudem einen wesentlichen Faktor in der Kostenstruktur eines Unternehmens dar, weil sie enorme Einsparungen eröffnen kann. Da die Cloudnutzung aber stets auch mit einer externen Datenbearbeitung einhergeht, muss nebst den Governance-, Cybersecurity- und Compliance-Anforderungen vor allem der Netzwerksicherheit oberste Priorität zukommen. Konkret kann dies bedeuten, dass das System etwa in der Lage sein muss, im Falle eines Cyberangriffs gewisse Segmente abzutrennen. Eine solche Zonierung und Segmentierung ist für Finanzdienstleister und ihre Outsourcingpartner sogar regulatorisch vorgeschrieben. Und in Zeiten von Cloud und Homeoffice und Co. wird die Sicherheit des Netzwerkes ohnehin immer kritischer.

Kann KI bereits geschulte Security-Fachpersonen ersetzen?
Angreifer können durch KI tatsächlich ausgefeiltere Szenarien erstellen, etwa mit Sprach- und Bildimitation. Aufseiten der Verteidigung wiederum kann KI dazu beitragen, Anomalien und Muster zu erkennen und damit die initiale Response auf Attacken zu beschleunigen sowie kritische Prozesse zu automatisieren, damit die Cybersecurity-Spezialisten für andere wichtige Tätigkeiten zur Verfügung stehen. Wichtig für Unternehmen ist zudem, KI auch aus Datenschutz- und Cybersecurity-Sicht konform zu nutzen. Menschliche Kompetenzen bleiben aber unersetzbar.

KI wird oft im Zusammenhang mit der Digitalisierung genannt. Wie gelingt die digitale Transformation?
KI kann für verschiedene Anwendungsfälle im Rahmen der Digitalisierung nützlich sein, zum Beispiel um manuelle Prozesse zu automatisieren, um Kundendaten zu analysieren und entsprechend personalisierte Angebote zu erstellen, oder auch in der Betrugsprävention und -erkennung. Um Effizienzgewinne und Kostensenkungen zu erzielen, müssen Organisationen klare Ziele formulieren und präzise Anforderungen definieren, was mit dem Einsatz von KI erreicht werden soll. Ferner benötigen sie die notwendigen Strukturen und müssen über eine durchgängige Informationsarchitektur verfügen. Oftmals sehen wir allerdings, dass die technischen Infrastrukturen historisch gewachsen sind. Diesem Umstand muss man ebenso Rechnung tragen wie der Tatsache, dass es in vielen Organisationen noch an durchgängigen Datenmodellen mangelt, die als ausreichende Grundlage für eine Digitalisierung bzw. Automation dienen könnten. Um hier die Interoperabilität zu fördern, setzt atrete auf Erfahrung, technologische Expertise sowie zwischenmenschliche Kompetenz – denn jede Digitalisierung bedeutet auch Change-Management und dafür ist es essenziell, die Betroffenen zu Beteiligten zu machen und sie auf die Reise mitzunehmen.

Wie wichtig ist in diesem Zusammenhang Ihr Angebot «CISO as a Service»?
Das Angebot kann eine zentrale Rolle spielen: Wenn etwa der Chief Information Security Officer (CISO) die Organisation verlässt, ist es oftmals entscheidend, kurzfristig jemanden hinzuzuziehen, der diese Aufgaben übernimmt. Mit unserem Angebot decken wir das ab: Unsere Experten springen sozusagen nahtlos in die Bresche und führen die Aufgaben des CISOs weiter, bis intern oder extern eine Nachfolge gefunden wurde. Alternativ ist «CISO as a Service» auch ideal, wenn eine Unternehmung zu klein ist, um einen eigenen CISO zu stellen oder sich die Kandidatensuche schwierig gestaltet. Gerade für Fondsleitungen oder Verwaltungen von Kollektivanlagen, die erst seit Kurzem im Bereich Cybersecurity und Cyberresilienz so streng reguliert sind, ist der Outsourcing-Service absolut optimal geeignet.

Weitere Informationen unter:
www.atrete.ch

atrete
IT consultants

Bild iStockphoto/BlackJack3D

KI in der Cyberwelt

In einer Welt, die zunehmend von digitalen Innovationen geprägt ist, eröffnet der technologische Fortschritt Unternehmen neue Horizonte. Mit der richtigen KI-Strategie können Unternehmen nicht nur ihre Effizienz steigern, sondern sich auch besser gegen die wachsenden Bedrohungen im Cyberraum wappnen.

Der digitale Wandel schreitet stetig voran und mit ihm die unzähligen Möglichkeiten, die sich für Unternehmen ergeben. Mit einer effizienten Implementierung von künstlicher Intelligenz (KI) lassen sich beispielsweise interne Prozesse vereinfachen und die Marktfähigkeit steigern. Durch den gezielten Einsatz von KI können Unternehmen ihre Sicherheitsstrategien deutlich verbessern und Bedrohungen schneller und effektiver erkennen und neutralisieren. Gleichzeitig ist es notwendig, die KI mit menschlicher Expertise zu kombinieren, um sicherzustellen, dass die Technologie nicht nur effizient, sondern auch flexibel genug ist, um auf neue und immer raffiniertere Bedrohungen zu reagieren. Es gibt diverse Wege, wie ein Unternehmen von KI in der Welt der Cybersicherheit profitieren kann:

– **Proaktive Bedrohungsanalyse:** KI ist nicht nur darauf ausgelegt, Bedrohungen zu erkennen, die bereits in das System eingedrungen sind, sondern auch, um potenzielle Risiken und Schwachstellen vorherzusagen. KI kann zukünftige Bedrohungen erkennen, indem sie aus früheren Angriffen und Mustern lernt. Dies ermöglicht Unternehmen, ihre Sicherheitsstrategien zu verbessern und sich gegen Bedrohungen abzusichern, bevor diese auftreten.

– **Erkennung von Bedrohungen:** KI-Systeme können in Echtzeit grosse Datenmengen durchstöbern und potenzielle Bedrohungen wie Hackerangriffe oder Malware-Attacken erkennen. Zudem sind sie in der Lage, gewisse Muster und Anomalien zu identifizieren, die auf Cyberangriffe hindeuten könnten. KI kann ständig lernen und ihre Erkennungsfähigkeiten verbessern, was zu einer genaueren Identifizierung von Bedrohungen führt. Dadurch können Unternehmen Bedrohungen frühzeitig erkennen und proaktive Massnahmen ergreifen, bevor ein Angriff grossen Schaden anrichten kann.

> **Durch den gezielten Einsatz von KI können Unternehmen ihre Sicherheitsstrategien deutlich verbessern und Bedrohungen schneller und effektiver erkennen und neutralisieren.**

– **Schnelligkeit und Skalierbarkeit:** KI-gestützte Sicherheitssysteme arbeiten mit aussergewöhnlicher Geschwindigkeit, indem sie Daten in Echtzeit analysieren und sofort auf Bedrohungen reagieren können. Dies ist besonders wichtig, da Cyberangriffe in der Regel sehr schnell und gezielt passieren. Die Geschwindigkeit, mit der KI Bedrohungen identifiziert und darauf reagiert, verringert das Risiko von Schäden. Zudem ist KI skalierbar, was bedeutet, dass sie mit dem Wachstum des Unternehmens und einer steigenden Menge an Daten und Nutzer:innen mithalten kann, ohne dass mehr manuelle Arbeit nötig ist.

– **Reduzierung von Fehlalarmen:** KI kann helfen, Fehlalarme zu reduzieren, die in traditionellen Sicherheitssystemen oftmals ein Problem darstellen. Durch maschinelles Lernen wird die KI trainiert, zwischen harmlosen und potenziell schädlichen Aktivitäten zu unterscheiden. Dadurch wird die Anzahl der Fehlalarme minimiert, die zu unnötigen Reaktionen und einer Verschwendung von Ressourcen führen können.

Expertise durch Menschen

Obwohl KI in der Lage ist, Bedrohungen schnell zu erkennen und darauf zu reagieren, benötigen diese Systeme die Unterstützung von Fachleuten, um ihre volle Wirksamkeit zu entfalten. Expert:innen helfen dabei, KI-Modelle mit relevanten Daten zu trainieren, sodass sie nicht nur bekannte Bedrohungen, sondern auch neue, unbekannte Risiken erkennen können. Zudem überwachen sie die Leistungen der Systeme, um sicherzustellen, dass die KI korrekt arbeitet und gegebenenfalls erforderliche Anpassungen vorgenommen werden. In komplexen oder aussergewöhnlichen Situationen, in denen die KI allein nicht ausreicht, um die richtige Entscheidung zu treffen, kommt das Fachwissen von Menschen zum Einsatz. Nur durch die enge Zusammenarbeit von KI und Fachpersonal können Unternehmen sicherstellen, dass ihre Sicherheitslösungen stets auf dem neuesten Stand bleiben und Bedrohungen effektiv abgewehrt werden.

Wo Chancen sind, lauern auch Risiken

Während KI in der Cybersicherheit potenziell enorme Vorteile bietet, indem sie Sicherheitslücken schneller erkennt und Angriffe effizient abwehrt, gibt es eine Reihe von Risiken, die mit ihrer Nutzung verbunden sind. Ein zentrales Problem ist der Missbrauch durch Angreifende: Cyberkriminelle könnten KI für die Automatisierung von Angriffen wie Phishing oder das Umgehen von Sicherheitsmechanismen einsetzen. Besonders bedrohlich sind sogenannte «Adversarial Attacks», bei denen Angreifer:innen die Eingabedaten so manipulieren, dass KI-Systeme falsche Entscheidungen treffen und Bedrohungen unentdeckt bleiben. Ein weiteres Risiko ergibt sich aus der Verzerrung (Bias) in den Trainingsdaten: Wenn KI-Modelle mit fehlerhaften oder unvollständigen Daten trainiert werden, kann dies zu falschen Sicherheitsanalysen führen, wodurch reale Bedrohungen übersehen oder falsch bewertet werden. Hinzu kommt die Gefahr einer Abhängigkeit von KI-Systemen: Wenn Unternehmen sich zu sehr auf KI stützen, könnte ein Ausfall des Systems die gesamte Sicherheitsinfrastruktur gefährden. Letztendlich gibt es auch rechtliche und ethische Unsicherheiten. Die rasante Entwicklung der KI geht oft schneller als die Gesetzgebung, was zu Unsicherheiten hinsichtlich der Verantwortung und der sicheren Nutzung dieser Technologie führt.

Es ist daher wichtig, KI-Technologien in der Cybersicherheit mit Bedacht und unter Berücksichtigung der möglichen Gefahren zu integrieren.

Text **Tatiana Almeida**

Für IT-Lösungen, die wirklich perfekt passen

Seit über 20 Jahren ist die Netsafe AG eine bewährte Partnerin für IT-Komplettlösungen. Von Tag eins an legte man auch höchsten Wert auf das Thema «Sicherheit». Dank dieser weitreichenden Erfahrung sowie des umfassenden Know-hows bietet man heute Unternehmen aller Grössen und Branchen massgeschneiderte Lösungen an – inklusive individueller KIs.

Mathias Ebneter
Geschäftsführer Netsafe AG

Herr Ebneter, die Netsafe AG ist seit mehr als zwei Jahrzehnten in der IT tätig. Wie beurteilen Sie vor diesem Hintergrund die aktuelle Lage hinsichtlich Cybersicherheit?
Man kann sicherlich festhalten, dass dem Feld der Cybersecurity heute eine enorme Relevanz beigemessen wird und Unternehmen aller Branchen und Grössen sich mit der Thematik auseinandersetzen müssen. Die Cybersecurtiy gehört also auf jede Agenda der höchsten Führungsebene – leider stellen wir fest, dass dies in vielen Firmen noch nicht ganz angekommen ist! Wir von der Netsafe AG vertreten ferner die Ansicht, dass man die IT-Security als Ganzes betrachten und fördern muss. Denn nur, wenn man die eigenen IT-Systeme umfassend resilient macht, ist man auch gegen Attacken aus dem Web gewappnet. Wir unterstützen Kundenfirmen zu diesem Zweck in unseren Kernfeldern Infrastruktur, Network, Storage/Back-up sowie Cloud-Services.

Welche Dienstleistungen erbringt die Netsafe AG spezifisch im Bereich der Cybersecurity?
Hier sind wir ebenfalls umfassend und breit aufgestellt: Wir stellen unseren Kunden ein Team aus zertifizierten Fachleuten zur Seite, das bewährte Dienstleistungen wie Penetrationstests und Audits durchführt sowie Sicherheitskonzepte erarbeitet und Risikomanagement anbietet. Auf diese Weise erkennen und beheben wir potenzielle Schwachstellen in IT-Infrastrukturen. Bei all diesen technischen Aspekten dürfen wir aber nicht den menschlichen Faktor vergessen, der für die Sicherheit ebenfalls absolut zentral ist.

> «Die Cybersecurtiy gehört auf jede Agenda der höchsten Führungsebene.
>
> – Mathias Ebneter, Geschäftsführer Netsafe AG

Inwiefern kommt denn der menschliche Faktor bei der Cybersicherheit zum Tragen?
Die raffiniertesten Security-Anwendungen können ihre Wirkung nicht entfalten, wenn die Userinnen und User kein sicheres Verhalten an den Tag legen und sich der heutigen Risiken nicht bewusst sind. Daher bieten wir von der Netsafe AG massgeschneiderte Schulungen an, bei denen wir das Personal von Organisationen zu den neuesten Sicherheitstechniken schulen. Auf diese Weise stellen wir sicher, dass die Mitarbeitenden die gängigen Gefahrenpotenziale kennen, umsichtig agieren und die Systeme aktiv auf dem neusten Stand halten. Zudem lernen sie, dass man im Falle eines Sicherheitsvorfalls schnell und gezielt informieren muss, um den Schaden möglichst in Grenzen zu halten. Unsere Schulungen entfalten im Zusammenspiel mit IT-Systemen, die den aktuellen Sicherheitsanforderungen entsprechen, ihre volle Wirkung. Ferner unterstützen wir Unternehmen auch auf der technischen und organisatorischen Ebene, da gehört unter anderem das Aufsetzen von Verträgen mit externen Dienstleistern dazu. Und natürlich stehen wir unseren Kunden auch zum Thema KI zur Seite.

Um welche Aspekte von künstlicher Intelligenz geht es dabei primär?
Zum einen wird KI künftig völlig neue Bedrohungsszenarien eröffnen. Doch bereits jetzt stehen viele Firmen vor einem anderen, oftmals unbewussten Problem: Wenn sie die Potenziale von KI nutzen möchten, müssen sie die künstliche Intelligenz zwangsläufig mit Geschäftsdaten «füttern». Doch dabei stellen sich viele sicherheitsrelevante sowie potenzielle rechtliche Fragen. Hier können wir als Audit-Anbieter Firmen überprüfen und ihnen nützliche Leitplanken geben. Auch in diesem Zusammenhang spielen Mitarbeiterschulungen eine wichtige Rolle, da sie in einem Betrieb Wissen darüber schaffen, was im Umgang mit KI erlaubt ist und was nicht. Ferner bieten wir Unternehmen auch die Möglichkeit, ihre individuelle KI-Anwendung zu erhalten.

Sie biete sozusagen massgeschneiderte KIs an?
Ja. Wir tun dies, indem wir ein Large Language Model (LLM) mit den entsprechenden Daten antrainieren und für die Bedürfnisse und Anwendungszwecke des jeweiligen Kundenbetriebs ausrüsten. Das kann zum Beispiel für die Gesundheitsbranche spannend sein, etwa für den Einsatz in Spitälern. Letztlich kann dieses LLM aber in jeder Branche sinnvoll eingesetzt werden. Die firmeneigene KI bieten wir zudem auf Wunsch «as a Service» an, wobei die Daten sicher in unserem Datacenter verwahrt bleiben. Wie bei all unseren Produkten und Dienstleistungen klären wir gerne im Rahmen eines persönlichen Gesprächs, wie wir die optimale, individuelle Lösung für die jeweilige Firma finden können.

Weitere Informationen unter:
netsafe.ch

Über die Netsafe AG
Das in St. Gallen beheimatete Unternehmen ist seit mehr als 20 Jahren im Feld der IT-Dienstleistungen tätig und versteht sich seit Tag eins als Partner: einer, der seine Kundschaft ganz genau kennt, zuhört und weiss, was ein Unternehmen in seinem individuellen Fall benötigt. Netsafe behandelt die Kunden-IT mit viel Sorgfalt, kümmert sich vollumfänglich um sämtliche Aspekte der Datensicherheit und setzt sich dafür ein, dass Prozesse optimal ablaufen.

Eine modulare Softwarelösung für Unternehmen

ioServices ist eine Swiss-Made-Lösung, die von der Firma ioWare entwickelt wurde und aus zwei Modulen besteht. Mit ihren einfachen und intuitiven Funktionen unterstützt sie Unternehmen sowohl bei der Projektverwaltung als auch bei der Arbeitszeiterfassung durch eine Zeiterfassungsuhr.

In einer sich stetig verändernden Wirtschaftswelt wird eine effiziente Verwaltung von Projekten und Humanressourcen zu einer zentralen Herausforderung, insbesondere für kleine und mittlere Unternehmen. Die Koordination von Teams, die Einhaltung von Fristen und die Kostenoptimierung erfordern angepasste Werkzeuge, die den spezifischen Anforderungen jeder Organisation gerecht werden. In diesem Kontext zeichnet sich ioServices als vielseitige und anpassungsfähige Lösung aus, die sich an unterschiedliche Unternehmensstrukturen und Mitarbeiterzahlen anpasst.

> «Neben der Leistungsverwaltung unterstützt die Software die Mitarbeitenden auch nach der Projektinitiierung.

Ursprünglich von ioWare entwickelt, um den eigenen Bedarf an Mandatsverwaltung zu decken, erkannte das Unternehmen schnell die steigende Nachfrage nach umfassenden, flexiblen und mobilen Tools. Das erste Modul bietet eine Vielzahl von Funktionen, darunter die Verwaltung einer unbegrenzten Anzahl von Leistungen. Es ermöglicht eine vollständige Flexibilität, indem Preisstrukturen definiert werden können, die von Kunden, Mandaten, Leistungen und Mitarbeitenden abhängen. Neben der Leistungsverwaltung unterstützt die Software die Mitarbeitenden auch nach der Projektinitiierung. Mit Funktionen wie der Festlegung eines maximalen Budgets, der Erstellung von Aufgabenlisten sowie Alarmen und Erinnerungen gewährleistet das Verwaltungstool eine vollständige Kontrolle über Projekte – von der Planung bis hin zur intuitiven und schnellen Rechnungsstellung.

Was ist mit mobilen Mitarbeitenden, die mehr im Aussendienst als im Büro tätig sind? Auch für sie ist die Lösung geeignet, da die Mandatsverwaltung von ioServices über das Smartphone verfügbar ist.

Im Sinne einer weiteren Vereinfachung für Unternehmen hat ioWare ein ergänzendes Modul entwickelt, das ebenfalls über das Smartphone zugänglich ist: die Zeiterfassung. Dieses Modul kann entweder als Ergänzung zur Mandatsverwaltung oder eigenständig genutzt werden, sei es für einzelne oder mehrere Mitarbeitende. Es überzeugt durch Präzision und Benutzerfreundlichkeit. Neben der Zeitersparnis für die Teams insgesamt erleichtert es die Verwaltung und Kontrolle der erfassten Arbeitszeiten. Insbesondere für Mitarbeitende mit flexiblen oder eingeschränkten Arbeitszeiten bietet es grosse Vorteile, da es auch die Verwaltung von Abwesenheiten, Urlaub und gesetzlich vorgeschriebenen Pausen ermöglicht.

Mit seinen Modulen und der gebotenen Flexibilität positioniert sich ioServices als unverzichtbares Werkzeug zur Optimierung der Mandatsverwaltung und Steigerung der Produktivität. Die sichere Ausgestaltung der Software schafft zudem Vertrauen. Von der Nutzung per Smartphone oder Computer bis hin zur Integration eines biometrischen Erkennungssystems wird die Installation an die Bedürfnisse des Unternehmens angepasst. ioServices ist die einfache, effektive und präzise Lösung für eine optimierte Unternehmensverwaltung.

Weitere Informationen unter:
ioware.ch

Was tun als KMU, wenn die Attacken immer perfider werden?

Mit der sogenannten «Adversary in the Middle»-Attacke gehen Cyberkriminelle besonders perfid vor und ergaunern sich den Account-Zugriff trotz Multi-Faktor-Authentifizierung. Wie soll man sich dagegen schützen?

Aladin Steiner
Head of Azure und Verantwortlicher für das SmartIT-SOC

Die Angriffsmethode «Adversary in the Middle» oder kurz AITM-Attacke ist eher neu. Dennoch hat sie sich unter Cyberkriminellen rasend schnell verbreitet und gehört heute bei Phishingangriffen auf Microsoft-Dienste fast schon zum Standard.

Neben dem Passwort und der E-Mail-Adresse entwenden die Angreifenden bei dieser Methode auch das sogenannte Session Cookie. Also die Information im Browser, in welcher die Multi-Faktor-Information gespeichert ist. Gelingt die Attacke, erhält die angreifende Person vollen Zugriff über den Microsoft-Account des Opfers und kann grossen Schaden anrichten.

Wie funktioniert die Attacke?

Wie bei normalen Phishingattacken ist eine täuschend echte E-Mail der Auslöser. Die manipulierte Seite sieht beispielsweise exakt wie die Anmeldeseite für die Microsoft-Dienste aus, inklusive der Möglichkeit zur Eingabe des zweiten Sicherheitsfaktors. Über einen

Drittserver wird nun das sogenannte Session Cookie des Browsers von den Angreifenden gestohlen. Dort sind alle notwendigen Eingaben inklusive der Zweifaktor-Authentifizierung hinterlegt, was den Angreifenden volle Kontrolle über einen gestohlenen Account gibt.

Wie kann man sich gegen diese Art von Angriffen schützen?

SmartIT beobachtet diese Art von Angriffen regelmässig. Es sind leider keine Einzelfälle – KMU werden regelmässig Opfer solcher Attacken. Mit dem Security Operations Center (SOC) der SmartIT ist ein sicherer Schutz gegeben. Auch die kleinsten Unregelmässigkeiten bei Logins werden vom SmartIT-SOC registriert. Durch die schnelle Analyse können betroffene Accounts sehr schnell isoliert werden, ohne dass die Angreifenden grossen Schaden anrichten können.

«Leider sind solche Angriffe keine Einzelfälle. Wir konnten sie aber bereits x-fach vereiteln.»
– Aladin Steiner, Head of Azure und Verantwortlicher für das SmartIT-SOC

Warum ist das Verteidigen solcher Angriffe so schwierig?

Die Tools, mit welchen das SOC der SmartIT solche Phishingangriffe identifiziert, sind für alle Unternehmen zugänglich. Oftmals fehlen die Ressourcen und das Know-how, um eine ausreichend schnelle Reaktion auf einen Angriff sicherzustellen.

«Alle IT-Systeme speichern in der Regel security-relevante Systemlogs. Vielfach werden die Logs auch zentral gespeichert und aufbewahrt. Aber wenn es täglich zig Log-Einträge gibt, hat oftmals niemand die Zeit und das Know-how, die relevanten Alarme herauszufiltern.»
– Aladin Steiner, Head of Azure und Verantwortlicher für das SmartIT-SOC

Kommt hinzu, dass es für Mitarbeitende eines Unternehmens immer schwieriger wird, die täuschend echt aussehenden Mails und Login-Seiten von den echten zu unterscheiden.

Mehrere Massnahmen für mehr Sicherheit

Ein Universalrezept für die Verhinderung solcher Angriffe gibt es nicht. Es lohnt sich jedoch, aus unterschiedlichen Richtungen das Problem zu attackieren. Einerseits über eine fortwährende Sensibilisierung der Mitarbeitenden. Nur mit stetiger Wachsamkeit und einem geschulten Blick lassen sich Klicks auf dubiose Links verhindern. Hinzu kommen technische Lösungen, um die Login-Methoden resistenter zu machen. Beispielsweise mit einem physischen Security-Key (Fido2) oder mit einer sogenannten «Certificate Based Authentication», wobei man sich mit Zertifikaten anstatt Passwörtern anmeldet.

Schliesslich ist ein SOC auch eine technische Lösung, die einen besser schlafen lässt. Durch das automatisierte Generieren von zahlreichen «Alarmen» und der sofortigen Analyse der Techniker:innen im Verdachtsfall erhält man einen mächtigen Sicherheitslayer zum Schutz des Unternehmens.

Weitere Informationen unter:
www.smartit.ch

SmartIT

Brandreport • linkyard

Den «Faktor Mensch» vom Sicherheitsrisiko zur Stärke machen

IT-Anwendungen werden technisch immer raffinierter und damit sicherer. Doch gerade in KMU und kommunalen Einrichtungen fehlt es oft an der notwendigen Sicherheitskultur – und genau diesen Umstand machen sich Cyberangreifer:innen zunutze. Die linkyard AG hält hier dagegen: mit einem Abomodell, das zur Errichtung einer «menschlichen Firewall» beiträgt.

Marcel Hostettler
CEO

Stefan Haller
Managing Partner

Herr Hostettler, Herr Haller, warum ist das Thema «Cybersicherheit» heute ein so brennendes?

Marcel Hostettler: Das hat mit der Tatsache zu tun, dass jede Person, die sich im Cyberspace aufhält, ein potenzielles Opfer verschiedener Gefahren ist. Zu den Kunden von linkyard gehörten sowohl Kommunen als auch Konzerne und KMU – und sie alle sind auf ihre individuelle Art und Weise gefährdet. KMU stehen ganz besonders im Fadenkreuz von Cyberkriminellen, weil sie hinsichtlich Security gewisse Maturitätslücken aufweisen.

Stefan Haller: Das Thema ist auch derart präsent, weil sich die Bedrohungslage deutlich verändert hat: Die Angreifer:innen agieren merklich professioneller als noch vor einigen Jahren. Während es sich bei Hackerangriffen früher um die Taten von Einzelpersonen handelte, die meist ideologisch getrieben waren, ist Cybercrime mittlerweile zu Big Business geworden – inklusive Arbeitsteilung, professionellen Tools und Spezialisierungen. Das verschärft die Gefahr deutlich und die Anzahl verübter sowie erfolgreicher Angriffe steigt. Das ist kritisch, denn Cybercrime wird damit zu einem lukrativen Geschäftsmodell, mit dem viel Geld gemacht wird. Ransomware-Angriffe etwa lassen sich vergleichsweise einfach monetarisieren und dank Bitcoin und Co. sind auch die (Löse-)Geldflüsse anonym.

Dennoch vertreten insbesondere KMU noch oft die Ansicht, dass sie zu wenig attraktiv seien für Cyberangriffe. Wie beurteilen Sie das?

Marcel Hostettler: Das ist leider ein grosser Trugschluss. Viele KMU sind mittlerweile in die Cloud migriert und verlassen sich darauf, dass die Betreiber dieser Infrastrukturen die Sicherheitsthematik abdecken. Doch das reicht bedauerlicherweise nicht aus, denn technische Sicherheit allein schützt leider nicht vor Attacken. Denn der Mensch ist noch immer das primäre Ziel von Cyberkriminellen und bleibt damit der Schlüssel für erfolgreiche Angriffe. Und genau dort wollen und müssen wir den Hebel ansetzen. Wir sprechen in diesem Zusammenhang von der «Human Firewall».

Was versteht man unter einer Human Firewall?

Marcel Hostettler: Wir sind der starken Überzeugung, dass Sicherheit über den Menschen gehen muss – schliesslich gilt er ja auch als Gefahrenquelle Nummer eins. Um also eine stabile und sichere menschliche Firewall gegen Cyberattacken zu bilden, muss die Sensibilität für ein sicheres Onlineverhalten gesteigert und in der Firmenkultur verankert werden. Doch in der Praxis zeigt sich immer wieder, dass die Aufmerksamkeit für das Thema enorm kurz ist. Das überrascht an sich nicht, denn Cybersecurity ist für Unternehmen nach wie vor ein Nebenschauplatz, nicht die Kernaufgabe. Darum führen Sicherheitstrainings in Betrieben meist nur zu einer kurzzeitig ansteigenden Sensibilitätskurve – die im Alltagsstress dann schnell wieder abflacht. Wir versuchen mit unserem Abonnementsansatz die Awareness auf einem konstanten Niveau zu halten. Und diese Konstanz bildet quasi das Fundament der Human Firewall.

Stefan Haller: Eine verlässliche Sicherheitskultur ist auch deswegen so wichtig, weil die Maturität der Technik enorm gestiegen ist. Anders als früher ist es heute beinahe aussichtslos, ein gut gewartetes Windowssystem angreifen zu wollen. Das Hosting solcher Anwendungen liegt ausnahmslos bei Firmen, die genau wissen, was sie tun. Angreifer:innen rennen nicht gerne gegen gut geschützte Infrastrukturen an, sondern spazieren lieber durch den offenen Hintereingang. Darum werden vermehrt die Enduser:innen als Sicherheitsschwachstelle genutzt. Cybercrime verlagert sich dementsprechend vermehrt in Richtung Betrugsversuche, wobei insbesondere künstliche Intelligenz zur Schlüsseltechnologie werden wird. Schon heute werden ganze Unternehmen simuliert und neue Mitarbeitende erhalten zum Beispiel eine Mail des vermeintlichen neuen Chefs, der sie um die Herausgabe von Passwörtern etc. bittet. Die notwendigen Infos für diese Betrugsmaschen zieht die KI automatisch von LinkedIn und anderen Plattformen und Websites ab und formuliert individualisierte E-Mails in der Sprache des Empfängers. Die Human Firewall ist ein Mittel gegen die Wirksamkeit dieses Ansatzes.

Wie aber verhindert man, dass das Interesse für die Sicherheitsthematik nach einem Workshop direkt wieder abflacht?

Marcel Hostettler: Wir setzen auf ein kontinuierliches Bespielen des Themas. Dabei achten wir darauf, die Leute nicht zu langweilen und unter anderem Mittel wie Gamification einzusetzen, um das Interesse akut zu halten. Zentral ist in diesem Zusammenhang unser bereits angesprochenes Abomodell. Dieses besteht aus drei wichtigen Komponenten. Die erste besteht im Aufsetzen eines Risikomanagements. Gerade in KMU sind diese wichtigen Managementtools für den IT-Bereich oft lückenhaft. Hier unterstützen wir, indem wir dabei helfen, ein IT-bezogenes Risikomanagement in die Gesamtstrategie des Betriebs zu integrieren. Als zweite Komponente fokussieren wir uns auf die Schaffung von Awareness, um den Schutz vor Ransomware, Social Engineering und Co. zu maximieren. Dabei identifizieren und schliessen wir auch Sicherheitslücken wie ungenügende Passwörter, betrachten die notwendigen Sicherheitsvorkehrungen für Remote Work und führen einen initialen Workshop für Risikomanagement durch. Anschliessend legen wir den Kampagnenfahrplan vor, der Security-Awareness-Kurse, simulierte Angriffe und verschiedene Schulungen umfasst. Diese Massnahmen und Events finden das gesamte Jahr über statt, in der angemessenen Dosierung. Je nach Maturität des Unternehmens ist der Fahrplan intensiver oder umfasst Spezialthemen, die den jeweiligen Betrieb in besonderem Masse betreffen.

Und wie lautet der dritte Abo-Aspekt?

Stefan Haller: Wir führen stetige Monitorings durch, um möglicher Angriffe präventiv zu erkennen und abzuwehren. Denn Indizien für einen bevorstehenden Angriff gibt es viele: So kann etwa ein Vorzeichen für einen Angriff lauten, dass URLs reserviert werden, die ähnlich klingen wie die des eigenen Unternehmens. Das lässt darauf schliessen, dass künftig Leute mit falschen Links in die Irre geführt werden sollen.

Marcel Hostettler: Unseren Kundinnen und Kunden kommt die Tatsache zugute, dass wir bei linkyard sehr breit aufgestellt sind und über eine umfassende Expertise verfügen. Denn wir wollen ein echtes Verständnis für Sicherheit schaffen – und das gelingt uns, weil wir die Sprache der Verwaltungen und der Industrie sprechen. Teil dieses Mindsets ist auch eine gelebte Agilität: Wir bieten das Erstellen eines praxistauglichen Risikomanagements für die IT auch losgelöst vom Abo an, wenn dies den Bedürfnissen eines Betriebs besser entspricht. Dieser kundenzentrierte Ansatz zeichnet uns aus. Die initiale Standortbestimmung kann später dann immer noch die Basis einer weiterführenden Zusammenarbeit bilden.

Weitere Informationen unter:
linkyard.ch

linkyard

Über linkyard
Die in Bern angesiedelte linkyard AG bietet IT- und Cybersicherheit «aus einer Hand» an. Der Kundenstamm von linkyard umfasst Finanzdienstleister, Betreiber von kritischen Infrastrukturen, Anbieter im Gesundheitswesen, öffentliche Verwaltungen und Organisationen im Bereich Verteidigung. Die Erfüllung höchster Compliance-Anforderungen ist dabei stets ein zentrales Anliegen. linkyard selbst verfügt über ein nach ISO 27001 zertifiziertes Informationssicherheits-Managementsystem.

Bild iStockphoto/MF3d

Cybersecurity – Massnahmen und Hilfsmittel

Cyberangriffe und ganz generell Bedrohungen mit Auswirkungen auf die IT gewinnen an Aufmerksamkeit. Wer trotz der steigenden Gefahren nichts tut, wird im Fall des Eintretens sein Verhalten erklären müssen. Der Beitrag zeigt, was Unternehmen vorbeugend konkret tun können und welche Hilfsmittel zur Verfügung stehen.

Heinrich A. Bieler
Leiter Zertifizierungsstelle Swiss Safety Center

Sicherheit kostet Geld, ist oft unbequem und verlangsamt ein System. Sicherheit trägt im Normalzustand nicht zur Wertschöpfung bei. So lange nichts passiert, ist man versucht, Investitionen in die Sicherheit tief zu halten. Je grösser die Bedrohung im Umfeld, umso grösser wird die Wahrscheinlichkeit eines Ereignisses und desto stärker der Druck, sich um die Sicherheit zu kümmern. Dieser Druck steigt stark, wenn ein Ereignis eintritt, wobei natürlich alle hoffen, dass es sie nicht als Erste erwischt.

Kosten quantifizieren

Mit dieser Situation gekonnt umzugehen, nennt man Risikomanagement. Aufgrund der systematischen Analyse im Rahmen des Risikomanagements findet jede Organisation für ihre aktuelle Situation die notwendigen Massnahmen und kann somit auch die Kosten quantifizieren. Es sollte selbstverständlich sein, dass die Massnahmen nur dann einen Wert haben, wenn sie konsequent umgesetzt werden. Aus der Erfahrung als Zertifizierungsstelle stellt das Swiss Safety Center oft fest, dass einerseits aufgrund unsystematischer Risikobeurteilung am falschen Ort investiert wird und andererseits Massnahmen nicht konsequent umgesetzt werden.

Die Bedrohung

Der Begriff Cybersecurity kommt in der täglichen Berichterstattung immer öfter vor. Es muss auch kaum mehr diskutiert werden, ob man sich als Unternehmen darum kümmern muss.

Aufgrund der Entwicklungen im Rahmen der Digitalisierung und der künstlichen Intelligenz (KI), die wohl in keiner Strategie mehr fehlt, nehmen die Gefahren zu.

Die zunehmende Digitalisierung und die Benutzung von Hilfsmitteln wie z. B. MS Teams erleichtern ortsunabhängiges Arbeiten, machen aber auch abhängig von funktionierenden Systemen und erhöhen die Verletzlichkeit.

Es gibt viele Risiken, von denen einige schwerwiegender sind als andere. Zu diesen Gefahren gehört Malware, die das gesamte System löscht, ein Angreifer, der in das System eindringt und Dateien verändert, eine Angreiferin, die Computer benutzt, um andere anzugreifen, oder ein Angreifer, der Kreditkartendaten stiehlt und unberechtigte Einkäufe tätigt. Es gibt keine Garantie dafür, dass selbst mit den besten Vorsichtsmassnahmen nicht doch etwas davon passiert, aber es gibt Schritte, die man unternehmen kann, um das Risiko zu reduzieren.

Dazu kommt, dass zunehmend Gesetze zu berücksichtigen sind, die zum Motiv haben, für die Gesellschaft eine sichere Basis zu ermöglichen, dazu zählt die DSGVO und die EU AI Act im EU-Raum und in der Schweiz das neue Datenschutzgesetz.

Wichtige Themen sind die Informationssicherheit, Netzwerksicherheit, Operative Sicherheit, Sicherheit der Anwendungen, Ausbildung der Endbenutzer und Planung der Geschäftskontinuität.

Cybersecurity muss als Grundlage für eine funktionierende, stabile Volkswirtschaft verstanden werden und liegt im Interesse jedes Einzelnen.

Die Verantwortung

Auch wenn die hundertprozentige Sicherheit nicht erreicht werden kann, ist es keine Option, nichts zu tun und im Fall des Eintretens zu argumentieren «dumm gelaufen», «das kann jedem passieren». Es muss bewusst Risikomanagement betrieben werden, das zu dokumentieren ist.

Unter Risikomanagement versteht man alle Tätigkeiten zur Identifikation, Einschätzung, Steuerung und Überwachung von Risiken bezüglich der Zielerreichung im Unternehmen.

Seit der Aktienrechtsrevision 2013 müssen ordentlich revisionspflichtige Unternehmen anstelle des Jahresberichts einen Lagebericht mit einer Risikobeurteilung erstellen. Der Verwaltungsrat muss ein System zur Risikoerfassung und des Risikomanagements einrichten, damit Risiken im Unternehmen erkannt und richtig behandelt werden. Der Verwaltungsrat selbst muss sich mit den Risiken auseinandersetzen, die für das Unternehmen von existenzieller Bedeutung sind, sowie die Gesamtrisikolage des Unternehmens steuern bzw. der Risikofähigkeit der Gesellschaft anpassen.

Diese Elemente der Risikosteuerung müssen zu einem sinnvollen Ganzen zusammengesetzt werden, das es ermöglicht, Risiken zu erkennen und, wo sie unvermeidbar sind, einzugrenzen. Die Ausgestaltung dieser Instrumente und die Intensität, mit der sie eingesetzt werden, hängt von der Komplexität, der Grösse und der Ausrichtung des Unternehmens ab. Cybersicherheit ist also ein Thema, mit dem sich die oberste Führung einer Organisation kompetent auseinandersetzen muss und das nicht nur einmalig, sondern der Situation entsprechend rollend.

> **«Cybersicherheit ist also ein Thema, mit dem sich die oberste Führung einer Organisation kompetent auseinandersetzen muss und das nicht nur einmalig, sondern der Situation entsprechend rollend.»**
>
> – Heinrich A. Bieler, Leiter Zertifizierungsstelle Swiss Safety Center

Die Massnahmen

Der erste Schritt, um sich zu schützen, besteht darin, die Risiken zu erkennen. Dazu muss man sich mit den Bedrohungen und möglichen Szenarien vertraut machen. Um die Risiken von Cyberangriffen zu minimieren, sollte man grundlegende bewährte Verfahren der Cybersicherheit befolgen.

In Anbetracht der vielen Möglichkeiten, die einem offen stehen, um an Informationen über Bedrohungen zu kommen, deren Relevanz für die eigene Organisation abzuschätzen und sich durch gezielte Massnahmen besser zu schützen, gibt es keinen Grund, nichts zu tun.

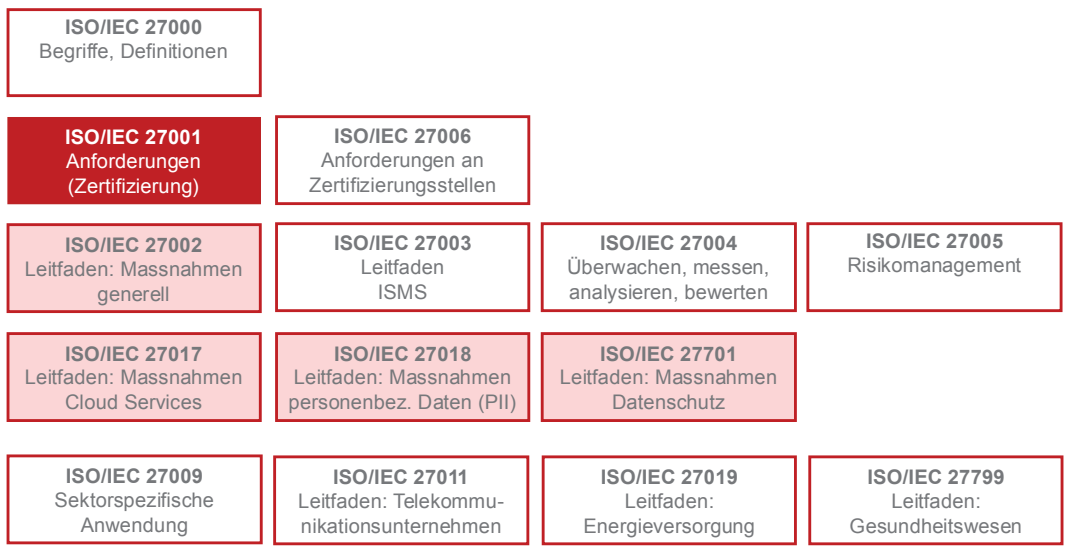


Abbildung 1: Struktur ISO/IEC 27000

Wertvolle und laufend aktualisierte Informationen findet man z. B. auf den Regierungsseiten im Internet. Es macht dabei sicher Sinn, über die Landesgrenzen hinauszuschauen. Man sollte nie vergessen: Das Internet ist international. In der Schweiz stellt der Bund viele aktuelle Informationen zur Verfügung, man muss sich diese Seite anschauen und es tun sich neue Welten auf: *ncsc.admin.ch*

Eine wertvolle und umfassende Quelle für mögliche Massnahmen ist das Dokument ISO/IEC 27002.

Normen helfen

Informationssicherheit muss in jeder Organisation ein Thema sein. Stellt sich die Frage, was konkret zu tun ist. Auch in einer komplexen Umgebung hilft systematisches Vorgehen. Der Einsatz von Methoden (wie ist etwas zu tun) und Vorgehensmodellen (was ist zu tun) erleichtert das Vorgehen und führt zum Erfolg. Sicher hilfreich wäre ein Katalog von Bedrohungen und Massnahmen, den man auf die eigene Organisation anwenden kann. Dieser Katalog steht in Form der Norm ISO/IEC 27002 zur Verfügung.

Es steht mit ISO/IEC 27001 eine etablierte, zertifizierbare Norm und eine grosse Anzahl (ca. 50) Leitfäden zur Verfügung, die bei der Umsetzung im spezifischen Umfeld eine grosse Hilfe sind und Sicherheit geben.

ISO/IEC 27001 beschreibt Anforderungen, die man erfüllen sollte, wenn man Informationssicherheit gewährleisten will. Diese Norm ist in der Struktur identisch aufgebaut wie andere, bekannte Normen: ISO 9001 – Qualitätsmanagement, ISO 14001 – Umweltmanagement, ISO 45001 – Arbeitsschutz etc. Das ist kein Zufall, sondern Absicht. Mit der sog. High Level Structure (HLS) will man es den Anwendenden einfacher machen, mehrere Normen anzuwenden. Dabei soll man nicht für jedes Bedürfnis ein isoliertes System aufbauen. Man sollte ein einziges, unternehmenseigenes System pflegen und weiterentwickeln, das alles Wichtige enthält. Damit erkennt man auch eher unerwünschte Nebenwirkungen, die zu Kollateralschäden führen können.

In einem Kapitel wird auf den Umgang mit Risiken und Chancen eingegangen (Kapitel 6.1). Informationssicherheitsrisiken sollten beurteilt und behandelt werden. Als Hilfestellung enthält die Norm den Anhang (A), der eine umfassende, wenn auch nicht abschliessende Liste von Massnahmenzielen und Massnahmen enthält. In den oben aufgeführten Leitfäden findet man weitere Massnahmen.

Zertifizierung ist nützlich

Die Frage ist nicht, ob man eine Zertifizierung benötigt, sondern welche Einstellung man dazu hat. Die Zertifizierung entfaltet in unterschiedlichen Dimensionen ihren Nutzen. Intern hilft sie das Ziel nicht aus den Augen zu verlieren, täglich und personenunabhängig die von der Kundschaft und interessierten Parteien erwartete Leistung zu erbringen. Die Organisation erhält zudem eine Rückmeldung über den Grad, in dem Massnahmen umgesetzt werden. Extern ist das Zertifikat ein Zeichen dafür: Man kann sich darauf verlassen, dass die mit der Norm verbunden Anforderungen erfüllt werden und dies von einer objektiven und unabhängigen Stelle bestätigt wird.

Vorgehen

Wer bereits ein Managementsystem implementiert hat und anwendet, ist klar im Vorteil (vgl. ISO 9001). Massnahmen, die mit einem System verknüpft sind, das Prozesse und ihre Wechselwirkung aufzeigt, entfalten ihre Wirkung zuverlässiger als Regeln, die ohne Zusammenhang zu befolgen sind.

- Die einhundertprozentige Sicherheit gibt es nicht. Das ist kein Grund, sich nicht zu schützen.
- Die Massnahmen müssen auf die Organisation abgestimmt sein.
- Eine Organisation muss wissen, wo sie angreifbar ist (Bedrohung, Gefährdung, Risiken).
- Eine Organisation muss sich über mögliche Massnahmen informieren und die für sie zweckmässigen aussuchen.
- Am Schluss zählen umgesetzte Massnahmen und nicht schöne Pläne.
- Zertifizierung schafft Vertrauen und hilft dranzubleiben.

Zusätzliche Informationen und Hilfsmittel (kostenfreie Checkliste und Formulare) zum Thema Informationssicherheit finden Sie unter: **safetycenter.ch/cs/Thema-ISMS**

swiss safety center

Sponsored.

Cybersecurity Awareness: Ein Muss für Unternehmen in der digitalen Ära

In der heutigen Zeit, die zunehmend von digitalen Technologien beeinflusst wird, stehen die Unternehmen vor immer grösseren Herausforderungen im Bereich der Cybersicherheit und Datenschutz. Cyberangriffe werden nicht nur immer häufiger, sondern auch immer raffinierter. Phishing, Ransomware und Social Engineering gehören mittlerweile zur täglichen Bedrohungslandschaft. Ein entscheidender Schutzfaktor: die Mitarbeitenden.

Studien zeigen, dass menschliches Fehlverhalten für fast 80 Prozent aller Sicherheitsvorfälle verantwortlich ist. Schon kleine Unachtsamkeiten wie das Anklicken eines gefälschten Links reichen oft aus, um Angreifer:innen Tür und Tor zu öffnen und dabei sensitive Daten offen zu legen. Die Digio AG hat sich darum darauf spezialisiert, Unternehmen durch Cybersecurity-Awareness-Schulungen zu unterstützen.

Die Mitarbeiterschulungen der Digio AG sind darauf ausgerichtet, Mitarbeitende aller Hierarchieebenen zu sensibilisieren und auszubilden. Es werden praxisnahe Strategien vermittelt, um Bedrohungen im Unternehmen, im Homeoffice und unterwegs frühzeitig zu erkennen und dabei richtig zu reagieren. Interaktive Module, realitätsnahe Szenarien und kontinuierliche Auffrischungskurse sorgen dafür, dass das Gelernte langfristig erhalten bleibt.

Durch gezielte Schulungen können Unternehmen nicht nur das Risiko von kostspieligen Sicherheitsvorfällen minimieren, sondern auch das Vertrauen gegenüber der Kundschaft und Geschäftspartner:innen stärken. Da Datenschutz und IT-Sicherheit zunehmend den Markterfolg bestimmen und strategisch relevant werden, sind Schulungen zur Cybersicherheit nicht länger eine Option, sondern eine unverzichtbare Notwendigkeit.

Sichern Sie Ihr Unternehmen und Ihre Mitarbeitenden ab, indem Sie eine individuell angepasste Schulung direkt bei Ihnen vor Ort vereinbaren.

Weitere Informationen unter:
digio.swiss

digio

SCION: Sicherheit, Kontrolle und Verfügbarkeit

Ein Netzwerk, das schneller, sicherer und widerstandsfähiger gegen Ausfälle und Angriffe ist – eine Lösung, die mehr Kontrolle und Flexibilität bietet und gleichzeitig den steigenden Anforderungen der digitalen Welt gerecht wird.

Samuel Hitz
Chief Technology Officer

Was ist SCION?

Der Begriff SCION ist eine Abkürzung für «Scalability, Control and Isolation On Next-Generation Networks». Es bezeichnet eine Netzwerktechnologie, die entwickelt wurde, um Sicherheits- und Zuverlässigkeitsprobleme der heutigen Internetinfrastrukturen zu lösen. Diese innovative Internetarchitektur soll hohe Sicherheit, Kontrolle und Verfügbarkeit bei der Datenübertragung gewährleisten. SCION wurde ursprünglich in der Forschung entwickelt und wird zunehmend in geschäftskritischen Anwendungen eingesetzt.

SCION wurde von Anfang an mit dem Fokus auf Sicherheit entwickelt. Ein zentrales Element dabei ist die Kontrolle darüber, welche Entitäten Zugang zu Pfadinformationen erhalten. Das ermöglicht es, private Netzwerke aufzubauen und Dienste zu schützen, indem diese im Netzwerk unsichtbar gemacht werden. Dies wird durch die integrierte Public Key Infrastructure (PKI) unterstützt, die sicherstellt, dass Routing-Informationen wie Netzwerkpfade nicht gefälscht oder umgeleitet werden können. Die PKI kann zudem verwendet werden, um zusätzliche Sicherheitsfunktionen wie die Verschlüsselung und Authentifizierung von SCION-Paketen zu implementieren. Darüber hinaus ermöglicht das Konzept der SCION-Isolationsdomänen die Bildung von Netzwerken unter einem gemeinsamen Governance-Rahmen und einer vertrauenswürdigen Root-Instanz. Diese Isolationsdomänen können länderspezifisch, wie etwa die Schweizer oder US-amerikanische Domäne oder branchenspezifisch wie die Domäne für Finanzinstitute in der Schweiz sein. Innerhalb einer Isolationsdomäne haben die verantwortlichen Entitäten die Befugnis zu bestimmen, wer Teil der Domäne ist, indem sie Zertifikate ausstellen, während externe Entitäten keinen Einfluss auf den Routing-Prozess innerhalb der Domäne nehmen können.

Doch worin liegt der Unterschied zwischen SCION und den allseits bekannten VPNs? «VPNs schützen Daten während der Übertragung vor Abhören und Manipulation, bieten jedoch keine Garantie für die Verfügbarkeit der Verbindung», erklärt Samuel Hitz, Chief Technology Officer. «SCION sorgt für zuverlässige Kommunikation, indem es Netzwerkteilnehmern ermöglicht, den Zugriff auf Pfadinformationen zu kontrollieren und Server unsichtbar zu machen.» Somit ergänzt es VPNs, indem es neben Vertraulichkeit und Integrität auch Verfügbarkeit und Geschäftskontinuität sicherstellt.

> «VPNs schützen Daten während der Übertragung vor Abhören und Manipulation, bieten jedoch keine Garantie für die Verfügbarkeit der Verbindung.
>
> – Samuel Hitz, Chief Technology Officer

Diverse Vorteile

Betreiber kritischer Infrastrukturen wie Finanzdienstleister, Gesundheitsorganisationen oder Versorgungsunternehmen schätzen die zusätzlichen Sicherheitsvorteile und die reduzierte Angriffsfläche, die SCION bietet. Gerade diese Branchen stehen aufgrund der Kritikalität ihrer Dienstleistungen und strenger regulatorischer Anforderungen vor besonderen Herausforderungen, wenn es darum geht, Remote-Arbeit für geschäftskritische Aufgaben sicher umzusetzen. SCION ermöglicht es, diese Hürden zu überwinden und sichere sowie zuverlässige Verbindungen bereitzustellen.

Zudem lassen sich die Betriebskosten eines Unternehmens durch die Einsetzung von SCION erheblich reduzieren, insbesondere für solche, die eine Vielzahl an Leased Lines oder MPLS-Verbindungen zu internen und externen Partnern unterhalten. «Durch die Nutzung von SCION können diese Unternehmen diese zahlreichen Verbindungen durch lediglich zwei SCION-Zugänge ersetzen und sich über eine gemeinsame Infrastruktur mit ihren Partnern verbinden, ohne Kompromisse bei Sicherheit und Zuverlässigkeit einzugehen», erläutert Hitz.

SCION kann in bestimmten Szenarien eine bessere Alternative zu MPLS-Netzwerken darstellen, insbesondere bei organisationsübergreifenden Netzwerken oder einer hybriden Infrastruktur aus On-Premises- und Cloud-Lösungen. Im Vergleich zu MPLS ermöglicht SCION eine einfachere Verbindung von Standorten über das SCION-Internet und die Bildung privater Netzwerke, bei denen Unternehmen die Kontrolle darüber haben, wer Zugriff auf Pfadinformationen erhält. Dies führt zu einer hohen Flexibilität und ermöglicht eine schnelle Anpassung des Netzwerks, ohne auf teure und komplexe MPLS-basierte Lösungen angewiesen zu sein. Zudem ist SCION von Grund auf als Interdomain-Architektur konzipiert, wodurch Multi-Provider-Lösungen Standard sind. Das bedeutet, dass Unternehmen problemlos mit verschiedenen Anbietern zusammenarbeiten können, um ihre Netzwerkinfrastruktur weiter zu optimieren und die Verfügbarkeit zu steigern.

Integration von SCION

«SCION in bestehende Netzwerke zu integrieren ist einfach», erklärt Hitz. «Da bestehende Netzwerke SCION nicht direkt unterstützen, gibt es spezielle Gateways, die die Verbindung zwischen normalen IP-Netzwerken und SCION ermöglichen. Diese Gateways machen es einfach, SCION in bestehende Systeme einzufügen, ohne dass Anwendungen geändert werden müssen.» Um sich mit dem SCION-Netzwerk zu verbinden, werden lediglich einen oder mehrere SCION-Zugänge benötigt, die mittlerweile viele Internetanbieter anbieten. Das SCION-Backbone nutzt dabei die Infrastruktur mehrerer Internetdienstanbieter (ISPs), was es besonders robust und zuverlässig macht. Unternehmen müssen für die Implementierung ihres Netzwerks nicht eng mit einem einzigen ISP zusammenarbeiten. Sie können SCION-Zugänge von verschiedenen SCION-fähigen ISPs beziehen und ihr Firmennetzwerk darauf aufbauen.

Text **Tatiana Almeida**

Schutz durch Managed-Workplace-Service vs. Risiken eines Cyberangriffs

Michael Freuler
Head of Solution Consulting

In der Geschäftswelt sind sichere und durchdachte Entscheidungen der Schlüssel zum Erfolg. Unternehmen analysieren Potenziale, Gewinne und Investitionen, um ihre Zukunft zu gestalten. Doch ein essenzieller Bereich wird oft übersehen: IT- und Cybersicherheit. Dabei liegt gerade hier eine enorme Chance. Durch gezielte Investitionen können Unternehmen nicht nur Risiken minimieren, sondern sich langfristige Wettbewerbsvorteile sichern. Besonders Schweizer KMU haben die Möglichkeit, mit den richtigen Massnahmen ihre Widerstandsfähigkeit zu stärken und aktiv in eine sichere Zukunft zu investieren.

Die wachsende Bedrohungslage

KMU stehen zunehmend im Fokus von Cyberkriminellen und die Gefahr nimmt stetig zu. Zu den häufigsten Cybersecurity-Risiken für Schweizer KMU zählen laut dem Bundesamt für Cybersicherheit BACS unter anderem:

1. Phishing-Angriffe: Täuschend echte E-Mails, die Mitarbeitende dazu bringen, sensible Daten preiszugeben.

2. Spam und Ransomware: Verschlüsselungstrojaner, die Unternehmen erpressen, ihre eigenen Daten zurückzukaufen.

Diese Risiken betreffen nicht nur IT-Systeme, sondern auch das Vertrauen von Kunden und Geschäftspartnern. Ein einziger erfolgreicher Angriff kann sowohl finanzielle Schäden verursachen als auch die Reputation eines Unternehmens nachhaltig beeinträchtigen. Doch es gibt gute Nachrichten: Viele KMU haben die Möglichkeit, ihre Vorbereitung entscheidend zu verbessern.

Mit einem durchdachten Managed-Workplace-Service, der alle essenziellen Punkte wie Notfallkonzepte und präventive Massnahmen beinhaltet und sämtliche sicherheitsrelevanten Konzepte abdeckt, können sie ihre Sicherheitslage nachhaltig stärken. Entscheidend ist, dass dieser Service ausgereift und professionell umgesetzt wird. So lassen sich Risiken effektiv minimieren und das Unternehmen sicher für die Zukunft aufstellen.

Managed-Services: Experten übernehmen die Verantwortung

Um der wachsenden Bedrohungslage zu begegnen, ist die Zusammenarbeit mit einem Managed-Service-Provider (MSP) eine sinnvolle Lösung. Diese Dienstleister bieten umfassende IT-Sicherheitslösungen an und überwachen IT-Systeme rund um die Uhr.

Effektive IT-Sicherheitsstrategien sind der beste Schutz gegen Cyberangriffe. Hier einige Massnahmen, die jedes Unternehmen umsetzen sollte:

1. Wiederkehrende Mitarbeiterschulungen: Gut informierte Mitarbeitende sind die erste Verteidigungslinie gegen Cyberangriffe.

2. Regelmässige Updates und Patches: Veraltete Software gehört zu bekannten Schwachstellen.

3. Umfassende Sicherheit: Fortschrittliche Sicherheitsfunktionen wie Zero-Trust-Architekturen, der Schutz von «besonders schützenswerten Personendaten» und zuverlässige Back-up-Lösungen gehören zur Grundausstattung und gewährleisten einen effektiven Schutz für Unternehmensdaten und Geräte.

4. Proaktive Sicherheit: Managed Services erkennen Bedrohungen frühzeitig und wehren diese ab, bevor sie Schaden anrichten können.

5. Rund-um-die-Uhr-Betreuung: Mit einem MSP ist die IT-Sicherheit des Unternehmens jederzeit in besten Händen.

Durch die Zusammenarbeit mit einem versierten Anbieter profitieren Unternehmen von einem ganzheitlichen Schutz und können sich voll und ganz auf ihr Kerngeschäft konzentrieren.

Was kostet ein Cyberangriff?

Die Folgen eines Cyberangriffs können Unternehmen hart treffen – finanziell und operativ:

– Direkte Schäden: Betriebsunterbrechungen, Verlust sensibler Daten oder hohe Kosten für die Wiederherstellung der IT-Systeme.

– Indirekte Auswirkungen: Imageschäden und der Verlust von Kundenvertrauen können langfristige wirtschaftliche Folgen haben.

Ein gutes Beispiel sind Ransomware-Angriffe, bei denen Daten verschlüsselt werden, um Lösegeld zu erpressen. Unternehmen ohne geeignete Sicherheitsstrategien sehen sich oft in einer schwierigen Lage. Expertinnen und Experten empfehlen jedoch klar, das geforderte Geld nicht zu zahlen, da dies keine Garantie bietet, dass die Angreifenden die Daten tatsächlich freigeben oder nicht erneut zuschlagen. Stattdessen sollte der Fokus auf einer starken IT-Sicherheitsstrategie liegen, um solche Situationen von vornherein zu verhindern.

Die Polizeiliche Kriminalstatistik 2023 zeigt, dass die Zahl der Straftaten mit einer digitalen Komponente im Vergleich zum Vorjahr um 31,5 Prozent gestiegen ist. Ein Grossteil dieser 43 839 Fälle betrifft Cyber-Wirtschaftskriminalität. Dabei sind finanzielle Schäden oft nur die Spitze des Eisbergs, da Reputationsverluste kaum quantifizierbar sind und können langfristige Auswirkungen haben.

Typische Kostenfaktoren bei Cyberangriffen:
1. Kosten wegen Umsatzverlust
2. Kosten aufgrund von Produktivitätsverlust
3. Wiederherstellungskosten
4. Immaterielle Kosten

Vorsorge ist besser als Nachsicht

Die Investition in IT-Sicherheit ist kein Luxus, sondern eine Notwendigkeit. Die Zusammenarbeit mit einem Managed-Service-Provider bietet Unternehmen nicht nur Schutz, sondern auch eine verlässliche Grundlage, um sich auf ihr Kerngeschäft zu konzentrieren.
Die Bedrohungslage durch Cyberkriminalität ist real und jedes Unternehmen, unabhängig von seiner Grösse, sollte darauf vorbereitet sein. Betrachten Sie IT-Sicherheitskosten als eine Investition in die Zukunft Ihres Unternehmens, als eine Massnahme, die langfristig Vertrauen, Stabilität und Erfolg gewährleistet.

Weitere Informationen unter:
dinotronic.ch

dinotronic
IT. Aber sicher.

Marc Ruef

«Zwischenfälle, bei denen viele Menschen empfindlich betroffen sind, werden zunehmen»

Das Thema «Cybersecurity» begleitet Marc Ruef praktisch sein gesamtes Leben lang. Er hat diese Faszination zum Beruf gemacht und verfügt damit über einzigartige Einsichten zum sicheren Verhalten im Cyberspace. Welche Learnings hat er daraus gezogen – und wie lauten seine Ratschläge und Prognosen?

Interview **SMA** Bild **zVg**

Herr Ruef, Sie sind in Sachen Cybersecurity ein «alter Hase». Wie kamen Sie mit dem Thema erstmals in Kontakt?
Als Kind durfte ich den Computer meines Vaters nutzen – natürlich zeitlich begrenzt. Daran habe ich mich aber selbstverständlich nicht gehalten. Mit der Zeit wurde ich jedoch zunehmend nervös, dass die Zeitangaben der veränderten Dateien mich verraten würden. Also ging ich zur Bücherei, um ein Fachbuch zu finden, das mir erklärt, wie ich Zeitstempel auf dem Dateisystem manipulieren könnte. Dabei bin ich über ein Buch mit dem Titel «Computerviren» gestolpert und war plötzlich vom Thema «Computersicherheit» fasziniert. Seither hat sich die Hacking-Subkultur natürlich stark verändert.

Welches sind für Sie die markantesten Veränderungen, die Sie seit den 1990er-Jahren in diesem Bereich erlebt haben?
Früher war alles familiärer. Man kannte sich und tauschte per E-Mail oder auf IRC Ideen aus. Der Antrieb bestand in der Neugierde sowie in der Anerkennung durch besondere Leistungen. Heute ist alles ein bisschen professioneller und vor allem kommerzieller.

Woran liegt das?
Diese Entwicklung ist in erster Linie der breiten Akzeptanz von Computersystemen und dem Internet geschuldet, die enorm zum gesellschaftlichen und wirtschaftlichen Wandel im Informationszeitalter beigetragen haben. Manchmal vermisse ich die «guten alten Zeiten», in denen die Dinge «simpler» waren. Es fühlte sich eher an wie ein Spiel. Heute ist es vielerorts zu einem knallharten Business geworden, mit all seinen Vor- und Nachteilen.

Sie haben mit *computec.ch* das bekannteste deutschsprachige Portal für Computersicherheit gegründet. Wie hat sich die Rolle von solchen Plattformen verändert?
Nach über 20 Jahren habe ich das Projekt schweren Herzens eingestellt und die Daten archiviert. Denn Webplattformen sind in der schnelllebigen Gegenwart von Social Media und Messenger-Diensten in der breiten Öffentlichkeit aus der Zeit gefallen. Anders ist dies hingegen im Darknet, das man als düsteres «Abbild» des normalen Internets verstehen kann. Dort werden nach wie vor solche Informationsplattformen betrieben. Vieles dort wirkt anachronistisch und erinnert dadurch an vergangene Tage. Manche Dinge ändern sich vielleicht also doch nie…

Sie haben im Laufe Ihrer Karriere zahlreiche Bücher und Fachartikel veröffentlicht. Welches Thema im Feld der Cybersecurity ist aktuell Ihres Erachtens unterbeleuchtet – und warum verdient es mehr Aufmerksamkeit?
Ich betätige mich nach wie vor sehr aktiv in der Grundlagenforschung. Das Entdecken und Dokumentieren von Schwachstellen ist ein Grundpfeiler moderner Cybersicherheit. Doch gilt dieses Thema – meines Erachtens unberechtigterweise – als langweilig und staubig. Hier gäbe es noch viel zu tun und alle anderen Bereiche könnten davon nachhaltig profitieren. Neu und sowohl technisch als auch gesellschaftlich spannend ist natürlich die Sicherheit von künstlicher Intelligenz. Hier tun sich komplett neue Forschungsfelder auf. Zwar kann auch hier auf altbewährte Ansätze zurückgegriffen werden (z. B. Injection-Angriffe). Jedoch müssen diese neu erdacht und nicht selten im gesellschaftlichen Kontext durchgesetzt werden. Diese interdisziplinäre Betrachtungsweise eröffnet einmal mehr eine neue Welt.

In der von Ihnen mitbegründeten Firma scip AG waren Sie lange für den Bereich Offensive Security Testing zuständig. Welche zentralen Learnings konnten Sie aus dieser Zeit/Tätigkeit ziehen?
Ganz viele! Eine essenzielle Erkenntnis besteht darin, dass Menschen gerne Risiken unterschätzen. Nur weil ein Angriff kompliziert erscheint, bedeutet das nicht, dass ihn nicht jemand anstreben wird. Probleme werden selten an der Wurzel gepackt. Und viele Managerinnen und Manager denken in Quartalszahlen, wodurch langfristige Investitionen – und dadurch Systematik und Nachhaltigkeit – verhindert werden.

«Computersysteme werden günstiger und effizienter, sie werden auch weiterhin an Wichtigkeit in unserem Alltag gewinnen. Dabei wird ihre Komplexität massgeblich zur Fragilität unserer Gesellschaft beitragen.

– Marc Ruef

Gibt es auch erbauliche Erkenntnisse?
Das waren jetzt tatsächlich alles Aspekte, denen eine negative Konnotation anhaftet (*lacht*). Aber es gibt durchaus auch Positives, denn Kreativität, Beharrlichkeit und Weitsicht werden meist belohnt. Nur weil jemand behauptet, dass etwas nicht möglich ist, heisst es noch lange nicht, dass man es nicht doch möglich machen kann. Das sind die Erfolge, auf die man hinarbeiten sollte.

Heute leiten Sie bei scip die Forschungsabteilung, die sich auf unorthodoxe Projekte wie Car Hacking und Medizinalgeräte spezialisiert hat. Was fasziniert Sie an solchen Projekten und welche Herausforderungen stellen sich dabei?
Im klassischen Bereich des Security-Testings hat man mit alltäglichen Technologien in handelsüblichem Kontext zu tun: Webapplikationen, Netzwerke, Firewalls, Antiviren-Lösungen etc. Im Forschungsbereich hingegen setzen wir uns mit «neuen» Problemen auseinander, die so noch nicht bewältigt wurden. Jedes Problem stellt eine gänzlich neue Herausforderung dar, die man nicht mit bewährten und standardisierten Mitteln angehen kann. Es braucht daher viel Mut und Kreativität, um sich diesen unbekannten Rätseln stellen zu können. Denn manchmal muss man auch eine Niederlage einstecken können. Denn auch aus einem Scheitern kann man wertvolle Erfahrungen für die Zukunft gewinnen.

Sie haben in Ihrer Forschung immer wieder neue Schwachstellen aufgedeckt. Gibt es einen speziellen Moment oder eine Entdeckung, die für Sie besonders unerwartet war?
Das ist eine sehr spannende Frage. Grundsätzlich komme ich zum Schluss, dass es nicht die technischen Herausforderungen an sich waren, die mich besonders fasziniert haben, sondern der jeweilige Kontext. Computersysteme beeinflussen Menschen in ihrem Alltag und das ist es, was eine Schwachstelle besonders spannend machen kann. Im Deutschen benutzen wir das Wort «Sicherheit» ja für verschiedene Aspekte. Doch im Englischen wird konsequent zwischen «Security» (virtuelle Sicherheit) und «Safety» (persönliche Unversehrtheit) unterschieden. Letztgenanntes ist mir besonders wichtig, da es das Ziel unserer Arbeit sein muss, dass Menschen nicht zu Schaden kommen. In diesem Zusammenhang naheliegend sind entsprechend Schwachstellen im Medizinalbereich. Aber auch Assistenzsysteme von Fahrzeugen oder Sensorik im Industriebereich gehören dazu. Alles IT-Mechanismen, die in unserem Alltag eher unbewusst als solche genutzt werden.

Sie unterrichten an verschiedenen Universitäten und Fachhochschulen. Wie haben sich die Erwartungen und das Wissen der Studierenden im Bereich Cybersecurity in den letzten Jahren verändert?
Spezialwissen ist viel einfacher zugänglich geworden als zu der Zeit, als ich als Kind in der Bibliothek nach Fachbüchern suchte. Es gibt heute unzählige Bücher, Webseiten und Youtube-Videos, die einzelne Themen im Detail besprechen. Nicht selten auf einem Niveau, für das man früher zig Jahre hätte investieren müssen, um sich dieses überhaupt zugänglich machen zu können. Entsprechend kann es vorkommen, dass Studierende technisch schon sehr gut vorbereitet sind und dementsprechend noch mehr wissen wollen. Das Verständnis für die eingesetzten Technologien ist unabdingbar, um sich sattelfest bewegen zu können. Die Schönheit entfaltet sich aber erst mit dem Mitbringen von Erfahrung, bei der man das technische Wissen mit dem effektiven Einsatz der Produkte in Einklang bringt. Aus den Büchern lernt man oft die starren Grundlagen. Das können die Studierenden auch ohne mich machen. In meinen Vorlesungen versuche ich stattdessen, sie für das Thema zu begeistern, indem ich spannende Geschichten aus meinem Berufsalltag erzähle und so den faden Grundlagen Leben einhauchen kann.

Wie sieht für Sie die Zukunft der Cybersecurity aus und welche Trends erwarten Sie in den nächsten Jahren?
Um es kurz zu sagen: höher, schneller, weiter. So lautet die Devise. Die etablierten Trends werden sich fortsetzen. Computersysteme werden günstiger und effizienter, sie werden auch weiterhin an Wichtigkeit in unserem Alltag gewinnen. Dabei wird ihre Komplexität massgeblich zur Fragilität unserer Gesellschaft beitragen. Die digitale Transformation darf ohne Rücksicht auf Cybersecurity nicht angestrebt werden, wird aber aus Gründen der wirtschaftlichen Optimierung gerne vernachlässigt. Die Anzahl der Zwischenfälle, bei denen viele Menschen empfindlich betroffen sind, wird die kommenden Jahre unweigerlich und stetig zunehmen. Ob und inwiefern irgendwann eine Umkehr zur Verbesserung stattfindet, kann ich nicht voraussagen. Zuerst muss ein grundlegendes Umdenken in unserer Gesellschaft allgemein und in der Computerindustrie im Speziellen stattfinden. Wir sind alle Teil davon.

Zur Person

Marc Ruef ist seit Ende der 1990er-Jahre im Cybersecurity-Bereich aktiv. Mit 18 Jahren gab er sein erstes Buch zur Sicherheit von Windows heraus. In den vergangenen 25 Jahren hat er an 16 Büchern mitgewirkt, über 275 Fachartikel in sieben verschiedenen Sprachen publiziert und mehr als 200 Interviews gegeben. Er gilt als einer der meistgelesenen deutschsprachigen Autoren auf seinem Fachgebiet. Zudem ist er Dozent an verschiedenen Universitäten und Fachhochschulen wie zum Beispiel an der ETH, HWZ, HSLU und IKF. Er ist Mitbegründer der Firma scip AG in Zürich, die seit 2002 Beratungen im Bereich Cybersecurity anbietet.

Cyberrisiken betreffen jedes Unternehmen

Thorsten Haeser
Chief Business Officer, Sunrise

Cybersecurity ist keine Frage der Unternehmensgrösse. Thorsten Haeser, seit September neuer Chief Business Officer von Sunrise, erklärt im Interview, wie flexible Sicherheitslösungen KMU und Grossunternehmen gleichermassen schützen – und ihnen dabei helfen, sowohl Kosten als auch operative Komplexität zu reduzieren.

Herr Haeser, KMU und Grossunternehmen stellen unterschiedliche Anforderungen an die eigene Cybersecurity. Wie bieten die Lösungen von Sunrise Business für beide einen umfassenden Schutz?
Die Risiken sind zwar universell, aber die Ressourcen, IT-Komplexität und operativen Anforderungen variieren je nach Unternehmensgrösse stark – genauso wie die Auswirkungen von Cyberangriffen. KMU stehen oft nur geringe Mittel für die Cybersecurity zur Verfügung. Hier bietet Sunrise Business flexible, kostengünstige und einfach implementierbare Lösungen wie DDoS Protection und DNS Security an. Um auch unterwegs Sicherheit zu gewährleisten, überwacht Lookout die Betriebssysteme, Apps und Dateien mobiler Endgeräte.

Grosse Unternehmen stehen vor komplexeren Herausforderungen. Mit unserem Security Service Edge (Teil unseres SASE-Angebots) bieten wir einen integrierten Ansatz für den sicheren Netzwerkzugriff. Unser Managed Extended Detection and Response Service (MxDR) verhilft Unternehmen zu IT-Sicherheit auf hohem Niveau und entlastet interne Security-Operations-Teams dank kontinuierlichem Monitoring. Mit SCION steht eine innovative Lösung für den sicheren, schnellen und transparenten Datentransfer zwischen Organisationen zur Verfügung.

Darüber hinaus bieten wir Phishing-Sensibilisierungsschulungen an. Um die stetig wachsenden Risiken durch Phishing-Angriffe und E-Mail-Betrugsfälle zu minimieren, sind diese für Unternehmen aller Grössen entscheidend.

Wie unterstützen die Sicherheitslösungen von Sunrise Business CISOs bei der umfassenden Umsetzung des NIST Cybersecurity Frameworks?
Sunrise Business stimmt seine Lösungen mit dem NIST Cybersecurity Framework ab, um für jedes Unternehmen umfassenden Schutz zu gewährleisten. Mit Assessments und Penetrationstests identifizieren wir IT-Schwachstellen unserer Kunden, damit diese ihre Strategien zur Risikominimierung priorisieren und die Abwehr stärken können (Identify im NIST Framework). Unsere Lösungen auf Protect-Ebene schützen den Zugang für Userinnen und User auf Systeme, reduzieren deren Angriffsfläche und wehren Bedrohungen wie schädliche Domains und DDoS-Angriffe wirksam ab.

Fortschrittliche Tools überwachen Systeme auf verdächtige Aktivitäten und liefern Empfehlungen für schnelle Schadensbehebungen (Detect und Respond im NIST Framework). Unser MxDR-Service bietet 24/7-Bedrohungserkennung, damit CISOs sich wieder verstärkt auf Governance-Aufgaben konzentrieren können. Bei akuten Cyberbedrohungen hilft unser Incident Response Service (Recover im NIST Framework), damit befallene Systeme schnell wiederhergestellt werden.

Cyberbedrohungen entwickeln sich ständig weiter, während Unternehmen zunehmend unter Kostendruck stehen. Wie trägt MxDR zu verbesserter Sicherheit, mehr Effizienz und langfristig tieferen Kosten bei?
CISOs stehen vor zwei Hauptproblemen: Mangel an qualifizierten Cybersicherheitsexpertinnen und -experten sowie hohe Kosten für deren Rekrutierung und Bindung. MxDR verbessert nicht nur die Sicherheit, sondern auch die betriebliche Effizienz von Unternehmen: Dank Echtzeitüberwachung und Frühwarnsystemen über die gesamte IT-Infrastruktur hinweg entfällt die Verwaltung mehrerer Security-Lösungen, was den Arbeitsaufwand deutlich reduziert. Der Sunrise Business Service setzt auf 24/7-Abdeckung durch Expertenteams, innovative Inhouse-Technologien und globale Bedrohungsdaten von Accenture, um bekannte und neue IT-Bedrohungen bei unseren Kunden schnell und wirksam zu identifizieren. Die Preistransparenz erleichtert zudem die Kostenplanung.

Wie stellt Ihr Unternehmen sicher, dass es mit den neusten Sicherheitstrends und den sich wandelnden Kundenanforderungen mithält?
Bei Sunrise Business steht die kundenorientierte Entwicklung im Vordergrund. Daher arbeiten unsere Account-Teams eng mit unseren Kundinnen und Kunden zusammen und schätzen deren Feedback sehr. Dank strategischer Partnerschaften mit führenden Unternehmen wie Cisco und Accenture bleiben wir technologisch an der Spitze. So können wir die Bedürfnisse, Herausforderungen und langfristigen Ziele unserer Kunden frühzeitig erkennen und darauf eingehen.

Abbildung: Cybersecurity Framework von NIST (National Institute of Standards and Technology)

Weitere Informationen zu MxDR von Sunrise Business:

Über Sunrise Business
Die Sunrise GmbH ist führende Anbieterin von Telekommunikationsdiensten in der Schweiz und bietet für Geschäftskunden massgeschneiderte Lösungen in den Bereichen Konnektivität, Security und IoT. Mit einem starken Partnernetzwerk und End-to-End-Services unterstützt Sunrise Business Unternehmen bei der Digitalisierung und schützt ihre Infrastruktur mit innovativen Cybersicherheitslösungen.

Sunrise BUSINESS

Bild iStockphoto/Kindamorphic

Cybersicherheit ist auch ein Managementthema

Cybersicherheit ist für alle Unternehmen wichtig, wie die Zunahme der Angriffe zeigt. Inzwischen haben die meisten Betriebe Cybersicherheitsmassnahmen eingeführt, auch wenn einige KMU noch hinterherhinken. Vielfach wiegen sich Unternehmen aber in falscher Sicherheit. Sie glauben, dass sie für Angreifer:innen nicht interessant sind oder legen den Schwerpunkt ihrer Sicherheitsmassnahmen zu sehr auf den IT-Aspekt. Dabei vernachlässigen sie die Rolle der Verantwortung und der Bereitschaft der Unternehmensleitung.

Egal wie gross oder klein ein Unternehmen ist, egal ob es für Hacker:innen interessant ist oder nicht, egal wie gut die technischen Cybersicherheitsmassnahmen sind, irgendwann wird ein Angriff erfolgen und die eingesetzte Technologie wird nicht ausreichen, um dies zu verhindern. Die Sensibilisierung und Vorbereitung eines Unternehmens auf einen möglichen Cyberangriff und dessen Folgen ist daher ein wichtiger Aspekt. Es gibt eine Reihe von Themen, mit denen sich das Management im Vorfeld eines Angriffs auseinandersetzen muss. Dazu gehören ein Geschäftskontinuitätsplan, ein Krisenmanagementplan, Risikobewertungen, Unternehmensprozesse, die Auswahl von Dienstleistern und vieles mehr. Es reicht nicht aus, diese Themen erst während eines Angriffs anzugehen. Dadurch geht wertvolle Zeit verloren und der Schaden – sei er finanzieller, rechtlicher oder rufschädigender Natur – wird noch grösser. Sobald ein Angriff stattfindet, muss sofort und effektiv reagiert werden.

Effektive Business-Continuity-Strategie

Unternehmen benötigen einen Plan, um im Falle eines Angriffs den Geschäftsbetrieb aufrechtzuerhalten. Dies hilft, finanzielle Verluste zu minimieren, den Ruf des Unternehmens zu schützen und schneller zur Normalität zurückzukehren.

Ein guter Business-Continuity-Plan beginnt mit einer Risikobewertung und einer Analyse der möglichen und wahrscheinlichsten Bedrohungen. Durch die Identifizierung der wahrscheinlichsten Gefahren, mit denen ein Unternehmen konfrontiert werden kann, ist es möglich, deren potenzielle Auswirkungen auf die Organisation im Voraus abzuschätzen. Darüber hinaus ist es wichtig, eine interne Analyse der zentralen Geschäftsprozesse durchzuführen, um Prioritäten zu setzen und Back-up-Lösungen zu entwickeln.

Basierend auf diesen Erkenntnissen sollte ein klarer Krisenkommunikationsplan entwickelt werden, wie im Falle eines Angriffs reagiert und kommuniziert werden soll. In dieser Phase sollten alle Mitarbeitenden einbezogen und darüber aufgeklärt werden, was zu tun ist. Ausserdem sollten gute Back-up- und Wiederherstellungsmechanismen eingerichtet werden, um den Schaden zu begrenzen und eine effiziente Wiederherstellung der Systeme nach einem Angriff zu ermöglichen. Schliesslich sollte der Plan regelmässig getestet und überarbeitet werden, um neuen Bedrohungen Rechnung zu tragen.

> **Das neue Gesetz verlangt von Unternehmen mehr Verantwortung für den Schutz personenbezogener Daten und sieht Sanktionen vor, wenn diese Massnahmen nicht eingehalten werden.**

Schadensbegrenzung durch Krisenmanagement

Teil des Business-Continuity-Plans ist ein Krisenmanagementplan. Diesem Aspekt ist besondere Aufmerksamkeit zu widmen, da er das Ausmass eines Cyberangriffs und dessen Folgen für das Unternehmen massiv beeinflussen kann. Wie der Business-Continuity-Plan setzt auch der Krisenmanagementplan idealerweise bereits vor einem Angriff an. Er definiert vor allem Schlüsselpersonen und Schlüsselprozesse, welche im Fall eines Angriffs zum Einsatz kommen. Zudem sollten Systeme zur Überwachung verdächtiger Aktivitäten und zur Früherkennung von Angriffen und deren möglichen Folgen vorhanden sein. Je früher eine Attacke erkannt wird, desto schneller kann der Krisenmanagementplan umgesetzt werden und umso geringer ist der Schaden.

Jeder gute Krisenmanagementplan wird von einem Incident-Response-Team geleitet. Dieses Team besteht aus Personen aus allen relevanten Abteilungen. In der Regel gehört mindestens eine Person aus der Marketing- oder PR-Abteilung dazu, jemand aus der IT-Abteilung und vielleicht auch jemand aus der Rechtsabteilung. Ihre Aufgabe ist es, sofort die notwendigen Massnahmen einzuleiten, um den Schaden zu begrenzen.

Der erste Schritt besteht natürlich darin, die betroffenen Systeme zu isolieren oder den Zugang zu beschränken, damit sich der Angriff nicht ausbreiten kann. Danach ist jedoch die Kommunikation über das Problem sowohl intern als auch extern von entscheidender Bedeutung. Eine schnelle und klare Kommunikation mit allen Betroffenen ist bei einem solchen Vorfall entscheidend, um das Vertrauen aller Beteiligten zu erhalten und die Verbreitung von Fehlinformationen zu verhindern. Transparenz ist ein wesentlicher Faktor in der Krisenkommunikation, denn sie hilft nicht nur, Reputationsschäden zu begrenzen, sondern auch mögliche rechtliche Konsequenzen zu minimieren.

Im Nachhinein ist es wichtig, nicht ausschliesslich die Sicherheitsmassnahmen, sondern auch den Krisenkommunikationsplan zu evaluieren und auf dieser Basis Anpassungen vorzunehmen. Es ist notwendig, Aufzeichnungen über Vorfälle und die Reaktion der Organisation zu führen, nicht nur für das Unternehmen, sondern ebenfalls für alle rechtlichen Anforderungen, die sich aus einem Angriff ergeben können.

Datensicherheit und rechtliche Konsequenzen

Viele Organisationen sind sich der rechtlichen Konsequenzen eines Cyberangriffs nicht ausreichend bewusst, insbesondere, seit das revidierte Datenschutzgesetz in Kraft getreten ist. Das neue Gesetz verlangt von Unternehmen mehr Verantwortung für den Schutz personenbezogener Daten und sieht Sanktionen vor, wenn diese Massnahmen nicht eingehalten werden. Die Bussgelder wurden erhöht, wenn festgestellt wurde, dass Datenschutzverpflichtungen vorsätzlich missachtet wurden. Darüber hinaus können Sanktionen gegen Unternehmen verhängt werden, wenn Datensicherheitsmassnahmen als unzureichend erachtet werden oder Sicherheitsvorfälle nicht ordnungsgemäss gemeldet werden.

Aus rechtlicher Sicht empfiehlt es sich daher, die Polizei zu informieren und das weitere Vorgehen mit ihr abzustimmen. Es ist wichtig, Beweise über die Angriffe zu sichern, damit sie in einem Gerichtsverfahren weiter untersucht werden können. Darüber hinaus sollten alle Angriffe, unabhängig davon, ob sie einen Schaden verursacht haben oder nicht, dem Bundesamt für Cybersicherheit (BCS) gemeldet werden.

Text **Valeria Cescato**

Bild iStockphoto/MTStock Studio

Strategien für robuste Softwaresicherheit

Software wird immer mehr in die Arbeitsprozesse von Unternehmen integriert und erleichtert Prozesse von der Finanzverwaltung bis zum Verkauf von Produkten. Viele Aktivitäten werden heute über digitale Kanäle abgewickelt, wodurch die Gefahr von Cyberangriffen gestiegen ist. Umso wichtiger ist es für Unternehmen, in Softwaresicherheit zu investieren.

Was ist Softwaresicherheit?
Ziel der Softwaresicherheit ist es, die mit der Nutzung von Software verbundenen Risiken zu minimieren und vor Angriffen zu schützen, denn unsichere Software gefährdet die Integrität, Authentifizierung und Verfügbarkeit von Daten und Anwendungen. Softwaresicherheit beinhaltet Prozesse und Mechanismen, die sicherstellen sollen, dass die Software funktionsfähig und widerstandsfähig bleibt, zum Beispiel wenn sie von Viren oder Malware angegriffen wird.

Diese Techniken werden bereits bei der Entwicklung und den Testprozessen von neuer Software eingesetzt. Die Absicht ist, Software zu entwickeln, die ohne zusätzliche Sicherheitselemente geschützt ist – obwohl diese in den meisten Fällen erforderlich sind. Durch die Testprozesse werden Schwachstellen aufgedeckt und behoben, bevor das Produkt auf den Markt kommt. Anschliessend ist es wichtig, die Benutzer:innen im sicheren Umgang mit der Software zu schulen, damit sie Angriffe erkennen und sich davor schützen können. Softwaresicherheit ist ein Prozess, der in jeder Phase des Software-Lebenszyklus stattfindet, von der Erstellung bis zur Nutzung.

> **Softwaresicherheit gewinnt zunehmend an Bedeutung, da die Nutzung von Software zunimmt und das Risiko von Cyberangriffen steigt. Unsichere Software ist anfällig für Hackerangriffe von innen und aussen sowie für Betriebsspionage.**

Softwaresicherheit wird immer stärker betont
Softwaresicherheit gewinnt zunehmend an Bedeutung, da die Nutzung von Software zunimmt und das Risiko von Cyberangriffen steigt. Unsichere Software ist anfällig für Hackerangriffe von innen und aussen sowie für Betriebsspionage. Darüber hinaus kann es erhebliche finanzielle Schäden verursachen, indem es die Verfügbarkeit von Anwendungen einschränkt und möglicherweise zu Produktionsausfällen führt.

Eine weitere Gefahr besteht darin, dass Daten gestohlen oder manipuliert werden können, sei es durch Phishing oder durch Angriffe auf Cloud-Services. Dies kann zu Datenschutzverletzungen führen, die mit Bussgeldern geahndet werden können. Vertrauliche Daten, sowohl von Kund:innen als auch von Unternehmen, müssen geschützt werden. Dies ist auch wichtig, da sich ein Datenleck negativ auf das Vertrauen der Kundschaft auswirkt und dem Ruf der Firma schadet. In letzter Zeit häufen sich Phishing-Vorfälle und Angriffe auf Cloud-Services.

Sicherheit bei der Herstellung
Wer Sicherheitssoftware selbst herstellt, sollte bewährte Sicherheitsverfahren anwenden. Zudem sollten Anwendungstests regelmässig durchgeführt werden, um potenzielle Schwachstellen zu identifizieren. Diese sollten behoben oder gepatcht werden, sobald sie entdeckt werden. Softwaresicherheit muss in allen Phasen des Entwicklungsprozesses berücksichtigt werden. Ausserdem müssen die Verantwortlichkeiten klar zugewiesen werden. Die sichere Herstellung von Software kann durch Tools und Services unterstützt werden, die beispielsweise Schwachstellen im Code oder zwischen Anwendungen und ihren Schnittstellen identifizieren.

Sicherheitsverfahren entwickeln sich laufend weiter und es ist unerlässlich, über diese Veränderungen informiert zu bleiben. Diese Verfahren sind jedoch kompliziert und zeitaufwendig, deshalb lohnt es sich für viele Unternehmen, in Sicherheitssoftware von Drittanbietern zu investieren. Dabei sollte Sicherheit ein wichtiger Faktor bei der Entscheidung sein.

Text **Valeria Cescato**

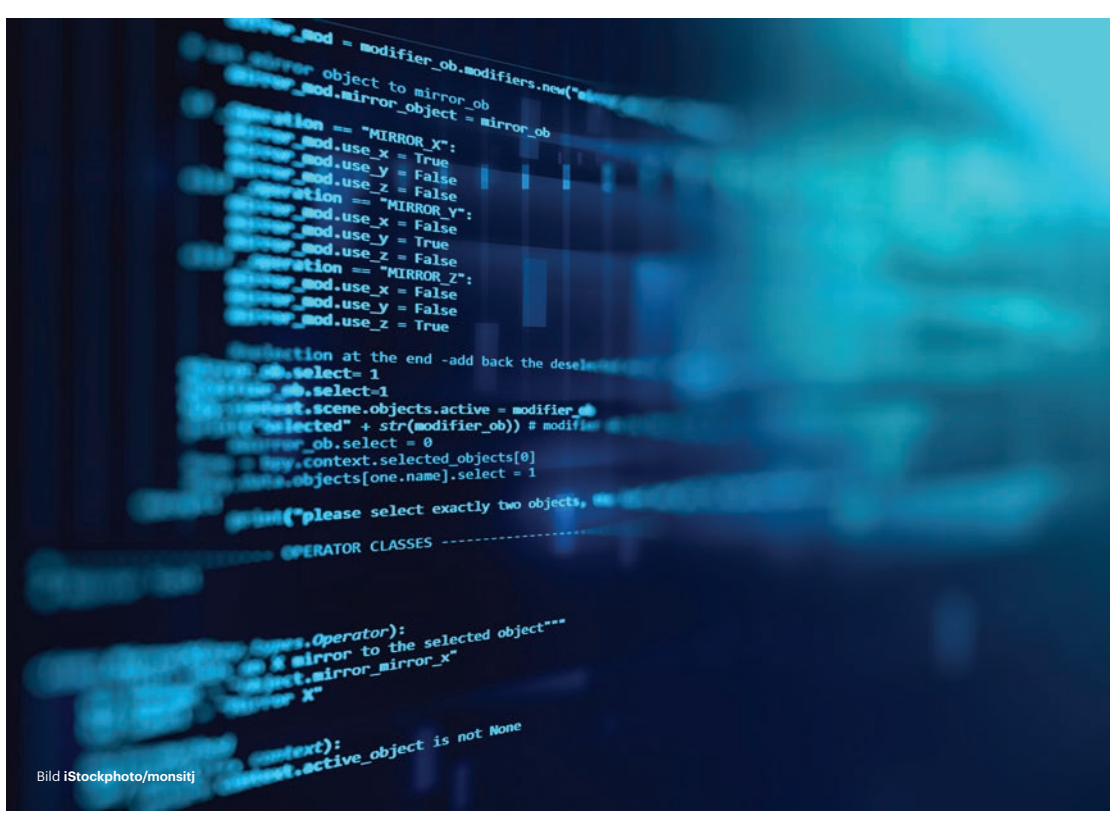


Bild iStockphoto/monsitj

Best Practices für Softwaresicherheit
Die meisten Unternehmen betreiben Anwendungssicherheit. Sie erhalten ihre Softwaresicherheitsprogramme von Drittanbietern und ihre Sicherheitsprotokolle befassen sich mit der sicheren Anwendung. Damit dies funktioniert, ist es wichtig, eine Strategie zu entwickeln und diese laufend zu aktualisieren.

Einige Beispiele für Best Practices im Bereich der Softwaresicherheit sind:

Least-Privilege-Prinzip: Das bedeutet, dass die Benutzer:innen nur eingeschränkten Zugang zu den Programmen haben und nur auf die Funktionen zugreifen können, die sie benötigen. Der Grund dafür ist, dass Hacker:innen nur so viel Zugriff auf das Programm haben wie die Benutzer:innen, die sie hacken. Durch eingeschränkte Zugriffsrechte kann so der Schaden minimiert werden.
Verschlüsselung von Softwaredaten: Datenverschlüsselung schützt Daten, indem sie in ein unlesbares Format umgewandelt werden. Wenn ein:e Hacker:in Zugriff auf die Daten hat, benötigt er oder sie auch den Verschlüsselungsschlüssel, um sie nutzen zu können. Daher ist es wichtig, dass alle gespeicherten und übertragenen Softwaredaten verschlüsselt werden.
Software aktualisieren & patchen: Software sollte auf dem neuesten Stand gehalten und regelmässig gepatcht werden, da jede Software Probleme haben kann, die oft von Hacker:innenn ausgenutzt werden. Für grosse Unternehmen können Wartungs- und Inventarisierungstools hilfreich sein, um den Überblick zu behalten.
Automatisieren: Die Infrastruktur muss regelmässig überprüft werden. Dies ist komplex, zeitaufwendig und für grosse Unternehmen manuell nicht machbar. Daher ist es sinnvoll, diese Aufgabe durch Sicherheitssoftware zu automatisieren, die dann Sicherheitskonfigurationen überprüft oder Änderungen an der Firewall analysiert.
Sicherheitsplan: Auch das beste Sicherheitssystem kann versagen, daher ist es wichtig, einen Plan für den Fall eines Angriffs zu haben. Der Plan sollte beschreiben, was im Falle eines Angriffs zu tun ist, wie ein Angriff erkannt wird, wie der Schaden begrenzt wird und was zu tun ist, um zur Normalität zurückzukehren.
Dokumentieren, Überwachen, Messen: Richtlinien sollten schriftlich festgehalten werden und für alle zugänglich sein. Zudem sollten Protokollierungs- und Überwachungsfunktionen implementiert werden, um Sicherheitsvorfälle in Echtzeit zu erkennen und darauf zu reagieren, einschliesslich unbefugter Zugriffsversuche, ungewöhnlichen Verhaltens und Verstösse gegen Sicherheitsrichtlinien.

Cybersecurity mit Schweizer Präzision: AGON PARTNERS setzt neue Standards

AGON INNOVATION – Über 15 Jahre Erfahrung Pioniere der Cybersecurity
Mit über 15 Jahren Erfahrung ist die AGON PARTNERS ein führender Anbieter von Cybersicherheitslösungen mit Sitz in Wilen bei Wollerau. Unser Unternehmen steht für Schweizer Präzision, technologische Exzellenz und höchste Datenschutzstandards. Unsere Expertise reicht von Multi-Faktor-Authentifizierung (MFA) über Identitätsmanagement bis hin zu massgeschneiderten Compliance-Lösungen, die vollständig in der Schweiz entwickelt und gehostet werden. Der ganzheitliche 360°-Ansatz von AGON PARTNERS vereint innovative Technologien mit einem tiefen Verständnis für die menschliche Komponente der Cybersicherheit.

Cyberangriffe: Die Gefahr, die Ihr Unternehmen zerstören kann

Angriffe treffen Unternehmen dort, wo es am meisten schmerzt: Daten, Prozesse, Vertrauen. Die Kosten für Wiederherstellung und Ausfallzeiten sind erst der Anfang – Reputationsverluste und rechtliche Konsequenzen gefährden langfristig die Existenz. Und eines ist sicher: Ohne Strategie ist es nur eine Frage der Zeit, bis Sie getroffen werden.

Cybersicherheit: Kein Kostenpunkt, sondern ein Wettbewerbsvorteil
Technologien wie Multi-Faktor-Authentifizierung, Zero Trust und KI-Bedrohungserkennung schützen nicht nur Systeme, sondern stärken Vertrauen und Resilienz. Unternehmen, die handeln, sichern ihre Zukunft – Unternehmen, die warten, riskieren alles.

Versicherungen? Ohne Sicherheit wertlos
Cyberversicherungen federn Schäden ab, doch ohne Zero Trust und moderne Schutzmassnahmen sind sie oft nutzlos. Versicherer verlangen klare Nachweise – wer diese nicht erbringt, zahlt teuer oder bleibt ungeschützt.

Die Botschaft ist klar
Warten ist keine Option. Jeder Angriff gefährdet nicht nur Ihre Systeme, sondern Ihr gesamtes Geschäft. Wer in Sicherheit investiert, gewinnt Vertrauen und Resilienz – und das Fundament für nachhaltigen Erfolg. **Die Frage ist nicht, ob Sie handeln, sondern wie schnell.**

Strategien für Unternehmen: Schutz durch Innovation und Weitblick

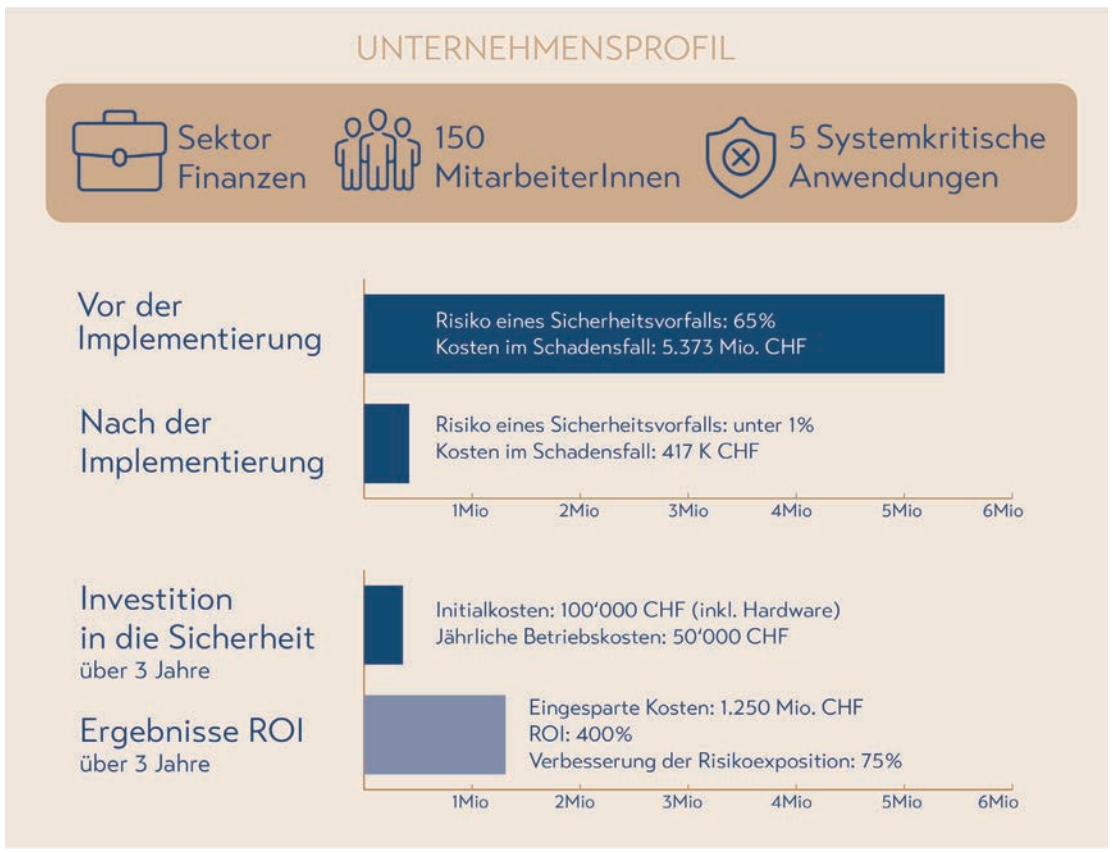
Sensible Daten als Schwachstelle und Chance
Daten sind der Treibstoff moderner Unternehmen – und zugleich eine der grössten Schwachstellen. Angriffe auf Kundendaten oder Geschäftsgeheimnisse gefährden nicht nur das Tagesgeschäft, sondern auch die Grundlage des Unternehmens. Moderne Cybersicherheitsstrategien setzen auf eine Mehrschicht-Architektur: Verschlüsselung und Multi-Faktor-Authentifizierung schützen sensible Informationen und senden ein klares Signal an Kunden und Partner: „Ihre Daten sind sicher."

Regulatorische Anforderungen als Wettbewerbsvorteil
Gesetze wie NIS2 und DORA zwingen Unternehmen, Sicherheitsmassnahmen und interne Prozesse zu verbessern. Doch statt diese Vorgaben als Belastung zu sehen, sollten sie als Chance genutzt werden. Unternehmen, die proaktiv handeln, sichern sich nicht nur Compliance, sondern auch einen Vorteil gegenüber dem Wettbewerb.

Best Practices: Technik trifft auf Kultur
Sicherheitsmassnahmen wirken nur, wenn Mensch und Technik zusammenarbeiten. Studien zeigen, dass menschliches Versagen für die meisten Sicherheitsvorfälle verantwortlich ist. Regelmässige Schulungen und Phishing-Simulationen reduzieren dieses Risiko deutlich. Ein von uns betreutes Unternehmen konnte die Erfolgsquote von Angriffen innerhalb eines Jahres um über 60 % senken – dank eines Sicherheitsprogramms, das Technologie und Mitarbeiter sensibilisiert.

Führungsebene in der Verantwortung
Cybersicherheit ist kein rein technisches Thema, sondern eine strategische Aufgabe des Managements. Führungskräfte müssen Ressourcen bereitstellen, Verantwortlichkeiten definieren und regelmässig überprüfen, ob die Sicherheitsstrategie aktuellen Bedrohungen standhält.

Vision: Unternehmen, die Cybersicherheit als langfristige Investition betrachten, schützen nicht nur ihre Systeme, sondern schaffen Vertrauen und Resilienz – die Grundlage für nachhaltigen Erfolg in einer digitalen Welt.



«Unser Unternehmen steht für Schweizer Präzision, technologische Exzellenz und höchste Datenschutzstandards.»

Cybercrime-Trends: Unsichtbare Bedrohungen, klare Lösungen

Cyberangriffe haben eine neue Ära erreicht. Sie sind nicht mehr die Tat einzelner Hacker, sondern hochprofessionelle Operationen, die gezielt Schwachstellen in Unternehmen jeder Grösse ausnutzen. Von Ransomware über Phishing bis hin zu Angriffen auf Lieferketten – die Methoden werden immer ausgeklügelter, die Bedrohung immer präsenter.

Die häufigsten Angriffsmethoden

1. **Ransomware:** Kritische Daten werden verschlüsselt, Unternehmen mit Lösegeldforderungen erpresst. Ein Ausfall über Tage oder Wochen kann für viele existenzbedrohend sein.
2. **Phishing und Social Engineering:** Täuschend echte E-Mails verleiten Mitarbeiter, sensible Informationen preiszugeben. Über 90 % aller Datenschutzverletzungen basieren auf menschlichen Fehlern.
3. **Angriffe auf Lieferketten:** Schwachstellen bei Zulieferern oder Partnern werden genutzt, um in grössere Netzwerke einzudringen. Eine ungesicherte Verbindung kann eine gesamte Wertschöpfungskette gefährden.

Die Konsequenzen

- **Finanzieller Schaden:** Hohe Kosten durch Lösegeldforderungen, Datenverluste oder langwierige Betriebsunterbrechungen.
- **Reputationsverlust:** Kunden und Partner verlieren das Vertrauen, was den langfristigen Erfolg gefährdet.
- **Regulatorische Strafen:** Unternehmen, die Vorgaben wie NIS2 oder DORA nicht erfüllen, riskieren empfindliche Geldstrafen.

Die unterschätzte Gefahr
Besonders alarmierend ist die zunehmende Bedrohung kritischer Infrastrukturen wie Energieversorger oder das Gesundheitswesen. Hier können Angriffe weitreichende Folgen haben und die Stabilität ganzer Systeme gefährden.

Die Lösung: Jetzt handeln statt abwarten
Angesichts dieser Bedrohungen ist eines klar: Warten ist keine Option. Unternehmen, die jetzt handeln, sichern nicht nur ihre Systeme, sondern auch ihre Zukunft. Unsere praxiserprobten Lösungen bieten einen umfassenden Schutz vor den wachsenden Gefahren:

- **Zero-Trust-Modelle** verhindern unbefugten Zugriff durch strikte Prüfungen für Nutzer und Geräte.
- **KI-gestützte Bedrohungserkennung** erkennt und neutralisiert Angriffe, bevor Schaden entsteht.
- **Phishing-resistente Authentifizierung** wie YubiKey schützt zuverlässig vor Identitätsdiebstahl.

Mit der **Swiss Made Cybersecurity Suite** und führenden Partnern wie Yubico und PEXIP setzen wir bei **AGON PARTNERS** neue Massstäbe. Unsere Strategien kombinieren modernste Technologie mit bewährter Expertise, um Unternehmen nicht nur abzusichern, sondern auch Vertrauen und Resilienz aufzubauen.

Die Botschaft ist klar: Cybersicherheit ist keine Option, sondern eine Notwendigkeit. Wer wartet, riskiert nicht nur Millionen, sondern auch das Vertrauen seiner Kunden. Mit uns haben Sie die **Lösung – heute, nicht morgen**.

Innovationen und Technologien: Die Zukunft der Cybersicherheit

Technologiegetriebene Cybersicherheit: Prävention statt Reaktion

- **Künstliche Intelligenz (KI):** KI erkennt Bedrohungen wie verdächtige Login-Versuche oder Datenabflüsse in Echtzeit und neutralisiert Angriffe, bevor Schäden entstehen. Proaktive Sicherheit ist Kern unserer Lösungen.
- **Blockchain:** Manipulationssichere Technologien schützen Datenflüsse und sichern Lieferketten – ideal für Branchen mit höchsten Sicherheitsanforderungen wie Logistik und Gesundheitswesen.
- **Zero Trust:** Kontinuierliche Authentifizierung verhindert unbefugten Zugriff und stärkt hybride Arbeitsumgebungen. Sicherheit und Effizienz nahtlos integriert.

Unsere Swiss Cyber Security Suite kombiniert diese Technologien, minimiert Risiken und gewährleistet Compliance – effizient, ohne hohe Kosten und Komplexität.

Zukunftssicher handeln
Mit Technologien wie Quantenkryptografie legen wir schon heute die Basis für morgen. Unsere Lösungen sind nicht nur praxiserprobt, sondern stärken das gesamte Unternehmen – jetzt und in der Zukunft.

Cybersicherheit: IT darf nicht Teil des Problems sein
Wir sind überzeugt: Sicherheit, die nur für die IT funktioniert, scheitert. Komplexe Lösungen, die Anwender überfordern, öffnen Tür und Tor für Fehler – von Passwiederverwendung bis zur Umgehung von Richtlinien. Genau hier liegt der Kern des Problems.

Unsere Lösungen sind anders: Sie sind für die Menschen gebaut, nicht für IT-Abteilungen. Einfach, intuitiv, effektiv – damit Sicherheit selbstverständlich wird. Mit unserer Swiss Cyber Security Suite machen wir Schutz unsichtbar, aber unverzichtbar. Denn echte Sicherheit beginnt nicht bei der IT, sondern bei den Anwendern.

Unser Versprechen: Mit der Swiss Cyber Security Suite bieten wir modernste Technologie, praxiserprobte Lösungen und klare Kostenkontrolle. Wir reduzieren Sicherheitsrisiken, ohne die Effizienz zu beeinträchtigen – für Unternehmen jeder Grösse. Handeln Sie jetzt und sichern Sie nicht nur Ihre IT, sondern Ihren nachhaltigen Erfolg.

Unsere 360°-Leistungen: Sicherheit ganzheitlich gedacht

Die AGON PARTNERS vereint Technologie, Prozesse und Menschen zu einem lückenlosen Schutzkonzept. Unser Ansatz: effizient, praxiserprobt und zukunftssicher.

- **Multi-Faktor-Authentifizierung & Identitätsmanagement:** Nur autorisierte Nutzer erhalten Zugang zu kritischen Systemen.
- **Verschlüsselte Kommunikation:** Sensible Informationen sind in allen Kanälen geschützt.
- **Proaktive KI-Bedrohungserkennung:** Angriffe abwehren, bevor Schaden entsteht.
- **Compliance & Audit-Support:** Sicher durch regulatorische Anforderungen.

Sicherheit aus einer Hand – umfassend und wirkungsvoll.

Echte Innovation kommt selten von denen, die nur verkaufen
Grosse Anbieter fokussieren sich auf Umsatz, nicht auf Ihre Sicherheit. Wir denken anders: Unsere Lösungen basieren auf Expertise, nicht auf Verkaufstricks. **Das Resultat? Keiner unserer Kunden hat je einen Breach erlitten.** Denn wir liefern keine Produkte von der Stange, sondern individuell angepasste Sicherheit, die wirklich schützt.

Weitere Informationen unter:
agon-solution.ch
071 999 22 92

Patrick Krauskopf, Chairman,
AGON GROUP

Tobias Gurtner, CEO,
AGON PARTNERS INNOVATION AG

Leslie Gurtner, CEO,
AGON PARTNERS SOLUTION AG

AGON PARTNERS INNOVATION

Bild iStockphoto/metamorworks

Unternehmen müssen sich selbst und ihre Stakeholder schützen – so gehts

Corporate Security soll ein Unternehmen nicht nur vor kriminellen Handlungen wie Cyberattacken schützen, sondern auch die Schwachstellen entlang der Wertschöpfungskette identifizieren. Sie soll die Sicherheit von Mitarbeitenden, Vermögenswerten und sensiblen Informationen gewährleisten.

Wie kann sich ein Unternehmen schützen?
Organisationen benötigen ein Sicherheitskonzept. Dieses soll Massnahmen enthalten, die die Sicherheit des Betriebes und seiner Stakeholder wie Mitarbeitende, Kund:innen und Lieferanten gewährleistet. Aber auch die Vermögenswerte und Reputation sowie unternehmensinterne Informationen sollen dadurch geschützt werden. Indem Gefahrenstellen entlang der Wertschöpfungskette – beispielsweise in der Produktion oder der Lieferung – identifiziert werden, soll die Unternehmensfortführung sichergestellt werden. Nur so kann ein Gefühl der Sicherheit und Vertrauenswürdigkeit in und um ein Unternehmen entstehen.

Auch ein Corporate/Chief Security Officer (CSO) ist in einem Unternehmen notwendig. Sie sind für die organisatorischen, rechtlichen, versicherungstechnischen, physischen, umweltspezifischen, IT-technischen, personellen, arbeitssicherheitstechnischen und gesundheitlichen Aspekte der Sicherheit zuständig. Sie sind verantwortlich für die Identifizierung, Bewertung und Priorisierung der Risiken eines Unternehmens. Anschliessend initiieren sie Massnahmen, um die Sicherheit des Betriebes zu gewährleisten. Bestenfalls leiten sie ein Team aus Datenschutzbeauftragten, Sicherheitsbeauftragten, Cloud- und IT-Security-Manager:innen und Krisenmanager:innen.

> **«Organisationen benötigen ein Sicherheitskonzept. Dieses soll Massnahmen enthalten, die die Sicherheit des Betriebes und seiner Stakeholder wie Mitarbeitende, Kunden und Lieferanten gewährleistet.**

Damit all diese Richtlinien und Schulungen auch verstanden werden, ist eine adressatengerechte Kommunikation auf Augenhöhe vonnöten. Dafür arbeitet die Sicherheitsabteilung im Optimalfall mit der internen Kommunikation zusammen.

Corporate Security – wofür?
Das Ziel der Corporate Security ist, Unternehmen vor finanziellen und rufschädigenden Belastungen zu schützen. Durch proaktive Sicherheitsmassnahmen können potenzielle Risiken minimiert und somit teure Sicherheitsvorfälle vermieden werden. Werden beispielsweise sensible Daten geleakt, kann auch das Vertrauen der Kundschaft in das Unternehmen schwinden. Langfristige Geschäftsbeziehungen sind plötzlich gefährdet.

Ein effektives Sicherheitskonzept kann Kundschaft und Partner beruhigen, das Vertrauen in die Integrität des Unternehmens stärken und somit als Wettbewerbsvorteil dienen. Das Ziel ist eine Kultur der Sicherheit, die über technologische Lösungen hinausreicht. Denn nur wenn die Sicherheit ein integraler Bestandteil der Unternehmensphilosophie ist, entsteht wahrhaftige Resilienz.

Text **Linda Carstensen**

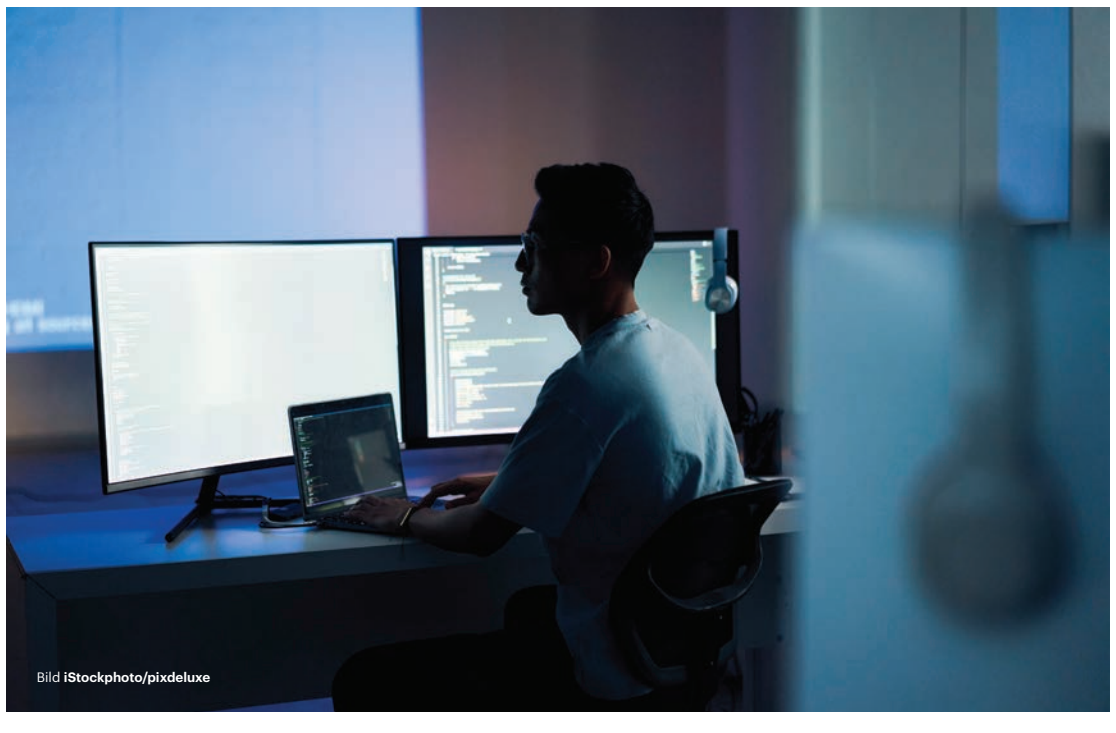


Bild iStockphoto/pixdeluxe

Es gibt mehrere Herausforderungen für das Corporate-Security-Team

Cyberkriminalität
Cyberkriminelle Angriffe sind eine zunehmende Bedrohung für Unternehmen. Datenlecks – wenn vertrauliche Informationen unbeabsichtigt oder aufgrund von Sicherheitslücken an die Öffentlichkeit gelangen – gehören zu den häufigsten Vorkommnissen. Auch bösartige Softwarearten wie Ransom- oder Malware kommen regelmässig vor. Oder Phishing-Versuche, die darauf abzielen, durch gefälschte E-Mails oder Nachrichten an sensible Daten zu gelangen. Um solche Cyberbedrohungen abzuwehren, braucht ein Unternehmen ein Bündel an Schutzmechanismen wie Firewalls, Verschlüsselungstechnologien und Sicherheitsschulungen für die Mitarbeitenden. Das Bundesamt für Cybersicherheit (BACS) hat ein Merkblatt für KMU erstellt, das ihnen helfen soll, die Informationssicherheit im Unternehmen zu erhöhen.

Verhalten der Mitarbeitenden
Die Sicherheit eines Unternehmens steht und fällt mit dem Verhalten seiner Mitarbeitenden. Unbeabsichtigtes, aber auch absichtliches Fehlverhalten können Sicherheitslücken entstehen lassen und somit Cyberangriffe und Datenverluste begünstigen. Um dies zu verhindern, sind einerseits Schulungen und Richtlinien zur Sensibilisierung der Mitarbeitenden beispielsweise für einen verantwortungsvollen Umgang mit Unternehmensinformationen notwendig. Andererseits sollten Mitarbeitende immer wieder auf fahrlässiges Verhalten überprüft werden.

Physische Sicherheit
Diebstahl, Einbruch und Vandalismus können erhebliche finanzielle und operationelle Schäden verursachen. Auch Gewalt und sexuelle Belästigung am Arbeitsplatz sind ernst zu nehmende Probleme, die die Sicherheit und das Wohlbefinden der Mitarbeitenden bedrohen. Um diesen physischen Bedrohungen entgegenzuwirken, können Unternehmen Zutrittskontrollsysteme, Überwachungskameras, Alarmanlagen und Sicherheitsschulungen einführen. Das Gleichstellungsgesetz (GIG) verpflichtet alle Arbeitgebenden in der Schweiz, die eigenen Mitarbeitenden vor Diskriminierungen zu schützen, präventive Massnahmen zu ergreifen und Belästigungen zu stoppen.

Um Übergriffe zu verhindern, sollten Arbeitgeber ein Merkblatt mit den wichtigsten Punkten zum Schutz vor sexueller Belästigung erstellen. Zudem müssen sie sicherstellen, dass alle Vorgesetzten und Mitarbeitenden den Inhalt des Merkblatts kennen und verstehen. Dieses Informieren sollte regelmässig wiederholt werden. Betroffene Frauen und Männer müssen sich im Fall einer sexuellen Belästigung an eine kompetente Ansprech- oder Vertrauensperson wenden können. Diese soll Betroffene über ihre Rechte und Vorgehensmöglichkeiten aufklären und sie in einer schwierigen Situation unterstützen.

Globale Sicherheitsanforderungen
Für international tätige Unternehmen ist die Sicherheit ungleich komplexer: Sie müssen sich an verschiedene rechtliche und kulturelle Rahmenbedingungen anpassen. Internationale Reisen und grenzüberschreitender Handel erfordern beispielsweise eine sorgfältige Planung und Anpassung an lokale Vorschriften. Hierbei geht es nicht nur um die Einhaltung internationaler Datenschutzgesetze, sondern auch um das Verständnis kultureller Unterschiede im Geschäftsverkehr und bei der Mitarbeiterführung.

Marcel Zumbühl

«Cybersicherheit ist mittlerweile zur DNA der Post geworden»

Die Post verbindet man in der Schweiz noch immer vornehmlich mit Brief- und Paketversand. Doch sie gehört auch zu den Betrieben, für die Cybersecurity in mehrfacher Hinsicht absolut essenziell ist. Marcel Zumbühl, Konzern-CISO der Post, erklärt, worauf dies zurückzuführen ist. Und warum so viele Cyberattacken mit gefälschtem Namen der Post verübt werden.

Interview **SMA**

Herr Zumbühl, das Thema «Cybersicherheit» ist für Unternehmen aller Branchen und Grössen relevant. Inwiefern betrifft es die Schweizerische Post?
Wir sind sogar in hohem Masse davon betroffen. Dies einerseits, weil es sich bei der Post um eine systemkritische Infrastruktur handelt. Der Schutz vor Attacken aus dem Web muss dementsprechend hohe Priorität für uns haben. Und andererseits wird die Post leider häufiger als jedes andere Schweizer Unternehmen als Vehikel benutzt, um Menschen mit Betrugsnachrichten anzugreifen.

Aus welchem Grund wählen denn Cyberangreifende gerade die Post so häufig als vermeintlichen Absender von Betrugsnachrichten?
Das hat mit der – an sich äusserst positiven – Tatsache zu tun, dass wir in der Bevölkerung ein hohes Mass an Vertrauen geniessen. Und wer mithilfe von Phishingmails an vertrauliche und sensible Informationen gelangen möchte, versucht natürlich, sich diese durch Vertrauen zu erschleichen. Dafür nutzen viele unseren etablierten Markennamen. Dies betrifft im Übrigen nicht nur uns: Seit der Coronapandemie werden sämtliche nationalen Postservices hierfür missbraucht, von Japan bis in die USA. Natürlich wollen wir die Leute so gut es geht vor solchen Angriffen schützen, weswegen Cybersecurity ein essenzielles Thema für uns darstellt.

Von wie vielen solchen Angriffen, die fälschlicherweise im Namen der Post verübt werden, sprechen wir?
Wir registrieren pro Monat bis zu 280 «Angriffswellen». Und jede davon trifft zumindest einige Personen. Meist werden Nachrichten versendet, welche die Empfängerinnen und Empfänger dazu anhalten, einen Link anzuklicken. Auf der verlinkten Landingpage werden dann Handynummer, Kreditkarteninfos usw. nachgefragt. Genau hier setzen wir an: Unsere IT- und Cybersecurity-Profis nehmen pro Tag bis zu fünf solcher Seiten vom Netz. Dann führt, selbst wenn jemand einen solchen Link anklickt, der Angriff ins Leere. Cybersicherheit ist mittlerweile zur DNA der Post geworden. Dies auch, weil wir die nationale Nummer zwei im öffentlichen Verkehr sind, E-Voting anbieten, als Dienstleister für das Digitale Patientendossier agieren sowie als Finanzdienstleister tätig sind. In all diesen Bereichen spielt die Cybersecurity eine essenzielle Rolle. Und auch unsere eigenen Infrastrukturen gilt es zu schützen: Die Schweizerische Post betreibt über zehn grosse Brief- und Paketcenter sowie zwei Rechenzentren. Um auf einer so breiten Front die bestmögliche Sicherheit zu gewährleisten, haben wir immer wieder neue Ideen aufgegriffen und Pionierleistungen erbracht.

Können Sie hierfür ein Beispiel anführen?
Wir gehörten zu den ersten Unternehmen, die im Rahmen von Bug-Bounty-Programmen die eigenen IT-Infrastrukturen rund um die Uhr durch Hackerinnen und Hacker auf Herz und Nieren prüfen liessen. Wir prüfen aber nicht nur IT auf Lücken, wir schauen uns auch Fahrzeuge an. So haben wir mithilfe von Experten die Cybersecurity unserer Postautos untersucht. Wir versuchen also, Gefährdungsszenarien gezielt weiterzudenken. Hierfür nehmen wir einerseits die Perspektive unserer Kundschaft ein und betrachten die Fälle andererseits auch aus der Sicht der Angreifenden. Wir erachten Cybersecurity also nicht einfach als einen Zustand, den man erreicht und dann aufrechterhält. Vielmehr handelt es sich um einen fortlaufenden Prozess mit dem Ziel, eine echte, kundenzentrierte Sicherheit bieten zu können.

Wie machen Sie bei der Post «Sicherheit» zum Teil der Unternehmenskultur?
Ich sehe den Menschen als das wichtigste und stärkste Glied in der Sicherheitskette. Denn wir Menschen können ein Sensor sein für Abläufe, die sich nicht richtig anfühlen. Doch damit Angestellte und Teammitglieder diese Rolle ausüben können, müssen wir eine Kultur schaffen, die Fehler nicht straft, sondern eine transparente Kommunikation fördert. Bei der Post trainieren wir deshalb regelmässig, ob unsere Mitarbeitenden Phishing-Angriffe erkennen – und ob sie es melden, wenn sie fälschlicherweise einen Link angeklickt haben. Eine von drei Personen meldet uns das zurück. Und ja: Auch mir als CISO (Chief Information Security Officer) ist es schon passiert, dass ich einen solchen Link betätigt habe. Solange ich aber transparent kommuniziere und alarmiere, können wir ein Learning daraus ziehen und Massnahmen einleiten. Das muss der Kern einer jeden Sicherheitskultur sein.

Wie sensibilisieren Sie die Kundschaft der Post für ein sicheres Verhalten im Web?
Zum einen müssen wir dem Sicherheitsaspekt von Anfang an in unseren Produkten und Dienstleistungen Rechnung tragen. Und zum anderen geht es darum, unseren Kundinnen und Kunden zu vermitteln, worauf sie achten müssen, wenn sie sich online bewegen. Hierzu führen wir regelmässig Informationskampagnen durch. Ein Thema, das wir künftig sicherlich vertieft behandeln werden, betrifft Deepfakes und KI. Hier lautet eine unserer aktuellen Empfehlungen etwa, dass man bei einem Video darauf achten sollte, ob kleine Fehler auftauchen, wie eine verschwindende Hand vor dem Gesicht, Fehler bei Profilbildern etc. Denn noch sind die KI-Deepfakes nicht perfekt.

Welche künftigen Trends und Entwicklungen zeichnen sich allgemein im Bereich Cybersecurity am Horizont ab?
Zum einen wird uns der Umgang mit neuen Technologien beschäftigen. Ein aktuelles Beispiel liefert das Thema Quantencomputing. Diese Technologie macht die Verschlüsselungsverfahren von heute obsolet. Dies wird vielleicht zum Ende der Dekade der Fall sein. Daher müssen wir uns schon heute mit neuen Verschlüsselungsverfahren auseinandersetzen. Anderseits bietet die Quantentechnologie auch die Chance, Informationen über grosse Distanzen abhörsicher zu übertragen. Wie bei jeder Technologie bieten sich also Chancen und Risiken. Ein weiteres Thema der Zukunft ist die identitätsbasierte Sicherheit. Unternehmen werden immer durchlässiger, sowohl was Menschen, aber auch Systeme anbetrifft, weswegen Unternehmen laufend prüfen müssen, wer sich darin aufhält und ob diese Menschen wirklich diejenigen sind, die sie zu sein vorgeben. Eine Eingangskontrolle reicht dafür nicht mehr aus, sondern man wird laufende Verifizierungsprozesse implementieren müssen.

Das gesamte Interview mit Marcel Zumbühl finden Sie online unter:

Fakten zur Cybersecurity bei der Post
Rund 100 Mitarbeitende kümmern sich bei der Post um die Cybersecurity. Hierfür wendet das Unternehmen rund 25 Millionen jährlich auf. Das Post-Team wehrt monatlich über 100 gezielte Hackerangriffe, gut 280 Phishing-Wellen gegen Kund:innen wie auch rund zehn Millionen Spam- und Phishingmails ab.

Effektive Risikominimierung in unsicheren Zeiten

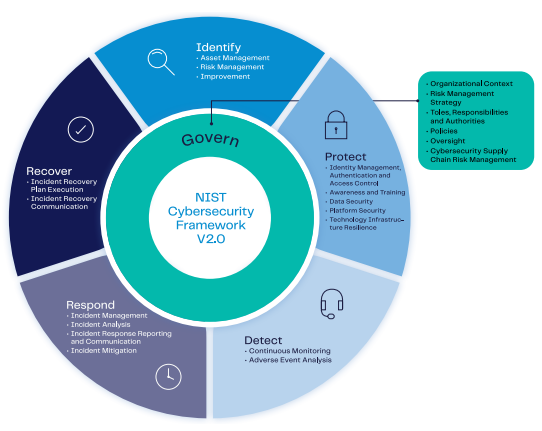
Risikomanagement ist heute ein wesentlicher Bestandteil der strategischen Planung und der Informationssicherheit. Angesichts zunehmender Cyberbedrohungen und komplex vernetzter Risiken setzen Unternehmen auf flexible Prozesse und innovative Technologien. Meti Rudaj, Expert Consultant bei Aveniq, gibt dazu spannende Einblicke.

Meti Rudaj
Expert Cyber Security Consultant bei Aveniq

Meti Rudaj, welche Massnahmen ergreift Aveniq, um sich gegen die zunehmenden Cyberbedrohungen abzusichern?
Wir verfolgen einen ganzheitlichen Ansatz gegen zunehmende Cyberbedrohungen. Informationssicherheit und Risikomanagement sind laufende Prozesse, die regelmässig überprüft werden. Prozess-Owner analysieren Risiken in ihren Bereichen, und die Risikomanagerin konsolidiert diese auf Gruppenebene, um Klumpenrisiken zu erkennen. Wir orientieren uns am NIST-2.0-Standard für eine umfassende Sicht auf Informationssicherheit.

In welchen Bereichen sehen Sie die grössten Herausforderungen bei der Einbindung externer Partner in Ihr Risikomanagement?
Eine der grössten Herausforderungen bei der Einbindung externer Partner sind die zunehmend komplexen regulatorischen Anforderungen sowie die wachsenden Lieferantenketten, insbesondere durch die Migration in Cloud-Umgebungen. Aveniq setzt daher auf einen umfassenden, aber gleichzeitig schlanken Lieferantenmanagement-Prozess, der den Fokus auf Compliance und Risikomanagement legt.

Welche neuen Herausforderungen erwarten Sie im Risikomanagement angesichts der zunehmenden Digitalisierung und globalen Vernetzung?
Die zunehmende Digitalisierung und Vernetzung führt zu einer grösseren Komplexität der Datenflüsse und einer stärkeren Abhängigkeit von Lieferanten. Ein gutes Beispiel dafür ist der Crowdstrike-Vorfall im Jahr 2024, der gezeigt hat, wie sich Vorfälle auch auf unbeteiligte Dritte auswirken können. Daher ist es wichtig, diese Abhängigkeiten im Risikomanagement sauber aufzuzeigen und zu managen.



Eine Risikobewertung nach dem NIST-Standard hilft dabei, potenzielle Sicherheitsrisiken zu erkennen und ihre Auswirkungen zu bewerten.

Welche Pläne und Massnahmen haben Sie entwickelt, um bei einer schwerwiegenden Sicherheitsverletzung schnell und effektiv zu reagieren?
Aveniq hat einen zweistufigen Incident-Management-Prozess etabliert. Dieser umfasst einen Master-Incident-Prozess, der kritische Vorfälle über ein teamübergreifendes Modell koordiniert. Sollte ein Vorfall eskalieren, übernimmt ein interner Krisenstab die Kontrolle. Wir sind zudem nach ISO 22301 (Business Continuity Management) und ISO 20000 (Service Continuity) zertifiziert, was unsere Fähigkeit zur Bewältigung von Krisen weiter unterstreicht.

Wie fördern Sie eine Kultur des Risikobewusstseins innerhalb der Organisation und wie wird dies auf allen Ebenen des Unternehmens kommuniziert?
Aveniq fördert eine Kultur des Risikobewusstseins durch ein umfassendes Informationsmanagement-System, das verschiedene Sicherheitsdisziplinen abdeckt. Zudem bieten wir regelmässig Schulungen und interne Informationskampagnen an, um sicherzustellen, dass das Risikobewusstsein auf allen Ebenen der Organisation verankert ist. Unsere ISO-Zertifizierungen und ISAE-Berichte tragen ebenfalls dazu bei, dass diese Kultur kontinuierlich überprüft und verbessert wird.

Weitere Informationen unter:
aveniq.ch

AVENIQ

Lassen Sie Worte Worte bleiben indem Sie Ihr Unternehmen schützen!

Verhindern Sie, dass Cyber-Bedrohungen Realität werden – mit dem gezielten Security Awareness-Training für Sie und Ihre Mitarbeitenden.

In einer zunehmend digitalen Welt sind Cyberangriffe eine allgegenwärtige Bedrohung, die mehr und mehr auch kleine und mittlere Unternehmen (KMUs) gefährden. Das international tätige IT-Unternehmen KYBERNA AG mit Hauptsitz im liechtensteinischen Vaduz bietet ein umfassendes Coaching-Programm an.

Warum Cyber Security Awareness?
Die digitale Transformation bringt viele Vorteile, aber auch erhebliche Risiken mit sich. Cyberangriffe werden immer raffinierter und gezielter. Phishing, Ransomware und Social Engineering sind nur einige der Bedrohungen, denen Unternehmen täglich ausgesetzt sind. Ein einziger erfolgreicher Angriff kann verheerende Auswirkungen haben – von finanziellen Verlusten bis hin zu schwerem Reputationsschaden.

Umso wichtiger ist es, dass Ihre Mitarbeitenden geschult und sensibilisiert sind. Sie sind die erste Verteidigungslinie gegen Cyber-Bedrohungen. Ein gut geschultes Team kann potenzielle Angriffe erkennen und abwehren, bevor sie Schaden anrichten.

KMUs sind täglich verschiedenen Cyber-Bedrohungen wie Phishing, Ransomware, Malware und vielen mehr ausgesetzt. Handeln Sie jetzt!

Cyber-Expertise für Ihr Unternehmen
KYBERNA's Security Awareness Training ist mehr als nur ein Kurs. Es ist ein umfassendes, nachhaltiges Schulungsprogramm mit simulierten Phishing-Plattformen. Jeder Mitarbeitende absolviert das Awareness-Training eigenständig vor seinem Computer, individuell und nicht in Gruppen, um gezielt und flexibel auf Cyber-Bedrohungen vorbereitet zu werden. Dieses Programm bietet umfassenden Schutz vor Cyberbedrohungen durch:

- **Interaktive Schulungsmodule:** Realistische Szenarien und praxisnahe Inhalte schärfen das Bewusstsein der Mitarbeitenden für Cybergefahren.
- **Phishing-Simulationen:** Regelmässige, simulierte Phishing-Angriffe helfen, das Erlernte anzuwenden und die Reaktionsfähigkeit zu verbessern.
- **Kontinuierliche Weiterbildung:** Laufende Updates und neue Inhalte sorgen dafür, dass die Belegschaft stets informiert bleibt.
- **Messbare Ergebnisse:** Fortschritte werden kontinuierlich überwacht und dokumentiert, um den Schulungserfolg sicherzustellen.

Ein überzeugendes Angebot für alle Unternehmen
Das Beste daran: Dieses Training ist nicht exklusiv für KYBERNA-Kunden. Unabhängig davon, wer Ihr IT-Dienstleister ist, können Sie das Trainings-Abo für Ihre Mitarbeitenden buchen. Die Vorteile auf einen Blick:

- **Sicherheit durch Wissen:** Mitarbeitende sind die erste Verteidigungslinie gegen Cyberangriffe.
- **Kostenersparnis:** Prävention ist günstiger als die Behebung von Cyberangriffen.
- **Vertrauensgewinn:** Kunden und Partner vertrauen Unternehmen mit gut geschulten Mitarbeitenden mehr.

Die gängigsten Cyber-Bedrohungen im Überblick
KMUs sind täglich verschiedenen Cyber-Bedrohungen ausgesetzt. Zu den häufigsten zählen:

Phishing
Betrügerische E-Mails oder Webseiten, die darauf abzielen, vertrauliche Informationen wie Passwörter, Kreditkartennummern oder andere persönliche Daten zu stehlen. Diese Angriffe sind oft schwer zu erkennen, da sie sehr professionell gestaltet sind und legitim erscheinen können. Schulungen helfen Mitarbeitenden, verdächtige Merkmale solcher Nachrichten zu identifizieren und angemessen zu reagieren.

Ransomware
Diese Schadsoftware verschlüsselt die Dateien auf einem infizierten System und verlangt ein Lösegeld für die Freigabe. Ransomware kann über verschiedene Wege, wie infizierte Anhänge oder unsichere Downloads, ins System gelangen. Eine geschulte Belegschaft kann verdächtige Aktivitäten frühzeitig erkennen und verhindern, dass Ransomware sich verbreitet.

***Social Engineering*:**
Angreifer nutzen psychologische Manipulation, um Mitarbeitende dazu zu bringen, sicherheitsrelevante Informationen preiszugeben oder sicherheitskritische Aktionen durchzuführen. Dies kann durch Telefonanrufe, E-Mails oder sogar persönliche Interaktionen geschehen. Ein tiefes Verständnis und Bewusstsein über diese Techniken kann Mitarbeitende davor schützen, auf solche Tricks hereinzufallen.

Malware
Schadsoftware, die Systeme infiziert, Daten stiehlt oder zerstört. Malware kann in verschiedenen Formen auftreten, einschliesslich Viren, Würmern und Trojanern. Regelmässige Schulungen und Sicherheitsübungen helfen dabei, die Mitarbeitenden für die Risiken und die Erkennung von Malware zu sensibilisieren.

Jetzt handeln!
Cyberbedrohungen kennen keine Pause. Jeder Tag, an dem Ihre Mitarbeitenden ungeschult bleiben, erhöht das Risiko für Ihr Unternehmen. Mit KYBERNA's Security Awareness Training investieren Sie nicht nur in die Sicherheit, sondern auch in die Zukunftsfähigkeit Ihres Unternehmens. Machen Sie jetzt den entscheidenden Schritt, um Ihr Unternehmen vor den stetig wachsenden Cybergefahren zu schützen.

Weitere Informationen zum Cyber Security Awareness Training sind unter **www.kyberna.ch/training** verfügbar.

«Security Awareness Training ist nicht nur eine Investition in Technologie; es ist eine Investition in Menschen. Als CISO ist es unsere Verantwortung sicherzustellen, dass jedes Mitglied unserer Organisation die Bedeutung von Informationssicherheit versteht und die Fähigkeiten besitzt, diese zu schützen. Denn die stärkste Firewall ist nutzlos, wenn der Mensch dahinter nicht geschult ist.»

– Daniel Link,
Chief Information Security Officer und Leiter Cloud & IT Services, KYBERNA AG

Über KYBERNA
KYBERNA AG – vom Lokalpionier zum internationalen Player in der Softwarebranche

Seit der Gründung vor bald 40 Jahren hat sich die KYBERNA AG vom regionalen Internetprovider zum international agierenden Softwarehersteller und IT-Systemhaus entwickelt. Seit 1999 mischt KYBERNA mit der hauseigenen IT- und Enterprise Service Management Software «ky2help®» den deutschsprachigen Markt auf. Zu Beginn als reine IT-Ticketing Software wird die Lösung heute im gesamten DACH-Raum sowie im Südtirol von über einer Million Usern verschiedener Branchen zielführend genutzt. Die Eigenentwicklung trägt dabei einen wichtigen Teil zur Digitalisierung der unternehmensweiten Arbeitsprozesse bei. Weiter spezialisiert sich KYBERNA auf


Ihre Mitarbeitenden müssen geschult und sensibilisiert sein, denn Sie sind die erste Verteidigungslinie gegen Cyber-Bedrohungen. Ein gut geschultes Team kann potenzielle Angriffe erkennen und abwehren, bevor sie Schaden anrichten.

zukunftsfähige IT-Infrastrukturlösungen für KMUs – einschliesslich Server- und Cloud-Technologien – und bietet professionellen Support. Eine Online-Auktions-Software rundet das Produktportfolio ab. Diese ermöglicht Kunden, Ihre individuelle Versteigerungsplattform im eigenen Corporate Design zu erstellen. Egal was Unternehmen verkaufen möchten, die webbasierte Auktionsplattform ist einfach zu bedienen und für jede Branche die perfekte Wahl. Weitere Details zu den Produkten finden Sie unter www.kyberna.ch

Weitere Informationen zum Cyber Security Awareness Training:

KYBERNA
Weil funktionierende IT glücklich macht

Bild iStockphoto/da-kuk

Wie ein Kulturwandel Cybersicherheit ermöglicht

Cybersicherheit ist ein komplexes, aber unverzichtbares Thema, das in der heutigen digitalen Welt zunehmend an Bedeutung gewinnt. Michael Müller, CEO eines führenden ICT-Dienstleistungsunternehmens, betont im Interview mit «Fokus», dass Unternehmen, die Cybersicherheit fest in ihre Abläufe integrieren, besser vor Angriffen geschützt sind und im Ernstfall schnell sowie effektiv reagieren können.

Michael Müller
CEO

Cybersicherheit ist kein Projekt, das man einmal abschliesst und dann wieder vergisst. Es ist vielmehr ein kontinuierlicher Prozess, der stetig angepasst werden muss. Die Bedrohungen ändern sich rasch, so auch die Technologie. Um mit diesen Veränderungen Schritt zu halten, müssen Unternehmen kontinuierlich in Know-how und Schulungen investieren. Es ist wichtig, regelmässig neue Trends zu beobachten und die eigenen Systeme anzupassen, um schliesslich nicht den Anschluss zu verlieren.

Michael Müller, mit welchen Schwierigkeiten haben Unternehmen in Bezug auf Cybersicherheit zu kämpfen?
Unternehmen stehen heute vor grossen Herausforderungen, wenn es um Cybersicherheit geht, welche stark von den verfügbaren Unternehmensressourcen abhängig sind. Eine der grössten Hürden sind die finanziellen Ressourcen, wie beispielsweise das Budget. Ausgaben für Cybersicherheit können nicht wieder zurückgewonnen werden, dennoch ist es wichtig, ausreichend in diesen Bereich zu investieren. Denn Unternehmen, die dies nicht tun, riskieren im Falle eines Angriffs wesentlich höhere Kosten. Das Budget wirkt sich natürlich auf die technologischen Ressourcen aus, die eine wesentliche Rolle spielen. Aber auch menschliche, zeitliche und organisatorische Ressourcen dürfen nicht vergessen werden, denn sie sind für die erfolgreiche Umsetzung von Sicherheitsmassnahmen von unschätzbarem Wert.

> «Eine der grössten Schwachstellen in puncto Cybersicherheit sind oft tatsächlich die eigenen Mitarbeitenden.
>
> – Michael Müller, CEO

Welche Massnahmen binden die Mitarbeitenden effektiv in die Cybersicherheitsprozesse ein?
Eine der grössten Schwachstellen in puncto Cybersicherheit sind oft tatsächlich die eigenen Mitarbeitenden. Viele Unternehmen sprechen das Thema nur selten an, was für eine dauerhafte Veränderung nicht ausreicht. Viel effektiver sind monatliche Schulungen oder kurze, regelmässige Updates. Dies muss nicht unbedingt vor Ort geschehen, sondern kann beispielsweise auch über eine Plattform mit informativen Videos erfolgen. Solche Schulungen helfen, das Bewusstsein der Mitarbeitenden für die aktuellen, sich ständig ändernden Risiken zu schärfen. Eine einmalige Schulung gerät meist schnell in Vergessenheit, während eine kontinuierliche Weiterbildung die Lerninhalte im Gedächtnis hält.

Ein weiterer essenzieller Schritt sind Praxistests wie etwa Phishing-Simulationen. So können die Mitarbeitenden das Gelernte anwenden und das Unternehmen erhält wertvolle Hinweise, wo noch Lücken bestehen. Auch dies sollte mehrmals im Jahr stichprobenartig erfolgen, um das Wissen der Mitarbeiterinnen und Mitarbeiter auf dem aktuellen Stand zu halten.

Wie kann eine Kultur der Cybersicherheit geschaffen werden, die über die Einhaltung von Vorschriften hinausgeht und ein proaktives Verhalten fördert?
Cybersicherheit muss ein Thema für alle Mitarbeitenden sein, die einen Account im Unternehmen haben. Um dies zu erreichen, muss eine Kultur und ein Bewusstsein für das Thema geschaffen werden. Dabei kann es hilfreich sein, einen internen Helpdesk einzurichten, an den sich Mitarbeitende bei Zweifeln oder Fragen wenden können. Wichtig ist, dass Fehler akzeptiert werden und niemand Angst vor Konsequenzen haben muss, wenn ein möglicher Vorfall gemeldet wird. Eine Kultur, die einen offenen Umgang mit Fehlern fördert, trägt wesentlich zur Sicherheitsstrategie des Unternehmens bei.

Wie kann ein Gleichgewicht zwischen Sicherheitsmassnahmen, Unternehmensproduktivität und Benutzerfreundlichkeit erreicht werden?
Es ist unvermeidlich, dass Sicherheitsmassnahmen bis zu einem gewissen Grad die Benutzerfreundlichkeit beeinträchtigen. Um die richtige Balance zu finden, muss jedes Unternehmen eine Risikoanalyse durchführen. Darauf aufbauend sollten die Massnahmen an die jeweilige Bedrohung angepasst werden. Je höher das Risiko, desto strikter sollten die Sicherheitsmassnahmen sein. Bei der Einführung solcher Verfahren ist eine klare und offene Kommunikation mit den Mitarbeitenden wichtig. Erklärt man den Zweck der Massnahmen und das potenzielle Ausmass der Schäden, wird die Akzeptanz deutlich erhöht.

Wie soll man im Falle eines Cyberangriffs reagieren?
Trotz aller Vorsichtsmassnahmen kann es zu einem Angriff kommen. In diesem Fall müssen sowohl das Unternehmen als auch die einzelnen Mitarbeitenden schnell reagieren. Wenn jemand bemerkt, dass etwas nicht stimmt, ist es wichtig, Ruhe zu bewahren und die internen Abläufe einzuhalten. Der erste Schritt sollte immer sein, die IT-Abteilung oder die verantwortliche Stelle zu informieren und deren Anweisungen zu befolgen. Das betroffene Gerät muss sofort von allen Netzwerken getrennt, aber nicht ausgeschaltet werden. Der Grund dafür ist, dass das forensische Team möglicherweise Zugriff auf Daten benötigt, die bei einem Neustart des Geräts verloren gehen könnten.

Es ist wichtig, dass das Unternehmen über einen klar definierten Notfallplan verfügt, der im Voraus geübt wurde. In diesem Plan sollte festgelegt sein, wer in welchem Fall welche Massnahmen zu ergreifen hat. Darüber hinaus muss es Pläne für die Geschäftskontinuität und die Wiederherstellung nach einem Zwischenfall geben. Im Ernstfall sollte das Unternehmen davon ausgehen, dass alle Systeme betroffen sein können, da der Angriff möglicherweise schon längere Zeit unbemerkt stattgefunden hat. Es ist daher ratsam, nicht nur den internen Notfallplan zu befolgen, sondern auch externe Prozesse und Absprachen mit Partnerunternehmen zu berücksichtigen. Insbesondere bei Lösegeldforderungen durch Ransomware kann es sinnvoll sein, externe Expert:innen hinzuzuziehen, die auf solche Vorfälle spezialisiert sind.

Text **Valeria Cescato**

UMB_Cyber Security Angel

Moderne und komplexe Angriffe sind heute an der Tagesordnung. Darum gehört das Thema Cybersecurity bei jeder Organisation ganz oben auf die Agenda. Selbst einfachste Dienste - wie eine Kopiermaschine, ein Drucker oder ein beliebiges anderes Bürogerät - können zum Einfallstor für Angriffe werden. Darum braucht es jemanden, der Sie hier berät und beschützt. Und dies nicht aus einer Perspektive, sondern als Teil einer Gesamtsicht auf Ihr Unternehmen. Genau das bietet der UMB Security-Angel als Teil des UMB Experten Teams und IT as a Service. **umb.ch**

UMB

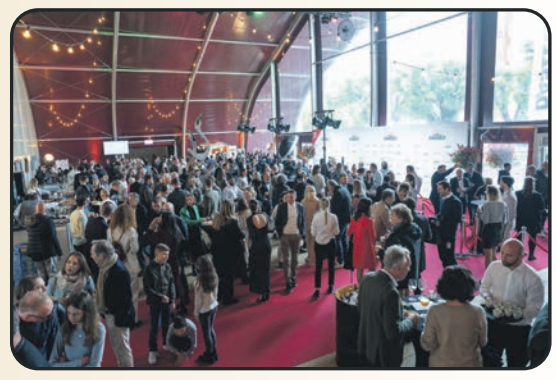
creating time®

DASZELT
INVEST

Werden Sie Teil von DAS ZELT, der grössten mobilen Kultur- und Eventplattform der Schweiz, welche Entertainment auf höchstem Niveau aus den Bereichen «Comedy, Concert & Circus» in alle Landes- und Sprachregionen bringt.

Ihre Vorteile:

- 9% Gutscheine oder 6.5% Zins
- Attraktive Prämien (Showtickets, Gold Packages, Backstage Führungen, Direktions Dinner, Meet & Greet)



Gleichzeitig tun Sie etwas Gutes:

- Förderung des Schweizer Nachwuchs im Bereich der darbietenden Kunst
- Soziale Integration durch Freikarten für weniger gut situierte Familien, Inklusion von Kindern mit Beeinträchtigung in Shows
- Investitionen in klimaschonende Infrastruktur

«DAS ZELT – der erfolgreichste Unterhaltungsbetrieb der Schweiz»
Blick, 07. September 2023

Investieren Sie jetzt in DAS ZELT
und werden Sie Teil der DAS ZELT-Family!

The Dome ist ausgestattet mit 1‘500 Sitzplätzen oder 5‘000 Stehplätzen.

daszelt.ch/invest

Adrian Steiner

Dr. Adrian Steiner
Direktor DAS ZELT