EINE PUBLIKATION VON SMART MEDIA

NOV 20

smartmedia

FOKUS.

SICHERHEIT

PREMIUM PARTNER
I see U — UMB Cyber Defense Center
UMB

Interview

FLORIAN SCHÜTZ

Delegierter des Bundes für Cybersicherheit

«Sicherheit geht uns alle an, sei es im privaten Rahmen oder im Arbeitsumfeld»

Lesen Sie mehr auf www.fokus.swiss

Sich nie in Sicherheit wiegen

Betrachten wir es für einmal von der positiven Seite: Die Coronapandemie hat einen längst fälligen Digitalisierungsschub ausgelöst. Wurde vor der Covid-19-Krise eher kritisch darüber nachgedacht, wie viel Homeoffice es denn sein darf, so ging alles auf einmal blitzschnell. Präsenzkultur ade – die Arbeit musste plötzlich zu Hause erledigt werden. Eine Herausforderung für die ganze Familie und den Arbeitgeber, der parallel dazu die digitale Infrastruktur auf- oder ausbauen musste. Vieles hat gut geklappt, auch wenn Zoom und Co. zuweilen mit dem teilweise langsamen Internetanschluss im Homeoffice Mühe haben. Solches lässt sich lösen. Gleiches gilt für einen anderen Punkt, den man nur zu gerne vergisst: die Ergonomie. Das Heimbüro will fachgerecht eingerichtet sein, mit der Gesundheit lässt sich nicht spassen. Der Arbeitgeber sollte dabei Unterstützung bieten!

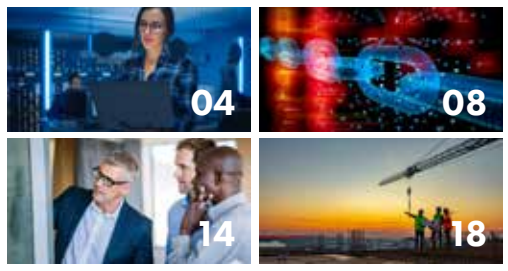
Ob zu Hause oder im Büro, die Welt wird digitaler und vernetzter, dadurch aber auch anfälliger. Wo nicht gut gesichert, lauern Schlupflöcher, die ambitionierten Hackern Tür und Tor öffnen, um ins IT-System einzudringen. In verschiedenen Branchen hat man erkannt, dass dieses Thema höchste Priorität hat. Sicherheitstechnische Einrichtungen wie Zutrittskontrollen oder Einbruchmeldeanlagen, um nur zwei Beispiele zu nennen, sind heutzutage meist in ein Gesamtsystem der Gebäudetechnik eingebunden. Wenn nur eine dieser Anwendungen in Sachen Cybersicherheit versagen würde, wäre der Schaden angerichtet. Seien Sie deshalb auf der Hut, wenn vollmundig von Smart Home und Smart Office geschwärmt wird. Was nicht niet- und nagelfest gegen Cyberkriminelle abgesichert ist, gehört nicht vernetzt.

Straftaten wie Einbruch und Diebstahl sind in der Schweiz seit Jahren rückläufig, nicht so die digitale Kriminalität. Sie ist im Aufwind, und landauf, landab müssen spezialisierte Polizeiteams aufgebaut werden, um den digitalen Gangstern das Handwerk zu legen. Wer im Computersystem, zu Hause oder im Unternehmen, einen Verschlüsselungstrojaner einfängt, hat nichts zu lachen. Die wertvollen Daten sind verloren, es sei denn, man bezahlt den modernen Raubrittern das geforderte Lösegeld.

> **Ob zu Hause oder im Büro, die Welt wird digitaler und vernetzter, dadurch aber auch anfälliger.**
>
> - ROGER STRÄSSLE, CHEFREDAKTOR DER FACHZEITSCHRIFT «SICHERHEITSFORUM»

Ob Cyberrisiko, Pandemie, Brand oder ein durch Hochwasser überflutetes Firmengebäude – auf solche Betriebsunterbrüche muss sich die weitsichtige Chefetage in «Friedenszeiten» vorbereiten; im Fachjargon ist die Rede von Business Continuity Management. Im Ernstfall müssen die Verantwortlichen möglichst schnell Plan B zücken können. Für viele Unternehmen kamen Instrumente wie ein Pandemieplan erst kürzlich zum Zug, und es kann gut sein, dass mit den jüngsten Erfahrungen das eine oder andere Kapitel im Krisenhandbuch umgeschrieben werden muss. Gab es Engpässe bei der Lieferkette? Konnte die Firma rasch ein Notlager errichten, damit die Servicemonteure trotzdem noch halbwegs funktionieren konnten, ohne die Kundschaft zu verärgern? Muss im Krisenfall die Firma in Zukunft mit Mitbewerbern zusammenarbeiten, um sich gegenseitig mit Ressourcen inklusive Manpower auszuhelfen? Fragen über Fragen, denen sich das verantwortungsvolle Management stellen muss. Wie resilient ein Unternehmen ist, zeigt sich meist im Ernstfall. Und klar ist auch: Nach der Krise ist vor der Krise.

TEXT **ROGER STRÄSSLE**



LESEN SIE MEHR...

FOKUS SICHERHEIT.

PROJEKTLEITUNG:
Margrith Scherrer
COUNTRY MANAGER:
Pascal Buck
PRODUKTIONSLEITUNG:
Miriam Dibsdale
TEXT:
Fatima Di Pane, Lars Meier, Patrik Biberstein
TITELBILD:
Keystone, Gaëtan Bally
LAYOUT:
Anja Cavelti
DISTRIBUTIONSKANAL:
Tages-Anzeiger, November 2020
DRUCKEREI:
DZZ Druckzentrum AG

SMART MEDIA AGENCY AG
Gerbergasse 5, 8001 Zürich, Schweiz
Tel +41 44 258 86 00
info@smartmediaagency.ch

gedruckt in der schweiz

Viel Spass beim Lesen!
Margrith Scherrer
Project Manager

Phishing-Mails erkennen und abwehren

Phishing-Mails sind immer noch eine der grössten Cybergefahren für Unternehmen. Im Interview erklärt Cornelia Lehle, Sales Director G DATA Schweiz, wie eine Phishing-Simulation den Status der IT-Sicherheit messbar macht und wie Security Awareness Trainings die Sicherheit im Unternehmen verbessern.

Cornelia Lehle

> **Cyberkriminelle verfolgen beim Phishing ein klares Ziel.**

Cornelia Lehle, warum müssen Unternehmen ihre Mitarbeiter für das Thema IT-Sicherheit sensibilisieren?
Cybercrime ist heutzutage rein wirtschaftlich orientiert und versucht dementsprechend mit möglichst geringem Aufwand den maximalen Profit zu generieren. Daher wird in der Regel das schwächste Glied in der Verteidigungsstrategie eines Unternehmens angegriffen, was sehr oft die Mitarbeiter sind. Daher müssen Unternehmen das Thema IT-Sicherheit ganzheitlich betrachten. Neben technischen Sicherheitsmassnahmen sollten sie ihre Mitarbeiter in die Verteidigungsstrategie integrieren.

Warum sind Menschen für Phishing-Kampagnen anfällig?
Cyberkriminelle verfolgen beim Phishing ein klares Ziel. Sie wollen, dass Menschen vertrauliche Informationen wie etwa Login-Daten preisgeben, auf einen Link klicken oder einen Mailanhang öffnen. So erhalten die Angreifer am Ende Zugriff auf Nutzerkonten, wie beispielsweise das E-Mail-Postfach oder können die Systeme mit Schadsoftware infizieren. Dabei nutzen sie das menschliche Verhalten konsequent aus. Im Unternehmensumfeld gehört der Umgang mit Bewerbungen auf ausgeschriebene Stellen oder Rechnungen zur Tagesordnung. Angreifer nutzen das gezielt aus, weil Mitarbeiter bei solchen Routinearbeiten schneller unaufmerksam sind.

Gleichzeitig werden Phishing-Kampagnen immer raffinierter. Die Gefahr gezielter Attacken ist gestiegen. So spähen die Angreifer in Sozialen Medien oder auf der Firmen-Homepage ihr Opfer aus und erstellen darauf aufbauend eine massgeschneiderte Phishing-Mail. In dieser nehmen sie etwa auf eine Veranstaltung Bezug, die ein Mitarbeiter besucht hat. Solche so genannten Spear-Phishing-Mails sind von echten Nachrichten kaum zu unterscheiden.

Wie können Unternehmen ihre Mitarbeiter unterstützen, damit sie keine Phishing-Mails anklicken?
Das Bewusstsein der Angestellten für IT-Sicherheitsrisiken zu verbessern, ist ein langfristiger Prozess. Regelmässige und umfangreiche Security Awareness-Trainings sind dabei ein adäquates Mittel. Wenn sich die Angestellten der Risiken bewusst sind, handeln sie vorsichtiger und gehen kritischer mit Mails um. Gleichzeitig haben sie dann auch Verständnis für Passwort-Vorgaben und andere sicherheitsrelevante Themen.

Welche Rolle spielen Phishing-Simulationen im Rahmen von Security Awareness Trainings?
Bei Phishing-Simulationen können Angestellte Erfahrungen mit gefährlichen Mails sammeln. Die Unternehmen können gleichzeitig den Awareness-Stand ihrer Mitarbeiter messen. Ein Reporting zeigt dem Verantwortlichen, ob und wie viele Mitarbeiter eine gefährliche Mail geöffnet und sogar den enthaltenen Link angeklickt haben. Damit ist klar, wie gross der Handlungsbedarf ist. Anschliessend sollten Firmen Security Awareness Trainings durchführen. Um das Bewusstsein der Mitarbeiter für Cybergefahren nachhaltig zu verbessern, sollten die Trainings regelmässig wiederholt werden. Nach circa drei Monaten sollte das Wissen erfahrungsgemäss aufgefrischt werden.

Weitere Informationen:
www.gdata.ch

Cyber Security Specialists: die Hacker, die für Sicherheit sorgen

Im November 2020 treten die ersten Fachpersonen zur eidgenössischen Berufsprüfung an, um den offiziell anerkannten Berufstitel «Cyber Security Specialist mit eidgenössischem Fachausweis» zu erwerben. Die praxisnahe, handlungsorientierte Berufsprüfung ist in ihrer Form ein Novum. Teilnehmende werden im Hacking-Lab mit simulierten Cyber-Attacken konfrontiert und müssen ihre Führungs- und Managementkompetenzen unter Beweis stellen. Durchgeführt wird die Prüfung von ICT-Berufsbildung Schweiz.

Immer wieder werden Organisationen Opfer von unerlaubten Zugriffen aus dem Cyber-Raum, was enorme Schäden wie Datenverluste oder Dienstleistungsausfälle zur Folge haben kann. Um kritische Informations- und Kommunikationssysteme entsprechend abzuschirmen und Cyber-Angriffe zu bewältigen, sind konkrete Schutzmassnahmen nötig, die von qualifizierten Spezialistinnen und Spezialisten ausgearbeitet und umgesetzt werden: den Cyber Security Specialists. Als Teil des ICT-Managements analysieren sie laufend die aktuelle Bedrohungslage im Cyber-Raum, antizipieren Risiken oder Schwachstellen und handeln mit präventiven oder reaktiven Schutzmassnahmen. Mit der ersten Berufsprüfung im November 2020 werden dem Arbeitsmarkt dringend benötigte Cyber Security Specialists mit eidgenössischem Fachausweis zugänglich gemacht.

Die Prüfung: praxisnah und handlungsorientiert
Die eidgenössische Berufsprüfung wird unter der Trägerschaft von ICT-Berufsbildung Schweiz, dem nationalen Verband für die berufliche Grundbildung und höhere Berufsbildung in der Informatik und Mediamatik, durchgeführt. Die einzelnen Prüfungsteile werden in Zusammenarbeit mit fachlich spezialisierten Organisationen erarbeitet, was eine hohe Prüfungsqualität garantiert. Die Prüfung ist stark praxisorientiert und besteht aus drei Teilen: «Cybersicherheit», «Projekte & Betriebswirtschaft» sowie «Führung & Kommunikation».

Teil 1: Cybersicherheit
Der erste Prüfungsteil findet an der Hochschule für Technik in Rapperswil (HSR) im virtuellen «Hacking-Lab» statt. Das Hacking-Lab ist eine Cyber Security Simulation, die durch das Schweizer Security Unternehmen Compass Security in Zusammenarbeit mit der Hochschule für Technik in Rapperswil entwickelt und betrieben wird. Dieses stark handlungsorientierte, praxisnahe Prüfungssetting stellt ein absolutes Novum dar. Die Kandidatinnen und Kandidaten werden simulierten aber wirklichkeitsgetreuen Bedrohungslagen ausgesetzt, wobei sie Schwachstellen in realen Systemen aufdecken und mit der Abwehr konkreter Cyber-Attacken konfrontiert werden.

Teil 2: Projekte & Betriebswirtschaft
Im zweiten Teil werden Projektmanagement und berufsspezifische betriebswirtschaftliche Aspekte geprüft. Dazu müssen realitätsnahe Praxissituationen schriftlich bearbeitet werden. Dabei zeigen die Teilnehmenden unter anderem ihre Fähigkeit, Projekte unter Berücksichtigung der gegebenen Ressourcen zu planen, leiten und überwachen, relevante Stellen bezüglich Sicherheitslösungen zu beraten und Aufwände für Sicherheitslösungen zu kalkulieren.

Teil 3: Führung & Kommunikation
Im dritten Prüfungsteil werden die persönlichen und sozialen Kompetenzen überprüft, über die ein Cyber Security Specialist verfügen sollte. Der Fokus liegt auf den Bereichen Teamführung und Kommunikation. Überprüft werden diese Handlungskompetenzen im Rahmen einer mündlichen Fallbearbeitung und eines Fachgesprächs. Dieser Prüfungsteil wird in Kooperation mit der Schweizerischen Vereinigung für Führungsausbildung SVF geprüft.

Wer eignet sich zum Cyber Security Specialist?
Die Berufsausübung erfordert zusätzlich zu fundierten Fachkenntnissen eine rasche Auffassungsgabe, ein hohes Mass an Analytik, System- und Prozessdenken, Diskretion, Integrität, Verantwortungsbewusstsein, Durchhaltewille, Frustrationstoleranz und ausgeprägte Kommunikations- und Teamfähigkeiten. Der Fachausweis richtet sich an Fachleute mit mehrjähriger Berufserfahrung auf dem Gebiet der Informations- oder Cybersicherheit. Die berufsbegleitende Weiterbildung wird von verschiedenen Ausbildungsstätten angeboten: bzb, Cisco CyberSecurity Academy, gibb, IFA, ISEIG, SATOM, SIW, Swiss Cyber Forum und WISS. Bei der Erstdurchführung der Prüfung werden hauptsächlich Absolvierende der SIW, die als erste in die Ausbildung gestartet sind, sowie Cyber-Lehrgang-Absolvierende der Armee teilnehmen. Letztere können sich die militärische Führungsausbildung an die Prüfung anrechnen lassen. Mit dem eidgenössischen Fachausweis werden die im Lehrgang angeeigneten Kompetenzen eidgenössisch zertifiziert.

Unabhängig geprüfte Handlungskompetenzen
Die Prüfungsabsolventinnen und -absolventen haben beste berufliche Aussichten, sowohl in der Privatwirtschaft als auch in öffentlichen Institutionen. Mit der digitalen Transformation in allen Branchen nimmt der Bedarf an spezialisierten Security-Fachkräften weiter zu. Cyber Security Specialists bewegen sich in einem hochsensiblen Arbeitsfeld. Deshalb sind eidgenössische Zertifikate, welche unabhängig geprüfte Handlungskompetenzen ausweisen, ein entscheidender Vorteil sowohl für Prüfungsteilnehmende als auch für rekrutierende Unternehmen. Der Fachausweis wurde von ICT-Berufsbildung Schweiz in Zusammenarbeit mit der Schweizer Armee (Führungsunterstützungsbasis FUB), dem Staatssekretariat für Bildung, Forschung und Innovation (SBFI) sowie der Mobiliar und UBS entwickelt.

Hohe Einstufung im Nationalen Qualifikationsrahmen
Das Staatssekretariat für Bildung, Forschung und Innovation (SBFI) hat die von ICT-Berufsbildung Schweiz beantragte Einstufung auf Niveau 6 im Nationalen Qualifikationsrahmen (NQR) bestätigt. Damit wird der Qualität des Abschlusses und den hohen Anforderungen an die Absolvierenden Rechnung getragen. Die Einstufung im NQR vereinfacht die internationale Vergleichbarkeit des Berufstitels und weist dessen hohe Qualität aus. Die Diplomzusätze basieren auf europäischem Standard und sind somit Arbeitgebern in ganz Europa vertraut.

Weitere Informationen:
www.ict-weiterbildung.ch

ICT Berufsbildung
Formation professionnelle
Formazione professionale

Jedes Unternehmen kann Ziel von Cyberangriffen werden

Die Cybersicherheit ist ein Thema von enormer Wichtigkeit. Und doch vernachlässigen viele Unternehmen diesen Aspekt, teilweise mit fatalen Folgen. Nicole Wettstein, Vize-Präsidentin der Kommission Cybersecurity von ICTswitzerland, klärt auf.

TEXT **FATIMA DI PANE**

Nicole Wettstein

> **Auch die besten technischen Massnahmen können nicht verhindern, dass ein Mitarbeitender einem Angreifer Tür und Tor öffnet.**

Digitalisierungsprozesse machen vielen Unternehmen das Leben nicht nur leichter. Was nebenbei oftmals nicht ernst genommen, oder schlichtweg vergessen wird, ist die Cybersicherheit. «Viele KMU gehen davon aus, selbst kein attraktives Ziel für Cyberangriffe zu sein», erklärt Nicole Wettstein, Programm Manager Cybersecurity SATW, Vize-Präsidentin Kommission Cybersecurity ICTswitzerland. «Sie nehmen fälschlicherweise an, für Angreifer aufgrund ihrer Grösse oder der geringen Bekanntheit ein uninteressantes Opfer zu sein.»

So wird das Thema Cybersicherheit oftmals unter den Tisch gekehrt. «Den KMU ist dabei meist nicht bewusst, dass die Angreifer häufig nicht gezielt Unternehmen angreifen, sondern im Internet grossflächig nach Schwachstellen suchen und diese ausnutzen – unabhängig davon, wer dahinter steht», erläutert Wettstein.

Schweiz überdurchschnittlich stark betroffen

Als Zentrum von Forschung und Finanzen ist die Schweiz überdurchschnittlich stark von Cyberangriffen betroffen, auch zwecks Industriespionage. Der Status der Schweiz als wohlhabendes Land tut dabei sein übriges, um Cyberkriminalität anzuziehen. «Zudem sind viele KMU in der Schweiz im Bereich der Digitalisierung vergleichsweise weit fortgeschritten. Ihr Geschäftsmodell ist daher von einem funktionierenden IT-System abhängig. Ein Cybervorfall hat entsprechend schwerwiegende Auswirkungen», weiss Wettstein.

Ein Paradebeispiel für einen Cyberangriff mit schweren Auswirkungen ist die Ransomware-Attacke.

Daten gegen Lösegeld

«Mit einer Ransomware-Attacke nutzen Angreifer bestehende Sicherheitslücken in den Betriebssystemen aus und verschlüsseln die Daten ihrer Opfer, um eine Lösegeldzahlung für die Entschlüsselung der Daten oder für die Nichtveröffentlichung der zuvor gestohlenen Daten zu fordern», erklärt Wettstein. Eine der grossen Sicherheitslücken für Ransomware-Attacken besteht in veralteter Soft- und Hardware, deren Schwachstellen nicht mehr durch Patches und Updates ausgebessert werden. Auch das WLAN eines Unternehmens kann von Hackern für einen Angriff genutzt werden. «Es ist daher wichtig, dass Unternehmen ihr WLAN mit einem sicheren Standard verschlüsseln und für Gäste ein separates WLAN verwenden», rät Wettstein.

Risiko: Mensch

Auch wenn ein Unternehmen rundum gegen Cyberangriffe gewappnet ist, darf der Gefahrenfaktor Nummer eins nicht ausser Acht gelassen werden: der Mensch. «Auch die besten technischen Massnahmen können nicht verhindern, dass ein Mitarbeitender einem Angreifer Tür und Tor öffnet», weiss Wettstein.

Ein Beispiel dazu sind Phishing-E-Mails. Diese E-Mails werden von Hackern professionell gestaltet und sollen beispielsweise den Eindruck erwecken, von einer offiziellen Stelle zu stammen. Der Empfänger soll damit motiviert werden, sensible Daten freizugeben. Vor allem Zugangsdaten sind bei Hackern populär. «Mit diesen Informationen haben die Angreifer die Möglichkeit, auf die Konten ihrer Opfer zuzugreifen und so beispielsweise in deren Namen Einkäufe in Onlineshops oder Zahlungen im Online-Banking zu tätigen», erklärt Wettstein. Aus diesem Grund ist es wichtig, für verschiedene Onlinedienste unterschiedliche und starke Passwörter zu benutzen. Denn so kann der Angreifer mit einem geklauten Passwort nicht auf alle Dienste zugreifen.

Post vom CEO

Laut dem nationalen Zentrum für Cybersicherheit NCSC lässt sich momentan eine Zunahme von CEO-Fraud beobachten. Dabei werden E-Mails an Mitarbeitende verschickt, welche vermeintlich vom CEO stammen. «In den E-Mails werden sie zu bestimmten Handlungen wie beispielsweise der Zahlung eines hohen Geldbetrages verleitet», erzählt Wettstein.

Auch Malware gelangt in vielen Fällen über eine E-Mail ins System eines Unternehmens. «Mitarbeitende klicken auf Anhänge oder Links. Häufig handelt es sich dabei um Verschlüsselungstrojaner, welche die Daten auf dem Computer oder im Netzwerk verschlüsseln. Für die Entschlüsselung der Daten wird Lösegeld gefordert», führt Wettstein aus.

Individuelle Lösungen

Das Thema Cybersicherheit sollte also in jedem Unternehmen sorgfältig bedacht werden. Die Herangehensweise und Bedürfnisse unterscheiden sich aber zwischen den Unternehmen stark. «Es hängt von der Grösse, dem Schutzbedürfnis des Unternehmens und den vorhandenen Fähigkeiten und Ressourcen ab», erklärt Wettstein. Für ein KMU mit wenigen Mitarbeitenden und geringen Anforderungen an die IT-Systeme zahle sich ein eigenes Team für Cybersicherheit vermutlich nicht aus, während dies für ein anderes Unternehmen, das sehr stark vom Zugang zu den digitalen Dienstleistungen abhängig sei und mehrere Mitarbeitende beschäftigt, anders aussehen könne.

«Eine eindeutige Antwort auf diese Frage gibt es nicht und jeder Fall muss individuell beurteilt werden», stellt Wettstein fest. Auf jeden Fall sollte aber Schulungen, gezielter Sensibilisierung der Mitarbeitenden sowie technischen Lösungen gleichermassen Aufmerksamkeit geschenkt werden.

Covid-19 ist immer noch ein Gesundheitsrisiko für die IT-Infrastruktur

Covid-19 gefährdet nicht nur die Gesundheit, sondern auch die IT-Infrastruktur. Das ist nicht nur eine Behauptung von IT-Sicherheitsexperten, die das grosse Geschäft wittern, sondern eine Tatsache, die durch Zahlen belegt wird. Auch Interpol hat diesbezüglich eine globale Warnung veröffentlicht.

Gemäss der internationalen Polizeiorganisation haben Kriminelle tausende von neuen Websites kreiert, um im Zusammenhang mit der globalen Pandemie Spam-Kampagnen und Phishing-Attacken auszuführen oder Malware zu verbreiten. Es gebe eine beträchtliche Anzahl von registrierten Domains im Internet, die die Begriffe «Coronavirus», «Corona-Virus», «Covid19» und «Covid-19» enthalten. Die Angreifer hoffen, dass die Cyber-Abwehrmassnahmen vieler Unternehmen wegen der Krise geschwächt sind. Die Websites werden als Basis für die Verbreitung von Spyware und Trojanern benutzt – gemäss Interpol wurde solche Malware auch auf interaktiven Coronavirus-Karten gefunden.

IBM X-Force, eines der bekanntesten IT-Security-Forschungsteams überhaupt, beobachtete einen signifikanten Anstieg der Bedrohungslage. Die X-Force Teammitglieder überwachen und analysieren die IT-Sicherheitslage kontinuierlich und liefern mit den Resultaten die Grundlage für das IBM Sicherheitsportfolio. Ihre Erkenntnisse unterstreichen die Analyse von Interpol – IBM spricht im Zusammenhang mit der gegenwärtigen Situation in einem aktuellen Report gar von einem Cyber War.

Eine Covid-19-Spam-Explosion

Die X-Force-Spezialisten beobachteten einen mindestens 60-fachen Anstieg von Spam mit Coronavirus-Themen sowie den Verkauf von Malware im Dark Web bezogen auf die Coronakrise – sogar virusbezogene Rabattcodes würden angeboten. Die Forscher stellen fest, dass Domains, die im Zusammenhang mit Covid-19 stehen, mit 50 Prozent höherer Wahrscheinlichkeit bösartig sind als andere, im gleichen Zeitraum registrierte Domains. Auch Phishing-Aktivitäten haben zugenommen. Als Beispiel nennt X-Force eine Phishing-E-Mail, die es auf Kleinunternehmer abgesehen hat, die sich um einen Notkredit bewerben wollen.

Die Folgen solcher Angriffe können brutal sein. Die Tendenz zu überhasteten Entscheidungen in Krisenzeiten beschleunige die Möglichkeit für Kriminelle, Daten zu stehlen und Geschäftsabläufe zu kompromittieren, sagen die X-Force-Sicherheitsexperten. So kann zum Beispiel ein Denial-of-Service-Angriff (DDoS-Angriff) in einer bereits überlasteten Infrastruktur weitaus schädlicher sein als ein Angriff, der gestartet wird, wenn zusätzliche Kapazitäten leicht verfügbar sind.

Spitäler sind besonders gefährdet

Laut Interpol ist auch die Ransomware-Problematik wieder top-aktuell. Besonders gefährdet sind Krankenhäuser, medizinische Zentren und andere öffentliche Einrichtungen. Da sie von der gegenwärtigen Situation besonders gefordert werden und es sich nicht leisten können, aus ihren Systemen ausgesperrt zu werden, gehen die Angreifer davon aus, dass sie leichter zu ihrem Lösegeld kommen werden. Die Ransomware kommt auf die bekannte Art in die IT-Systeme: durch E-Mails mit infizierten Links oder Anhängen, durch kompromittierte Mitarbeiterdaten oder durch das Ausnutzen einer Schwachstelle im System.

Das aktuelle globale IT-Sicherheitsproblem betrifft natürlich auch Schweizer Unternehmen. Das Nationale Zentrum für Cybersicherheit des Bundes hält fest, dass Kriminelle versuchen, gezielt Ängste und Sorgen der Bevölkerung für ihre Machenschaften auszunützen. Gewarnt wird vor Phishing E-Mails, die angeblich von der World Health Organisation (WHO) oder dem Bundesamt für Gesundheit (BAG) stammen und auch vor Anrufen im Namen des Bundesamtes für Gesundheit (BAG), um an persönliche Informationen zu gelangen. Es gebe ausserdem vermeintliche Wohltätigkeitsorganisationen, die zu Spenden aufriefen, um einen Impfstoff für Covid-19 zu entwickeln und Onlineshops, die medizinische Produkte wie Schutzmasken anböten, die dann nicht geliefert werden.

Reihenweise Herausforderungen

Die Covid-19-Pandemie kam sehr schnell und sehr überraschend. Den geschäftlichen Herausforderungen waren (und sind) viele Beteiligte nicht gewachsen. Das ist kein Wunder: Die Situation brachte gleich reihenweise neue Herausforderungen und verlangte nach schnellen Problemlösungen. Was die IT-Sicherheitslage betrifft, kann UMB unterstützen und mit seinen Kunden sicherstellen, dass sie und ihre IT auch aussergewöhnlichen Situationen gewachsen sind. Das UMB Security Team kann das Risiko quantifizieren und den Sicherheitsgrad der Assets nach Kritikalität und Komplexität einordnen.

Weitere Informationen: **www.umb.ch**

UMB creating time®

Erschwingliche Cyber Security Services für KMUs – endlich!

Hacker machen auch vor KMUs nicht Halt. Im Gegenteil: Viele Schweizer KMUs sind in ihrer Nische marktführend und entsprechend interessant, weshalb sie in den letzten Monaten Ziele von Angriffen wurden.

Bisherige Cyber Security Services waren für KMUs in gewissen Branchen nicht erschwinglich. Mit den «Managed Security Services for SME» bietet bw digitronik besten Schutz zu einem adäquaten Preis.

Das oberste Ziel ist, dass die IT-Risiken eines Unternehmens identifiziert und überwacht werden können. In einem zweiten Schritt geht's darum, im Rahmen der Überwachung, die entsprechenden Schwachstellen der IT-Umgebung zu erkennen und mögliche Einfallstore für Angriffe so rasch als möglich zu schliessen. Doch auch wenn die IT-Abteilung einen guten Job gemacht hat, versuchen Hacker Wege zu finden, in Netzwerke einzudringen, um Systeme zu destabilisieren und vertrauliche Daten zu entwenden. Darum ist es wichtig, dass solche versuchten oder erfolgten Angriffe in Echtzeit erkannt und entsprechend geblockt werden. Ein rasches Handeln hilft, Schäden zu minimieren und die Kosten tief zu halten.

bw digitronik bietet mit den «Managed Security Services for SME» die entsprechenden Technologien, Prozesse und die Manpower mit der langjährigen Expertise, um auch KMUs einen erschwinglichen Cyber Schutz zu gewährleisten.

Weitere Infos:
www.managed-securityservices.ch
www.bwdigitronik.ch

bw digitronik
CYBERTECH GROUP

bw digitronik / Cybertech Group

bw digitronik ist seit über 30 Jahren in der IT-Security tätig und gehört zur europäischen Cybertech Group. Über 350 Cyber Security Spezialisten stehen für Ihre IT-Sicherheit bereit, davon 65 im Security Operation Center (SOC). Über 600 Kunden vertrauen auf unsere Expertise.

Freundlich bei Kunden, wehrhaft bei Angreifern: Die Vorteile einer intelligenten, vorgelagerten Security-Lösung

Können IT-Sicherheitslösungen wirklich agil sein? Und kann der Zielkonflikt zwischen Benutzerfreundlichkeit und Angreiferschutz zuverlässig gelöst werden? Darüber haben wir mit dem Security-Experten Roman Hugelshofer gesprochen. Seine Antwort: Ja, das ist möglich – und so nötig wie nie zuvor.

Roman Hugelshofer
Managing Director Application Security

Aus Ihrer Sicht als Security-Experte – was sind neben den allgemein bekannten Sicherheitsthemen die grossen Herausforderungen, mit denen Unternehmen heute konfrontiert sind?
Die gute Nachricht vorweg: IT-Security-Themen sind heute auf Geschäftsleitungsebene angekommen. Viele Unternehmen haben in den letzten Jahren spezialisierte Stellen und Abteilungen geschaffen, die oft direkt an die Geschäftsleitung rapportieren. Es gibt aber ein Schlagwort, das IT-Verantwortliche umtreibt – heute mehr denn je: Agilität. Unternehmen müssen heute schneller auf neue Anforderungen reagieren, sei es wegen neuer Bedrohungen oder auch wegen neuer Business-Initiativen. Wie schnell dieses Reagieren manchmal sein muss, hat sich gerade in den letzten Monaten gezeigt.

Sie sprechen die Corona-Pandemie an, die der Digitalisierung einen neuen Schub verliehen hat?
Ja, Covid-19 hat etwas beschleunigt, das die Unternehmen schon seit Längerem umtreibt: Die digitale Transformation. Was sich dabei besonders gezeigt hat, ist die Tiefe dieser Transformation. Denn während des Lockdowns ging es ja nicht nur darum, sich über Videoplattformen auszutauschen. Vielmehr war ein neues Arbeiten in verteilten Teams und die Möglichkeit zu Homeoffice gefragt. Deshalb wurden auch grundsätzliche Aspekte der IT-Infrastruktur tangiert, besonders hinsichtlich der Sicherheit.

Können Sie ein konkretes Beispiel nennen?
Viele unsere Kunden sind im Finanz- oder Versicherungsumfeld tätig – also in einem Bereich, in dem Sicherheit und Compliance-Standards sehr wichtig sind. Wenn die Mitarbeitenden einer Privatbank nun im Homeoffice arbeiten, dann sollten sie sich Kundendaten nicht einfach per WhatsApp zusenden. Dafür braucht es sichere und zuverlässige Tools, so dass die Angestellten jederzeit auf ihren Arbeitsplatz zugreifen können – sicher und vor externen Angriffen geschützt.

Das klingt spannend, denn Sie deuten hier neue Möglichkeiten der virtuellen Kollaboration an.
Sie sind nicht gänzlich neu, aber oft waren z.B. VPN's (Virtuelle private Netzwerke) zu wenig gut abgesichert, insbesondere was die Authentisierung betrifft. Das Grundproblem ist, dass sich nicht nur die Mitarbeitenden über Homeoffice freuen, sondern natürlich auch Hacker - ein Problem, das noch immer unterschätzt wird.

Können Sie diese Herausforderung mit Zahlen belegen?
62 Prozent der Firmen haben Bedenken bezüglich Applikationssicherheit und bei 43 Prozent kam es bereits zu

> **Die moderne IT-Security sollte ein Enabler der Digitalisierung sein.**

erfolgreichen Angriffen auf ihre Applikationen[1]. Zudem zeigt die Cybersecurity Studie 2020 von Ergon Informatik AG und IDG Research deutlich: 86 Prozent der Unternehmen sind von Cyber-Angriffen betroffen und bei über 50 Prozent der Firmen führen diese Attacken zu wirtschaftlichen Schäden. Dabei muss man sich bewusst sein, was wirtschaftliche Schäden heute bedeuten können – Stichwort Internet-of-Things (IoT) und der mögliche Eingriff in ganze Produktionsprozesse. Oder der Diebstahl von personenbezogenen Daten, der nicht nur für die Finanzbranche, sondern auch für Versicherungen, den Health-Care-Bereich, die öffentliche Hand und weitere datengetriebene Branchen ein grosses Risiko darstellt.

Jetzt gibt es ja eine wahre Digitalisierungs-Euphorie. Ist die IT-Security also die Spassbremse, die nur die Risiken sieht, aber kaum die Chancen?
Wir sind vor allem die, die mit beiden Augen sehen und nicht unter einer partiellen Blindheit leiden (*lacht*). Doch im Ernst: Die moderne IT-Security sollte ein Enabler der Digitalisierung sein. Mit einem gewissen Stolz kann ich sagen – mit unseren Lösungen haben wir es bei vielen unserer Kunden geschafft, diesen Status einzunehmen.

Das müssen Sie kurz erläutern.
Nehmen wir zum Beispiel den Zahlungsverkehr: Heute sind wir es gewohnt, Bankgeschäfte online zu erledigen. Doch bevor man das macht, muss man einen Sicherheits-Check durchlaufen und sich authentisieren – am liebsten passwortlos über Fingerprint, Gesichtserkennung oder sogar ganz ohne physischen Kontakt. Für den User läuft dieser Prozess fast schon unbewusst ab. Und genau dieses nahtlose und dennoch sichere Kundenerlebnis wird heute gefordert.

Der moderne Kunde ist also verwöhnt?
Er ist eher digital affin und erwartet unkomplizierte Prozesse. Zum einen, weil vorgelagerte, integrierte Security-Systeme die User-Experience ermöglichen, die die Digital Natives nun mal gewohnt sind. Zum anderen, weil sich in den letzten Jahren das Bild der IT-Sicherheit grundlegend gewandelt hat.

Inwiefern?
Früher hat man sich die IT-Security als einen grimmigen Burgwächter vorgestellt, der alle Neuankömmlinge mit bösen Blicken beäugt und am liebsten verjagen würde. Doch heute? Heute sind wir der Concierge am Welcome-Desk – immer auf eine optimale Sicherheit bedacht, dabei aber stets freundlich und sehr zuvorkommend. Für dieses Verhalten gibt es gute Gründe.

Welche Gründe sind das?
Vor allem die Erwartung der Kunden. Dazu muss man sich vor Augen führen, dass die Digital Natives bereits heute die Mehrheit der Schweizer Bevölkerung ausmachen. Sie haben punkto Geschwindigkeit, Verfügbarkeit von Services und einer intuitiv verständlichen User Führung ganz andere Erwartungen als die Digital Immigrants. Das Spannende dabei: Diese Erwartungshaltung betrifft nicht nur den Consumer-, sondern auch den Business-Bereich.

Heisst das, auch im Business müssen Sicherheitsprozesse mit Gamification-Elementen auftrumpfen?
Soweit würde ich nicht gehen. Aber lassen Sie mich zwei konkrete Beispiele machen: Bei einem Finanzinstitut, das auf Remote-Work umstellt, ist nicht nur der sichere Zugriff auf Daten wichtig, sondern auch, wie die Mitarbeitenden mit der virtuellen Plattform interagieren können. Bis vor kurzem war das oft nur über Passwort und Hardware-Token möglich. Das ist mühsam, fehleranfällig und teuer. Doch wenn neu eine nahtlose Authentisierung möglich ist – mit Single Sign-On und über eine passwortlose Zweifaktor-Authentifizierung – dann ist das nicht nur bequem, sondern auch sehr sicher.

Und das andere Beispiel?
Nehmen wir einen anderen Kunden von uns, der im Industriesektor tätig ist – weltweit und mit mehreren tausend Mitarbeitenden. Dieses Technologieunternehmen bietet einen digitalen Zugriff auf Instandhaltungsservices an, also «Predictive Maintenance» mit Cloud-Anbindung und IoT-Infrastruktur. Was hier bei Angriffen auf dem Spiel steht, ist klar: noch nicht eingereichte Patente, Geschäftsgeheimnisse und wichtige Projektinformationen, also die Kronjuwelen eines Unternehmens. Dennoch soll die Kundenplattform einen einfachen Zugriff ermöglichen, sowohl in Brüttisellen als auch in Boston und Bangkok. Auf den ersten Blick sehen wir also einen klassischen Zielkonflikt zwischen Sicherheit und Benutzerfreundlichkeit.

Und wie löst man diesen Konflikt?
Mit vorgelagerten Sicherheitslösungen. Denn trotz immer komplexer werdenden IT-Architekturen ist damit nicht nur eine durchgängige User Experience möglich, sondern auch eine hohe Kosteneffizienz und ein schnelles Time-to-Market für neue Business-Services

Vorgelagerte Lösungen klingen überzeugend. Doch mit welchen Herausforderungen müssen Unternehmen bei der Umsetzung rechnen?
Viele IT-Systeme basieren auf einem monolithischen Aufbau mit grossen Applikationen, die zwar sehr mächtig, aber auch sehr schwerfällig sind. Darum sind in den letzten Jahren vermehrt Microservices aufgekommen, bei

> **Die Herausforderung ist also, beide Welten sinnvoll zu verknüpfen.**

denen die meist komplexe Anwendungssoftware aus unabhängigen Prozessen komponiert wird. Die grosse Herausforderung ist, dass die «alte» Welt der monolithischen Applikationen noch immer präsent ist – und das wird in den nächsten Jahren auch so bleiben. Schliesslich haben sich die bestehenden Systeme bewährt und waren mit grossen Investitionen verbunden. Die Herausforderung ist also, beide Welten sinnvoll zu verknüpfen: Die alte Welt der grossen, schweren Silos. Und die neue Welt mit ihren kurzen DevOps-Zyklen, agilen Innovationsprozessen und einer schnellen Time-to-Market.

Gibt es noch weitere Argumente, die für eine integrierte Gesamtlösung sprechen?
Ja natürlich – von einfachen Registrierungsprozessen über ein erleichtertes, zentrales Compliance-Management bis hin zu schnellen Entwicklungsprozessen für das Business Development. Aber einen Punkt möchte ich noch besonders erwähnen.

Welchen denn?
Unternehmen werden immer weniger im Alleingang erfolgreich sein können. Eine vernetzte Welt hat zur Folge, dass wir auch bei der Digitalisierung in vernetzten Ökosystemen denken müssen. Die Konsequenz: Die Fähigkeit, Services von Drittanbietern einzubinden, wird künftig ein entscheidender Erfolgsfaktor sein. Deshalb ist eine nahtlose Integrationsfähigkeit unabdingbar – gerade punkto Sicherheit. Und hier schliesst sich der Kreis: genau deswegen lohnt sich eine vorgelagerte IT-Security-Lösung.

Quelle: [1]Verizon 2019 DBIR

AIRLOCK® SECURE ACCESS HUB ergon

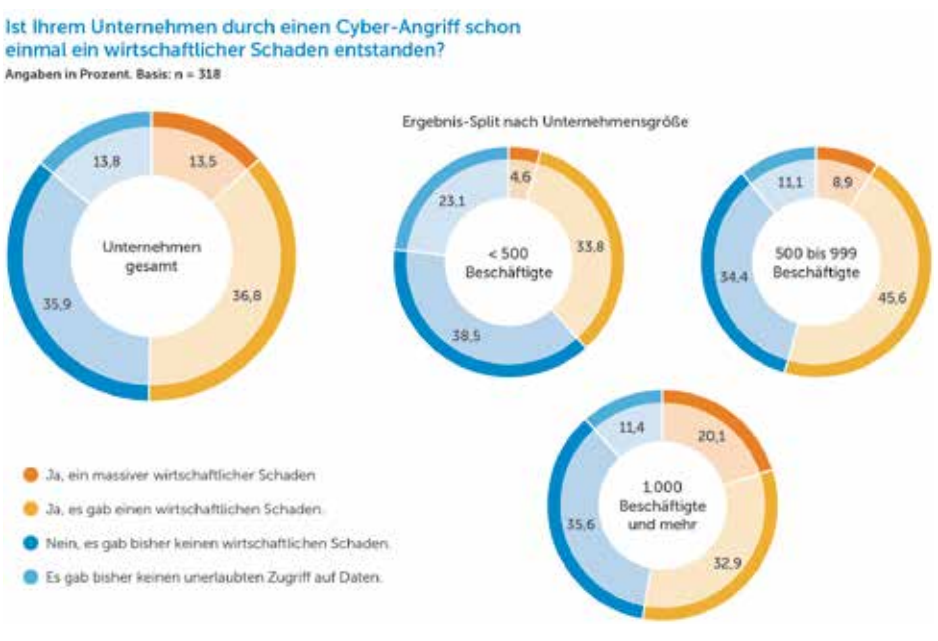
Studie Cyber Security 2020

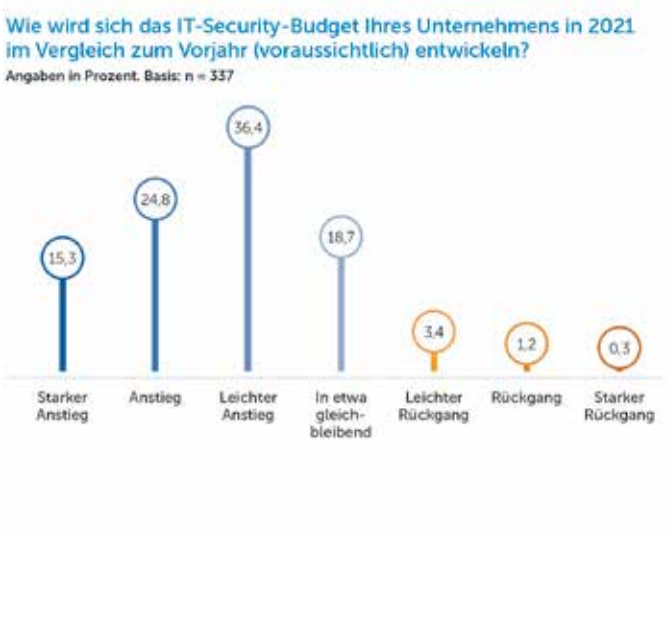
Die brandaktuelle Studie zeigt, mit welchen Security-Herausforderungen Unternehmen heute konfrontiert sind und welche Lösungen sich anbieten – mit übersichtlichen Infografiken und fundierten Informationen. Jetzt gratis über den QR-Code runterladen!

SCAN ME

Roman Hugelshofer – Managing Director Application Security bei Ergon Informatik AG

Roman Hugelshofer ist Experte für die Sicherheit und Verfügbarkeit von kritischen Businessanwendungen. Als Mitglied der Ergon Geschäftsleitung kennt er die Herausforderungen von Unternehmen bei der Digitalisierung. Hugelshofer ist für die Weiterentwicklung des Airlock Secure Access Hub sowie den Aufbau von strategischen Partnerschaften und die internationale Expansion zuständig.





Airlock – Security Innovation by Ergon Informatik AG

Der Airlock Secure Access Hub vereint alle wichtigen IT-Sicherheitsthemen in einem gut abgestimmten Gesamtpaket, das Massstäbe in Sachen Bedienbarkeit und Services setzt: Von einer Web Application Firewall (WAF) über ein Customer Identity & Access Management (cIAM) mit starker Authentifizierung (2FA) bis hin zu einer API-Sicherheit. Airlock schützt heute mehr als 20 Millionen digitale Identitäten und 30 000 Back-Ends von über 550 Kunden auf der ganzen Welt.

Weitere Informationen unter **www.airlock.com**.

Airlock ist eine Security Innovation des Schweizer Softwareunternehmens Ergon Informatik AG.

swiss safety center

Informationssicherheit

Wer Risiken kalkuliert, hat einen grösseren Raum, um Chancen zu nutzen

swiss safety center ISO/IEC 27001 certified system

Informationssicherheit ist heute (über-)lebensnotwendig für Organisationen aller Art. Vertraulichkeit, Integrität und Verfügbarkeit von Information werden zum strategischen Erfolgsfaktor, wenn es um das Vertrauen der Kunden, Geschäftspartner und der Öffentlichkeit geht.

ISO/IEC 27001

Die akkreditierte Zertifizierung nach ISO/IEC 27001 zeigt bestehenden und potenziellen Kunden, dass eine Organisation Best-Practice-Prozesse zur Informationssicherheit definiert und umgesetzt hat.

Die ISO/IEC 27001 ist die einzige internationale Norm, die Anforderungen an ein Informationssicherheitsmanagementsystem (ISMS) durch eine akkreditierte Zertifizierung nachweisbar macht.

Ein ISMS ist eine Reihe von Richtlinien, Verfahren, Prozessen und Systemen, die Informationsrisiken wie Cyber-Angriffe, Hacks, Datenlecks oder Diebstahl verwalten.

Was nützt es?

- Wer den anerkannten Standard erfüllt, schützt sich vor Geldstrafen und Verlusten im Zusammenhang mit Datenverstössen.
- Das effiziente und effektive Erreichen der Ziele wird unterstützt.
- Die kontinuierliche Verbesserung wird gefördert.
- Einhaltung der geschäftlichen, rechtlichen, vertraglichen und regulatorischen Anforderungen.
- Die Qualität der Lieferantenbeziehung wird gepflegt.
- Die Einarbeitung von Mitarbeitenden wird vereinfacht.
- Die Kompetenz der Mitarbeitenden wird gefördert.

Wieso Zertifizierung?

- Die unabhängige und objektive Zertifizierung erhöht die Reputation und Aussenwirkung.
- Reduzieren Sie den Bedarf an häufig wiederkehrenden Audits durch Ihre Kunden.
- Das Zertifikat ist auch ein Werbemittel.
- Erhalten Sie eine unabhängige Meinung in Bezug auf Ihre Sicherheitslage durch praxiserprobte Experten.
- Erhöhen Sie den Nutzen und die Glaubwürdigkeit durch die externe Bewertung.
- Sie erhalten eine unabhängige und objektive Bewertung, die sich im Zertifikat zeigt, aber inhaltlich vertraulich bleibt.

Swiss Safety Center

Heinrich A. Bieler
cs@safetycenter.ch
044 877 62 30
www.safetycenter.ch

Checklisten:
safetycenter.ch/shop

Code of Practice ISO/IEC 27002

Das ist eine Art Praxisrichtlinie für die Entwicklung organisationsspezifischer Sicherheitsstandards. Die Norm bezieht sich auf die im Anhang A von ISO/IEC 27001 beschriebenen Sicherheitsmassnahmen und gibt praktische Hinweise zur Umsetzung. In 14 Bereichen sind allgemeine Richtlinien und Empfehlungen für ein verbessertes Informationssicherheits-Management in Unternehmen oder Organisationen zu finden. Die Norm kann von allen Arten von Organisationen angewendet werden.

Entwickeln Sie sich zu den Best Practices und machen Sie den ersten Schritt mit unserer Checkliste.

Cloud Services ISO/IEC 27017

Definiert spezifische Empfehlungen für die Anbieter von Cloud-Dienstleistungen und ist eine Erweiterung von ISO/IEC 27002. Die Norm erzeugt durch ein Analyseraster und den gezielten Austausch von Informationen eine Standardisierung der Beziehungen zwischen Kunden und Cloud-Service-Providern und erleichtert so das Management der Geschäftsbeziehung erheblich, insbesondere dort, wo das «shared responsibility model» verwendet wird. Also wo die Cloud-Anbieter die Sicherheit der Cloud garantieren, während die Unternehmen für die Sicherheit ihrer Daten sorgen.

Datenschutz ISO/IEC 27701

Beschreibt Anforderungen für die Einführung, Aufrechterhaltung und kontinuierliche Verbesserung eines PIMS (Privacy Information Management System) und ist eine Ergänzung zu ISO/IEC 27001 mit Anforderungen an den Datenschutz, mit einem starken Bezug zur DSGVO. Themen sind z.B. Verantwortlichkeiten, Datenschutz-Schulung der Mitarbeitenden, Verschlüsselung, Protokollierung von Zugriffen und Veränderungen. Es findet der «Privacy by Design» Grundsatz Berücksichtigung. Das Vorgehen bei der Überprüfung von Sicherheitsvorfällen auf Datenschutzverletzungen wird geregelt.

Business Continuity (BCM) ISO 22301

Es war bisher schwer, die Notwendigkeit und den Nutzen eines BCM eindrücklich zu erklären. In der Zeit einer Pandemie können wir uns das nun schenken. Es geht darum sich in guten Zeiten auf schlechtere vorzubereiten, um sich möglichst rasch erholen zu können. BCM ist hochaktuell und muss jede Organisation beschäftigen. Es geht um den Plan, wie man schrittweise möglichst rasch zur Normalität zurückfindet und das wünschen wir allen. Es ist nie zu spät damit zu beginnen und man muss immer besser werden.

ZLI ZÜRCHER LEHRBETRIEBSVERBAND ICT

«Das ZLI Ausbildungszentrum überzeugt mit hoher Qualität und Praxisbezug»

In 2 Jahren zum EFZ
Informatik & Mediamatik

Durchstarten mit der Berufslehre für Erwachsene

Infos & Anmeldung: **www.zli.ch/weiterbildung**

Zürcher Lehrbetriebsverband ICT | Edenstrasse 20 | 8045 Zürich | T 044 552 8200 | info@zli.ch

Die Herausforderungen der DSGVO der Europäischen Union

Seit über zwei Jahren gilt die Datenschutz-Grundverordnung der EU (DSGVO; eng. GDPR). Diese hat auch Konsequenzen für Schweizer Unternehmen und erfordert deshalb ein umsichtiges Vorgehen, um die Vorschriften effizient einzuhalten.

TEXT **SMA**

Im Mai 2018 trat die DSGVO als Update der Datenschutzvorschriften von 1995 in Kraft. Sie regelt den Datenschutz von Konsumenten in der EU und erhöht die Transparenz der Datensammlung von in der EU tätigen Unternehmen. Trotz dessen, dass die Schweiz kein Mitglied der EU ist, haben diese Verordnungen Auswirkungen auf Schweizer Unternehmen. Um sicher vor Bussen zu sein ist es essentiell, die Übersicht über die gesammelten Daten zu behalten. Die Experten der Butos AG liefern Informationen zu den Anforderungen, die erfüllt werden müssen.

Nicht nur rechtliche Gründe für eine Datensicherheitsstrategie

Daten gehören für die meisten Unternehmen zum zentralen Tätigkeitsbereich. Dahingegend können die Strafen bei Nichteinhalten der DSGVO happig ausfallen: Eine Busse kann die Höhe von 20 Millionen Euro oder vier Prozent des globalen Jahresumsatzes erreichen. Aber auch die Reputation kann Schaden nehmen. Die erforderte Transparenz im Umgang mit persönlichen Daten kann dazu führen, dass potenzielle Kunden das Vertrauen in das Unternehmen verlieren, wenn die Datensicherheit nicht zur Genüge gewährleistet wird.

Dazu regeln die Verordnungen vor allem die Sicherheit in den Bereichen der Protokollierung, Organisation und Schutz der Daten von natürlichen Personen. Umso wichtiger ist es, eine effiziente Strategie zur Einhaltung der DSGVO zu implementieren – leider ist das oft noch nicht der Fall.

Die wichtigsten Schritte

Kurz zusammengefasst sind es vier Vorgaben, die ein Unternehmen realisieren muss, um erfolgreich mit Daten unter diesen Verordnungen umzugehen. Zuerst muss man die Daten, die bereits gespeichert sind, genau unter die Lupe nehmen und ihr angehaftetes Risiko beurteilen. Zudem sind Reformen in der weiteren Datensammlung nötig. Die Datenkontrolle muss spezifische Prozesse und Regeln zur Sammlung, Speicherung und Löschung neuer Daten beinhalten. Ein dritter Punkt ist die Vorbereitung auf ein mögliches Datenleck. Dazu gehört die Planung eines Notfallszenarios, welche die schnelle Identifikation und Untersuchung einer Verfehlung ermöglicht. Ausserdem muss auch ein Vorgehen zur internen und externen Meldung eines Vorfalls festgelegt werden. Denn die DSGVO sieht bei derartigen Situationen auch einen Bericht zu den jeweiligen Autoritäten vor. Zuletzt ist es wichtig, dass ein einheitliches und bereichsübergreifendes Compliance-Management aufgebaut wird, das alle gesammelten Daten dokumentiert und verfolgt.

Automatisierte Verwaltung der Daten

Der Ansatz, die Daten nur mit Spreadsheets und manuellen Prozessen zu verwalten, ist aufwändig und wird den Anforderungen der DSGVO nicht gerecht. So kann man kaum die Übersicht über die Datenmenge aufrechterhalten. Die folgenden Fragen sollten stets einfach zu beantworten sein: Welche persönlichen Daten sind vorhanden? Zu welchem Zweck wurden sie gesammelt? Wer ist der rechtliche Eigner der Daten? Wie lange werden die Daten aufbewahrt? Das ist aber nur der Anfang: Ebenso muss man den Prozess der Datenlöschung akkurat handhaben, kontrollieren und dokumentieren werden. Eine übergreifendes Daten- und Implementierungsmanagement ist also unerlässlich. Ein weiterer wichtiger Ansatz ist, dass nur die Daten gesammelt werden, die auch für einen definierten Zweck bestimmt sind. Es lohnt sich, genau zu definieren, welche Daten für welche Ziele interessant sind. Daten auf Vorrat einzusammeln verfehlt den Nutzen und verkompliziert die Verwaltung aller Daten.

Datenregulierung

In der DSGVO ist klar geregelt, dass natürliche Personen in der EU der Verwendung ihrer Daten zustimmen müssen. Ausserdem kann diese Zustimmung jederzeit teilweise oder komplett zurückgezogen werden. Die Datenkontrolle muss also Prozesse beinhalten, die Einverständnisse regeln und Anträge auf Löschung abhandeln. Das Unternehmen muss darlegen können, dass der Verwendung der Daten zugestimmt wurde und es Aufträgen zur Löschung nachkommt. Für einige Branchen oder bestimmte Unternehmen kann es unter Umständen sinnvoller sein, den Personen die Möglichkeit zu bieten, selbst auf sichere Weise ihre Daten einzusehen und zu löschen. Egal, wie die Datenkontrolle organisiert wird: Das Unternehmen muss auch bei Dritten, welche die Daten verwalten, sicherstellen, dass hohe Sicherheitsstandards eingehalten werden. Eine nahtlose Dokumentation von Einverständnissen ermöglicht zudem, dass EU-Regulatoren überzeugt sind, dass man die DSGVO ernst nimmt.

Datensicherheitslücken

Für lange Zeit sprach man vor allem über den Schutz der Daten vor äusseren Angriffen, wenn es um Datensicherheit ging. Die DSGVO weitet diese Definition allerdings aus von der Prävention zur Alarmbereitschaft. Die Kultur rund um Datensicherheit wird so durch die neue Wichtigkeit der Krisenkommunikation im Falle eines Lecks ergänzt. Das Augenmerk sollte hier also darauf fallen, dass die Zeit zwischen dem Vorfall und einer Reaktion und dessen Meldung so kurz wie möglich gehalten wird. Häufig werden diese Vorfälle von Aussenstehenden und nicht intern entdeckt. Für den Ruf eines Unternehmens kann dies erheblichen Schaden verursachen. Neben dem Schutz der persönlichen Daten, muss man auch sicherstellen, dass brenzlige Situationen intern entdeckt, behoben und nach aussen kommuniziert werden. Rufschädigungen werden so verhindert oder zumindest in Grenzen gehalten.

Was passiert bei einem Ausfall kritischer Systeme in der Schweiz?

In den vergangenen Jahren hat der Bund viel in den Schutz kritischer Infrastrukturen (SKI) investiert: von der ersten SKI-Strategie 2012, der Überarbeitung 2017 bis zur laufenden Umsetzung 2018 - 2022.

Aber wie sieht es mit den Unternehmern und deren Mitarbeitern aus, wie mit der Bevölkerung? Wer hat die Strategie gelesen und wann fand die letzte Simulation statt? Wer wusste vor der laufenden Pandemie, wie auf einen Lockdown zu reagieren ist? Wo stand, dass es zu Grenzschliessungen kommen kann? Wir stellen uns zur Zeit viele Fragen, oft im Kontext von harten Interessenskonflikten.

Die aktuelle Krise macht Krisenszenarien greifbar. Was früher nur einem kleinen Kreis transparent war, spürt heute jeder im täglichen Leben. Eine Frage geht unter: Wie binden wir Unternehmen und Bevölkerung in die Umsetzung der SKI-Strategie ein, um auf zukünftige grosse Ausfälle unserer SKI vorbereitet zu sein, besser vorbereitet als auf die Pandemie?

Was müssen und können wir tun, wenn es zu einem flächendeckenden grossen Cyber-Incident kommt? Ein Szenario, von dem wir seit Jahren reden, das wir allerdings ausserhalb der SKI-Arbeitsgruppen nie wirklich zu Ende gedacht haben. Nun wäre die Zeit reif. Jeder ist sensibilisiert.

Sind wir alle auf den grossen Cyber-Shutdown vorbereitet?

Wenn wir heute von kritischen Infrastrukturen sprechen, dann sind diese weitgehend abhängig von einer funktionierenden IT-Infrastrukur, sowie IT-gesteuerten Netzinfrastrukturen (Strom, Wasser, etc.). Eine Abhängigkeit, deren sich heute weder Unternehmer, noch Bevölkerung tatsächlich in aller Konsequenz bewusst sind – bis zu dem Tag, an dem das Mobile Phone nicht mehr funktioniert, die Onlineshops innert eines Sekundenbruchteils verschwunden sind und Zahlsysteme nicht mehr reagieren.

Unternehmen und Mitarbeiter waren im Lockdown der Pandemie (weitgehend) erstaunlich flexibel in der Umstellung auf das Arbeiten im Homeoffice. Digitalisierung sei Dank. Im Cyber-Shutdown dürfte es dann schwierig werden. Man muss schon sehr genau nachdenken, um zu identifizieren welcher Service dann noch verfügbar ist.

Der Vorteil des Pandemie-Szenarios ist, dass es sich langsam entwickelt – man sieht es kommen, anfangs fast unbeachtet, doch stetig. Ein Cyber-Shutdown entwickelt sich in wenigen Minuten bis Stunden und im Extremfall instantan. Auch das Recovery verläuft nach komplett anderen Mustern.

Lässt uns die Cloud im Stich?

Die fortschreitende Digitalisierung unserer Gesellschaft geht einher mit einer nicht mehr umkehrbaren und rasant zunehmenden Abhängigkeit von Cloud-Diensten. Nun sind gerade diese besonders anfällig, sollte es zu einem Cyber-Shutdown kommen. Wenn wir also von Resilienz-Massnahmen sprechen, dann müssen diese insbesondere im Bereich der Cloud-Service-Nutzung wirken. Dabei gilt es einiges zu bedenken, was wir in der Vergangenheit in grossen Teilen vernachlässigt haben. Interessant ist, dass Cloud-Dienste oberflächlich betrachtet sehr anfällig wirken, allerdings aufgrund der zugrundeliegeneden Architektur gerade auch eine Lösung für Resilienz-Optimierungen bieten. Cloud-Dienste können über Geo-Zonen hinweg resilient verfügbar sein. Funktioniert mein Mobile Phone in der Schweiz nicht, gehe ich ins Nachbarland und kommuniziere weiter.

Wir müssen die Cloud-Anbieter eng in die Pflicht nehmen und auch über Notfall-Szenarien nachdenken, wo wir aus anderen Geo-Zonen auf unsere Daten und Services zugreifen können. Das wird für Schulen nicht funktionieren, sicher aber für private Dienste und Unternehmen.

Wie setzen wir das Gelernte um?

Wir haben durch Covid-19 vieles zu Krisenbewältigungsszenarien gelernt und jeden Tag kommt Neues dazu. Nun gilt es das Erlernte auch konkret umzusetzen. Wir kennen alle das im Covid-19 Fall aktivierte Shutdown-Skript. Die meisten waren völlig unvorbereitet und hatten Mühe mit der Entwicklung Schritt zu halten.

Es sind nun alle gefordert, das bisher Vernachlässigte nachzuholen. Auf einen grossen Cyber-Shutdown müssen wir alle vorbereitet sein. Jeder, ob privat, in der Schule oder im Unternehmen sollte sein Cyber-Incident-Shutdown-Script kennen und aktivieren können. Für zukünftige Szenarien reicht es nicht mehr, in Facharbeitsgruppen an SKI Aktionsplänen zu arbeiten. Es gilt alle einzubeziehen und jeder sollte auch seinen Beitrag leisten.

Beruhigend ist, dass Schulen und Gastrobetriebe im Cyber-Shutdown nach alten Mustern weitgehend weiter funktionieren werden. Unternehmen und Behörden werden praktisch ausgeschaltet, sollten sie nicht vorbereitet sein.

Über BearingPoint

BearingPoint ist eine unabhängige Management- und Technologieberatung mit europäischen Wurzeln und globaler Reichweite, die von 178 Partnern geführt wird. Das Unternehmen agiert in drei Bereichen: Consulting, Business Services und Software.

Für weitere Informationen:
www.bearingpoint.com

Kontakt
Herr Jürgen Stückle, Cybersecurity Advisor

Data Protection – eine Utopie?

«Das Recht hinkt der Entwicklung hinterher.» Was wohl auf viele Rechtsgebiete zutreffen mag, galt bisher insbesondere für das Schweizer Datenschutzrecht. «Cloud Storage», informationelle Selbstbestimmung, Onlineshop usw. waren 1993 bei der Redaktion des bis heute geltenden Datenschutzgesetzes (DSG) noch kein Thema.

Die Bedeutung des Schutzes der persönlichen Daten nimmt mit den täglich besser werdenden Algorithmen und der exponentiell steigenden Datenmenge rasant zu. Das Parlament verabschiedete deshalb am 25. September 2020 die erste Totalrevision des DSG.

> **«Niemand ist von einer Verletzung der Persönlichkeit durch ungerechtfertigte Bearbeitung der Personendaten gefeit.**

Niemand ist von einer Verletzung der Persönlichkeit durch ungerechtfertigte Bearbeitung der Personendaten gefeit; die Weitergabe von Personendaten an Dritte ist nur eines der vielen Beispiele. Der Gesetzgeber wollte deshalb die Rechte des Einzelnen stärken. Dies gilt jedoch nicht für juristische Personen, denn deren Daten sind neu generell vom Anwendungsbereich des DSG ausgenommen. Voraussetzung für die Abwehr einer Persönlichkeitsverletzung ist die Auskunft darüber, inwiefern überhaupt persönliche Daten bearbeitet wurden.

Das Auskunftsrecht wird deshalb von einer momentan abschliessenden Liste an Pflichtinformationen auf «jede Information, die für eine betroffene Person erforderlich ist, um ihre Rechte nach DSG geltend zu machen», erweitert.

Den erwähnten Herausforderungen wird auch mit erweiterten Compliance-Vorgaben für die sogenannte «Datenbearbeiter» (insbesondere auch KMUs) begegnet. So sind diese neu zum Führen eines Verzeichnisses aller Bearbeitungstätigkeiten verpflichtet, welches unter Anderem den Bearbeitungszweck und die Aufbewahrungsdauer der Personendaten beinhalten muss. Weiter wird eine Meldepflicht bei Datenverlusten bzw. Datensicherheitsverletzungen eingeführt. Das revidierte Gesetz wird voraussichtlich anfangs 2022 in Kraft treten, wobei keine Übergangsfristen vorgesehen sind. Eine frühzeitige Auseinandersetzung mit den Folgen für das eigene Unternehmen ist deshalb unumgänglich. Dies gilt aufgrund Abweichungen des neuen DSG von der europäischen Datenschutz-Verordnung (DSGVO), auch für bereits DSGVO-konforme Unternehmen.

Ob das neue DSG einen effektiven Beitrag zu einem griffigeren Persönlichkeitsschutz zu leisten vermag, muss sich in der Anwendung noch weisen.

www.h-h.ch

HAFNER & HOCHSTRASSER
RECHTSANWÄLTE ATTORNEYS AT LAW

«Cybersicherheit ist ein Prozess und kein Zustand!»

Seit August 2019 nimmt sich Florian Schütz als Delegierter des Bundes für Cybersicherheit verschiedensten Cyberthemen an. Im Interview mit «Fokus» verrät er, wie sich Unternehmen präventiv vor Cyberangriffen schützen können, was über das Denken und Handeln von Cyberkriminellen bekannt ist und welche Ziele es in Sachen Cybersicherheit noch anzugehen gilt.

INTERVIEW **LARS MEIER** BILD **KEYSTONE, GAËTAN BALLY**

Herr Florian Schütz, vor über einem Jahr wurden Sie zum ersten Delegierten des Bundes für Cybersicherheit bestimmt. Wie kann man sich Ihre Arbeit vorstellen?
Ich koordiniere die verschiedenen Cyberthemen beim Bund. Das ist ein komplexes Feld mit vielen Akteuren und unterschiedlichen Bedürfnissen. Entsprechend bin ich in stetigem Austausch mit den diversen involvierten Stellen. Eine meiner zentralen Aufgaben ist die koordinierte Umsetzung der Nationalen Strategie zum Schutz der Schweiz vor Cyberrisiken (NCS). Zudem leite ich das Nationale Zentrum für Cybersicherheit (NCSC), also die zentrale Anlaufstelle für Wirtschaft, Bevölkerung, Behörden und Bildungsinstitutionen, wenn es um Cyberthemen geht. Seit Januar nehmen wir Meldungen über Vorfälle einheitlich entgegen, prüfen diese und leiten sie an die entsprechend richtige Stelle weiter.

Was ist der Unterschied Ihrer Arbeit bei der öffentlichen Hand im Vergleich zur Privatwirtschaft?
In der Privatwirtschaft war Schnelligkeit ein wichtiger Faktor. Beim NCSC ist es zudem wichtig, die politischen Prozesse einzuhalten und insbesondere alle wichtigen Akteure einzubeziehen. Die Herausforderung besteht darin, einen Rahmen zu schaffen, der für alle beteiligten Stellen akzeptabel ist. Das erfordert eine gewisse Zeit. Wenn es um die Umsetzung geht, verwende ich dann einen agileren «Fail Fast»-Ansatz – so hole ich entsprechend wieder Zeit auf.

Bei Zalando musste ich eine Organisation aufbauen, die in hohem Masse skalierbar und messbar ist. Skalierbarkeit ist ein Schlüsselfaktor für den Erfolg und ist auch für das Nationale Zentrum für Cybersicherheit von hoher Bedeutung.

Welches sind die grössten Irrtümer, wenn es um Cybersicherheit geht?
Die Annahme, dass Cybersicherheit eine rein technische Angelegenheit ist. Das ist völlig falsch! Sicherheit geht uns alle an, sei es im privaten Rahmen oder im Arbeitsumfeld. Auch die Auffassung, dass der Mensch das Problem ist und man vor allem sensibilisieren muss, ist falsch. Vielmehr geht es darum, Sicherheit als integralen Aspekt der zu erledigenden Tätigkeit zu betrachten und sich Massnahmen zur Risikosenkung zu überlegen – technische und nicht technische. Damit ist bei einer Firma auch klar, wo die Verantwortung liegt – auf oberster Stufe. Wir müssen uns von der Idee verabschieden, dass es für Cybersicherheit einfach eine Spezialistin gibt, die dann schon weiss, was zu tun ist.

Cybersicherheit befindet sich in stetigem Wandel. Welche Rolle spielt im Zuge dessen die richtige Aufklärung in diesem Gebiet?
Aufklärung und Information sind wichtig. Aber wir betrachten das heute viel zu oberflächlich. Unter Aufklärung verstehen wir oft, dass man erklärt, was Phishing ist oder wie CEO Fraud funktioniert. Wichtiger ist, dass wir bei allen, die mit Technologien arbeiten sicherstellen, dass sie die Cybersicherheitsaspekte ihrer Arbeit verstehen und umsetzen können. Eine Automechanikerin sollte heute auch etwas von den Fahrzeugcomputern verstehen und wissen, wenn ein Protokolleintrag auf eine Manipulation schliessen liesse. Nur durch die Aus- und Weiterbildung der Cyberaspekte in den verschiedenen Fachgebieten wird Prävention möglich.

Wie häufig ist die Schweiz effektiv von Cyberangriffen betroffen?
Seit Anfang Jahr erhebt das NCSC die eingegangenen Meldungen und publiziert die wöchentlichen Statistiken. Da es in der Schweiz für Cybervorfälle keine Meldepflicht gibt, sind diese Zahlen nicht repräsentativ – die Dunkelziffer kennen wir nicht. Unsere Zahlen geben jedoch einen Eindruck, welches aktuell die häufigsten Bedrohungen sind.

Konkret gehen derzeit wöchentlich zwischen 200 und 300 Meldungen ein, die bearbeitet und weiterverfolgt werden.

Unser Anliegen ist es, dass uns möglichst alle Betroffenen ihre Vorfälle melden: Das hilft nicht nur uns, sondern auch den Firmen und Privatpersonen. Bei einer Meldung erhalten die Betroffenen Unterstützung für das weitere Vorgehen – und uns hilft es, die grossen Trends besser zu erfassen.

Wo steht die Schweiz in Sachen Datenschutz und -sicherheit?
Cyberbedrohungen sind vielfältig, und es gibt keine einheitlichen Messkriterien. Daher lässt sich keine abschliessende Antwort auf diese Frage geben. In der Schweiz sind im Vergleich zu anderen Ländern die Herausforderungen wegen des föderalistischen Systems unterschiedlich. Jeder Kanton hat einen anderen Digitalisierungsgrad und will seine Eigenständigkeit bewahren. Meine allgemeine Einschätzung ist, dass in verschiedenen Bereichen des Grundschutzes noch Nachholbedarf besteht. Verschiedene Studien zeigen, dass die Mehrzahl der erfolgreichen Angriffe auf Schwächen beruht, die seit Monaten bekannt sind und längst hätten beseitigt werden können.

Sie sind bereits lange im Gebiet der Cybersicherheit tätig – welches ist die wichtigste Lektion, die Sie in diesem Feld gelernt haben?
Angreifer sind sehr wandelbar und passen sich sehr schnell neuen Gegebenheiten an. Sie sind effizient und agieren in einem komplett deregulierten Umfeld. Daraus resultiert, dass man sein Sicherheitsdispositiv auch möglichst agil aufstellt und konstant gegenüber den identifizierten Risiken ausrichtet.

Viele Unternehmen kümmern sich erst um ihre Cybersicherheit, wenn es bereits zu spät ist. Wie können sich Unternehmen präventiv vor Cyberangriffen schützen?
Ein wichtiger Punkt, denn präventiver Schutz wird zu oft vernachlässigt. Hier geht es vor allem um das korrekte – und damit sichere – Bauen und Einsetzen von Systemen. In der Unternehmenswelt bedingt dies eine Kombination aus technischen und organisatorischen Massnahmen. Dabei stehen im präventiven Bereich ein durchgängiges Identitäts- und Access Management, rigoroses Testen in allen Entwicklungs- und Betriebszyklen, sowie ein umfassendes Daten- und Asset-Management im Vordergrund. Ein Beispiel: Wenn Mitarbeitende unternehmensintern eine neue Stelle antreten oder das Unternehmen verlassen, müssen die Benutzerrechte unverzüglich angepasst werden! Dies funktioniert nur, wenn klare Prozesse für den Umgang mit Benutzerrechten definiert und die technischen Systeme entsprechend ausgelegt und manipulationssicher sind.

Was geben Sie Unternehmen weiterhin auf den Weg, um sich vor Cyberangriffen zu schützen?
Wichtig ist in erster Linie die Erkenntnis, dass kein Unternehmen vor Angriffen sicher ist. Tönt selbstverständlich, aber hinter verschlossenen Türen sagen mir ab und zu Opfer von Cyberangriffen, dass sie das Risiko einfach nicht ernst genommen haben. Jedes Unternehmen muss Risikoanalysen durchführen und den Schutz der unterschiedlichen Systeme je nach Kritikalität des Systems entsprechend definieren.

Apropos Cyberangriffe: Ist bekannt, wie Cyberkriminelle jeweils vorgehen? Was lässt sich über ihr Denken und Handeln sagen?
In den meisten Fällen geht es einfach nur um Geld. Die klassische Kriminalität verlagert sich zunehmend ins Netz. Es gibt viele Phishing-Kampagnen gegen Einzelpersonen. Firmen wiederum werden immer wieder Opfer von Ransomware, also Erpressungsfällen, bei denen Daten verschlüsselt und nur gegen Bezahlung wieder freigegeben werden.

Am 1. Juli 2020 trat die vom Bundesrat verabschiedete Verordnung über den Schutz vor Cyberrisiken in der Bundesverwaltung (CyRV) in Kraft. Inwiefern prägt diese die Gesellschaft in Bezug auf Cybersicherheit?
Die Cybersicherheit spielt eine zentrale Rolle in der nationalen und internationalen Aussen- und Sicherheitspolitik und wird immer stärker zu einem wichtigen Faktor für den Wirtschaftsstandort und die Bevölkerung der Schweiz. Der Bund trägt dieser Entwicklung mit der Verordnung und den organisatorischen Massnahmen Rechnung. Eine der Hauptaufgaben des NCSC ist es, die Bevölkerung, die Wirtschaft, Bildungseinrichtungen und die Verwaltung beim Schutz vor Cyberrisiken zu unterstützen und die Sicherheit der eigenen Systeme zu verbessern.

Sie haben unter anderem für den Bereich Business Development Cyber & Intelligence ein Jahr lang in Israel gearbeitet – welche Unterschiede in Bezug auf Cybersicherheit können Sie allgemein international beobachten?
Die im Thema Cyber führenden Staaten – zu welchen Israel gehört – gehen das Thema gesamtheitlich und nicht nur sicherheitspolitisch an. Denn dadurch können sie die notwendigen Abwehrmassnahmen treffen, gleichzeitig aber Chancen nutzen, was zu einer positiven statt einer negativen Gesamtbilanz führt.

Besteht in der Schweiz noch Aufholbedarf in Sachen Cybersicherheit? Wenn ja, wo?
Wir müssen das Thema gesamtheitlicher betrachten und gleichzeitig auch die Rollen schärfen. Zum Beispiel muss der Staat Rahmenbedingungen schaffen, in denen auch in einer digitalisierten Schweiz ein Leben und Geschäften nach unseren Werten möglich ist. Firmen und Organisationen haben im Gegenzug eine Eigenverantwortung, sich zu schützen. In beiden Bereichen gibt es noch Luft nach oben. Ein weiterer Aspekt ist die Ausbildung nicht nur von Fachkräften, sondern der Cyberaspekte in Berufsgattungen, die mit Technologie in Kontakt kommen. Ein weiterer sehr wichtiger Punkt ist, dass Geschäftsleitungen und Verwaltungsräte erkennen, dass Leute aus der «Technik» auch in die Chefetagen gehoben werden müssen. Ein VP Technology muss etwas von Technologie verstehen und gehört in die Geschäftsleitung. Sie haben auch keinen CFO der nichts von Finanzen versteht.

Kann man Cybersicherheit messen? Wenn ja, wie?
Cybersicherheit per se ist schwer zu messen, da Cybersicherheit ein sehr weites Feld von Fachdisziplinen umfasst. Für die jeweiligen Fachgebiete kann man jedoch Key Performance Indikatoren (KPIs) etablieren. Diese sollten eine Aussagekraft über Themen haben, die die Organisation gerade beschäftigen. Zum Beispiel könnte man die durchschnittliche Zeit, die man vom Erkennen einer Schwachstelle bis zu deren Behebung messen, wenn man seine Angriffsfläche konstant minimieren möchte.

Welchen Wert messen Sie Cybersicherheit in Zukunft bei und warum?
Wie bereits gesagt, hat die Cybersicherheit in den vergangenen Jahren stark an Bedeutung gewonnen und sie wird auch in Zukunft weiter an Bedeutung gewinnen. Die Digitalisierung wird nicht weniger, sondern wird immer stärker. Das ergibt ein riesiges Potential in allen Lebensbereichen, bringt aber auch neue Risiken mit sich. Cybersicherheit heisst nicht zuletzt, mit diesen Risiken umgehen zu können.

Apropos Zukunft: Welche Ziele gilt es in Bezug auf Cybersicherheit noch zu erreichen?
Wir müssen uns davon verabschieden zu denken, dass wir, wenn wir alle heute gesetzten Ziele erreichen, sicher sein werden im Cyberbereich. Wir werden nie «fertig» sein – Cybersicherheit ist ein Prozess und kein Zustand!

Stadtwerke schliessen sich zum Schutz vor Cyberkriminalität zusammen

Stromausfall infolge eines Hackerangriffs – eine Gefahr, die real ist. Damit es nicht so weit kommt, bilden Schweizer Stadtwerke gemeinsam mit der Stadtwerke-Allianz Swisspower und der Stiftung Switch eine Kooperation für Cybersicherheit. Geprüft wird zudem ein gemeinsames Security Operations Center, um die Stadtwerke im Monitoring ihrer kritischen Netzwerke mit operationeller Technologie, also Leitstellen und Kraftwerke, zu unterstützen.

Adrian Märklin

Stromnetze, Gas- und Wasserversorgung zählen zu den kritischen Infrastrukturen – fallen sie aus, hat dies rasch gravierende Folgen für unser Gemeinwesen. Ein grossflächiger Stromausfall etwa wirkt sich auf zahlreiche andere Bereiche aus: Verkehrsleitsysteme brechen ebenso zusammen wie der elektronische Zahlungsverkehr, die Lebensmittel- und Trinkwasserversorgung sowie die Abfallentsorgung. Die Infrastrukturbetreiber in der Schweiz treffen deshalb umfangreiche Vorkehrungen, um Unterbrüche zu verhindern. Im internationalen Vergleich nimmt die Schweiz punkto Versorgungssicherheit eine Spitzenposition ein.

Cyberkriminalität

Eine besondere Gefahr hat sich jedoch in den vergangenen Jahren akzentuiert: Energieversorger müssen sich daran gewöhnen, dass Cyberkriminalität mittlerweile ein ebenso grosses Risiko für sie darstellt wie Stürme, Überschwemmungen oder Brände; mit dem Unterschied, dass Cyberattacken kein einmaliges Ereignis sind, sondern dauernd und zum Teil automatisiert ausgeführt werden.

Je vernetzter die Systeme, desto grösser die Gefahr

Die Digitalisierung im Infrastrukturbereich erhöht das Risiko eines Ausfalls substanziell. Denn die Leitsysteme, welche die Strom-, Gas- und Wasserversorgung steuern, werden zunehmend mit Sensoren ausgestattet, um Netze und Anlagen zentral zu steuern und zu überwachen – interessante Ziele für Hacker. Die grösste Schwachstelle im System ist dabei nach wie vor der Mensch. 80 Prozent aller Cyberattacken in Unternehmen werden über die Handlung eines Mitarbeitenden ausgelöst, sei dies durch importierte Malware (bösartige Software), den Besuch infizierter Webseiten oder unsichere Speicherorte von vertraulichen Daten und Passwörtern. Im Home-Office ist das Risiko, Opfer einer Attacke zu werden, noch höher, denn Internetanschlüsse, die von der Kontrolle durch das Unternehmen ausgeschlossen sind, bieten eine grössere Angriffsfläche.

Zusätzlich integrieren wir nun unter dem Stichwort «Smart City» eine Unmenge von kleinen Intelligenzen (Internet of Things) in unsere Netze: untereinander vernetzte Sensoren, die in Echtzeit Daten analysieren und Aktionen auslösen – vom intelligenten Stromzähler im Haushalt (Smart Meter) bis hin zu Parkplatz-Sensoren. Je mehr solch smarte Elemente im Energiesystem miteinander kommunizieren, desto wichtiger wird ein verlässliches Sicherheitsdispositiv.

Prävention fordert Infrastrukturbetreiber heraus

Wie real die Gefahr von Cyberattacken auf kritische Infrastrukturen ist, zeigt sich an den häufiger werdenden Berichten über solche Fälle in den Medien. Sie sind aber nur die Spitze des Eisbergs. Gut gerüstete Unternehmen können die Attacken teilweise isolieren oder den Schaden begrenzen, doch die Prävention fordert Infrastrukturbetreiber personell wie auch finanziell zunehmend heraus. Die Eidgenössische Elektrizitätskommission führte 2019 eine Umfrage zur Cybersicherheit unter den 92 grössten Netzbetreibern durch, die zusammen für 90 Prozent des schweizerischen Stromumsatzes zuständig sind. Erst ein Viertel gab an, über eine spezifische Organisationseinheit zu verfügen, die Cyberattacken aktiv überwacht und Abwehrmassnahmen ergreift, ein sogenanntes Computer Emergency Response Team (CERT) oder ein Security Operations Center (SOC).

Stadtwerke profitieren von der Zusammenarbeit

Der Aufbau und der Betrieb solcher Organisationen benötigen Ressourcen. Firmen- und branchenübergreifende Kooperationen liegen deshalb auf der Hand, insbesondere für kleinere und mittlere Energieversorgungsunternehmen. So können die einzelnen Unternehmen ihre Kräfte bündeln, Erfahrungen teilen und mit den immer professioneller werdenden Angreifern Schritt halten. Swisspower, die Allianz der Schweizer Stadtwerke, hat darum gemeinsam mit der Stiftung Switch eine Plattform lanciert, in der Stadtwerke im Bereich Cybersecurity firmenübergreifend zusammenarbeiten. Nach der einjährigen Testphase hat dieses CERT für Stadtwerke im Herbst 2020 den regulären Betrieb aufgenommen. Der Testbetrieb hat gezeigt: Die Stadtwerke profitieren stark von der Zusammenarbeit und dem vertraulichen Erfahrungsaustausch untereinander sowie von der Unterstützung durch die Experten von Switch.

Massgeschneiderte Angebote für grössere und kleinere Energieversorger

Das Swisspower-CERT umfasst derzeit fünf schweizerische Stadtwerke und soll sukzessive auf acht bis zehn Mitglieder erweitert werden. Ein erklärtes Ziel der Initiative ist es, auch kleinere Energieversorgungsunternehmen, die über einen weniger umfangreichen IT-Sicherheits-Betrieb verfügen, auf pragmatische Weise zu unterstützen. Hierzu bietet Swisspower die Möglichkeit zur Teilnahme an einem «Outer Circle» des CERT. Dessen Mitglieder erhalten relevante Informationen zur Cybersecurity und Unterstützung im IT-Security-Betrieb zur Erreichung der IKT-Minimalstandards des Bundes.

Als weiteres Angebot prüft Swisspower aktuell ein gemeinsames Security Operations Center, um die Stadtwerke im Monitoring ihrer kritischen Netzwerke mit operationeller Technologie, also Leitstellen und Kraftwerke, zu unterstützen.

Weitere Informationen:
www.swisspower.ch/cybersecurity

Adrian Märklin ist Senior Consultant bei Swisspower und beschäftigt sich seit zehn Jahren mit dem Thema IT- und Netzwerksicherheit.

TEXT **ADRIAN MÄRKLIN**

swisspower

«Wir wollten den Konflikt mittels friedlicher Gespräche beilegen»

In der Berg-Karabach-Region der Republik Aserbaidschan kommt es zurzeit wieder zu bewaffneten Konflikten zwischen Armenien und Aserbaidschan. Aufgrund der weltweiten Gesundheitslage findet das Thema allerdings wenig mediale Beachtung. Hanum Ibrahimova, Botschafterin Aserbaidschans in der Schweiz, legt ihre Sicht der Dinge dar.

Frau Hanum Ibrahimova, wie hat der Konflikt zwischen Armenien und Aserbaidschan begonnen?

Der Berg-Karabach-Konflikt begann 1988 mit Gebietsansprüchen auf historisches Land Aserbaidschans und ethnischen Provokationen von armenischer Seite. Durch militärische Aktionen besetzte Armenien rund 20 Prozent des Territoriums der Republik Aserbaidschan: die Region Berg-Karabach und sieben angrenzende Bezirke. Die Streitkräfte Armeniens töteten während des vierjährigen Krieges über 20 000 ethnische Aserbaidschaner, verwundeten 50 000 und vertrieben eine Million.

Wie stehen diesmal die Chancen auf eine friedliche Beilegung des Konflikts?

Wir denken, dass mit dieser armenischen Regierung die Aussichten auf eine friedliche Lösung leider sehr gering sind. Kontraproduktive sowie provozierende Erklärungen und Aktionen seitens der armenischen Regierung machen die Verhandlungen sinnlos. Wenn der armenische Premierminister erklärt, dass «Karabach Armenien ist», und er Raketenangriffe auf friedliche Städte anordnet, gibt es nicht viel Raum für Verhandlungen.

Wir wollten den Konflikt mittels friedlicher Gespräche beilegen. Dies war aber aufgrund der Haltung der Armenier und provokanter Handlungen nicht möglich. Deshalb befreien wir jetzt unsere Territorien auf dem Schlachtfeld. Dabei sahen wir, dass es dort zu illegalen Aktivitäten kam – leider auch mit Schweizer Beteiligung. Der Gründer der Firma Goldstar und Besitzer von «Franck Muller»-Uhren in der Schweiz, Vartan Sirmakes, war in illegale Aktivitäten verwickelt und beutete Goldvorkommen in den besetzten Gebieten, insbesondere im Distrikt Zangilan, aus. Die aserbaidschanische Generalstaatsanwaltschaft wird diesen strafrechtlichen Tatsachen nachgehen und Geschäftsleute entsprechend anklagen.

Sie haben Angriffe auf einige Städte erwähnt. Was genau ist passiert?

In der Nacht vom 17. Oktober griffen die Streitkräfte Armeniens die aserbaidschanische Stadt Ganja mit ballistischen Raketen an. Dies war der dritte grausame Angriff in Folge auf die zweitgrösste Stadt Aserbaidschans, welche weit von der Frontlinie entfernt liegt – eine neuerliche Aggression Armeniens gegen Aserbaidschan. Der Angriff verursachte schwere Verluste unter der Zivilbevölkerung.

Damit verstösst Armenien sowohl gegen humanitäres Völkerrecht als auch gegen den vereinbarten Waffenstillstand. Die gezielte Tötung friedlicher Menschen stellt ein Kriegsverbrechen, ein Verbrechen gegen die Menschlichkeit, dar, für welches die Führung Armeniens die volle Verantwortung trägt.

Zudem attackierten die armenischen Streitkräfte wiederholt die Regionen Aghjabadi, Barda, Goranboy und Tartar mit schwerer Artillerie, was enormes menschliches Leid und Schäden an der zivilen Infrastruktur verursachte. Die aserbaidschanische Nationale Agentur für Minenräumung (ANAMA) berichtete ausserdem, dass die Region Barda mit einer nach dem Völkerrecht verbotenen Streumunition angegriffen wurde.

Am 28. Oktober beging Armenien im Rahmen seiner erklärten Terrorpolitik ein weiteres abscheuliches Verbrechen gegen die Zivilbevölkerung in Aserbaidschan: Um ein Uhr nachmittags Ortszeit beschoss Armenien dicht besiedelte (Wohn-)Gebiete der Stadt Barda mit Streumunition; der zweite vorsätzliche Angriff mit verbotener Munition innerhalb von 20 Stunden. Dies ist ein weiteres Kriegsverbrechen, das Armenien in den letzten Tagen unter grober Verletzung des vereinbarten humanitären Waffenstillstands und seiner Verpflichtungen nach dem humanitären Völkerrecht, begangen hat.

Die von den Streitkräften Armeniens begangenen Verbrechen sind ein klarer Beweis dafür, dass sie an einer politischen Lösung des Konflikts nicht interessiert sind.

Ilham Alijew, Präsident Aserbaidschan:

«Wir sehen die Zukunft der Region Karabach als ein Gebiet des Friedens. Mit Investitionen und unserer Entwicklungserfahrung können wir diese Region in eine der wohlhabendsten Regionen der Welt verwandeln und friedlich koexistieren. Doch dafür müssen die Folgen des Krieges beseitigt werden.»

«Wir setzen die Resolutionen des UN-Sicherheitsrates im Alleingang um, obwohl dies Aufgabe des UN-Sicherheitsrates wäre. Wir haben eine neue Realität geschaffen, mit welcher jetzt jeder rechnen muss.»

«Die Co-Vorsitzenden der Minsker Gruppe der OSZE sollten unparteiisch bleiben und sich nicht für eine Seite entscheiden. Sie müssen Armenien davon überzeugen, die Besetzung zu beenden, den Waffenstillstand einzuhalten und sich zum Rückzug aus den Gebieten zu verpflichten. Die Charta der Vereinten Nationen gewährleistet das Recht jedes Landes auf Selbstverteidigung: Wir verteidigen uns selbst und befreien das international anerkannte Territorium Aserbaidschans von der Besetzung.»

Der oberste Berater des Präsidenten, Hikmat Hajiyev:

«Wir sind bereit, der Zivilbevölkerung und den armenischen Soldaten, welche in durch die aserbaidschanischen Streitkräften kontrollierten Gebiete kommen, alle notwendige humanitäre Unterstützung auf der Grundlage der Prinzipien des Humanismus und der Genfer Konventionen zu gewähren. Aserbaidschan ist immer zu diplomatischen Verhandlungen bereit.»

Sicherheit hat viele Facetten

Nadia Glaus
Data Protection Officer,
Ypsomed AG

Sicherheit bedeutet für mich...

Vertrauen, Ehrlichkeit, Transparenz und Freiheit sind für mich die Pfeiler von Sicherheit. Das gilt nicht nur zu Hause oder in einer Beziehung, aus meiner Sicht sind das auch wichtige Werte beim Thema Datenschutz.

Personendaten haben heute einen hohen finanziellen Wert. Viele kostenlose Dienstleistungen finanzieren sich mit den Daten, die wir bei der Nutzung hinterlassen. Die gesammelten Daten verbessern Marketingstrategien, lassen Verhaltensvorhersagen zu und werden leider auch für kriminelle Zwecke missbraucht.

Bevor ich meine Personendaten bekannt gebe, höre ich auf meinen Bauch und prüfe, ob ich der empfangenden Person vertrauen kann. Schützt sie meine Daten vor Missbrauch? Informiert sie mich transparent, aus welchen Gründen und für welche Zwecke sie meine Daten bearbeitet und an wen sie diese weiterleitet? Ist sie ehrlich und sammelt nur die Personendaten, die sie auch tatsächlich benötigt, um die vorgesehenen Zwecke zu erreichen? Habe ich die Freiheit, die Verarbeitung der Daten auf das Nötigste zu beschränken?

Solche Überlegungen sind umso wichtiger, wenn wir besonders schützenswerte Daten bekannt geben – die z.B. unsere Gesundheit, Intimsphäre oder unsere Weltanschauung betreffen. Denn wie fühlen Sie sich, wenn solche persönlichen Daten über Sie veröffentlicht werden?

Peter Waldenberger
Leitung Corporate Administrative Support,
Gebrüder Weiss

Sicherheit bedeutet für mich...

Die Tools und das Wissen zu haben, wie man Risiken bei sich verändernden Herausforderungen minimiert. In Richtung Kunde bedeutet das, durch Digitalisierung Transparenz zu schaffen: vom einfachen Online-Track & Trace bis zum TAPA-Transport mit 24/7 Fahrzeugmonitoring. Und das kombiniert mit einer maximalen Datensicherheit und unter Berücksichtigung der DSGVO-Vorgaben. Also so viel Transparenz wie möglich bei gleichzeitiger Minimierung von Sicherheitsrisiken wie etwa Datenlecks oder Fehlinformationen.

Ebenfalls muss sichergestellt sein, dass auch die Risiken beim physischen Transport minimiert werden, vom eingesetzten Verkehrsmittel über die Ladungssicherung bis hin zu ausreichendem Versicherungsschutz. In Richtung Mitarbeiter sind Massnahmen zum Schutze der Gesundheit am Arbeitsplatz zu setzen, besonders jetzt in Zeiten von Corona, aber auch generell durch Aufklärungsarbeit, laufende Arbeitsplatzevaluierungen, Evakuierungsübungen etc. Ziel ist es, dass die Mitarbeiter die optimalen Tools zur Verfügung haben, um ihre Arbeit zu erledigen. Zugleich muss sichergestellt sein, dass kritische Datenströme grösstmöglich geschützt sind. Nur mit laufendem Lernen und Verbessern ist es möglich, diese vielschichtigen Herausforderungen zu bewältigen.

So bleibt man im Wettrennen mit Hackern in Führung

Der Kampf gegen Hacker ist wie ein Formel-1-Wettrennen, beschreibt Markus Raff, Senior Solutions Engineer bei Flexera. «Denn das Tempo ist enorm hoch und nur der Schnellere gewinnt.» Was meint er damit? In Deutschland kommt es pro Tag zu rund 47 Millionen Hackerangriffen auf Unternehmen. «Und meistens fallen Eindringlinge über bekannte Schwachstellen von Software in die IT-Systeme von Firmen ein.»

Wissen ist Sicherheit

Wie können sich Unternehmen davor schützen? «In erster Instanz müssen Firmen zuerst Klarheit darüber erlangen, wie ihre IT-Umgebung genau aufgestellt ist und wo sich eventuelle Sicherheitslücken auftun», erklärt Markus Raff. Natürlich wird dies umso schwieriger, je mehr Applikationen ein Unternehmen benutzt. Hier kommt Flexera Software Vulnerability Research ins Spiel: «Damit bieten wir unseren Kunden die Möglichkeit, auf vertrauenswürdige Schwachstellendaten von über 65 000 Anwendungen zuzugreifen.»

Das Wissen über mögliche Schwachstellen allein reicht allerdings noch nicht aus, um einen Betrieb nachhaltig vor Hackerangriffen zu schützen. Denn Firmen müssen die Anfälligkeit ihrer Software kennen und beheben können. Zu diesem Zweck bietet Flexera den Software Vulnerability Manager an. Diese Komplettlösung unterstützt die Firmen-IT u.a. bei der Behebung von Schwachstellen mit den richtigen Patches. Damit man das Rennen gegen die Hacker nachhaltig gewinnt, ist ein nahtloser Prozess – von der Erkennung über die Bewertung bis hin zur Behebung von Schwachstellen unumgänglich. «Und das gelingt nur mit automatisierten Lösungen», führt Raff aus. Die Software Vulnerability Management-Lösung von Flexera umfasst entsprechende Tools, die jährlich über 20 000 Softwareschwachstellen verifizieren, dokumentieren und über Metacrawler über 1000 Darknet-Quellen durchsuchen. Die daraus generierten Informationen werden dann direkt ans Sicherheitsteam von Flexera weitergegeben, das auf Basis dieser Daten zeitnah über geeignete Gegenmassnahmen entscheiden kann.

Markus Raff
Senior Solutions Engineer
Flexera

Sie möchten mehr Transparenz zu Ihrer IT erlangen, Ihre Prozesse und Kosten optimieren sowie mögliche Schwachstellen beheben?

Dann kontaktieren Sie Flexera jetzt unverbindlich für eine erste Beratung: **www.flexera.de**

Software Vulnerability Manager
Flexera
Inform IT. Transform IT.

Als Unternehmen mit Risiken umgehen

Auf jede Eventualität vorbereitet zu sein, ist ein Erfolgsfaktor, den Unternehmen nicht ausser Acht lassen sollten. «Fokus» weiss, was modernes Risikomanagement ausmacht.

TEXT **FATIMA DI PANE**

Der Erfolg eines Unternehmens wird stets von Risiken bedroht, seien sie unmittelbar, in weiter Ferne oder fast unmöglich. Sich auf Eventualitäten vorzubereiten, ist für langfristigen Erfolg essenziell. Im Jahre 2020 befinden wir uns mitten in einer globalen Pandemie, welche den Alltag aller Unternehmen auf den Kopf gestellt hat. Unternehmen mit einem effektiven Risikomanagement überstehen solche Zeiten um einiges leichter. Doch was bedeutete Risikomanagement genau und – noch wichtiger – wie läuft dieses ab?

Externe und interne Risiken

Ein effektives Risikomanagement bereitet ein Unternehmen auf eventuell-kommende Krisen vor. Dabei lassen sich die möglichen Risiken in mehrere Kategorien aufteilen. Grob kann man zwischen externen und internen Risiken unterscheiden. Externe Risiken sind beispielsweise eine Pandemie, politische Umbrüche oder konkurrierende Firmen. Bei internen Risiken kann es sich beispielsweise um Fehler in der Führung oder Interessenskonflikte und Fehleinschätzungen innerhalb der Firma handeln. Wenn sich ein Unternehmen darüber klar wird, welche Risiken die Firma bedrohen, kann man vorzeitig handeln. Beispielsweise kann die Kontrolle und die Früherkennung verbessert werden, und bereits ein Plan beim allfälligen eintreten einer Krise festgesetzt werden.

Verschiedene Sichtweisen mit einbeziehen

Doch wie läuft der Prozess beim Risikomanagement ab? Das Unternehmen muss sich erstmal über die möglichen Risiken und deren Auswirkungen bewusst werden. Dies mag sich simpel anhören, ist jedoch aufwendiger als es scheint. Um alle möglichen Risiken zu sammeln, müssen Mitarbeiter aus allen Sparten und Abteilungen des Unternehmens zu Wort kommen, vom CEO bis zu Einsteigenden.

Bei der Sammlung der Risiken besteht die Tendenz, den Blick zu sehr nach aussen zu richten und die internen Risiken ausser Acht zu lassen. Dies muss unbedingt verhindert werden: Untersuchungen der 50 grössten Firmenpleiten der letzten Jahre haben gezeigt, dass die Gründe für sämtliche Zusammenbrüche in internen Risiken zu finden waren. Beispielsweise gehörte der Energiekonzern Enron einst zu den grössten Unternehmen der USA. Aufgrund Bilanzfälschungen musste das Unternehmen 2001 jedoch Insolvenz anmelden. 20 000 Menschen verloren ihre Jobs.

Minimierung und Strategie

Der nächste Schritt liegt in der Bewertung der Risiken. Dazu muss bei jedem Risiko die Wahrscheinlichkeit eines Eintretens ermittelt werden. Auch muss sich das Unternehmen bewusst machen, welcher Schaden bei Eintreten des Risikos entsteht. Dann werden Strategien für die Minimierung des Risikoeintritts festgelegt. Dies kann anhand angepasster Kontrollmassnahmen oder zusätzlichen Versicherungen geschehen. Ebenso werden Massnahmen festgelegt, welche umgesetzt werden, wenn das Risiko eintritt. Dabei macht es Sinn, sich vor allem auf die wahrscheinlichsten Risiken zu konzentrieren. Auf diese gilt es am umfassendsten vorbereitet zu sein.

Was wäre wenn?

Mit der Grundlage, die das Risikomanagement bietet, können dann weitere Massnahmen getroffen werden, wie beispielsweise das Business Continuity Management (BCM). BCM steht für Kontinuitäts- oder Weiterführungsmanagement. Dabei betrachtet es nicht nur die unmittelbare Ereignisbewältigung, sondern auch nachgelagerte Aspekte bis zu dem Zeitpunkt, an dem sich der Vollbetrieb wieder eingestellt hat. Jedes Risiko wird im BCM so betrachtet, als wäre es bereits eingetreten. Der Einfluss des Risikoszenarios auf verschiedene Faktoren wird ermittelt; dazu gehören der Ruf des Unternehmens, die finanzielle sowie die gesetzliche Lage. Kurz gesagt überlegt man sich, was alles unternommen werden muss, um den Schaden zu begrenzen.

Better safe than sorry

Bei Risikomanagement sowie BCM handelt es sich um komplexe Unterfangen. Daher lohnt es sich, externe Hilfe von Experten zu holen, sich aber gleichzeitig auch selbst umfassend zu informieren. Eine externe, neutrale Partei ist eine wertvolle Schlüsselfigur, wenn es darum geht, Risiken effektiv zu ermitteln und richtig einzuschätzen. So steht einer effektiven Vorbereitung nichts mehr im Wege – komme, was wolle.

Auf Eventualitäten vorbereitet

Bereits seit über zwölf Jahren unterstützt die Beratungsfirma i-Risk GmbH Unternehmen dabei, für jedes Risiko gewappnet zu sein. Geschäftsleiter Dr. Eric Montagne erzählt mehr.

Dr. Eric Montagne
Geschäftsleiter i-Risk GmbH

Dr. Eric Montagne, welche Fehler machen Unternehmen im Risikomanagement am häufigsten?

Aufgrund mangelnder Erfahrung führen Unternehmen oft zu komplexe Risikomanagementsysteme ein. Es fehlt dabei eine auf das Unternehmen angepasste Struktur zur Identifikation, Kategorisierung und Bewertung der Risiken. Aus Furcht etwas zu vergessen, werden zu viele und nicht-relevante Risiken aufgeführt. In der Folge werden auch keine effizienten Massnahmen zur Risikosteuerung abgeleitet. Trotz grossem Aufwand werden nur bescheidene Resultate generiert. Dies führt zur Demotivation aller Beteiligten und das Risikomanagement wird zum «Papiertiger».

Warum ist es wichtig, externe Spezialisten zum Risikomanagement dazu zu holen?

Nach einer Analyse des Unternehmens und der für das Risikomanagement verfügbaren Ressourcen wird eine angebrachte Struktur definiert. Der externe Berater unterstützt die Firma mit einer stringenten Methodik und bei der Auswahl der angemessenen Flughöhe zur Definition der Risikoszenarien. Seine Aussensicht und das von ihm erstellte Benchmarking zeigen blinde Flecken bei der Risikoerhebung auf. Somit baut man ein System auf, durch welches rasch die kritischen Risiken aufgezeigt und Gegenmassnahmen effizient ergriffen werden können. Die Wirksamkeit des Systems wird erhöht und dies mit einem vernünftigen Aufwand.

Für welche Unternehmen sind die Dienstleistungen von i-Risk besonders interessant?

Über die letzten zwölf Jahre hat i-Risk bei über 130 Organisationen Risikomanagement aufgebaut und weiterentwickelt. Sowohl die Privatwirtschaft als auch die öffentliche Hand konnten von unseren Ansätzen profitieren. Vom Kleinunternehmen bis zum Grosskonzern ist Risikomanagement für jede Firma interessant, welche Stabilität schaffen und Überraschungen vermeiden will. Ein zentraler Erfolgsfaktor ist dabei die Unterstützung vom Management und die Fokussierung auf das Wesentliche. So kann i-Risk zusammen mit dem Kunden ein lebendiges und effektives Risikomanagement verankern sowie pragmatische Tools bereitstellen, welche die effiziente interne Weiterführung in Zukunft sicherstellen.

Weitere Informationen unter **www.i-risk.ch**

INTERVIEW **FATIMA DI PANE**

Das Unvorhersehbare vorhersehen

Nicht erst seit Corona werden sich Unternehmen bewusst, dass externe Ereignisse sich plötzlich auf das Funktionieren eines Betriebs und ganze Produktionsketten auswirken können.

Unternehmen sind vielerlei Gefährdungen ausgesetzt: Auf einen Schlag fallen grosse Teile des Personals aus, fragile just-in-time Lieferketten werden unterbrochen oder die Produktionsmittel werden bei Elementarereignissen beschädigt.

Um sich auf solche Störungen vorzubereiten, führen Unternehmen häufig ein Business Continuity Management ein. So können Unternehmensrisiken analysiert und anschliessend nachhaltige Strategien zum Umgang mit den grössten Gefahren entwickelt werden.

Was könnte das Unternehmen gefährden? Mit welchen Schäden müsste gerechnet werden und wie wahrscheinlich ist ein solches Szenario? Mit einer Business Impact Analysis verschafft sich das Management zusammen mit einem Sicherheitsingenieur einen vertieften Einblick in die Achillesfersen des Unternehmens. Dabei werden nicht nur die naheliegenden Gefährdungen, sondern auch weniger offensichtliche Szenarien einbezogen. Dazu gehört oftmals der Betriebsunterbruch mit den damit verbundenen Umsatzeinbussen und Problemen, die durch den Ausfall wichtiger Zulieferer entstehen.

Anhand der Erkenntnisse aus der Analyse werden gezielt Massnahmen ergriffen, um die Risiken zu eliminieren und minimieren. In letzter Instanz kommt ergänzend die Versicherung für die Restrisiken ins Spiel. Durch diese ganzheitliche Risikobetrachtung aus verschiedenen Perspektiven kann das Weiterführen eines Betriebes im Ereignisfall sichergestellt werden. Vor allem in Zeiten wie diesen hilft ein ausgefeiltes Business Continuity Management, um für das Unvorhersehbare gewappnet zu sein.

Dr. Matjaz Ros, Sicherheitsingenieur
SRB Assekuranz Broker AG
Tel: 044 497 87 87

«Wer gutes Krisenmanagement betreibt, kommt gestärkt aus der Krise»

Wie bereitet man ein Unternehmen auf eine Krise vor? Was sind dabei häufige Fehler? Und was genau ist überhaupt eine Krise? Diese und weitere Fragen beantwortet Almut Eger, BCM- und Krisenmanagerin, Geschäftsleitung der 4 Management 2 Security GmbH, im Interview mit «Fokus».

Almut Eger
Geschäftsleitung 4m2s
Leiterin Geschäftsbereich Integriertes Management

> Welche Bereiche prioritär für ein Krisenmanagement sind, ist von Firma zu Firma unterschiedlich.

Frau Almut Eger, was gilt im Sinne des Krisenmanagements überhaupt als Krise?
Wir definieren Krisen als etwas Unvorhergesehenes, das mit der normalen Alltagsorganisation nicht mehr bewältigt werden kann. Zum Beispiel weil ein Mehr an Denkleistung sowie an Über- und Quersicht nötig ist. Der Unterschied zur Notfallsituation: darauf kann man sich eher vorbereiten – im Sinne von Wenn-Dann-Entscheiden. Zum Beispiel: Wenn ein Feuer ausbricht, dann helfen unter anderem Feuerwehr und Polizei das Ereignis zu bewältigen. In einer Krisensituation steht das Unternehmen ohne diese Hilfen da.

Kann man sich denn überhaupt auf das Unvorhersehbare vorbereiten?
Man kann sich sehr gut vorbereiten, nicht aber auf jedes Szenario. Deshalb ist es zielführender, sich konkret zu fragen: «Was sind meine Kronjuwelen – die essenziellen Prozesse? Was schütze ich wie vor einem Ausfall?». Diese Erkenntnisse gewinnt man aus dem Business Continuity Management. Das ist die beste Grundlage für die Vorbereitung auf Krisensituationen.

Was gilt es beim Business Continuity Management im Vorfeld der Krise besonders zu beachten?
Wir reden hier von den essenziellen Prozessen, Ressourcen oder Partnerschaften; zusammenfassbar unter Kritikalität – was muss wirklich geschützt werden? Um das zu verstehen, sind auch Erkenntnisse aus dem Riskmanagement und anderen Bereichen wichtig. Wenn die essenziellen Prozesse und heiklen Ressourcen bekannt sind, kann deren Schutz konkret vorbereitet werden. z.B. mit Stützmassnahmen und Rahmenbedingungen für mögliche Reaktionen im Ereignis.

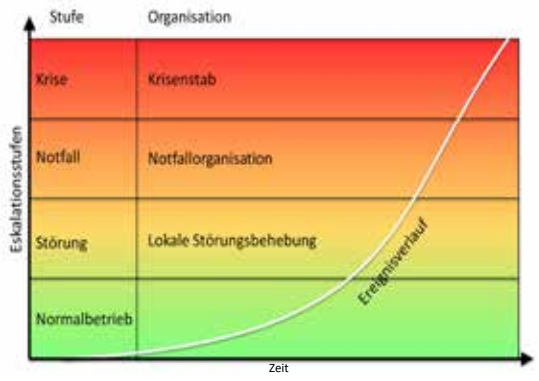
Welche Bereiche prioritär für ein Krisenmanagement sind, ist von Firma zu Firma unterschiedlich. Letztendlich sind es finanzielle Einbussen, rechtliche Probleme und Reputationsschäden, die verhindert werden müssen. Das sind auch die Bereiche, in welchen sich jetzt die meisten Folgeschäden der Coronakrise zeigen.

Was sind häufige Fehler oder Missverständnisse in Bezug auf Krisenmanagement?
Aus meiner langjährigen Erfahrung beim Coachen und Begleiten von Krisenstäben stehen häufig Kompetenz-Fragestellungen im Raum: «Wer entscheidet was». Es stellen sich Fragen wie «Wofür braucht es einen Krisenstab? Wozu die Geschäftsleitung (GL)? Oder ist die GL direkt der Krisenstab?». Das ist für jedes Unternehmen unterschiedlich – die eine richtige Lösung gibt es nicht. Ausgangspunkt ist für uns immer das, was im Alltag gut funktioniert. Zusätzliches soll nur in Fällen zum Zug kommen, wenn mehr Quersicht, rasche Reflexionen und Entscheidungen erforderlich sind.

Im Zuge der Coronapandemie wurden viele erstmalig mit einer grösseren Krise konfrontiert. Worin unterscheidet sich die Situation von Unternehmen, welche mit gutem Krisenmanagement in diese Krise gegangen sind, von solchen, deren Krisenmanagement suboptimal oder nicht vorhanden war?
Da gibt es klar ersichtliche, signifikante Unterschiede: Je besser die Vorbereitung war, desto schneller konnte eine Firma in der veränderten Situation aktiv werden und den Schutz der kritischen Prozesse und Ressourcen organisieren. Wer nicht vorbereitet war, musste erst die «Hausaufgaben» erledigen. Dasselbe galt auch für Unternehmen, die ein sehr starres Krisenmanagement hatten, welches beispielsweise nur auf Naturkatastrophen vorbereitet war: Dem Unternehmen selbst ging es primär noch gut, aber wichtige Wirkungsketten vor allem in der Supply Chain funktionierten nicht mehr oder anders.

Unternehmen, die bei der Planung Anfang Jahr auch Eventualitäten betrachtet haben, können auch Monate später noch viel besser mit der Virus-Situation umgehen, während die anderen fast bei jeder Änderung der Situation am Straucheln sind.

Würden sich mit einem gelungenen Krisenmanagement aufgrund der vollzogenen Innovationen auch gewisse Chancen ergeben aus der Krise?
Auf alle Fälle. Wer von Anfang an gut aufgestellt war im Business Continuity und Krisenmanagement, der konnte durch Innovationen in Prozessabläufen, in Produkten oder mit neuen Partnerschaften die Krise abfedern. Diese Firmen sind nun gestärkt, konnten sich sogar Marktvorteile erarbeiten und sind bereits mit Neuerungen gut unterwegs.



Eskalation eines Ereignisses vom Normalzustand bis zur Krisensituation und die in der Regel zuständige Organisation. ©4 Management 2 Security GmbH

Lohnt es sich im Hinblick auf die Coronapandemie überhaupt, jetzt, nach Eintritt der Krise, noch Beratung in Sachen Krisenmanagement in Anspruch zu nehmen?
Ja, definitiv. Unsere Begleitung bezieht sich oft auf die Zusammenarbeit in einem Stab und die Umsetzung in der Linie, auf die Unterstützung bei den «Hausaufgaben» zu BCM und Krisenmanagement, oder auf das Analysieren einer Situation mit unserer Quer- und Aussensicht, die wir mit unserer breiten Erfahrung einbringen können.

TEXT **PATRIK BIBERSTEIN**

Mehr Informationen:
www.4m2s.com

4 Management 2 Security
Mit Sicherheit zum Erfolg

Risikomanagement ist Chefsache

Eine zentrale Grundvoraussetzung für ein effizientes und zielgerichtetes Risikomanagement ist die hierarchische Anordnung der Sicherheitsabteilung oder der Sicherheitsverantwortlichen im Unternehmen.

Das Ziel der Unternehmenssicherheit sollte stets sein, die Firma vor Bedrohungen und Gefährdungen bestmöglich zu schützen und Massnahmen zu treffen, damit die Geschäftstätigkeit mit minimalen wirtschaftlichen Einbussen auch unter besonderen Umständen weitergeführt werden kann. Dies kann jedoch nur gelingen, wenn der Umgang mit Risiken zur Chefsache erklärt wird. Die Geschäftsleitung entscheidet über das Mass an bewusst in Kauf genommenen Restrisiken und verantwortet potenzielle Schäden. Es ist daher angebracht, die Sicherheit als Stabsstelle direkt der Geschäftsführung zuzuordnen und diese nicht irgendeiner Organisationseinheit zu unterstellen.

Die drei wesentlichen Säulen des Risikomanagements

Ein erfolgreiches Risikomanagement basiert in der Regel auf drei wesentlichen Grundlagen, welche nur als Gesamtprodukt einen wirtschaftlich sinnvollen Umgang mit Risiken ermöglichen. Als erstes sollte eine Business Impact Analyse (BIA) erstellt werden. Ein fundiertes Verständnis der Funktionsweise der Unternehmung, deren interne und externe Abhängigkeiten sowie insbesondere der wirtschaftlichen Folgen eines Ausfalls von Teilsystemen, ist die Basis jedes Risikomanagements. Die Positionierung der Sicherheit als Stabsstelle der Geschäftsführung vereinfacht hierbei ganz erheblich die interdisziplinäre Informationsbeschaffung und erspart mühsame Kompetenzstreitigkeiten und träge Prozesse.

Sobald dieses Verständnis geschaffen und monetär beziffert wurde, kann eine Risikoanalyse erarbeitet werden. Diese basiert in der Regel auf einer Mischform von eigenen und externen Erfahrungswerten sowie dem aktuellen Stand der Forschung. Wichtig ist, dass zu Beginn möglichst vielfältige Gefährdungen und Bedrohungen identifiziert werden. Durch deren Bewertung in Eintretenswahrscheinlichkeit und Schadensausmass werden die Szenarien zu Risiken. Nun gilt es, zusammen mit der Geschäftsleitung zu entscheiden, welchen Risiken in welchem Mass entgegengewirkt werden soll (Reduktion Eintretenswahrscheinlichkeit resp. Schadensausmass), welche Risiken abgewälzt werden können (bspw. Versicherungen, Outsourcing) und welche Restrisiken das Unternehmen bewusst in Kauf nehmen will. Selbstverständlich sollten dabei, neben wirtschaftlichen Entscheidungskriterien, stets auch die Rechtsgüter berücksichtigt werden.

Die dritte Säule besteht aus dem Business Continuity Management (BCM). Durch die Erarbeitung von Eventualplanungen zur Aufrechterhaltung der Geschäftstätigkeit bei Eintreten von identifizierten Szenarien (insbesondere solcher, bei welchen sich Eintretenswahrscheinlichkeit oder Schadensausmass nicht wesentlich beeinflussen lassen), werden das Risiko der Gefährdung der Geschäftsexistenz sowie der wirtschaftliche Schaden minimiert. Durch die Etablierung des BCM wird das Fundament des Risikomanagements fertiggestellt.

Stolperstein «Credible Worst Case» Szenario

Die gängig etablierte Art und Weise der Visualisierung von Risiken sowie deren vereinfachte «Berechnung» führen leider oft dazu, sogenannte «Credible Worst Case» Szenarien zu vernachlässigen resp. zu ignorieren. Es ist nachvollziehbar, dass sich Unternehmen nicht auf jedes erdenkliche Szenario vorbereiten können. Jedoch gibt es plausible Ereignisse, deren Eintretenswahrscheinlichkeit sehr gering sind, das Schadensausmass jedoch potenziell sehr hoch ist. Solche Szenarien müssen vom Risikomanagement zwingend berücksichtigt werden (*vgl. dazu Grafik*). Beispiele für diese Kategorie von Risiken sind Epidemien, Pandemien oder grossflächige Stromausfälle mit Infrastrukturversagen (sog. «Blackouts»).

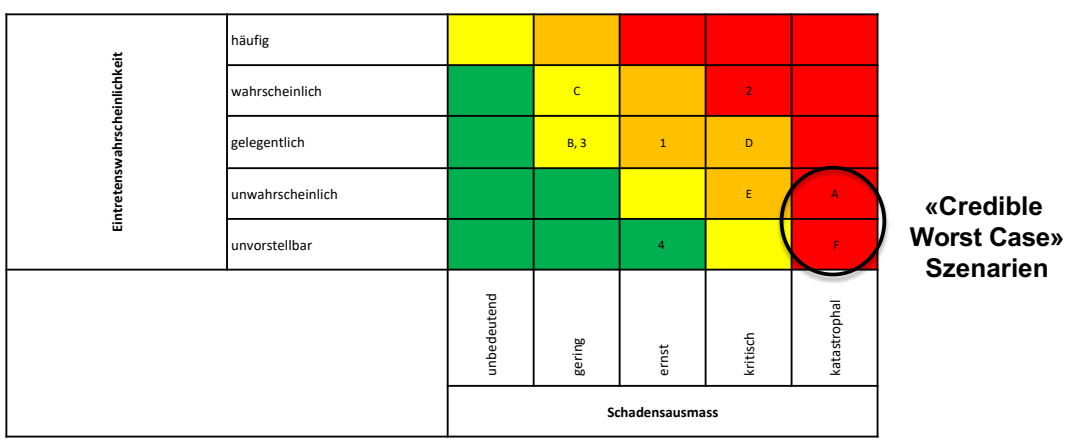


Abbildung 1: Mögliche Gestaltung Risikomatrix - eigene Darstellung

Risikomanagement ist ein Prozess, kein Archiv

Wenn die Grundlagen erst einmal erstellt und die Massnahmen etabliert sind ist es wichtig, das Risikomanagement als dynamischen Prozess zu verstehen. Ziel sollte nicht sein, eine möglichst grosse und schöne Dokumentation in einem Regal oder einer Ordnerstruktur zu haben, sondern aktuelle Analysen, welche die gesellschaftliche, wirtschaftliche und politische Landschaft und deren Entwicklung berücksichtigen resp. antizipieren. Nur so kann für die Geschäftsleitung ein Mehrwert hinsichtlich Entscheidfindungsprozess generiert werden.

Die Amstein + Walthert Sicherheit AG berät Sie gerne zu sämtlichen Themen der Unternehmenssicherheit und hilft Ihnen, Risiken zielführend und wirtschaftlich zu begegnen.

AMSTEIN + WALTHERT SICHERHEIT AG

Kontakt

Lucien Schibli, MSc
Consultant Safety und Security
Amstein + Walthert Sicherheit AG
Bresteneggstrasse 5 / CH-5033 Buchs
lucien.schibli@amstein-walthert.ch
Tel. +41 62 723 05 10
amstein-walthert.ch

Moderne Prozesse im Arbeits- und Gesundheitsschutz stärken Unternehmen in der Krise

Sicherheit und Gesundheit bei der Arbeit ist eines der wichtigsten Themen in der Coronavirus-Pandemie. Markus Becker, CEO des HSE-Softwareanbieters Quentic, gibt einen Einblick, wie die Digitalisierung von Arbeitssicherheit die Bewältigung der Krise unterstützen kann.

Markus Becker

Herr Markus Becker, wie wird die Covid-19-Krise das Arbeitssicherheits-management nachhaltig verändern?
Es wird in Zukunft eine noch viel bedeutendere Rolle spielen. Die Sicherheit, und vor allem der Gesundheitsschutz am Arbeitsplatz, stehen schon jetzt im Zentrum der Anstrengungen aller Unternehmen. Nur mit intelligenten Hygieneplänen, Krisenkonzepten und Risikobewertungen können wir die zweite Welle gesund überstehen. HSE-Manager tragen hier eine grosse Verantwortung, gangbare Wege zu finden und Prozesse im Bereich Arbeitssicherheit und Arbeitsgesundheit zu überdenken.

Welche Rolle spielt die Digitalisierung dabei?
Dass die Pandemie die Digitalisierung der Arbeit im Allgemeinen schon sehr beschleunigt hat, haben wir alle in den letzten Monaten zu spüren bekommen. Aber auch das HSE-Management wird hier einen deutlichen Schub erfahren. Wir sprechen für unseren Safety Management Trend Report jährlich mit Expertinnen und Experten aus der ganzen Welt und haben ihnen eben diese Frage auch gestellt. Sie bestätigen, dass gerade Unterweisungen und Schulungen auch in Zukunft deutlich orts- und zeitflexibler – also online – stattfinden werden. Das ist nur einer von vielen Bereichen, der im Arbeitsschutz sehr gut online abgebildet werden kann.

Quentic ist eine Software für Arbeitsschutz- und Umweltmanagement. Wie unterstützt Ihre Plattform Sicherheitsfachkräfte dabei, diese Prozesse digital zu steuern?
Der Bereich des HSE-Managements ist für Unternehmen zu einem komplexen Labyrinth aus Gesetzen, Vorschriften und Normen geworden, in dem sie sich zurechtfinden müssen. Dennoch müssen viele Sicherheitsfachkräfte noch immer wichtige Zahlen über unzählige Excel-Tabellenblätter im Auge behalten und Dokumente in Word-Dateien verarbeiten. Dies bedeutet nicht nur, dass Informationen unvollständig oder inkonsistent sein können, sondern auch, dass es viel Zeit kostet, relevante Dokumente und Daten zu finden.

Quentic führt alle Daten und Prozesse aus den Bereichen Arbeitssicherheit, Umwelt- und Nachhaltigkeitsmanagement in einer integrierten Lösung zusammen. Die Software bietet neun spezialisierte Module und eine App. So können Unternehmen sich eine Lösung zusammenstellen, die ihren individuellen Anforderungen entspricht. Im Zentrum steht dabei ein integriertes Datenmanagement, sodass Informationen aus dem einen Modul auch in einem anderen verwendet werden können. Das verhindert doppelte Eingaben und somit mögliche Fehler. Ausserdem sorgt das dafür, dass Daten unternehmensweit – auch über Standort- und Ländergrenzen hinweg – konsistent sind.

Bei der Umsetzung der neuen Corona-Verordnungen, konnten zum Beispiel insbesondere die Module Arbeitssicherheit, Risks & Audits, Legal Compliance und natürlich Online-Unterweisungen dabei unterstützen, neue Standards rechtskonform umzusetzen.

Welche besonderen Herausforderungen gab es für Ihre Kunden dabei?
Natürlich musste alles schnell gehen. Einige mussten innerhalb weniger Tage tausende Mitarbeiterinnen und Mitarbeiter online zum Infektionsschutz oder zur Arbeit im Homeoffice unterweisen. Zahlreiche grosse Unternehmen standen vor der Frage, wie lokale rechtliche Anforderungen erfüllt und gleichzeitig abweichende Risikoeinschätzungen zur Pandemielage in allen Standorten im Blick behalten werden können. Unsere Softwarelösung Quentic hat hier eine entscheidende Rolle gespielt, diese Fragen für sie zu beantworten und Lösungen zu schaffen.

Neben der Pandemie gibt es noch ein Thema, das viele Unternehmen umtreibt: nachhaltig und trotzdem effizient zu wirtschaften. Wie verbindet Quentic Umwelt- und Arbeitsschutzmanagement?
Aus unserer Perspektive gehen diese Themen schon immer Hand in Hand. Ich persönlich bin überzeugt, dass ökologische Verantwortung und ökonomischer Erfolg sich nicht ausschliessen, sondern sich gegenseitig beflügeln. Unsere Umwelt, also unser Ökosystem zu schützen, schliesst den Menschen mit ein. Und so sind Arbeitssicherheit, Gesundheit und Nachhaltigkeit eng miteinander verzahnt.

Ein Beispiel ist der Umgang mit Gefahrstoffen. Auf der einen Seite gibt es die Aufgabe, den Stoff selbst sicher zu handhaben, damit er zum Beispiel nicht in den Boden oder in Gewässer gelangt. Zum anderen kann es aber auch Fragen der Arbeitssicherheit geben, wenn Beschäftigte unsicher damit umgehen oder während der Arbeit mit dem Stoff die falsche Schutzausrüstung tragen.

Dies ist nur ein Beispiel, welches veranschaulicht, dass alle Unternehmensaktivitäten miteinander verbunden sind und dabei der Mensch immer im Mittelpunkt steht. Quentic bildet die Grundlage, um das gesamte HSE-Ökosystem an einem Ort zusammenzubringen.

Weitere Informationen: **www.quentic.ch**

Quentic
connect. engage. inspire.

Lernende haben ein erhöhtes Unfallrisiko

Jeder achte Lernende erleidet während seiner Ausbildung einen Berufsunfall. Die Zahlen der Suva zeigen, dass der Einstieg in die Berufswelt nicht nur interessant, sondern auch gefährlich sein kann. Anfang August haben mehrere Tausend Jugendliche den Start in das Berufsleben gewagt. Warum Berufseinsteiger besonders unfallgefährdet sind und wie man die Sicherheit für Lernende erhöht.

TEXT **ADRIAN VONLANTHEN**

Im August begann für viele Jugendliche ein neuer Lebensabschnitt. Während manche eine weiterführende schulische Ausbildung bevorzugten, wagten andere den Einstieg in das Berufsleben. Jedes Jahr sind es laut Bundesamt für Statistik (BfS) über 60 000 Jugendliche, die sich für eine Berufslehre entscheiden. 2019 verzeichnete das BfS gesamthaft rund 213 000 Jugendliche, die in einem Lehrverhältnis standen.

Lernende verunfallen doppelt so häufig

Dass der Einstieg ins Berufsleben auch mit Gefahren verbunden ist, zeigen die Zahlen der Suva. Denn das Risiko bei der Arbeit zu verunfallen, ist bei Lernenden 50 Prozent höher als bei den übrigen Arbeitnehmenden. In der Freizeit ist das Unfallrisiko sogar doppelt so hoch. Gesamthaft sind es im Schnitt 25 000 Lernende, die in der Schweiz jährlich verunfallen, zwei von diesen Unfällen enden gar tödlich.

Meist geschehen die Unfälle bei klassischen handwerklichen Arbeiten. Rund 40 Prozent der Unfälle passieren bei Arbeiten von Hand oder mit der Maschine. Beispielsweise bei handwerklichen Tätigkeiten wie Bohren, Schleifen, Schmirgeln oder an Maschinen beim Fräsen und Drehen. Am häufigsten werden Lernende von Fremdkörpern wie Splitter oder Spänen getroffen. Auch Schnittverletzungen sind häufige Unfallhergänge.

Wichtige Vorbilder haben grossen Einfluss

Die Gründe warum Lernende häufiger verunfallen liegen auf der Hand. Für Berufseinsteiger ist alles neu, sie sind sich nicht gewohnt, mit Handwerkzeug und Maschinen umzugehen. Ausserdem unterschätzen viele die Gefahren oder überschätzen die eigenen Fähigkeiten. Viele Unfälle passieren zudem, weil Lernende sich nicht trauen, bei Unsicherheiten nachzufragen. Darum haben Berufsbildner, Vorgesetzte aber auch Mitarbeitende eine zentrale Rolle. Diese dienen als Vorbilder und haben die Aufgabe, die Lernenden an die Sicherheitskultur des Unternehmens heranzuführen.

In diesem Zusammenspiel nimmt der Berufsbildner eine Schlüsselrolle ein. Er ist dafür verantwortlich, dass die Lernenden über die lebenswichtigen Regeln der Suva Bescheid wissen und diese Regeln systematisch instruiert und regelmässig wiederholt werden. Dazu gehört auch die Anwendung der persönlichen Schutzausrüstung (PSA). Bei der praktischen Umsetzung empfiehlt es sich, dass die Berufsbildner den Sicherheitsberater des Unternehmens einzubeziehen, damit die Lernenden von dessen Wissen profitieren und aus erster Hand am Ort des Geschehens erleben, wo die Gefahren auf der Baustelle oder im Betrieb lauern. Nicht zuletzt können die Mitarbeitenden ihren Teil dazu beitragen, die Sicherheit für Lernende zu erhöhen, indem sie sich selbst an die Regeln halten und die Berufseinsteigerinnen und Berufseinsteiger darauf hinweisen, wenn lebenswichtige Regeln verletzt werden.

Gut zu wissen

Keine Arbeit ist so wichtig, dass man dafür einen Unfall oder gar sein Leben oder das Leben seiner Arbeitskollegen riskieren muss.

Um Unfälle bei Lernenden nachhaltig zu verhindern, sind folgende Punkte wichtig:

- Lernende sagen bei Gefahr und in unsicheren Situationen STOPP und klären gemeinsam mit dem Vorgesetzten die Situation.
- Die Vorgesetzten und Berufsbildner führen Lernende systematisch in die Sicherheitsregeln ihres Berufs und Betriebs ein. Sie sind Vorbilder und wiederholen Schulungen zum Thema Sicherheit in regelmässigen Abständen.
- Lernende sind sich aufgrund ihrer Einführung durch Vorgesetzte und Berufsbildner der Risiken am Arbeitsplatz und in der Freizeit bewusst und tragen konsequent ab dem ersten Ausbildungstag ihre persönliche Schutzausrüstung.

Mit Arbeitssicherheit und Gesundheitsschutz kann viel Geld eingespart werden

Unternehmen in der Schweiz, die mehr als zehn Mitarbeitende beschäftigen und besondere Gefährdungen in ihren Prozessen aufweisen, benötigen aus rechtlicher Sicht ein umfassendes Sicherheitssystem und Sicherheitsbeauftragte im Betrieb.

Die Ausbildung von Sicherheitsbeauftragten und Erstellung eines Sicherheitssystems liegen in der Verantwortung der Arbeitgeber. Ein Sicherheitssystem beschreibt, wie die gesetzlichen Vorgaben zum Unfallversicherungs- und Arbeitsgesetz intern umgesetzt werden. Sicherheits- aber auch Gesundheitsbeauftragte übernehmen hierbei wichtige Aufgaben zur Entlastung des Arbeitgebers und bilden in der Umsetzung des Sicherheitssystems das Bindeglied zwischen Mitarbeitenden, Geschäftsleitung und Behörden.

Weiter lernen die Sicherheitsbeauftragten während der Ausbildung ihre Aufgaben zur Erfüllung der rechtlichen Vorgaben, aber auch Methoden und Techniken kennen, wie Unfälle und Krankheiten präventiv verhindert werden können. Ein Arbeitsunfall kostet schnell über 100 000 Franken – wovon nur die direkten Kosten von der Versicherung übernommen werden. Die anderen Kosten, die in der Regel massiv höher ausfallen, hat das Unternehmen zu tragen! Um böse Überraschungen zu vermeiden, sollten Unternehmen deshalb Arbeitssicherheit und Gesundheitsschutz unbedingt in den Fokus stellen.

Wie gehen Unternehmen am besten vor?
Schweizweit anerkannte Kurse aber auch Unterstützung im Aufbau eines Sicherheitssystems werden von der Qualitätswerk GmbH angeboten, welche Kurse im Schulungsnetzwerk der SUVA durchführt. Qualitätswerk passt ihre Dienstleistungen und Schulungsangebote laufend an die Kundenbedürfnisse an. Dies hat sich auch während der aktuellen Situation zur Pandemie gezeigt: Als einziger Anbieter in diesem Bereich war die Qualitätswerk GmbH in der Lage, ihre Kurse in den virtuellen Raum zu verlegen. Roger Weber, der den digitalen Kurs zum Sicherheitsbeauftragten im Oktober 2020 abgeschlossen hat, berichtet:

Herr Roger Weber, wie erlebten Sie die digitalen Kurse von Qualitätswerk?
Nach erfolgter Anmeldung erhielt ich innert wenigen Tagen das Paket von Qualitätswerk mit Schulungsordner, USB-Stick und einer Anleitung zur Durchführung. Das Vorgehen war sehr simpel; auf dem USB-Stick waren die Lernmodule in Form einer vertonten Bildschirmpräsentation abgespeichert, mit welcher die Schulung wie live vor Ort ablief.

Die Schulung erlebte ich als sehr kurzweilig und spannend. Besonders gefallen hat mir die ansprechende Präsentation mit eindrücklichen Bildern und Filmen, die mir einerseits geholfen haben, die Theorie in der Praxis einzuordnen und andererseits die Schulung spannend machten.

Welchen Mehrwert versprechen Sie sich von diesem Kurs?
Ich bin derzeit auf der Suche nach einer neuen Stelle. In den Inseraten wird oft die Ausbildung zum Sicherheitsbeauftragten vorausgesetzt oder erwünscht. Mit dieser Ausbildung und dem anerkannten Zertifikat bin ich überzeugt, mehr Chancen auf dem Arbeitsmarkt zu erlangen.

Wieso haben Sie sich für Qualitätswerk als Anbieter entschieden?
Wegen der Pandemie wollte ich den SIBE-Kurs online absolvieren. Auf der Suche hatte ich hierbei nur Qualitätswerk finden können, die den Kurs digital anbieten. Da Qualitätswerk zudem die beste Kurs-Bewertung auf «ausbildung-weiterbildung.ch» erhielt, war für mich der Fall schnell klar. Weiter entsprachen auch die Kurskosten meinem Budget.

Weshalb würden Sie Qualitätswerk weiterempfehlen?
Der digitale Kurs war kurzweilig und hat meine Erwartungen vollumfänglich erfüllt. Ich fühle mich nun fähig, die Rolle als Sicherheitsbeauftragter wahrzunehmen und weiss, dass ich mich bei Fragen immer an Qualitätswerk wenden darf, was ich auch bereits getan habe: Der Kontakt war angenehm und meine Fragen wurden äusserst kompetent beantwortet. Ich wüsste nicht, wie der Kurs sowie die Dienstleistungen noch besser gemacht werden könnten.

Kurs SIBE

Die Ausbildung für Sicherheitsbeauftragte dauert zwei Tage und beinhaltet die von der Suva vorgegebenen Inhalte und Lernziele. Unter anderem werden folgende Themen während der Schulung behandelt:

- Grundlagen und Einführung in die Thematik
- Unfälle, Krankheiten und ihre Folgen
- Persönliche Schutzausrüstung
- Umgang mit und Reduktionen von Gefahren
- Rechtliche Aspekte der Arbeitssicherheit
- Aufgaben von Sicherheitsfachpersonen
- Vorgaben für Unternehmen
- Kontrollmechanismen

Nach erfolgreich absolviertem Kurs wird den Teilnehmenden ein schweizweit anerkanntes Zertifikat ausgestellt.

Weiterführende Informationen:
qualitaetswerk.ch

Qualitätswerk GmbH

Kurs Lehrgang Safetycoordinator

Qualitätswerk geht sogar noch einen Schritt weiter! Ab 2021 bietet das Unternehmen den neuen Lehrgang zum «Safetycoordinator» an. Dieser Lehrgang beinhaltet nebst dem Grundkurs für Sicherheitsbeauftragte zusätzliche wichtige Bausteine in der Unfall- und Krankheitsprävention. In zehn Tagen werden die Teilnehmenden nebst Arbeitssicherheit und Gesundheitsschutz auch in den Bereichen Gefahrguttransport, Brandschutz und Erstellung eines Sicherheitssystems u.v.m. ausgebildet.

Kurs GEBE

Gesundheitsschutz wird auf Grund der Vorgaben in der Ausbildung für Sicherheitsbeauftragte nur am Rande thematisiert, obschon die Krankheitskosten generell um ein Vielfaches höher ausfallen als die Unfallkosten. Deshalb lancierte Qualitätswerk als erster Schweizer Anbieter mit der ergänzenden Ausbildung zum Gesundheitsbeauftragten eine Erweiterung der bestehenden SIBE-Ausbildung.

Continental
The Future in Motion

Echt schweizerisch: zuverlässig und sicher. Aber ohne Kompromisse.

GERMAN
TECHNOLOGY

Seit rund 150 Jahren sind wir die Pioniere des Reifenbaus: Eintausend Wissenschaftler, Designer und Ingenieure arbeiten bei uns an Innovationen, Entwicklungen und Tests – damit Sie nicht nur sicher durch den Winter kommen, sondern auch ebenso sicher durch Frühling, Sommer und Herbst.