FOCUS

Nr. 31 | Juli 2018

tcbe.ch
ICT Cluster Bern, Switzerland

Security/ Datenschutz Enabler für die Digitalisierung

DSGVO – Das neue Datenschutzgesetz

Digital Forensics

Drohnen – Chancen & Risiken

Grüsse aus dem Darknet

E-Government – stärkt den Staat

Digitalisierung – Faktor Mensch

be advanced

TSBE Bern

Höhere Fachschule

www.tsbe.ch

Neue Studienlehrgänge ab 2. Februar 2019

Wissen ist der Weg zu Deinem Erfolg, wir begleiten Dich:

dipl. Techniker/In HF Telekommunikation
dipl. Techniker/In HF Informatik
dipl. Techniker/In HF Informatik Systemtechnik

Berufsbegleitende Ausbildung in 5 Semestern.

Eine Institution der gibb Weiterbildung

Kellerhals Carrard

Old Economy vs. Industry 4.0, Legal Tech, Robotics, Fintech, Building Information Modeling, Big Data, e-Government, Smart Contracts, Blockchain Technology, Cloud Solutions, XaaS, Internet of Things.

Ihre kompetenten Partner – analog und digital.

www.kellerhals-carrard.ch

No security by obscurity

«No security by obscurity» ist ein wichtiger Grundsatz in der modernen Kryptographie, der auf einer bereits 1883 publizierten Arbeit des niederländischen Linguisten und Kryptologen Auguste Kerckhoffs basiert. Die Aussage «Keine Sicherheit durch Verschleierung» besagt, dass die Sicherheit eines Verschlüsselungsverfahrens besser auf der Geheimhaltung des Schlüssels beruht anstelle auf der Geheimhaltung des Verschlüsselungsalgorithmus. So ist es bekanntermassen einfacher, einen Schlüssel (ein langes Passwort) geheim zu halten als einen Algorithmus (ein kurzes Computer-Programm). Und falls der Schlüssel doch einmal in falsche Hände geraten sollte, kann er einfacher durch einen neuen Schlüssel ersetzt werden als dass ein Algorithmus neu programmiert wird. Der transparente Quellcode eines Algorithmus hat ausserdem den Vorteil, dass Fachleute besser Fehler und Schwachstellen identifizieren können. Damit wird auch die Gefahr minimiert, dass jemand eine versteckte Hintertür («Backdoor») einbauen kann.

Nach diesem Transparenz-Prinzip «No security by obscurity» sind alle modernen asymmetrische Kryptosysteme (Public-Key-Verschlüsselungsverfahren, Public-Key-Authentifizierung, digitale Signaturen) entwickelt, die heute überall in der Informatik angewendet werden: Verschlüsselung von Emails, sichere Kommunikation im Webbrowser (mittels HTTPS – Hypertext Transfer Protocol Secure), signierte PDFs, Kryptowährungen wie Bitcoin und andere Blockchain-Anwendungen, usw. Bei all diesen Verfahren ist der Quellcode der Verschlüsselungsverfahren zwar offen zugänglich, aber der eigentliche Schlüssel (das Passwort) bleibt geheim.

Neben diesen technischen Grundlagen ist aber auch immer der «Faktor Mensch» entscheidend, ob die Sicherheit im Unternehmen und bei Behörden gewährleistet ist oder nicht. So zeigen die spannenden Beiträge dieser neuen FOCUS-Ausgabe, dass alle technischen Massnahmen nichts nützen, wenn die Mitarbeitenden nicht genügend zu IT-Security ausgebildet und auf aktuelle Gefahren sensibilisiert sind (siehe Seite 9: «Warum technische Massnahmen alleine nicht ausreichen, um die IT-Sicherheit meines Unternehmens zu gewährleisten»). Auch ist es entscheidend zu verstehen, wie die Dynamik des Darknet funktioniert, was böswillige Hacker antreibt und welche Gegenmassnahmen möglich sind (siehe Seite 13: «Grüsse aus dem Darknet von ‹Petya›, ‹WannaCry› und Co.»). Ein praktisches Beispiel, wie offene Standards in Sicherheits-Systemen einen Mehrwert schaffen und Herstellerabhängigkeiten reduzieren, zeigt die Schaffung einer Interessensgemeinschaft von Offline-RFID Endanwendern (siehe Seite 28: «Zutrittssysteme: Ein Offline-Zutritts-Standard ist gefordert»). Zahlreiche weitere Beiträge des vorliegenden FOCUS behandeln ausserdem die neuen Entwicklungen beim Datenschutz, insbesondere der neuen EU Datenschutzgrundverordnung (DSGVO, siehe Seiten 5 «Ein Überblick über die laufenden Datenschutzrevisionen in Europa und der Schweiz» und Seite 7 «Handlungsbedarf für Schweizer Firmen und Organisationen».)

Die DSGVO war auch an der diesjährigen tcbe.ch Generalversammlung ein wichtiges Thema, als Dr. Monique Sturny von Walder Wyss AG die Auswirkungen der neuen EU-Gesetzgebung auf Schweizer Unternehmen aufzeigte (Folien auf www.tcbe.ch/gv2018 publiziert). Daneben lief viel beim tcbe.ch in den letzten 12 Monaten: wir führten einen Abendanlass zu Smart City und Open Government im September 2017 durch, veranstalteten einen Event zum Internet der Dinge im Oktober 2017, feierten im November 2017 das 20-jährige Jubiläum des tcbe.ch und starteten mit Scratch-Programmierkursen für Kinder und Jugendliche ins 2018. Auch bereits im aktuellen Jahr führten wir einen Abendanlass zur Rolle des Menschen in der Digitalisierung durch und organisierten um 7 Uhr früh den ersten Digital Morning zum Thema Augmented und Virtual Reality im Bauwesen.

Als Präsident des tcbe.ch freut es mich, nun mit 14 Kolleginnen und Kollegen im

Vorstand und insbesondere mit Rebeca Sanchez als neue Office Managerin die Zukunft des tcbe.ch zu gestalten. Bald schon werden wir diesbezüglich ein neues Kapitel beginnen: Wie bereits an der diesjährigen Generalversammlung angetönt, wollen wir uns als tcbe.ch einen neuen, zeitgemässen Namen und einen komplett überarbeiteten visuellen Auftritt geben. Wir freuen uns deshalb, Ihnen am diesjährigen Digitaltag am Donnerstag, 25. Oktober 2018 den neuen Namen inklusive Logo und Website vorzustellen – die Einladung folgt!

Dr. Matthias Stürmer
Präsident tcbe.ch – ICT Cluster Bern, Switzerland

Impressum

FOCUS>tcbe.ch
Organ des tcbe.ch – ICT Cluster Bern, Switzerland
Erscheint 1 bis 2-mal jährlich

6000 Exemplare

Herausgeber
tcbe.ch – ICT Cluster Bern, Switzerland
c/o Impact Hub
Spitalgasse 28
3011 Bern
Tel. +41 (0)31 388 70 70
Fax. +41 (0)31 388 87 88
E-Mail: info@tcbe.ch, www.tcbe.ch

Redaktion, Inseratemanagement
Andreas Dürsteler, Swisscom AG
E-Mail: andreas.duersteler@tcbe.ch,
Tel. 079 277 54 90

Gesamtherstellung
Stämpfli AG,
Dienstleistungen und Produktion
Wölflistrasse 1, Postfach, 3001 Bern
Tel. 031 300 66 66, Fax 031 300 66 99
E-Mail: info@staempfli.com
www.staempfli.com

Titelbild: Security

Inhaltsverzeichnis

DATENSCHUTZREVISION

E-DSG und EU-DSGVO als unternehmerische Herausforderung:

Ein Überblick über die laufenden Datenschutzrevisionen in Europa und der Schweiz

Das Datenschutzrecht ist zurzeit in aller Munde. Sowohl in der Schweiz, wie auch in der EU laufen konkrete Bestrebungen zur Revision der Datenschutzgesetzgebungen. In der Schweiz wurde am 15. September 2017 der Gesetzesentwurf zum revidierten Datenschutzgesetz (E-DSG) publiziert. Wann das E-DSG in Kraft treten wird, ist derzeit aber noch offen. Bereits einen Schritt weiter ist die EU. Die Verordnung zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten (EU-DSGVO), welche in der EU direkt geltendes Recht darstellen wird, tritt per 25. Mai 2018 in Kraft. Die nachfolgenden Ausführungen erfolgen deshalb schwergewichtig zur EU-DSGVO, die erhebliche Auswirkungen auf Schweizer Unternehmen hat, ohne aber den Vergleich zum E-DSG zu vernachlässigen.

Geltung der EU-DSGVO in der Schweiz

Der Anwendungsbereich der EU-DSGVO ist sehr weit und reicht über die Grenzen der EU hinaus. Die Verordnung findet extraterritorial Anwendung, wenn der Verarbeiter der Personendaten gegenüber Personen in der EU Waren oder Dienstleistungen anbietet oder wenn er durch die Datenbearbeitung das Verhalten der betroffenen Personen in der EU beobachten will.

Für die Beantwortung der Frage, ob Waren oder Dienstleistungen angeboten werden, ist relevant, ob das (Schweizer) Unternehmen offensichtlich beabsichtigt, betroffenen Personen in der EU Waren oder Dienstleistungen anzubieten. Hinweise für eine solche Absicht ergeben sich aus Kriterien wie der Verwendung einer Sprache oder Währung, die im jeweiligen EU-Mitgliedsstaat, nicht aber in der Schweiz gebräuchlich ist, in Verbindung mit der Möglichkeit, Waren oder Dienstleistungen in dieser anderen Sprache zu bestellen, oder die Erwähnung von anderen Kunden oder Nutzern, die sich in der EU befinden.

Die Absicht, durch die Datenverarbeitung das Verhalten betroffener Personen in der EU zu beobachten, wird bspw. daran festgemacht, ob Internetaktivitäten dieser betroffenen Personen nachvollzogen (z.B. durch Google Analytics) und/oder Techniken zur Profilerstellung natürlicher Personen eingesetzt werden.

Aufgrund dieses weit gefassten Anwendungsbereichs wird die Mehrzahl der Schweizer Unternehmen von der EU-DSGVO betroffen sein.

Definition der Personendaten

Das Verständnis, was unter Personendaten zu verstehen ist, ist in der Schweiz und der EU identisch und umfasst alle Angaben, die sich auf eine bestimmte oder bestimmbare Person beziehen. Diese Definition umfasst gegebenenfalls auch Cookies und IP Adressen, sofern diese nicht nur z.B. einer schnelleren Anmeldung dienen. Strengere Vorschriften gelten für besonders schützenswerte Personendaten (z.B. betreffend Religion oder Gesundheit), welche zusätzlich geschützt sind.

Grundsätze der Bearbeitung

Bearbeiten von Personendaten meint jeden Umgang mit Personendaten, unabhängig von den angewandten Mittel und Verfahren. Dabei gilt in der Schweiz (sowohl unter geltendem, wie voraussichtlich auch unter neuem Recht), dass die Bearbeitung grundsätzlich erlaubt ist, wenn die Bearbeitung gewissen Grundsätzen genügt. Insbesondere muss die Bearbeitung transparent und zweckgebunden erfolgen.

Demgegenüber sieht die EU-DSGVO vor, dass jede Bearbeitung verboten ist, sofern diese nicht ausdrücklich durch die Verordnung erlaubt ist. Erlaubt ist die Bearbeitung u.a. dann, wenn die betroffene Person in die Bearbeitung einwilligt, oder wenn sie für die Erfüllung eines Vertrages oder rechtlicher Pflichten notwendig ist.

Pflichten für Unternehmen

Die EU-DSGVO enthält zahlreiche Pflichten für die von der Verordnung betroffenen Schweizer Unternehmen. Nachfolgend werden deshalb nur die Wichtigsten erörtert, welche in dieser Form im E-DSG nicht vorgesehen sind.

1. Einwilligung

Ausgehend vom in der EU-DSGVO vorherrschenden Grundsatz des Verbots mit Erlaubnisvorbehalt, haben die Unternehmen verschiedene Pflichten zu erfüllen, damit eine gültige Einwilligung der betroffenen Person vorliegt.

Die Einwilligung ist nur dann gültig, wenn sie von der betroffenen Person freiwillig abgegeben wird, wobei ihr eine «echt Wahl» gelassen werden muss. Verboten sind insb. sog. Koppelungsgeschäfte, wonach der Abschluss eines Vertrages nicht von der Verarbeitung weiterer Daten abhängig gemacht werden darf, die für die eigentliche Vertragserfüllung gar nicht benötigt werden. Zudem muss die betroffene Person über den Zweck der Beschaffung

und Verarbeitung der personenbezogenen Daten informiert werden. Die Einwilligung an und für sich ist an keine bestimmte Form gebunden und kann auch elektronisch erfolgen. Jedoch ist eine aktive Handlung der betroffenen Person gefordert, was eine stillschweigende Zustimmung oder die Zustimmung durch bereits angekreuzte Kästchen ausschliesst. Schliesslich muss die Einwilligung jederzeit widerrufbar sein.

2. «Privacy by Design» und «Privacy by Default»

Die EU-DSGVO verlangt, dass der Datenschutz bei Produkten und Dienstleistungen bereits in der Planungsphase berücksichtigt wird. So müssen die Grundsätze des Datenschutzes bereits bei der technischen Ausgestaltung berücksichtigt werden (Privacy by Design; z.B. durch ein neues IT-System) und zusätzlich müssen die Produkte und Dienstleistungen mit datenschutzfreundlichen Voreinstellungen angeboten werden (Privacy bi Default). So muss beispielsweise eine Webseite Einkäufe ermöglichen, ohne dass dabei ein Benutzerprofil erstellt werden muss.

3. Ernennung eines Vertreters in der EU

Sofern eine regelmässige Bearbeitung der Personendaten erfolgt, müssen Unternehmen, welche dem Anwendungsbereich der EU-DSGVO unterstehen einen Vertreter in der EU bezeichnen.

4. Weitere Pflichten

Als weitere nennenswerte Pflicht, welche auch im E-DSG vorgesehen ist, muss das der EU-DSGVO unterliegende Unternehmen ein Verzeichnis der Verarbeitungstätigkeiten führen. Wenn eine Form der Verarbeitung wahrscheinlich ein hohes Risiko verursacht (z.B. bei noch unbekannten Technologien), muss sowohl nach E-DSG, wie auch nach der EU-DSGVO eine sog. Datenschutz-Folgeabschätzung gemacht und gegebenenfalls die Aufsichtsbehörde informiert werden.

Folgen der Verletzung

Verletzungen des Schutzes personenbezogener Daten müssen innert 72 Stunden der Aufsichtsbehörde gemeldet werden. Eine Verletzung ist aber zusätzlich mit einer Busse von bis zu 20 Millionen Euro oder bis zu 4% des gesamten, weltweit erzielten Jahresumsatzes im vergangenen Geschäftsjahr – je nach dem welcher Wert höher ist – bedroht. Zu erwähnen ist schliesslich, dass die EU-DSGVO ein Verbandsklagerecht vorsieht, womit Konsumentenschutzverbände die Rechte der Betroffenen geltend machen können. Ein derartiges Verbandsklagerecht ist der schweizerischen Zivilprozessordnung (ZPO) bisher unbekannt, aber in der anstehenden ZPO-Revision ebenfalls vorgesehen.

Autoren

Patrick Mettler, MLaw, Rechtsanwalt, Associate Kellerhals Carrard

Dr. Christoph Zimmerli, LL.M. (Europäisches Recht), Rechtsanwalt, Partner Kellerhals Carrard, Vorstandsmitglied tcbe.ch

Fazit

Die umfassenden Änderungen im Datenschutzrecht sind für Schweizer Unternehmen mit nicht unerheblichem Aufwand verbunden und stellen eine echte Herausforderung dar. Jedoch wäre es fehl am Platz aufgrund des horrenden Bussenkataloges gemäss EU-DSGVO in Panik zu verfallen. Sofern nicht mutwillig gegen die Vorschriften verstossen wird, ist davon auszugehen, dass aufgrund der diversen noch vorherrschenden Unklarheiten (zunächst) nicht mit drakonischen Strafen zu rechnen ist. Auf jeden Fall lohnt es sich für Schweizer Unternehmen aber, ihre Datenschutzsituation durch Fachpersonen überprüfen zu lassen und wo nötig in ihren Grundlagen und/oder Prozessen Anpassungen vorzunehmen, um «compliant» zu sein.

DSG-GESETZ

EU-Datenschutzgrundverordnung (DSGVO):

Handlungsbedarf für Schweizer Firmen und Organisationen

Am 25. Mai 2018 tritt die neue EU-Datenschutzgrundverordnung (DSGVO) in Kraft. Damit werden die Regeln für die Verarbeitung personenbezogener Daten, die Rechte der Betroffenen und die Pflichten der Verantwortlichen EU-weit vereinheitlicht. Die Panik im Vorfeld der DSGVO ist beachtlich, nicht zuletzt wegen des drastischen Bussenkatalogs von bis zu 20 Millionen Euro bzw. 4% des weltweiten Jahresumsatzes. Die DSGVO betrifft nicht nur in der EU ansässige Unternehmen, sondern auch sämtliche Schweizer Unternehmen und Organisationen, die Leistungen an Kunden in der EU anbieten oder in der EU eine Niederlassung oder Tochtergesellschaft haben. Der schweizerische Gesetzgeber hinkt mit dem hiesigen Datenschutzgesetz noch etwas hinterher. Es ist jedoch zu erwarten, dass wesentliche Teile der DSGVO übernommen werden, damit das schweizerische DSG durch die EU als gleichwertig anerkannt wird.

Es soll hier nicht näher auf die DSGVO und deren Auswirkungen eingegangen werden. Diese werden im Beitrag von Christoph Zimmerli (Seite 5/6 in diesem Magazin) ausführlich dargestellt. Wir konzentrieren uns den nachfolgenden Ausführungen auf die konkreten Massnahmen, die von Firmen und Organisationen in der Schweiz getroffen werden müssen. Einerseits ist bei praktisch allen die Wahrscheinlichkeit gross, dass in irgend einem Bereich ein EU-Bezug besteht (EU-Bürger als Mitarbeiter, Kunden oder Lieferanten mit Adresse im EU-Raum), und andererseits ist zu erwarten, dass sich die neue schweizerische Datenschutzgesetzgebung weitgehend der DSGVO angleichen wird. Deshalb empfehlen wir den Unternehmen und Organisationen in der Schweiz, sich künftig grundsätzlich DSGVO-konform zu verhalten. Ein wesentlicher Punkt dabei ist, dass es sich hier nicht um ein reines IT-Thema handelt. Die Firmenleitung (Verwaltungsrat, Geschäftsleitung) ist in der Verantwortung und tut gut daran, diese wahrzunehmen.

Welche Schritte müssen Sie vorkehren, damit auch Ihr Unternehmen den Anforderungen der neuen Datenschutzvorgaben genügen wird? Wir unterscheiden verschiedene Handlungsfelder, welche parallel anzugehen sind:

Organisatorische Massnahmen

Als Erstes gilt es, ein Inventar zu erstellen von allen Datenbeständen natürlicher Personen (auf juristische Personen ist die DSGVO nicht anwendbar). Dabei sollte geprüft werden, welche dieser Daten wirklich gebraucht werden, und welche Daten als besonders schutzwürdig gelten. Anschliessend müssen Prozesse einführt, dokumentiert und dann auch regelmässig kontrolliert werden für deren Erfassung, Bewirtschaftung, sowie Archivierung und Löschung. Dabei ist der Grundsatz zu berücksichtigen, dass von den Betroffenen grundsätzlich die Zustimmung zu einer Datenschutzerklärung (s. unten) vorliegen muss. Ausserdem ist ein/e Datenschutzverantwortliche/r zu bestimmen.

Massnahmen im Bereich Marketing

Die Zustellung von Newsletters ist beispielsweise neu nur bei vorhandener Einwilligung des Empfängers erlaubt. Mit dieser Bestimmung wird unter Umständen das Marketing-Konzept eines Unternehmens in Frage gestellt. Das bestehende CRM (Customer Relation Management) muss ebenfalls den neuen Bestimmungen entsprechen. Es gilt deshalb, die Auswirkung der DSGVO auch mit den Marketingverantwortlichen genau zu analysieren und bei Bedarf die notwendigen Anpassungen vorzunehmen.

Technische Massnahmen

Mit der Umsetzung der technischen Massnahmen wird die IT beauftragt, allenfalls unterstützt von weiteren Experten. Hier geht es um verschiedene, ganz unterschiedliche Aspekte:

- Organisation der Datenbestände und Zugriffsberechtigungen
- Ort (bzw. Land) der Datenspeicherung
- Zugriffsschutz auf die IT-Infrastruktur (Systeme, Netzwerk)
- Allfällige Verschlüsselung besonders schützenswerter Daten
- Schutzmassnahmen im Bereich Cyber Security (Firewall, DMZ, usw.)
- Unterhaltsmassnahmen, Service Level Agreements
- Datensicherung und –archivierung
- Physischer Schutz der IT-Systeme gegen Diebstahl und Zerstörung
- Notfallkonzept
- Controlling-Prozess und periodische Audits

Juristische Massnahmen

Für diese Aufgaben ist die Unterstützung durch Fachjuristen sinnvoll. Minimal sollte eine Datenschutzerklärung zur Datenhaltung der Firma verfasst werden, welche separat von den Allgemeinen Geschäftsbedingungen publiziert wird. Je nach Art der bewirtschafteten Datenbestände braucht es weitere Massnahmen, wie beispielsweise eine Datenschutzfolgeabschätzung bei besonders schützenswerten Daten.

Je nach Branche und Art der Geschäftstätigkeit können die erforderlichen Mass-

nahmen sehr unterschiedlich sein. Wir empfehlen allen Verwaltungsräten von Firmen und Vorständen von Organisationen, umgehend eine verantwortliche Person aus ihrem Kreis zu bestimmen, welche mit der Umsetzung der notwendigen Massnahmen beauftragt wird. Dazu wird diese mit Fachleuten aus den jeweiligen Bereichen zusammenarbeiten müssen. Sofern intern das notwendige KnowHow fehlt (was bei den meistens KMU der Fall sein dürfte), sollten sie sich von externen Fachleuten beraten und begleiten lassen.

Autor

Daniel Stucki
DS Management Consulting GmbH
VR-Präsident Keller Informatik AG
mail@dsmc.ch / 079 334 55 67

Weitere Informationen:
www.dsmc.ch
www.kellerinfo.ch/dsgvo
www.e-forum.ch/dsgvo

IT-SICHERHEIT IM UNTERNEHMEN

Warum technische Massnahmen alleine nicht ausreichen, um die IT-Sicherheit meines Unternehmens zu gewährleisten

Die Vorteile von Digitalisierung, Cloud-Technologien, Self-Service-Portalen, Apps und ähnlichen Themen sind in aller Munde. Wenn man dann aber bei Firmen, die sich mit diesen Vorhaben konkret auseinandersetzen, genauer nachfragt, dann kämpfen sie neben technischen Hürden und Fallstricken vor allem mit offenen Fragen zur IT-Sicherheit, mit (zu) vielen und teils unklaren Vorschriften und mit dem «Faktor Mensch». Als CISO oder Mitglied des IT-Managements bin ich dafür verantwortlich, diese Klippen zu umschiffen, um einen sicheren Einsatz der oben genannten Themen zu gewährleisten. Doch was gilt es für mich denn genau zu beachten, um dies zu erreichen?

Aus der Erfahrung der Sicherheitsexperten von e3 müssen hier zwei Bereiche besonders beachtet werden:

- Das Ziel: Zuerst muss ich mir – zusammen mit dem Business – darüber klar werden, was eigentlich erwartet wird. Tönt trivial, wird aber oftmals vernachlässigt. Dabei ist es auch wichtig, meine Mitarbeitenden mit einzubeziehen, denn nur so habe ich danach eine Lösung, die akzeptiert und verwendet wird.
- Der Faktor Mensch: Ich muss meinen Mitarbeitenden klarmachen, wie sie mit den neuen Technologien umgehen sollen. Nur so werden sie die Grundsätze der IT-Sicherheit einhalten und mithelfen, die gesteckten Sicherheitsziele zu erreichen. Die technischen Massnahmen können noch so gut sein, ohne die Mithilfe jedes einzelnen Mitarbeitenden kann die IT-Sicherheit meines Unternehmens nicht gewährleistet werden.

Das Ziel

Was will/kann/darf ich denn überhaupt? Egal, ob es um das Verschieben von Daten oder Apps in die Cloud, das Erstellen eines Self-Service-Portals (eGov) oder die Einführung digitaler Kundendossiers geht, zuerst einmal muss ich ein paar grundsätzliche Fragen beantworten. Und dabei geht es nicht nur um IT-Sicherheit, sondern natürlich vor allem um das Business. Das tönt logisch, in diesem Punkt steckt aber
a) viel Arbeit und
b) der Grundstein zum späteren Erfolg

Wenn ich bei diesem Punkt nur von möglichen Einsparungen oder den üblichen «Quick-Wins» geblendet werde und dabei die konkreten Rahmenbedingungen und Anforderungen ausser Acht lasse, dann habe ich am Ende des Projektes zwar eine neue Technologie eingeführt, aber nicht den vollen Nutzen davon. Ausserdem ist es wichtig, zuerst zu klären, ob ich mir diese Fragen ev. auch für das nächste Vorhaben wieder stellen muss. Es kann sich lohnen, ein übergreifendes Strategiepapier zu erstellen, auf das ich bei jedem Vorhaben wieder zurückkommen kann.

Erarbeitung einer Strategie

Startpunkt für jedes Thema ist die eigene Strategie: Was wollen Business und IT denn eigentlich erreichen? Geht es um Einsparungen, einen besseren Service für meine Kunden, eine Vereinfachung der internen Abläufe oder einfach den Einsatz einer «coolen», neuen Technologie? Wie stark kann und will ich die Kontrolle über die Infrastruktur und die Prozesse abgeben? Welche Risiken bin ich bereit, einzugehen? Wie passt das Thema zu meiner bestehenden Infrastruktur und meinen bestehenden Prozessen? Wie viel Veränderung kann und will ich meinen Mitarbeitenden zumuten? Wie kann ich die Mitarbeitenden in das Vorhaben mit einbeziehen, um ihre Anforderungen und gegebenenfalls auch ihre Ängste genügend zu berücksichtigen?

Ebenso wichtig sind rechtliche, regulatorische und strategische Rahmenbedingungen. Was darf ich denn überhaupt? Kenne ich die gesetzlichen Grundlagen, die für mein Unternehmen gelten? Gibt es gesetzliche oder regulatorische Vorgaben, die mein Unternehmen einhalten muss (z.B. Finma, GDPR, HIPAA, …)? Gibt es Standards, die mein Unternehmen erfüllen muss (z.B. ISO27000, PCI-DSS, …)? Gibt es strategische Vorgaben meines Unternehmens, die zur Anwendung kommen (z.B. nur Anbieter mit Datenhaltung in der Schweiz)?

Diese und andere Fragen muss ich – zusammen mit dem Business – beantworten, bevor es überhaupt sinnvoll ist, Zeit und Geld in weitere Abklärungen zu investieren.

Der Faktor Mensch

Um die Digitalisierung des eigenen Unternehmens weiter voranzutreiben und möglichst stark von den neuen Technologien zu profitieren, wird alles Mögliche an Sicherheitssystemen eingesetzt. Ziel ist es immer, die eigenen Daten und Applikationen zu schützen und Angriffe der «Bösen» zu verhindern (Antivirus, Firewalls, automatische Updates und Patches, Security-Policies, Zwei-Faktor-Authentisierung, Web-Proxies, Intrusion Detection Systems, Netzwerksegmentierung, …). Diese Systeme sind sicherlich alle sinnvoll und wichtig, dabei geht aber leider oft ein wichtiger

Aspekt vergessen: der Faktor Mensch. Egal, wie gut die eigenen Abwehr- oder Kontrollsysteme sind, es gibt immer jemanden, der irgendwo – willentlich oder aus Versehen – einen Knopf drücken kann und dann ist der Schaden trotz aller Sicherheitssysteme eben doch da. Genau hier setzen auch Angriffe an, die sich durch kein Sicherheitssystem verhindern lassen. Ein Beispiel dafür ist Social Engineering, das gezielte Beeinflussen und Manipulieren einer Person mit dem Ziel, sie zu einer Aktion zu bewegen, die sie eigentlich gar nicht machen will respektive machen darf.

Um auch dieses «Risiko Mensch» aktiv zu bearbeiten, bietet sich die Durchführung einer Kampagne zur Ausbildung und Sensibilisierung an, damit meine Mitarbeitenden die eingesetzten Systeme, die Gefahren und das richtige Verhalten kennen. Aus dieser Awareness-Kampagne sollte ich einen laufenden Prozess machen, um Vermitteltes zu festigen und auf Veränderungen zu reagieren (z.B. neue Mitarbeitende, neue Systeme).

Abbildung 1: mögliche Themen einer Awareness-Kampagne

Ziele einer Awareness-Kampagne:

- Die Mitarbeitenden kennen die Gefahren der IT
- Die Mitarbeitenden sind sich bewusst, was ihre Aufgaben in der Abwehr dieser Gefahren sind
- Die Mitarbeitenden kennen die Vorgaben des Unternehmens (die leider oft erst bei der Vorbereitung einer Awareness-Kampagne erarbeitet werden)
- Die Mitarbeitenden wissen, wie sie im Fall der Fälle reagieren müssen (z.B. Verlust eines Laptops)

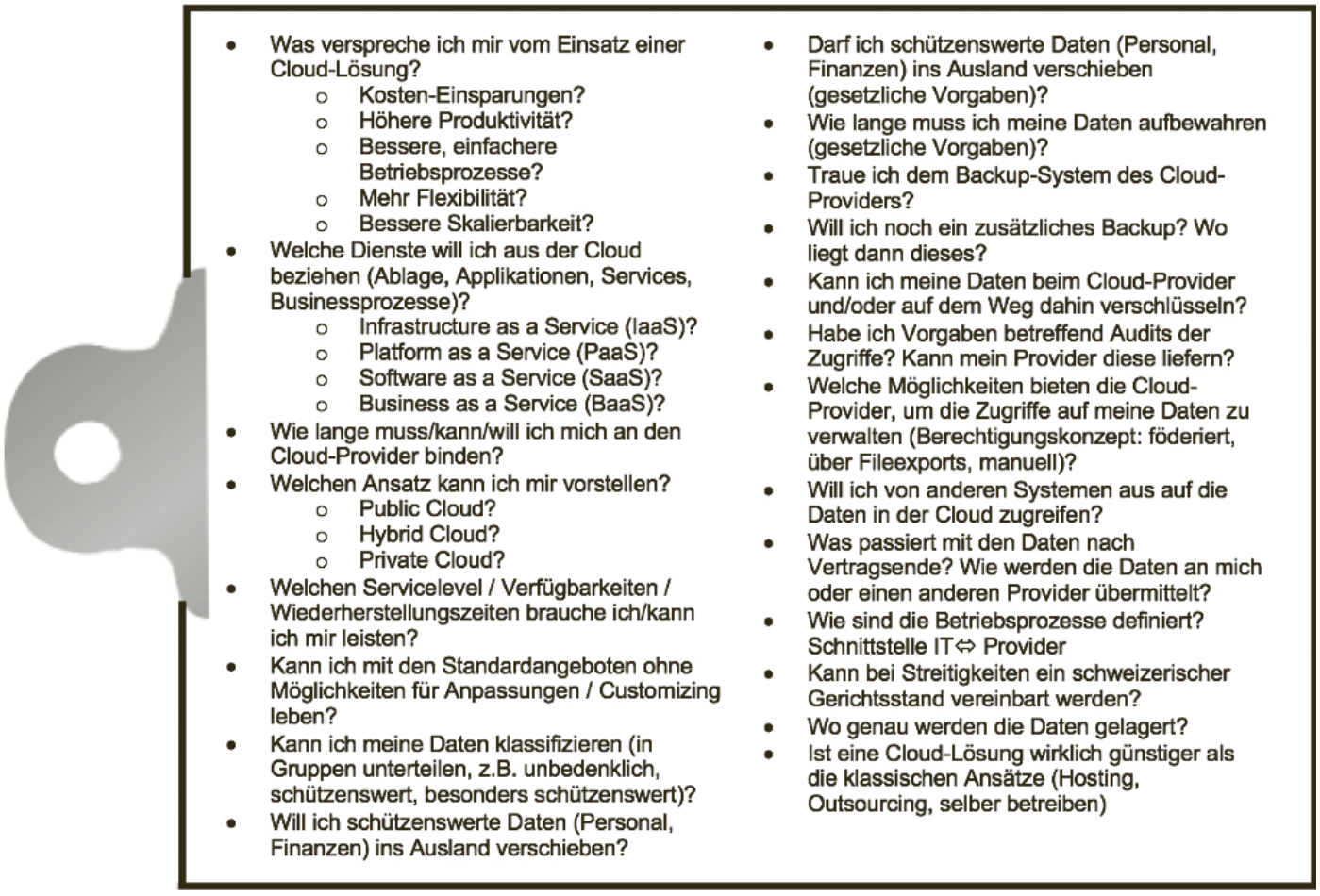


Abbildung 2: Beispiel eines Fragenkatalogs zum Thema Cloud

– Die Mitarbeitenden kennen Tipps und Tricks, um den Gefahren zu begegnen und sie zu vermeiden
– Offene Fragen sind diskutiert und geklärt

Da IT-Sicherheit ein sehr breites Thema ist, ist es wichtig, meinen Mitarbeitenden einen groben Überblick über möglichst viele Themen zu geben, ohne zu sehr ins Detail zu gehen. Nicht jeder Mitarbeitende hat das gleiche technische Knowhow, daher muss ich das Ganze einfach verdaubar und ganz konkret formulieren. Jedes Unternehmen wird dabei andere Schwerpunkte haben. Auch hier gilt es, zuerst zu definieren, wo denn die eigenen Schwerpunkte liegen sollen. Auch muss ich sicherstellen, dass meine Vorgaben zur vorhandenen Infrastruktur und zu den vorhandenen Prozessen passen. So bringt es zum Beispiel wenig, den Einsatz von Dropbox und Co. zu verbieten, aber den Mitarbeitenden keine (sichere) Alternative für den betrieblich notwendigen Datenaustausch anzubieten.

Ein weiterer Aspekt, den ich dabei beachten sollte: es ist wichtig, den Mitarbeitenden den Zugang zu den Informationen auf verschiedenen Kanälen zu ermöglichen, da jede/r auf andere Reize und Medien anspricht. Neben der klassischen Ausbildung gibt es diverse Möglichkeiten: Intranet-Seiten, Videos, Webinare, eLearning, Wettbewerbe, Plakate, Give-Aways, Newsletter, bedruckte Zuckertüten, Bonbons und vieles mehr.

Auch die Frage einer allfälligen Erfolgskontrolle muss ich klären, so kann z.B. eine Awareness-Kampagne mit einem Phishing-Test gestartet werden. Dieser Test kann während respektive nach der Kampagne wiederholt werden. Ein Wettbewerb mit Fragen zu den Gefahren und dem korrekten Vorgehen ist eine weitere Möglichkeit, zu prüfen, ob das Vermittelte auch wirklich angekommen ist. So lässt sich klären, inwieweit die Kampagne eine Verbesserung gebracht hat.

Und nicht zu unterschätzen: Von grossem Wert für das Thema Awareness ist die Unterstützung des Managements. Wenn die Chefs mit gutem Beispiel vorangehen, so hat das eine sehr starke Signalwirkung!

Im Review beim Kunden
Was sagen Kunden zum Thema Awareness?
Die Privera ist die führende unabhängige Immobiliendienstleisterin mit 12 Niederlassungen in der ganzen Schweiz mit rund 400 kaufmännischen Mitarbeitenden. Privera hat zusammen mit e3 eine Awareness-Kampagne aufgebaut. Adrian Blum, Leiter IT-Services, beantwortet uns einige Fragen dazu.

Frage: Warum wurde Awareness für Privera ein Thema?
Antwort: Die Privera hat ihren IT-Betrieb und insbesondere die Sicherheitsinfrastruktur ausgelagert und vertraut da auf ihren langjährigen Partner. Es zeigte sich aber, dass im Tagesgeschäft immer wieder Unsicherheiten bezüglich sicherem Verhalten auftauchten. Es ist uns wichtig den Mitarbeitenden zu vermitteln, dass IT-Sicherheit nicht nur ein IT Thema ist, sondern, dass sie auch einen Teil der Abwehrkette sind.

Frage: Warum haben Sie sich zum Thema Awareness externe Unterstützung geholt?
Antwort: Ich habe gezielt Fachspezialist mit dem richtigen Knowhow im Bereich IT-Sicherheit gesucht, die mir eine Aussensicht auf Privera geben können und mir helfen, blinde Flecken aufzudecken.

Frage: Bei welchen Themen (siehe Abbildung 2) liegt für die Privera der Schwerpunkt?
Antwort: Langfristig wollen wir in unserer Kampagne viele Themen abdecken. Aufgrund unserer Anforderungsanalyse haben wir in der ersten Phase die Themen Grundsätze, Internet, Email und Phishing sowie mobiles Arbeiten adressiert.

Frage: Was sind für Sie die wichtigsten Punkte, die man bei einer Awareness-Kampagne beachten muss?
Antwort: Sie muss vom Management getragen werden. Zudem ist es wichtig, dass den Mitarbeitenden konkrete Verhaltensanweisungen gegeben werden können.

Dranbleiben
Für beide Themen – die Strategie und den Faktor Mensch – gilt das gleiche: Dran bleiben!

Ich muss sicherstellen, dass ich das Portfolio meines Unternehmens an strategischen Entscheidungen, Vorgaben, Vorschriften und Regulatorien aktuell halte. Zudem muss ich meinen Risikokatalog laufend aktualisieren und ihn an sich ändernde Rahmenbedingungen inner- und ausserhalb meines Unternehmens anpassen. Das ist kein Projekt, sondern ein fortlaufender Prozess.

Ähnliches gilt bei der Ausbildung und Sensibilisierung der Mitarbeitenden, der Awareness. Auch bei diesem Thema muss ich dranbleiben. Es gilt, Wichtiges im Gedächtnis der Mitarbeitenden zu verankern, regelmässig aufzufrischen und das Interesse an der Thematik hochzuhalten. Auch hier ist es nicht mit einem einmaligen Projekt gemacht, sondern es braucht einen fortlaufenden Awareness-Prozess.

e3 AG
Die e3 AG mit Sitz in Zürich und Bern ist selber Hersteller von IT-Sicherheits-Systemen (Data Loss Prevention, Cloud-Verschlüsselung) und Anbieter diverser Dienstleistungen im Bereich IT (Strategieberatung, Business Analyse, Testing/QS und Security-Consulting). Wir unterstützen Sie gerne in allen Bereichen «rund um IT-Sicherheit» und freuen uns auf Ihre Kontaktaufnahme!

Autoren

Markus Meier Knuchel, Senior Security Consultant (CISSP), e3 AG

Adrian Blum, Leiter IT-Services, Privera AG

Martin Schor
Senior Security Consultant
e3 AG
awareness@e3ag.ch

CYBER-DEFENCE

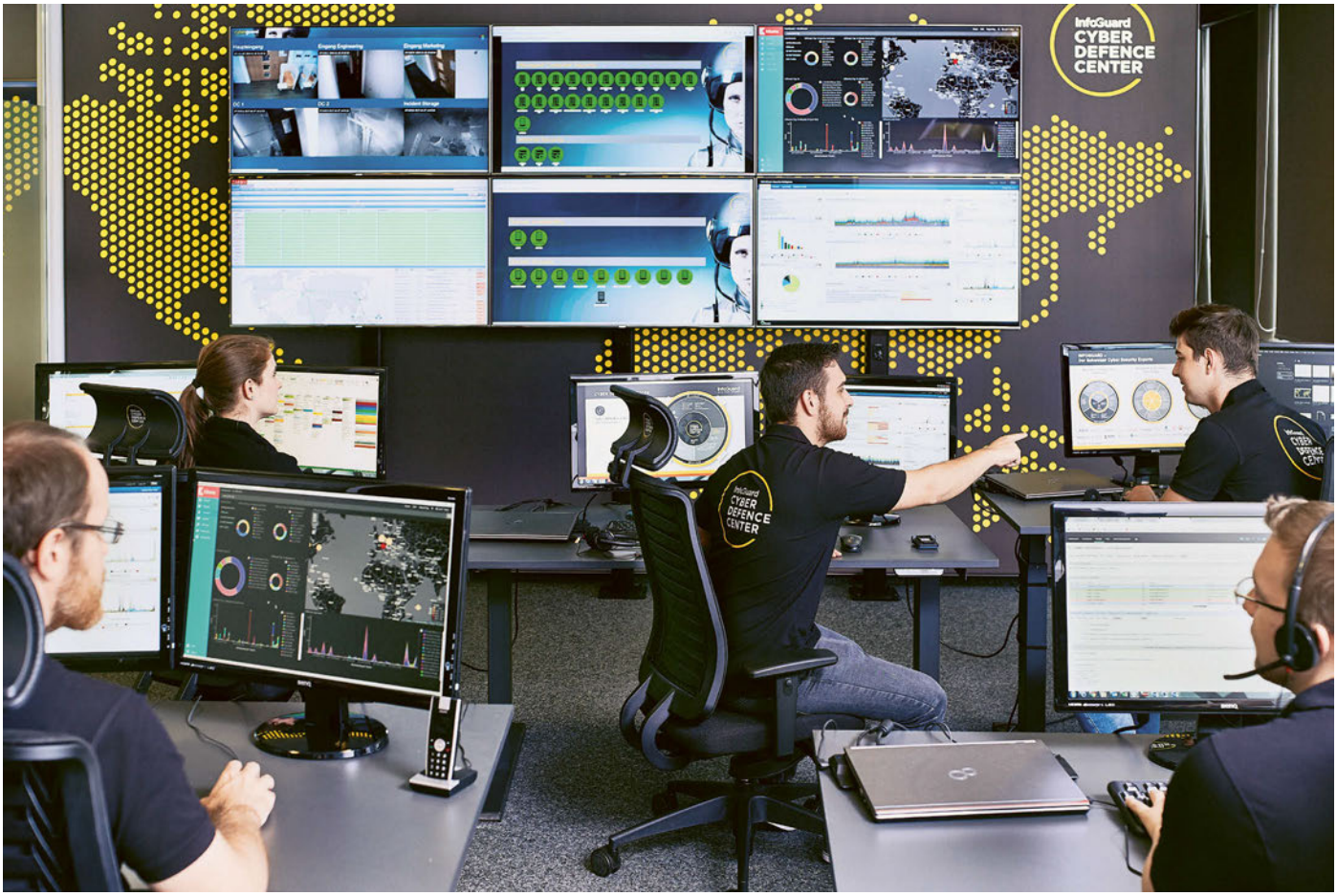
Grüsse aus dem Darknet von «Petya», «WannaCry» und Co.

Die Anzahl der Cyber-Angriffsversuche wie «Petya/NotPetya», «WannaCry», Hacker- und DDoS-Attacken steigt täglich an – mit kaum noch bezifferbaren Schäden für die betroffenen Unternehmen. Heutzutage müssen Unternehmen davon ausgehen, dass ihre Systeme bereits infiltriert sind – oder aber, dass sie nächstens Opfer einer Attacke werden. Es ist deshalb entscheidend, Infiltrationen zu erkennen, schnell darauf zu reagieren und das Sicherheitsdispositiv entsprechend zu optimieren.

Die Nachrichten sind voll mit Meldungen von Hackerangriffen. Betrachtet man rein die Top 15 Cyber-Bedrohungen der ENISA, findet man Ausprägungen wie Malware-Angriffe, Phishing, Bot-Netze, Cyber-Spionage, Identitätsdiebstahl, Insider-Attacken sowie Spam, Gerätediebstahl und Online-Erpressung (Ransomware), beispielsweise «Petya» resp. «NotPetya» und «WannaCry». 2017 ging aber auch als «Das Jahr der DDoS-Angriffe» in die Annalen der Cyber Security-Geschichte ein. Und erst vor ein paar Tagen sorgte ein gigantischer Denial-of-Service-Angriff wieder für mächtig Gesprächsstoff.

Das Tor ins Darknet

Die zunehmende Digitalisierung und die immer dichtere Vernetzung durch das Internet der Dinge bieten Hackern laufend neue Angriffsflächen. Inzwischen poppen täglich fast 400 000 neue Schadprogramme auf – das sind beinahe fünf pro Sekunde! Diese Entwicklung macht klar: Die Angreifer sind in der Regel keine Einzeltäter. Internetkriminalität ist inzwischen professionell organisiert. Das Internet ist zu einem digitalen Schlachtfeld geworden. Ein Schlachtfeld, auf dem immer professioneller Daten gestohlen werden. Dazu trägt auch massgeblich das Darknet bei. Und dort gibt es einiges zu finden: von Drogen und Waffen über gefälschte Pässe bis hin zu Auftragsmördern, vertraulichen Informationen oder Hackern. Diese nutzen das Darknet, um mit Exploit-Kits, Ransomware und gestohlenen Informationen zu handeln. Aber auch staatliche Hackergrup-



pen greifen immer häufiger nicht nur andere staatliche Organisationen an, sondern auch private Unternehmen – und all das, unter Einsatz nahezu unbegrenzter Mittel.

Um ins Darknet zu gelangen, benötigt man einen speziellen, aber für jedermann downloadbaren Tor-Browser, welcher als eine Art digitales Schutzschild dient und die Pfade verschlüsselt. Grundsätzlich kann man damit jedoch genau gleich surfen wie mit den gängigen Browsern. Der Unterschied: Man kann damit auf Seiten zugreifen, auf denen illegal gehandelt wird oder auf spezielle Foren, ohne Spuren zu hinterlassen. Für den anonymen Zugriff auf Darknet-Dienste werden meist Zugangsinformationen wie Login und Passwort benötigt. Zusätzlich muss man teils Aufgaben lösen oder ein Rätsel entschlüsseln. Das Darknet-Pendant zu Google heisst «Grams». Mit dieser Suchmaschine und der entsprechenden Software kann mit dem Hidden Service im Darknet «gegoogelt» werden. Allerdings sollte man auf jeden Fall den Tor-Browser verwenden, damit die Privatsphäre gewahrt wird.

Exploits verkaufen ist nicht illegal, aber lukrativ

Kriminelle nutzen bei den meisten Cyber-Angriffen Sicherheitsschwachstellen aus, beispielsweise veraltete Browser Plugins (Flash, Java, Silverlight) oder alte Browserversionen. Die Angriffe sind sehr hinterlistig, perfide und können selbst besonders achtsame Benutzer hinters Licht führen. Unter der Bezeichnung Exploit versteht man die Ausnutzung eines Software-Bugs, um eine oder mehrere vorhandene Sicherheitsbarrieren zu umgehen. Von Zero-Day-Exploits spricht man, wenn Hacker eine noch weitgehend unbekannte Schwachstelle ausnutzen, für die noch kein Patch verfügbar ist. Für die Verbreitung von Malware nutzen Cyber-Kriminelle sogenannte Exploit-Kits. Das sind vorverpackte Toolkits mit Schadwebseiten oder -software, die Kriminelle kaufen, lizenzieren oder leasen können, um Malware in Umlauf zu bringen. Anstatt selbst herauszufinden, wie man eine Webseite präparieren muss um Besucher zu infizieren, verlassen sich die Angreifer auf einen vorgefertigten Angriffscode im Exploit-Kit. Dieser testet eine Reihe bekannter Sicherheitslücken in der Hoffnung, dass eine funktioniert. Neben Exploit-Kits, die als Übertragungsweg das Internet nutzen, existieren auch eine Reihe ähnlicher Exploit-Kits für E-Mail- und Phishing-Kampagnen. Bei diesen versendet der Angreifer einen Dateianhang an nichts ahnende Nutzer, die diesen im Optimalfall öffnen und dadurch die Malware installieren.

(ICT-)Sicherheitsmauern reichen nicht aus

Der Schutz von Netzwerken und Unternehmenswerten wird dadurch immer schwieriger, insbesondere vor anspruchsvollen Attacken, die durch herkömmliche Sicherheitssysteme nicht erkannt werden. Daher müssen Unternehmen heutzutage davon ausgehen, dass ihre Systeme bereits infiltriert sind – oder aber, dass sie nächstens Opfer einer Attacke werden. Unternehmen müssen hinsichtlich ihrer Cyber Security umdenken und dürfen sich nicht nur auf (immer) höhere ICT-Sicherheitsmauern verlassen. Der Trend geht klar in Richtung einer intensiveren Überwachung von Sicherheitssystemen und der Erkennung von Vorfällen, wie es auch das NIST Cyber Security Framework empfiehlt. Es braucht neue Sicherheitsansätze, bei welchen die Detektion im Vordergrund steht und die Reaktion auf Angriffe ein wesentlicher Bestandteil der IT-Prozesse ist. Dazu braucht es ein Cyber Defence Center (CDC). So lässt sich die Prävention zielgerichtet und kontinuierlich verbessern.

In einem CDC laufen alle Fäden zur Erkennung, Analyse und Abwehr von Cyber-Angriffen zusammen. Erforderlich sind dafür erfahrene Experten mit einem umfassenden Know-how, Security-Tools und nicht zuletzt ein physisch geschützter Operationsraum mit den notwendigen Arbeitsplätzen.

Zur Erkennung von Attacken oder Infiltrationen braucht es entsprechende Werkzeuge und IT-Spezialisten, aber noch viel wichtiger sind Cyber Threat- und Intelligence-Analysten sowie Security Experten. Aber genau hier liegt das nächste Problem: der globale Mangel an gut ausgebildeten Cyber Security-Fachleuten. Cyber Defence ist eine anspruchsvolle Arbeit – und geht weit über ICT-Sicherheitsmassnahmen hinaus. Und da Attacken rund um die Uhr erfolgen, muss ein CDC natürlich auch 7 Tage, während 24 Stunden, funktionieren. Dies erhöht den Personalbedarf natürlich zusätzlich. Selbstlernende Systeme und Lösungen auf Basis Künstlicher Intelligenz können hier bis zu einem gewissen Grad Abhilfe schaffen. Diese gilt es zu nutzen, gerade weil hier auch weitere Fortschritte zu erwarten sind, die ein CDC noch effizienter machen.

Cyber Defence aus der Schweiz

Das Schweizer Unternehmen InfoGuard mit Sitz in Zug und Bern hat sich auf Cyber Security und Cyber Defence spezialisiert. So zählen nebst massgeschneiderten Dienstleistungen im Bereich der Sicherheitsberatung und Security Audits sowie in der Architektur und Integration führender Netzwerk- und Security-Lösungen zu ihren Kompetenzen. Aus dem 250m2 grossen Cyber Defence Center in Baar/Zug bietet InfoGuard umfassende Cyber Defence Services an. Diese umfassen Vulnerability Management, Security Information & Event Management (SIEM), Breach Detection, Threat Intelligence, -Hunting und -Analysis, Incident Response und Forensik. Das Cyber Defence Center verfügt über ein mehrstufiges, physisches Sicherheitskonzept, wobei die Sicherheitssysteme rund um die Uhr, während 365 Tagen im Jahr, überwacht werden.

InfoGuard
SWISS CYBER SECURITY

Autor *Mathias Fuchs,*
Head of Cyber Defence,
InfoGuard AG
InfoGuard AG,
Lindenstrasse 10,
6340 Baar,
www.infoguard.ch

The Evolution of Digital Forensics: Past, Present, and Future

Historical Origins

The word forensics originates from the from the original Latin word "forensis", meaning "of the forum". In ancient Rome the forum was a location for public debate, criminal trails, and dispute resolution. Here criminal cases were verbally presented, and judgment was made based on arguments from both sides. Verbal arguments did not always produce fair results, and the gradual introduction of science and technology helped to provide more reliable and conclusive outcomes to criminal cases. With the transformation of society into the digital and information age, a new aspect of forensics was born – digital forensics. This article describes the history and development of digital forensics over the past few decades.

Early Computer Forensics – the 1980s

In the 1980s, organizations had large central computer systems with terminals and dial-in access, and home computers were becoming increasingly popular. During this decade the beginnings of computer crime started appearing. The first viruses appeared (transferred via floppy diskette), the first worms appeared (Morris worm), and war-dialing was a hacking method popularized by the feature film War Games. During this time the FBI developed the capability to analyze computer evidence, and the Computer Emergency Response Team (CERT) created at Carnegie Mellon University. Society was facing new computer crimes and new types of evidence – digital evidence.

Early Computer Forensics – the 1990s

The Internet became internationally popular during the 1990s, and the development of the World Wide Web made the Internet easier to use for the general public. This pushed computer crime and computer evidence into a multi-jurisdictional landscape. Law Enforcement around the world had a developed a significant interest in the investigation of crimes involving the Internet and digital technology. Federal agencies like the FBI and international agencies like INTERPOL held meetings to discuss the growing problem. Formal bodies were created such as IOCE (International Organization of Computer Evidence) and SWGDE (Scientific Working Group on Digital Evidence). The first open source forensic software was developed – "The Coroner's Toolkit" (TCT).

Influencing factors after Y2K

Until the year 2000 digital forensics was primarily the domain of law enforcement, but a number of factors triggered growth in the private sector. The 2001 September 11 tragedy forced the world to rethink disaster recovery, incident response, and investigations. Corporate accounting scandals such as Enron, Anderson, and Worldcom, resulted in the creation of the Sarbanes-Oxley (SOX) Act in the USA, which included requirements for digital evidence collection capabilities, investigation, and incident response processes in corporations. During this time popular peer-to-peer file sharing like Napster created intellectual property concerns which needed investigation and digital evidence collection. The corporate reliance on the Internet introduced new types of employee misconduct, fraud, and infrastructure attacks. Brand abuse, fake web sites, phishing, and online banking trojans started to become a wide-spread problem.

Formalization of Digital Forensics after Y2K

These influencing factors forced digital forensics into becoming a formal scientific discipline. Models and frameworks were developed. Tools, methods, and procedures were created. A professional community had formed with practitioners and academics, scientific journals like Elsevier's Digital Investigation, and international conferences like DFRWS (Digital Forensics Research Workshop). Formal standards, best practices, and processes were developed. During this decade the scope of digital forensics expanded beyond simple computers and hard disks, and started to include software forensics (malware analysis), live system foren-sics (memory, running processes), embedded device analysis (mobile phones, PDAs, GPS devices, etc.), and network forensics (captured traffic, remote collection).

Influencing factors since 2010

After digital forensics became more established, the focus began to change towards the investigation and analysis of cyber incidents. Wikileaks and other leak sites began publishing leaked/stolen information. Hactivism became an international concern with DDoS threats from groups like Anonymous, or high profile breaches by hacking groups like LulzSec. Nation State APTs like Stuxnet and APT1 became widely known, the Snowden leaks (and others) revealed the extent of government hacking, and private company leaks such as Hacking Team and HBGary publicly exposed the commercial hacking industry. Private sector breaches such at Sony, Target, JPMC, Anthem, Equifax, etc. created a renewed interested in cyber-security, cyber investigations, and the need for digital evidence found online. New forms of fraud (cyber-fraud) became popular, such as online banking trojans (Zeus, Dridex, GOZI, etc.), core banking system at-tacks (such as the Bangladesh SWIFT incident), and social engineering attacks like Business Email Compromise (BEC) and CEO

impersonation fraud. Classic phishing attacks evolved to include Voice Phishing ('Vishing'), SMS Phishing ('Smishing'), and other attacks involving social media platforms. Most recently, the criminal underground has discovered ransomeware attacks to be effective and profitable.

The advancement of digital forensics since 2010

Digital forensics has overcome a number of challenges since 2010. Tools have become much easier to use and no longer require the same specialist technical knowledge to use. Managing large datasets and "Big Data" has become commonplace, especially with enterprise tools (E-discovery for example). The analysis of mobile devices such as tablets and smartphones has become a primary evidence source for law enforcement. Professional digital forensic labs now have advanced hardware capabilities for "Chip-off" (de-soldering chips to extract data) and accessing data via JTAG (debug) interfaces. These hardware forensic techniques are especially useful for the analysis of "Internet of Things" (IoT) devices. More recently, digital forensics is including areas such as vehicle forensics (automobile, drones, etc.), and the analysis of crypto currencies such as Bitcoin and online payment systems.

Digital forensics in the next decade

An number of challenges require further research and development by the digital forensics community. Issues surrounding data encryption are a difficult problem to solve when balancing the safety and security of individuals with the need to collect digital evidence (especially with serious crimes and threats to society). Personal privacy issues exist, big web companies are harvesting large amounts of data, and new legislation such as the EU GDPR will impact the availability of digital evidence as well as forensic readiness (data retention). The analysis of wearable devices, medical implants, smart buildings, and industrial control systems will become more interesting on the hardware forensics side. In the area of network forensics, the collection and analysis of telemetry data sent by applications and operating systems will become an evidence source and useful for investigations. Like server systems have already done, the desktop PC will transition towards virtual machines the cloud (VDI technology) and will change how we do traditional computer forensics.

Conclusion

The tools and technologies for collecting and analyzing evidence are always changing. The methods used by criminals to commit crimes are always changing. The location and sources of digital evidence are changing. But there are several factors that always remain constant. There will always be perpetrators and victims of criminal activity. There will always be a need for evidence to convict criminals. Digital forensics will continue to have a fundamental role to collect, analyze, and interpret digital evidence.

About the author

Bruce Nikkel is the director of Cybercrime Intelligence & Forensic Investigation at UBS. He has worked for the bank's Security and Risk departments since 1997. Bruce also works part-time as a professor at the Bern University of Applied Sciences, teaching and researching digital forensics and investigative methods. He holds a PhD in network forensics and is the author of the book 'Practical Forensic Imaging'.

DROHNEN

Drohnen: Chancen und Risiken in der dritten Dimension

Einführung – das Drohnen 1x1
Über 100 000 unbemannte Luftfahrzeuge, sogenannte Drohnen oder Multicopter, sind in der Schweiz in der Luft unterwegs. Die Verkaufszahlen von Drohnen steigen exponentiell. In Fachkreisen werden Drohnen auch als oder «pilotenferngesteuert» (Remotely Piloted Aircraft Systems – RPAS) oder «nicht bemannte Luftfahrzeuge» (unmanned aerial vehicle – UAV's) bezeichnet. Häufig sind sie mit Kameras für Foto- und Filmaufnahmen ausgestattet. Drohnen bilden eine neue Freizeitaktivität, stellen in Kombination mit modernen Telekommunikationsmitteln aber auch ideale Instrumente für kommerzielle und gewerbliche Tätigkeiten dar (z.B. für Fotografen oder Reporter). Zivile Drohnen kommen weltweit auch im Dienste der Wissenschaft und für die Überwachung kritischer Infrastrukturen wie Dämme, Geleise oder Stromnetze zum Einsatz.

Das Bundesamt für Zivilluftfahrt (BAZL) erlässt Drohnen-Vorschriften: Bis zu einem Gewicht von 30 Kilogramm dürfen sie grundsätzlich ohne Bewilligung eingesetzt werden. Voraussetzung ist allerdings, dass der «Pilot» jederzeit Sichtkontakt zu seiner Drohne hat. Zudem dürfen keine Drohnen über Menschenansammlungen betrieben werden. Innerhalb von Jagdbanngebieten oder Schutzgebieten für Wasser- und Zugvögel ist das Fliegen von Drohnen ausnahmslos verboten.

Luftaufnahmen sind zulässig, sofern die Vorschriften zum Schutz militärischer

Fig 1: Flugverbotszonen /(BAZL)

- Zone mit eingeschränktem Flugverbot (150m über Grund)
- Zone mit Flugverbot (5km Pistenabstand)

Anlagen berücksichtigt werden. Zu beachten sind dabei auch der Schutz der Privatsphäre und die Vorschriften des Datenschutzgesetzes. Über Menschenansammlungen (beziehungsweise im Umkreis von 100 Metern von Menschenansammlungen) dürfen Drohnen grundsätzlich nicht betrieben werden. Wer eine Drohne oder ein Flugmodell mit mehr als 500 Gramm Gewicht betreibt, muss für allfällige Schäden eine Haftpflichtdeckung im Umfang von mindestens 1 Million Franken gewährleisten. In der Nähe von Flugplätzen bestehen weitere Einschränkungen für Drohnenflüge: Es ist zum Beispiel nicht gestattet, solche Fluggeräte näher als 5 Kilometer von den Flugplätzen entfernt fliegen zu lassen.

Das BAZL stellt eine interaktive Karte zur Verfügung, welche die schweizerischen Flugverbotszonen darstellt. (Fig. 1)

Einsatz von Drohnen im professionellen und kommerziellen Bereich

Drohnen finden vermehrt Anwendung in der Geschäftswelt. Post/Matternet setzt Drohnen ein, um Produkte auszuliefern. In der Landwirtschaft existieren Drohnen, die Pflanzenschutzmittel, Biozidprodukte und Dünger aus der Luft abwerfen. Bei Swisscom überlegt man sich, Drohnen für Inspektionen von eigener Infrastruktur einzusetzen. Weitere Einsatzgebiete von professionellen Drohnen sind z.B.:

- Schadenaufnahmen bei Unwettern und Einsätzen der Blaulichtorganisationen
- Gebäude- und Dach-Inspektionen, z.B. Solaranlagen
- Wärmebildaufnahmen für Personensuche oder Brandbekämpfung
- Lieferungen aller Art: Ersatzteile, Medikamente oder Blutproben
- Meteorologische Anwendungen
- Verlegung von Kabeln, z.B. bei Strommasten oder Brücken
- Produktion von Filmaufnahmen von Sportereignissen und Events

In Spitälern werden Drohnen eingesetzt, damit Laborproben von einem Spital in ein anderes geliefert werden können. Damit umgeht man z.B. das Problem des hohen Verkehrsaufkommens, dass oftmals in Verkehrsstaus mündet. Bei all diesen Einsatzgebieten stellt sich auch die Frage nach der Sicherheit (z.B. Safety, Privacy, Integrität, Nachvollziehbarkeit) und Risiken bei der Nutzung von kommerziell eingesetzten Drohnen.

Jede Firma, die Drohnen einsetzt, muss die Risiken und die Problemstellungen beim Einsatz von Drohnen analysieren und beurteilen. Weiter sollten die Firmen sich überlegen, ob sie sich und ihre Infrastruktur (z.B. ein Fabrikations- oder Firmengelände) vor Drohnen schützen müssen (z.B. Eindringen von Drohnen in der dritten Dimension bei einem Atomkraftwerk). Dazu gehört auch die Überlegung, wie man sich gegen die Verletzung der Privatsphäre aus der Luft schützt. Kritische Bereiche, bei denen das Thema Drohnenschutz besonders beachtet werden sollte, sind z.B.:

- Gefängnisse
- Botschaften
- Golfplätze
- Firmen- Betriebsgelände (Tests eines neuen Protoypen)
- Kritische Infrastrukturen (Staudamm/Kraftwerke, Rechenzentren)
- Öffentliche Veranstaltungen (Open Air Event, Weihnachtsmarkt, Konzert, Schwingfest, Sportanlässe)
- Konferenzen (Swiss Economic Forum – SEF, World Economic Forum – WEF)

DroneGuard, ein Swisscom Startup, leistet genau in diesem Bereich wertvolle Dienste. Das Startup wird im Rahmen des Swisscom Kickbox-Innovationsprogrammes gefördert. Das wird nachfolgend vorgestellt.

Phase 1 – Red Box	**Phase 2 – Blue Box**	**Phase 3 – Gold Box**
Verfeinerung der Idee	Proof of Concept mit Kunden	Idee wird zur Wirklichkeit
Datenbasierte erste Tests	Marktanalyse	Marktfähiges Produkt
Erste Suche nach Investoren	Klärung finanzielle Aspekte	Lancierung des Produkts
Unterstützung durch Dritte	Erstes Produkt-Design	Joint-Venture/Spin Off
Red Box Pitch	Blue Box Pitch	
Dauer: 2 Monate	Dauer: 4–6 Monate	Dauer: 1 Jahr
Arbeitszeit: 20%	Arbeitszeit: 20%	Arbeitszeit: bis zu 100%
Budget: 1000.–	Budget: =/<10'000.–	Budget: individuell

Tabelle: Kickbox Innovationsprogramm

Swisscom Kickbox

Kickbox ist ein internes Innovationsprogramm der Swisscom, das sich ursprünglich an das Innovationsprogramm von Adobe anlehnte. Es ermöglicht Mitarbeitenden, eine innovative Idee in drei Phasen umzusetzen. Die Mitarbeitenden dürfen Arbeitszeit für das Ausarbeiten der Idee einsetzen und erhalten weiter ein monetäres Budget. Die obige Tabelle zeigt die wichtigsten Informationen der einzelnen Phasen auf.

Sämtliche Phasen werden durch das Kickbox-Team unterstützt, hinzu kommen einzelne Gutscheine für externe Leistungen (z.B. Unterstützung durch Software-Entwickler, Legal Check durch einen Juristen). Selektiv werden einzelne Ideen vor einer Bereichsleitung oder vor der Konzernleitung vorgestellt.

Kickbox und die Idee Drone Guard

Dominique Brack und Klaus Gribi haben 2017 die Idee lanciert, dass Swisscom verschiedene Drohnen-Services anbieten könnte. Ein Telco-Provider wie Swisscom verfügt über ideale Voraussetzungen und alle benötigten Plattformen/Services (z.B. 4G und künftig 5G Mobilfunknetz, Low Po-

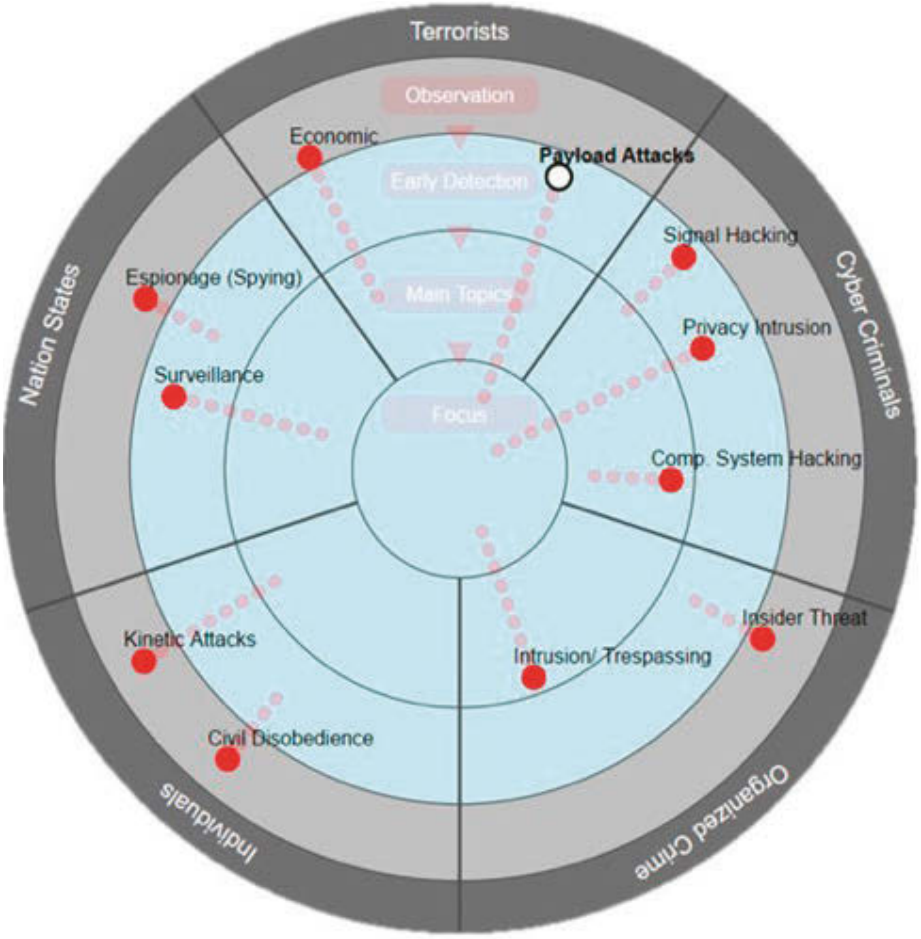


Fig 2: Bedrohungsradar

wer Network, Cloud Services, Alarmierungsplattform, Blockchain, Operation Centers), damit solche Drohnen-Services angeboten werden können. PWC stellt dies im Report «Telecom operators in the age of drones» ebenfalls fest. Die eingereichte Idee wurde im Rahmen der Red Box ausgearbeitet, so dass nun seit anfangs 2018 ein erster Proof of Concept (Phase 2 – Blue Box) ausgearbeitet wird. Das Projekt Drone Guard wird zudem in der Konzernleitung vorgestellt, da eine interne Jury das Potential dieser Idee erkannt hat.

Drone Guard bietet in einem ersten Anwendungsfall strategische und taktische Beratungen bezüglich Drohnen (Multicopter) an:

- Analyse der Bedrohungslage
- Erstellen von Risiko-Katalogen
- Ausarbeiten eines vollständigen Drohnen-Abwehrdispositivs
- Planen und Betreiben stationärer und mobiler Drohnenabwehr-Systeme

In diesem Sinne werden Consulting-Dienstleistungen rund um die drei Themen «Detect, Protect, Response» (Schutz, Abwehr und Prävention) angeboten. Zur Bereitstellung von Drohnenabwehr-Systemen wird mit entsprechenden Partnern wie Dedrone Convexum zusammengearbeitet. Damit Drohnenbedrohungen analysiert und dargestellt werden können, hat Drone Guard eine spezifische Methodik entwickelt, welche sich eines gängigen Bedrohungsradars bedient: (Fig. 2)

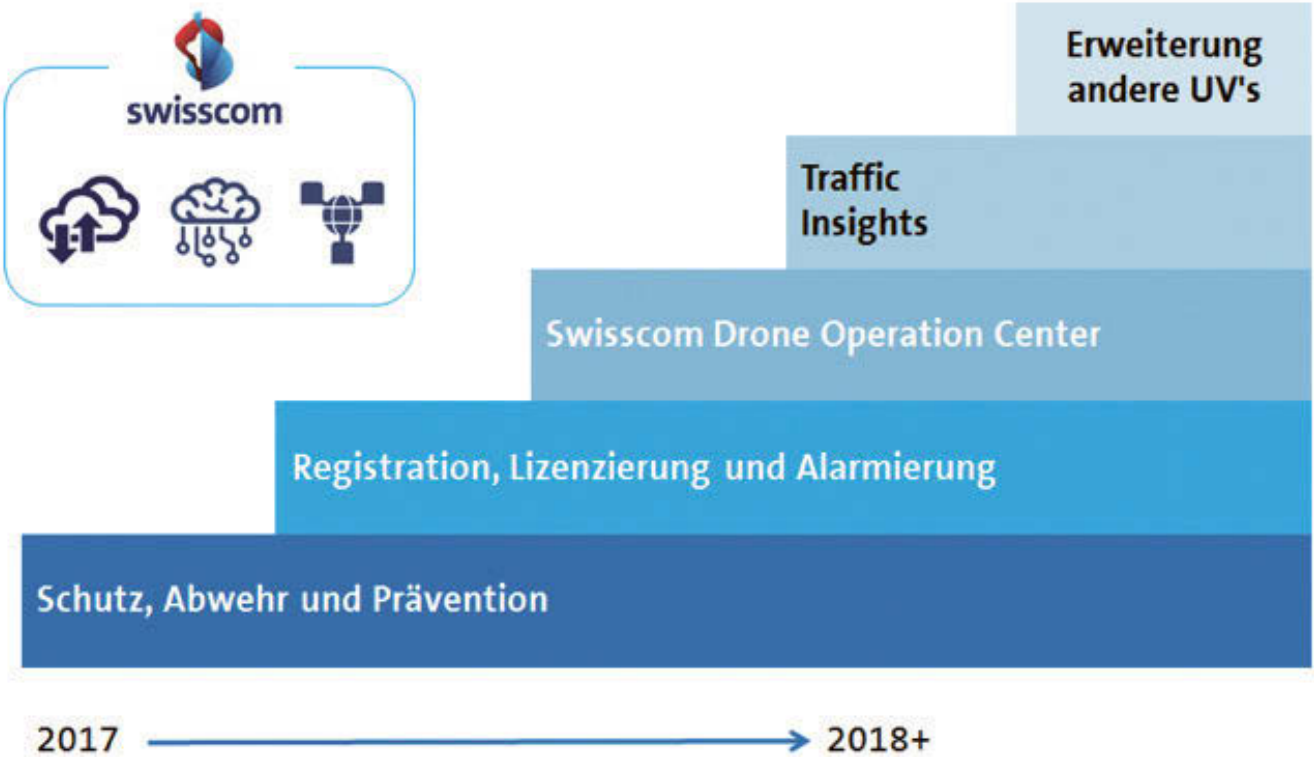


Fig 3: Drohnen-Services Swisscom

Dieser Radar stellt die Bedrohungen kundenspezifisch dar und bildet damit die Basis für das Planen eines Drohnenabwehr-Systems. Der Bedrohungskatalog umfasst zurzeit 140 detailliert ausgearbeitete Bedrohungen, welche nun kundenspezifisch im Bedrohungsradar dargestellt werden können.

In weiteren – später folgenden – Anwendungsfällen sollen zusätzliche Services angeboten werden: (Fig. 3)
- Drohnen-Registrierung, -Lizenzierung und -Alarmierung
- Betreiben eines Swisscom Drone Operation Centers (DOC)
- Over the top services (Traffic Insights)
- Integration weiterer unbenannter Fahrzeuge (Unmanned Vehicle – UV)

Damit diese weiteren Anwendungsfälle erbracht werden können, beabsichtigt Swisscom (Drone Guard) mit verschiedenen Partnern zusammen zu arbeiten.

Autoren

Klaus Gribi
Senior Security Consultant
Swisscom (Schweiz) AG
3000 Bern

Dominique Brack
Senior Security Consultant
Swisscom (Schweiz) AG
3000 Bern

CYBERSECURITY

Cybersecurity als Service

Hackerangriffe auf die deutsche Bundesregierung füllen die Schlagzeilen. Doch nicht nur Regierungen – vor allem auch Unternehmen sind im Visier von Cyberkriminellen. Es geht um handfeste Wirtschaftsspionage oder auch einfach um böswillige Erpressung. Immer komplexere IT-Infrastrukturen, die zunehmende Vernetzung und Digitalisierung – aber auch fehlende Ressourcen und mangelndes Know-how öffnen Schwach-stellen. Drei Schlüsselbereiche lassen sich erkennen, in denen Sicherheitsmanagement neuen Trends unterworfen ist.

Aus einer Ende letzten Jahres von vier Verbänden gemeinsam vorgelegten Studie geht hervor, dass fast jede dritte Schweizer KMU bereits Opfer einer Cyberattacke wurde. Der Schweizerische Versicherungsverband (SVV), ICTswitzerland, Information Security Society Switzerland (ISSS) und die Schweizerische Vereinigung für Qualitäts- und Management-Systeme (SQS) konstatierten in ihrer Studie, dass sich dennoch nur eine Minderheit für gefährdet hält. Ein Trugschluss, wie die Studienautoren meinen. Denn das Bewusstsein für Cybergefahren sei bei den Verantwortlichen noch nicht allzu ausgeprägt. Nur 20 Prozent der befragten Firmen hätten nämlich Systeme eingeführt, um Cyberangriffe überhaupt zu erkennen. Und bloss 18 Prozent haben ihre Mitarbeitenden in der Behebung von Cybervorfällen geschult; lediglich 15 Prozent lehren ihren Mitarbeitern den sicheren Umgang mit IT.

Positiv heben die Autoren hingegen hervor, dass 45 Prozent der Befragten in den nächsten zwei bis drei Jahren ihren Schutz vor Cyberangriffen verbessern wollen.

Doch das Feld der Cybersecurity ist breit, und wer sich bislang noch wenig damit befasst hat, steht vor einer riesigen Herausforderung angesichts der vielfältigen Gefahren, die sich durch die fortschreitende Digitalisierung im Hinblick auf den Da-tenschutz ergeben.

Cyberattacken mit schwerwiegenden Folgen

Eine Auslegeordnung tut not, was ein Unternehmen selbst tun kann und muss – und wo man das Feld am besten Spezialisten überlässt. Denn Fakt ist: Mit der neuen Europäischen Datenschutz-Grundverordnung, die im Mai dieses Jahres in Kraft tritt, werden Datenschutzverletzungen – auch von Schweizer Firmen und von Schweizer Boden aus – streng geahndet und ziehen hohe Bussen nach sich.

Doch auch ohne Verordnungen sollten gerade die hochspezialisierten Technologie-Unternehmen im Berner Mittel- und Oberland sich dessen bewusster werden, dass ihr technisches Know-how, mit dem sie es oftmals zum Weltführer in ihrer spezifi-schen Nische gebracht haben, in einer digitalisierten und globalisierten Welt völlig neu geschützt werden muss. Ein hohes Cyberrisiko stellt demnach beispielsweise ein Hackerangriff auf besonders schützenswerte Geschäftsgeheimnisse dar – seien es die CAD-Daten für die nächste Innovation oder kunden- resp. auftrags- und pro-jektrelevante Informationen.

Es sind nicht immer nur gezielte Attacken auf ein konkretes Unternehmen: Mal- oder Ransomware, Viren und Trojaner können ganze IT-Infrastrukturen lahmlegen, so

dass beispielsweise Aufträge und Bestellungen weder erfasst noch ausgeführt werden können. Mit der im Internet-of-Things zunehmenden Vernetzung öffnen sich Unternehmensgrenzen und damit neue Einfallstore für Cyberrisiken.

Schlüsselbereiche für die Sicherheit

Indem die Cyberattacken sich mehr und mehr auf Geschäftsabläufe richten, die für die Wertschöpfung von Firmen unentbehrlich sind, wird es für Unternehmen aller Grössen zwingend, ihre Cyberstrategien laufend anzupassen. Doch den meisten Unternehmen fehlen hierfür sowohl die Ressourcen als auch das Know-how.

Insbesondere drei Bereiche erfordern in Zukunft mehr Augenmerk:

1. Eine ganzheitliche Sicht auf alle Sicherheitselemente

In der Vergangenheit konzentrierten sich Sicherheitsmassnahmen im Wesentlichen auf statische Abwehrmassnahmen wie beispielsweise eine Firewall. In der Regel werden zudem Einzellösungen von verschiedenen Herstellern für Teilbereiche der IT-Sicherheit eingesetzt: Firewalls, Virenscanner und Intrusion Prevention Systeme haben unterschiedliche Managementsysteme, Sicherheitsberichte müssen mühsam aus verschiedenen Quellen erstellt werden. Und mit dem Einzug von Cloud Computing, virtuellen Teams und Collaboration über die Unternehmensgrenzen hinweg bieten all diese Sicherheitselemente ohnehin keinen ausreichenden Schutz mehr. Nötig ist eine ganzheitliche Sicht auf die übergreifende Sicherheit, die alle zu schützenden Elemente einbezieht. Wer seine Cyber-Detection- und Response-Fähigkeiten der Bedrohungslage nicht anpasst, hinkt den komplexen und zielgerichteten Angriffen fortwährend hinterher. Um diese ebenso riskante wie frustrierende Verfolgerrolle zu überwinden, müssen Unternehmen ein intelligentes Sicherheitsmanagement aufbauen, das Informationen aus verschiedenen Datenquellen verknüpft und in Echtzeit auswertet. Ziel dieser proaktiven Vorgehensweise ist es, sich nicht nur gegen bekannte Angriffe zu schützen, sondern auch unbekannte Angriffs-methoden zu erkennen und sofortige Gegenmassnahmen einzuleiten.

Doch angesichts der zunehmenden Professionalisierung der Cyberkriminalität sind selbst Grosskonzerne kaum mehr in der Lage, die vielfältigen Gefährdungen im Alleingang zu beherrschen. Es braucht 24/7-Überwachung, Erkennung und Schutz vor Gefahren in Echtzeit, die Aufklärung von sicherheitsrelevanten Vorkommnissen und eine «digitale Spurensicherung», um die Schadsoftware selbst wie auch das Vorgehen der Angreifer zu analysieren und last but not least die Anpassung der Sicherheitsdispositive an neue Verfahrensweisen der Angreifer.

Es empfiehlt sich daher, das Sicherheitsinformationsmanagement bei Spezialisten zu beziehen. Im Idealfall sollten diese Spezialisten Teil einer Organisation sein, die globale Einblicke in entstehende Sicherheitsprobleme hat und mit einem breiten Spektrum an Lösungen beraten kann. Über Security Operation Center (SOC) können die Spezialisten sowohl Remote- wie auch Vor-Ort-Unterstützung bei Sicherheitsvorfällen in vorab definierten Reaktionszeiten bieten. Als Experten auf ihrem Gebiet sind sie zudem technologisch eher up to date als es ein Unternehmen mit anderen Kernaktivitäten je sein kann.

Mehr noch: IT-Dienstleister, die Security als integralen Bestandteil ihrer IT-Services verstehen, bündeln ihr Serviceportfolio zumeist in Partnerschaften mit führenden Security-Spezialisten. Auf diese Weise kommen die Kunden in den Genuss von attraktiven Servicemodellen bei gleichzeitig höchster Security-Expertise. Cybersecurity kann «as a Service» bezogen werden und bietet in diesem Bezugs-modell eine ganze Reihe von Vorteilen [siehe Kasten]. Security Operation Center Services können als Hybrid-Modell erbracht

Cyber Defense as a Service bieten eine Reihe von Vorteilen. Bei der Wahl eines Partners ist darauf zu achten, dass die folgenden Services im Paket abgedeckt sind, um höchstmögliche Sicherheitsstandards zu garantieren:

- Keine Investition in unternehmenseigene Cyber-Defense-Infrastrukturen. Keine Bindung an eine Mindestvertragslaufzeit im Service
- 24/7 Security Operation Center für Incident Detection & Response
- Erfahrene Security Experten analysieren 24/7 das Security Event Aufkommen und alarmieren im Eventfall
- Dynamisches Threat Intelligence Feed
- Global agierende Threat Intelligence Services sammeln permanent Informa-tionen zu neuen oder sich verändernden Bedrohungen und liefern diese zur direkten Weiterverarbeitung an das Security Information and Event Management (SIEM)
- Content Engineering
- Kontinuierliche Optimierung der Use Case Libraries sowie optionale Services zur individuellen Überwachung von Angriffsvektoren und Auswertung im Security Reporting
- Security Reporting
- Der Stand der Informationssicherheit der Unternehmens-IT kann jederzeit und überall über Dashboards auf einer Weboberfläche eingesehen werden. Vordefinierte Reports können abgerufen werden und helfen Entscheidungen für geeignete Massnahmen zur Abwehr von Cyber Angriffen zu treffen
- Penetration Testing und Vulnerability Scanning
- Tool-basierter Security Check der Unternehmens-IT. Cyber Defense as a Service bietet optional die Durchführung von verschiedenen Penetrationstests an, wahlweise als Netz- oder Applikations-Pentest
- Soforthilfe im Incident Vorfall oder Angriffssimulationen
  Die Soforthilfe als Ergänzung eines funktionierenden Security Incident Mana-gements hält ein Kontingent für Digitale Forensic und Malware Analyse zum Abruf bereit und unterstützt alle Phasen der Reaktion auf einen Sicherheitsvorfall
- Optionale und erweiterte SOC Services zur Individualisierung der Kunden-umgebung ermöglichen die Anpassung an Kundenbedürfnisse

werden. Zu berücksichtigen sind Compliance-Vorgaben, die national, branchen- oder unternehmensspezifisch zu wahren sind. Zugleich kann international, ja global, auf Ressourcen zurückgegriffen werden, die rund um die Uhr Monitoring und Threat Intelligence aus möglichst vielen Datenquellen garantieren.

2. Business-fokussierte Sicherheit

Bereits heute entfallen gemäss der Marktforschung von MSM Research 47% der Security-Budgets auf Dienstleistungen externer Anbieter im Bereich der ICT-Sicherheit. Und dieser Anteil wird weiter wachsen. Eine steigende Anzahl von Unternehmen wird ihre ICT-Sicherheit künftig in Form von Managed Security Services oder als Dienstleistung aus der Cloud beziehen. Die Ausgaben für Security Dienstleistungen werden 2018 insgesamt um deutlich über 5% wachsen. Und basierend auf dieser überdurchschnittlichen Zunahme dürfte bis in zwei Jahren jeder zweite Franken des Budgets für Security auf Services entfallen.

Für diesen Trend spielt eine grosse Rolle, dass Digitalisierungsvorhaben nicht mehr zwingend durch die IT-, sondern mehr und mehr durch die Fachabteilungen voran-getrieben werden. Sicherheit wird damit zunehmend businessfokussiert. Damit einher gehen hohe Anforderungen an Sicherheitsfunktionen wie Identitäts-, Datenschutz-, Integritäts- und Verfügbarkeitsdiensten zum Schutz digitaler Kanäle und Systeme in der direkten Interaktion mit Kunden und Partnern. Dementsprechend nehmen die Investitionen in Security Appliances und Hardware ab, während die Gesamtsicherheit dennoch steigt. Bemerkenswert an dieser Entwicklung ist zudem, dass auch die Budgetkontrolle von der technischen zur Business-Seite wandert und als Bestandteil der Business Solution angesehen wird. Die Breite der für das Business relevanten Aspekte reicht hier von «Security by Design»-Ansätzen für neue Businessapplikationen bis hin zur Compliance-gerechten Implementation von Vorgaben wie der DSGVO in Businessprozesse.

3. IoT-Sicherheit

Die Sicherheit der durch das Internet vernetzten smarten Dinge schwingt sich zum absoluten Trendthema auf, denn noch stecken die meisten Unternehmen in der Experimentierphase, und die Skepsis ist ebenso gross wie die Hoffnungen auf das künftige Potential, das sich durch das Industrie-4.0-Konzept ergeben soll. Denn wenn Milliarden von Dingen miteinander vernetzt werden, steigert sich automatisch deren Verwundbarkeit. Die Bedrohung im Internet der Dinge und der Industrie 4.0 betrifft auch nicht nur die klassische Business IT, sondern auch in Produkten verbaute Software, Architekturen und Produktions-IT sowie die Vernetzung dieser Produkte.

Die Industrie investiert in Lösungen, um das Operational Technology (OT) En-vironment und die industrielle Prozesskontrolle in ein einheitliches, durchgängiges Sicherheitsnetz einzubinden. Erforderlich sind Lösungen, die Authentifizierung und Integrität sowohl innerhalb der OT-Umgebung wie auch für die Verwaltung des externen Lieferantenzugangs sichergestellt werden können.

Drei Bausteine sind besonders wichtig, um die Sicherheit von IoT-Systemen zu erhöhen: Security-Tests für die Stärkung der Sicherheitsinfrastruktur, die Sicherheit rund um die Cloud und das Kontroll-Netzwerk und als dritter Punkt die Sicherstellung der Unternehmensumwelt, beispielsweise durch eine entsprechende Security-Beratung. Eine gute Schutzstrategie setzt eine ganzheitliche Bestandsaufnahme voraus. Eine flächendeckende Qualitätssicherung ist jedoch nach wie vor in weiter Ferne. Das liegt daran, dass das IoT sehr komplex und heterogen ist. Einzelmass-nahmen können da nicht viel bewirken. Unternehmen müssen sich darüber klar werden, welche digitalen Prozesse geschäftskritisch sind, welche Anforderungen an die Anwendung bestehen und welche Risiken es zu eliminieren gilt. Ausgereifte Testverfahren können dem Unternehmen dabei helfen Schwachstellen und Sicher-heitslücken in Infrastrukturen früh aufspüren und anschliessend zu beheben. Die Möglichkeiten zu einer besseren Absicherung sind also schon gegeben, doch was fehlt, ist die Sensibilisierung der Nutzer. Erst, wenn Nutzer und Unternehmen die Risiken kennen und sich dieser bewusst sind, können die Geräte flächendeckend gesichert und Angriffe somit erschwert werden.

Autor

Dr. Andrew Hutchison
CyberSecurity
Specialist
bei T-Systems
Schweiz

Der Weg zur föderierten E-Identität im E-Government

Einleitung

Seit Jahren wird versucht, die Authentifizierung von elektronischen Identitäten im Geschäftsbereich auf sichere Verfahren anzuheben und zu standardisieren. In letzter Zeit kommen auch Anwendungen aus den Bereichen Government und Gesundheit hinzu, denn auch hier stehen Anforderungen im Raum, welche Richtlinien für ein qualitativ hochstehendes Identitäts-Management verlangen. Die Authentifizierung eines Benutzers kann dabei auf unterschiedliche Art und Weise erfolgen. Die Vor- und Nachteile möglicher Architekturen werden in diesem Artikel dargelegt.

Lokal verteilte E-Identitäten

Wir kennen das alle aus unserem Alltag: Um mit einem Webshop oder einem anderen Online-Webdienst eine Geschäftsbeziehung aufbauen zu können, müssen wir personenbezogene Daten eingeben. Dazu gehören Vorname, Nachname, Adresse, E-Mail, usw. Beim Dienstanbieter wird dabei ein Konto erstellt, um die Geschäftsbeziehung zu erstellen und um sicherzustellen, dass sich der Benutzer zu einem späteren Zeitpunkt wieder anmelden kann. Dieses Konto ist schützenswert. Es geht niemanden etwas an, wer welche Waren bei wem bestellt hat und wieviel es gekostet hat. Daher wird der Zugriff auf ein Konto mit einem Passwort geschützt, welches der Benutzer frei wählen kann.

Die meisten Benutzer kaufen aber nicht nur bei einem Webshop ein, sondern erwerben diverse Waren (Bücher, Elektronikartikel, Musik usw.) von verschiedenen Anbietern.

Aus Bequemlichkeit wählen die Benutzer beim Registrieren vielfach den gleichen Benutzernamen und dasselbe Passwort. Da die Wiederverwendung gleicher Zugangsinformationen für unterschiedliche Online-Dienstanbieter aber fatale Folgen haben kann, wird von diesem Verhalten abgeraten, obwohl es für den Benutzer so natürlich am Einfachsten ist. Wie zahlrei-

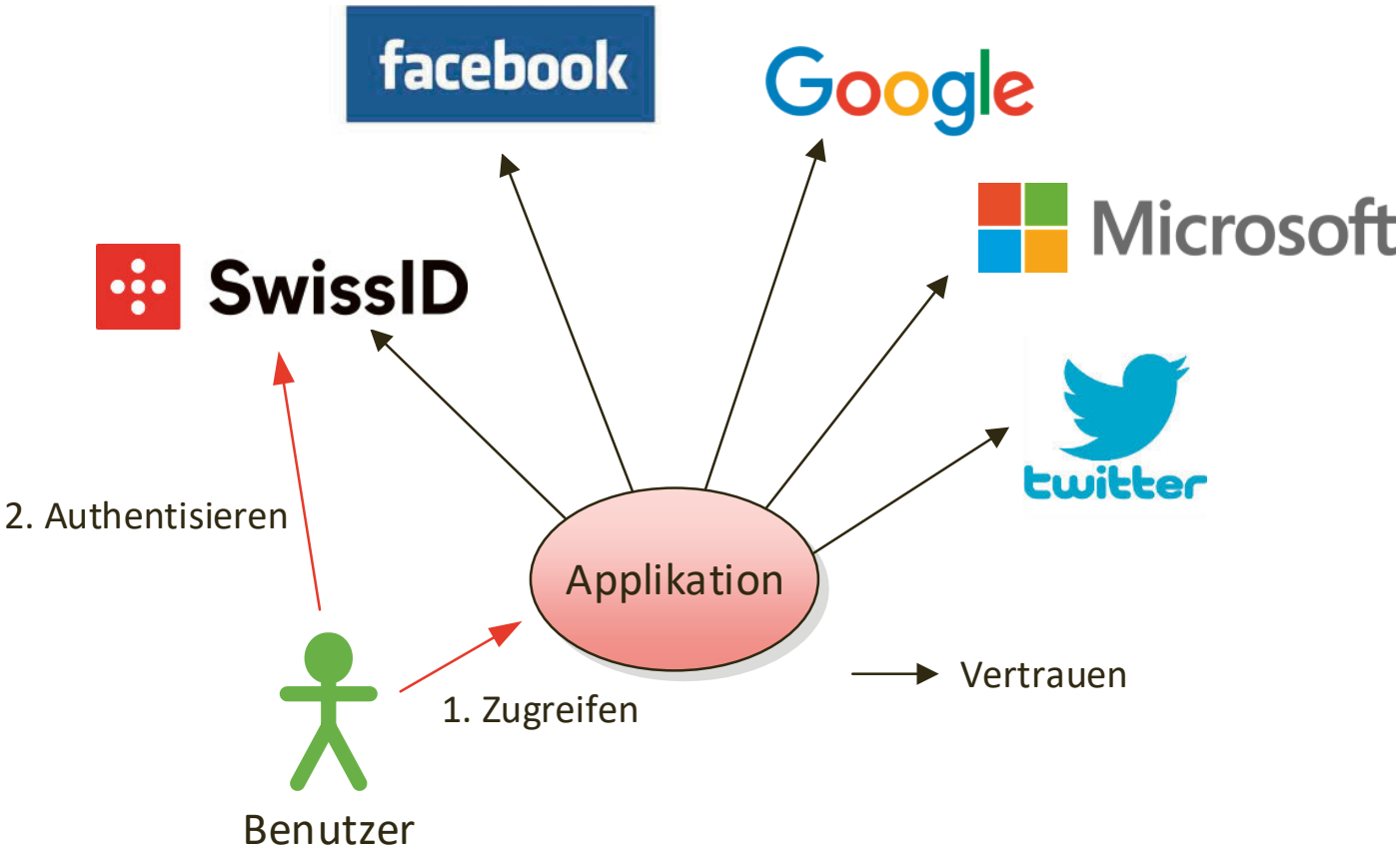


Abbildung: Login mit einer föderierten Identität

che Ereignisse in der Vergangenheit gezeigt haben, können diese Benutzerinformationen durch Schadsoftware oder unehrliche Insider entwendet werden und damit in falsche Hände geraten. Ein Angreifer kann die so gewonnenen Zugangsinformationen auf anderen möglichen Online-Diensten ausprobieren, um sich so einen unberechtigten Zugang zu verschaffen. Den betroffenen Benutzern wird nach Bekanntwerden eines solchen Vorfalls empfohlen ihr Passwort schnellstmöglich auf allen möglichen Systemen zu wechseln. Aber wer weiss dann schon, wo überall eine gewisse Zugangsinformation bereits verwendet wurde.

Um dies zu vermeiden, werden Benutzer dazu angehalten für jeden Webshop oder Online-Dienst möglichst ein anderes Passwort zu verwenden. Diese Forderung skaliert aber bei der heutigen Fülle von Internetdiensten, die wir täglich nutzen nicht mehr. Im Idealfall kommt man dieser Forderung nach und versucht das daraus entstandene Problem mit einem lokalen oder Online-Passwortlisten Verwaltungssystem (Passwort-Manager) in den Griff zu kriegen. Oder man missachtet diese Empfehlung gänzlich und verwendet ein und dasselbe Passwort für möglichst viele Online-Dienstanbieter.

Ein weiteres Problem liegt darin, dass wir bereits heute und in Zukunft vermehrt Online-Dienste in ganz unterschiedlichen sozialen Bereichen nutzen werden. Mit dem Aufkommen von Online Diensten im Gesundheitswesen und ganz allgemein im E-Government Bereich, werden unterschiedliche Qualitäten an die Authentifizierung und Identifizierung eines Benutzers (bzw. Bürgers) gelegt. Es ist also undenkbar bzw. viel zu gefährlich, wenn man dieselben Zugangsinformationen, welche man für den Webshop A eingegeben habe, auch für sein Login als Bürger auf einem Dienst seiner Gemeinde verwenden würde oder gar als Zugang zu seinem elektronischen Patientendossier.

Eine Entschärfung dieser Problematik kann dadurch erreicht werden, dass für einen Zugang nicht nur Benutzernamen/Passwort, sondern zusätzlich ein weiterer Authentifizierungsfaktor verlangt wird. Gerade beim Zugriff auf sensitive Daten (Gesundheitswesen, Bankenapplikationen, Versicherungsportalen, usw.) wird davon rege Gebrauch gemacht. Diese Dienstanbieter verlangen für einen Zugang, dass der Benutzer beweisen kann, dass er Zugriff auf einen weiteren Authentifizierungsfaktor hat (z.B. auf das Handy, auf eine Smartphone-App oder auf ein spezielles Gerät). Diese Form der Mehrfaktoren-Authentifizierung lohnt sich aber nicht in jedem Fall, denn sie ist mit erheblichem Aufwand und Mehrkosten auf Seiten Dienstanbieter verbunden.

Dennoch hat das System der verteilten Identitäten einen Vorteil. Dieser liegt darin, dass die personenbezogenen Daten vom Webshop, also dezentral erhoben und abgelegt werden. Wenn sich ein Benutzer bei einem Webshop direkt registriert sind keine Drittsysteme beteiligt und auch bei der Nutzung des Dienstes sind in der Regel keine anderen Systeme involviert, ausser diejenigen der beteiligten Infrastruktur- und Netzwerkanbieter. Die Kommunikation erfolgt also «direkt» zwischen Browser/Applikation und dem jeweiligen Webdienst.

Der Weg zur föderierten E-Identität

Wir kennen und verwenden föderierte Identitäten bereits seit einiger Zeit, wenn wir uns z.B. mit einem Facebook- oder Google-Konto auf einem Webshop einloggen. Diese Form der Authentisierung ist für den Benutzer einfach und transparent, auch wenn man sich nicht bewusst ist, was dabei genau passiert. Ein Benutzer greift auf eine Applikation zu und diese lässt den Benutzer bei einem entfernten Identitätsdienst (wie Google, Facebook, Twitter, usw.) authentifizieren. Die Applikation vertraut dabei dieser Authentifizierung.

Auch in der Schweiz wird der Versuch unternommen die lokal verteilten E-Identitäten durch andere Lösungen zu ersetzen. Mit der SuisseID wurden 2010 erstmals elektronische Identitäten mit einer gesetzlichen Basis geschaffen, welche von mehreren Anbietern zum Kauf angeboten wurden. Der durchgreifende Erfolg blieb aber aus. Die neuesten Bemühungen gehen in dieselbe Richtung. So soll im eID-Gesetz* eine nationale E-Identität verankert werden und die neue SwissID der Post und SBB sind ein weiterer Versuch diese umzusetzen. *(https://www.bj.admin.ch/bj/de/home/staat/gesetzgebung/e-id.html)

Hier preist man nun aber genau das Gegenteil zu den bisher geforderten individuell verwendeten Passworten an: Eine E-Identität (mit zentral geführten personenbezogenen Daten und einem sicheren Authentifizierungsverfahren soll nun für alle möglichen Services bedenkenlos eingesetzt werden. Sogar in unterschiedlichen sozialen Bereichen, soll man diese E-Identität bedenkenlos einsetzen können.

Mit anderen Worten: «Wenn man eine E-Identität mit einem Login über ein föderiertes Identitätssystem für den Zugriff auf einen Webshop und gleichzeitig für den Zugriff auf die Steuererklärung seines Kantons verwendet, sind diese Regeln hinfällig und es scheinen keine Sicherheitsbedenken zu bestehen.» Warum und weshalb?

Die Antwort ist relativ einfach: Weil die Authentifizierung eines Benutzers nicht mehr von einer Applikation selbst ausgeführt wird, sondern von dieser an einen dafür speziell abgesicherten Dienst delegiert wird. Die Applikationen, welche diesen Dienst verwenden, müssen die Authentisierungsinformationen eines Benutzers nicht mehr selbst kennen und diese zwecks Authentifizierung als Referenz lokal abspeichern. Es ist sogar so, dass sie diese beim Login eines Benutzers gar nie zu Gesicht kriegen. Nur dieser spezielle Dienst (nennen wir ihn Identitätsdienstleister) authentifiziert den Benutzer und macht in der Folge eine Aussage darüber, ob sich der Benutzer bei ihm erfolgreich authentisieren konnte und mit welcher Qualität. Die Applikation vertraut dieser Aussage und entscheidet selbstständig, ob sie dem Benutzer den Zugriff gewähren will oder nicht. Ein solcher Identitätsdienstleister hat den Vorteil, dass er bezüglich Aufbewahrung der gesamten Identitätsinformationen eine abgesicherte Umgebung bieten kann. Zusätzlich ist er in der Lage verschiedene Authentisierungsmethoden (Benutzername/Passwort, SMS, Smartphone App, starke Authentisierungsverfahren) zu unterstützen und je nach Anforderung der Webapplikation diese auch vom Benutzer einzufordern. Dies alles führt zur Entlastung einer Web-Applikation beim Identitätsmanagement.

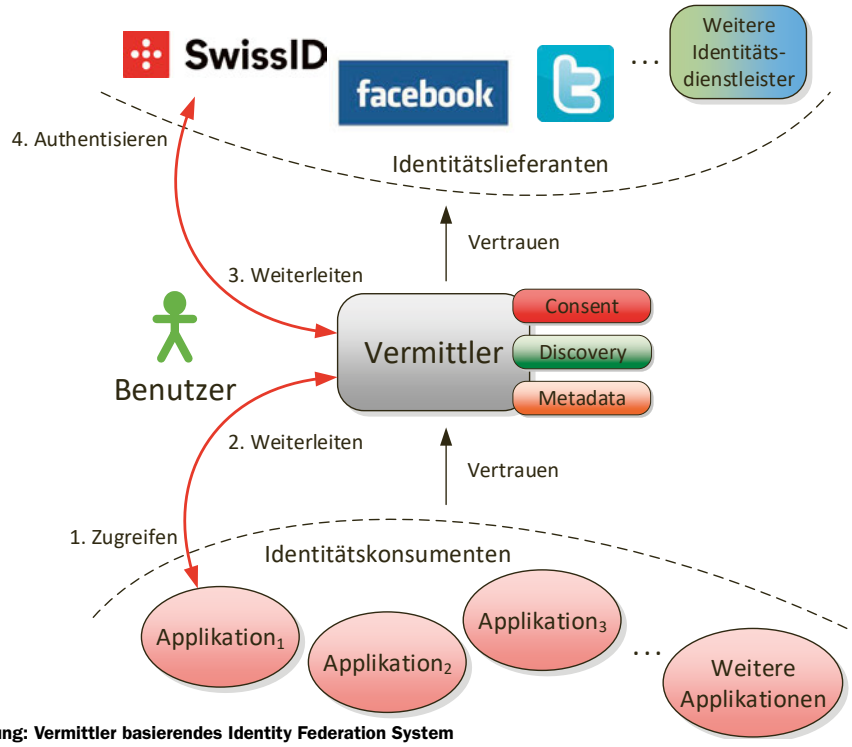


Abbildung: Vermittler basierendes Identity Federation System

Deshalb bieten Webshops und Online-Dienste heute vermehrt ein Login mit einer föderierten Identität an, wie z.B. Google, Twitter oder Facebook.

Wie sieht es mit dem Schutz der Privatsphäre aus?

Wenn die Authentifizierung eines Benutzers an einen speziellen Dienst delegiert wird, so erhält eine Web-Applikation Informationen darüber, bei welchem Identitätsdienstleister ein Benutzer ein Konto hat und umgekehrt erfahren die Identitätsdienstleister bei welchen Web-Applikationen sich ihre Benutzer Zugang verschaffen wollen. Die Sichtbarkeit von Identitätsdienstleister für eine Web-Applikation stellt im Normalfall kein grosses Problem dar, da aus den gewonnenen Informationen nur ein begrenzter Nutzen gezogen werden kann. Umgekehrt kann es aber für

einen Identitätsdienstleister sehr interessant sein, die besuchten Webdienste eines Benutzers zu erfassen, da diese Information für eine mögliche Profilbildung sehr wertvoll sein kann. Mit genau diesen Informationen können z.B. Facebook, Google und Twitter laufend ihre Nutzerprofile anreichern.

Zusätzlich kann es für Applikationen aus verschiedenen sozialen Bereichen von grossem Interesse sein, die aus den erhaltenen Identitätsinformationen erhaltenden Daten zu einem Gesamtbild eines Benutzers zu vervollständigen.

Föderierte Identitäten mit Vermittlersystem

Nebst der oben beschriebenen Einbusse der Privatsphäre kommen weitere Nachteile hinzu. Die Teilnehmer (Webapplikationen und Identitätslieferanten) in einem solchen System kommen schnell mal an ihre Grenzen, wenn zu viele Identitätslieferanten mit Web-Applikationen verbunden werden müssen. Die Anforderungen an die Identitätsvermittlung müssten entweder für alle gleich sein, oder in einem umfassenden Regelwerk konfiguriert und auf die jeweiligen Teilnehmer verteilt werden. Nur so kann ein bestimmtes Mass an Vertrauen zwischen den Systemen aufgebaut werden. Aus diesen Gründen werden vermehrt Lösungen angestrebt, die auf einem Vermittlersystem beruhen. Mit einem Vermittler im Zentrum kann die Komplexität eines föderierten Identitätssystems stark reduziert werden.

Bei diesen Lösungen agiert ein Vermittler (Broker) zwischen Identitätslieferanten und -konsumenten. Damit können zwar viele der soeben beschriebenen Nachteile entschärft werden, aber es entstehen auch neue Nachteile. Ein wichtiger Vorteil liegt darin, dass dieser Vermittler die direkte Kommunikation bei der Authentifizierung in zwei unabhängige Abschnitte teilt.

Wenn sich ein Benutzer authentisieren will, so wird er von der Applikation an den Vermittler weitervermittelt. Der Vermittler lässt den Benutzer den Identitätsdienst auswählen. In einem zweiten Protokollabschnitt leitet der Vermittler den Benutzer zur Authentifizierung an diesen weiter und sendet das Ergebnis der Authentifizierung an die anfragende Applikation zurück als wenn der Vermittler die Authentifizierung des Benutzers selbst vorgenommen hätte. Ein Identitätslieferant «sieht» so nicht mehr automatisch auf welchen Webdienst ein Benutzer zugegriffen hat und die Web Applikation ‹sieht› nicht mehr, bei welchem Identitätsanbieter sich ein Benutzer authentisiert hat. Man spricht von «double blinding».

Ein grosser Vorteil dieser Struktur liegt also darin, dass die Applikationen (Identitätskonsumenten) nur einen Ansprechpartner benötigen und damit nur ein Vertrauensverhältnis zum Vermittler aufbauen müssen. Dasselbe gilt für die Identitätslieferanten; auch sie liefern ihre Ergebnisse nur an eine Instanz – dem Vermittler, welchem sie vertrauen. Ein weiterer Mehrwert liegt darin, dass unter anderem die Funktionen – wie die Auswahl eines möglichen Identitätslieferanten (Discovery), die Einwilligung eines Benutzers zur Weitergabe von Informationen an eine anfragende Web-Applikation (Consent), wie auch eine zentral geführte Datenbank aller beteiligten Systeme im Ökosystem (Metadata) elegant an den Vermittler ausgelagert werden können.

Vermittler als «Datenkrake»

Diese Abschottung von Informationslieferanten und -konsumenten birgt umgekehrt aber auch eine Gefahr. Der Vermittler agiert als zentrale Informationsdrehscheibe. Alle so vermittelten Benutzerinformationen fliessen durch ihn hindurch. Kritiker warnen zurecht vor einer möglichen «Datenkrake». Es bestehen aber technische Möglichkeiten, auch die «Sicht» des Vermittlers auf die ausgetauschten Informationen eines Benutzers einzuschränken. Je nach Strenge dieser Anforderung, kann dies mit kryptographischen Mitteln umgesetzt werden. Wenn diese nicht ausreichen, müssen regulatorische Massnahmen getroffen werden, um die Privatsphäre eines Benutzers bestmöglich schützen zu können.

Privacy bewahrende föderierte Identitätssysteme

Einen anderen Ansatz um die Wahrung der Privatsphäre eines Benutzers in einem föderierten Identitätssystem noch besser sicherstellen zu können, verfolgen sogenannte Anonyme Attribut Systeme wie U-Prove[1] oder Idemix[2]. Im Gegensatz zu klassischen Online-Verfahren wie SAML[3] oder OIDC-OAuth[4] hat nur der Benutzer die Hoheit über seine Daten in Form eines Tokens, welches lokal auf seinem Rechner erstellt und abgelegt wird. Der Identitätslieferant tritt nur beim Generieren des Tokens als Aussteller in Aktion, indem er die Identitätsinformationen eines Benutzers fälschungssicher beglaubigt. Beim eigentlichen Login Prozess des Benutzers ist dieser Aussteller in der Regel gar nicht mehr involviert. Die vertrauende Partei als Applikation erhält die Identitätsinformation und die Leseberechtigung einzelner Attribute direkt vom Inhaber des Tokens, statt vom Aussteller über das Netzwerk. Solche Lösungen verhindern einerseits die Verkettung von unterschiedlichen Authentifizierungsprozessen eines Benutzers und andererseits ermöglichen sie die selektive Offenlegung einer Identität durch den Benutzer selbst. Der Nachteil dieser Systeme ist die zurzeit noch fehlende Verbreitung. Es benötigt noch einige Zeit, bis solche Architekturen eine genügend grosse Akzeptanz erlangt haben, um im E-Government Bereich breit eingesetzt werden zu können.

Fazit

Gerade im Umfeld der Hochschulen, bei Behörden und im privaten Bereich setzen sich vermehrt Vermittler-basierende föderierte Identitätssysteme durch, da sie auf standardisierten Technologien, bekannten Protokollen und bewährten kryptographischen Algorithmen aufbauen. Beispiele dazu sind die Swiss edu-ID[5], die neue SwissID[6] von SwissSign und IDV-Schweiz[7] ein Projekt des Schwerpunktplans E-Government Schweiz. Auch die staatlich anerkannte elektronische Identität (E-ID) schlägt in ihrem Konzept und in der bevorstehenden Gesetzgebung ein ähnliches System vor, in welchem künftig zertifizierte Identitätsanbieter mit Identitätsdaten eines Bürgers vom Bund beliefert werden können. Damit sollen in Zukunft kommerzielle Webshops und besonders Anwendungen aus dem E-Government sich auf staatlich erfasste und überprüfte Benutzerinformationen verlassen können.

Institute for ICT-Based Management

Das Institute for ICT-Based Management der Berner Fachhochschule[8] berät Firmen und Behörden bei der Umsetzung und Integration von Identity Federation Systemen und leistet einen wichtigen Beitrag bei der Standardisierung solcher Systeme in der Schweiz, mit dem Ziel eine grösstmögliche Interoperabilität zwischen Behörden, Bürgern und privaten Organisationen zu erlangen.

Autor

Gerhard Hassenstein
Dozent für Internet-Security
Berner Fachhochschule (BFH)

1 Eine von Stefan Brands entwickelte und von Microsoft übernommene Technologie: https://www.microsoft.com/en-us/research/project/u-prove
2 Ein von IBM entwickeltes Anonymous Credential System: https://www.zurich.ibm.com/identity_mixer
3 'Security Assertion Markup Language' von OASIS: https://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf
4 'OpenID Connect' http://openid.net/connect/ und OAuth2.0: https://tools.ietf.org/html/rfc6749
5 https://projects.switch.ch/eduid
6 https://www.swissid.ch
7 https://www.idv-fsi.ch
8 https://www.ti.bfh.ch/forschung/institute_for_ict_based_management/

Unternehmens-werte schützen. Zukunft sichern.

Höchster Schutz für Ihre Daten

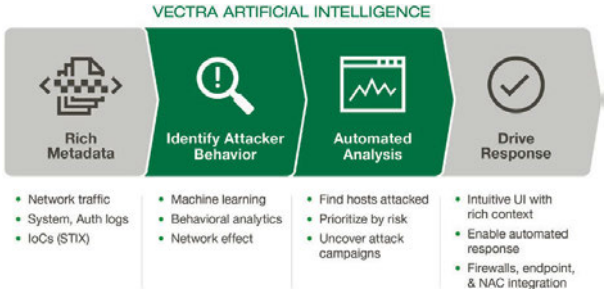
Angriffe werden immer «intelligenter» und mit der zunehmenden Digitalisierung steigt die Angriffsfläche: die Zahl von Maschinen, Anlagen, Geräten und auch Produkten mit Zugang zum Internet schnellt in die Höhe. Ebenso die Nutzung mobiler Geräte. Ziel ist oft der Datenabfluss geschäftsrelevanter Informationen, denn der elektronische Datenhandel ist ein lukratives kriminelles Geschäft und traditionelle Security Abwehrmassnahmen von Organisationen sind bekannt und können oft umgangen werden. Unternehmen müssen daher mehr für den Schutz von Daten und Netzwerken tun.

LC Systems bietet Ihnen ein erprobtes und innovatives Portfolio für eine sichere Zukunft. Und das Beste: Sie benötigen mit unseren Lösungen so gut wie keine Ressourcen!

VECTRA

Kompromisslose, visuelle Klarheit von laufenden Cyber-Attacken in Echtzeit

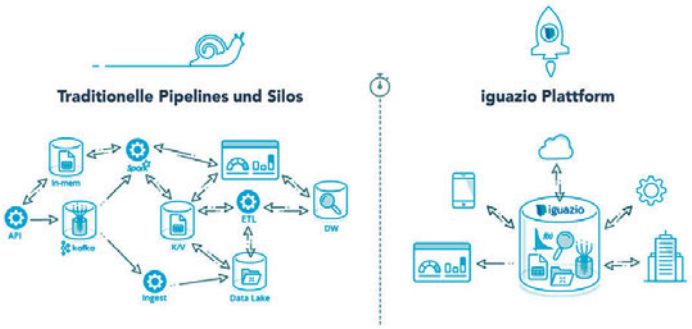
Mit Vectra erhalten Sie eine Plattform für Bedrohungserkennung und Response. Sie automatisiert die Jagd auf Cyber-Angreifer mittels künstlicher Intelligenz und zeigt, wo sie sich verstecken und was sie tun.



iguazio

Moderne Analytik Plattform für Security und IoT

iguazio ermöglicht das Speichern, Anreichern und Analysieren von Daten auf einer einzigen, einfachen und höchst sicheren Plattform. Sie beschleunigt den Einsatz verschiedenster Data Science Services für Security Analyse und Forensik und kommt ohne komplexe Datenpipelines aus. Durch die Vereinfachung der Architektur lassen sich mit iguazio Big Data Projekte schneller und sicherer umsetzen als je zuvor.



LC SYSTEMS

Offline-Zutrittssysteme: Endlich kommt der lang erwartete Standard

Im Bereich der Bezahlfunktionen (Standard Cash) und Online-Zutrittskontrollsysteme (Standard Access) hat sich auf RFID-Medien ein herstellerneutraler Standard etabliert. Was bislang fehlte, war etwas Vergleichbares im Bereich des Offline-Zutrittsmanagements. Eine Interessengemeinschaft von Endanwendern hat diesen Standard nun im Segment «Standard Offline» der «Open-Security-Standards OSS» definiert.

In diversen Anwender-Bereichen werden die Rufe nach Standards immer lauter, so z.B. normierte Ladegräte für Handy. Eine ähnliche Entwicklung zeichnet sich auch für Bezahlfunktionen mittels RFID-Medien ab. Die Endanwender sind es leid, für jede Bezahlfunktion, für jeden Standort oder gar für jeden Automaten ein separates Guthaben auf den Badge zu laden. Auch hier wurde ein herstellerunabhängiger Standard entwickelt, der sich mittlerweile etabliert hat.

Für Online-Zutrittskontrollsysteme existiert ebenfalls ein gut funktionierender Standard (Online Standard Access), der von sämtlichen dem Autor bekannten Herstellern verarbeitet werden kann. Wieso soll das also nicht auch für Offline-Zutrittslösungen möglich sein? In diesem Bereich existierte nämlich bis vor Kurzem nichts, was mit den oben erwähnten Beispielen vergleichbar wäre. Es stellt sich nun die Frage, weshalb das so ist.

Die Herausforderung

Historisch gewachsen existieren im Bereich der Offline-Zutrittskontrolle nur herstellerspezifische (proprietäre) Programmierrichtlinien. Bis anhin hat das auch kaum Probleme verursacht. Der Endanwender ist in aller Regel glücklich mit sei-

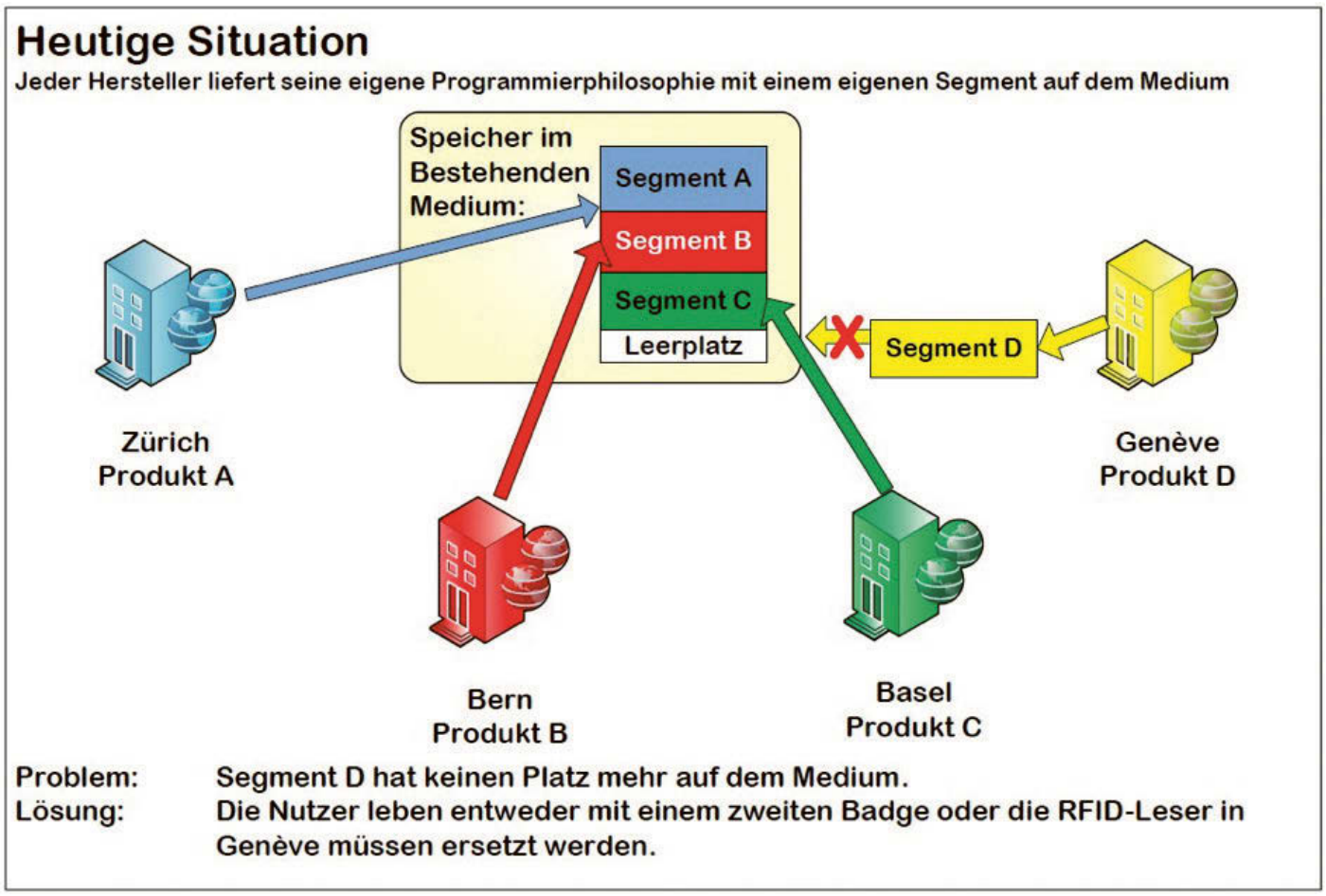


Abbildung 1: Neben den bestehenden Standorten Zürich, Bern und Basel wird die Integration der neuen Niederlassung in Genf zu einer echten Herausforderung.

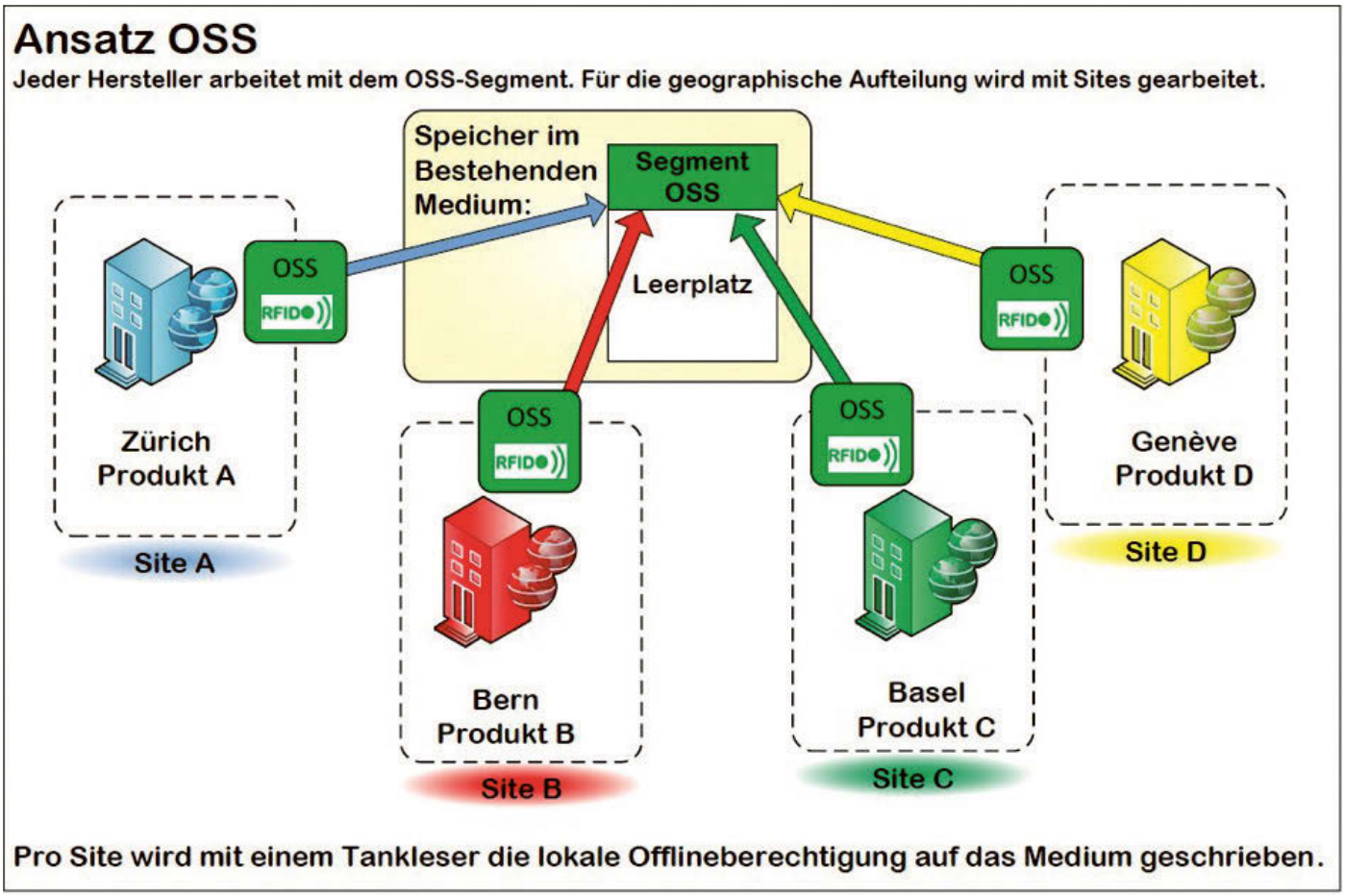


Abbildung 2: Mit Hilfe des Standardsegments der OSS lassen sich Badgeleser unterschiedlicher Hersteller mit einem einzigen Segment bedienen.

nem System und der Hersteller kann sich darauf verlassen, dass er einen treuen Kunden hat, der immer wieder Komponenten nachbestellt. Nun gilt es aber verschiedene Faktoren zu berücksichtigen, die einen Endanwender vor erhebliche Probleme stellen können. In der immer flexibler werdenden Arbeitswelt wechseln Gebäude schnell den Nutzer und/oder den Besitzer. Die bestehende Zutrittskontrollanlage des Anwenders muss diese Änderungen ebenfalls rasch bewerkstelligen können oder mit den am neuen Standort bereits montierten Komponenten kompatibel sein. Hinzu kommt, dass Konzerne beginnen, an all ihren Standorten einheitliche Standards einzuführen. Firmen fusionieren oder übernehmen einander. Es werden Kooperationen und ARGEs gebildet. Unternehmen, die dem öffentlichen Beschaffungsrecht unterstellt sind, müssen Schliess- und Zutrittskontrollsysteme unter Umständen für jedes Bauprojekt neu ausschreiben. Dadurch steigt die Anzahl unterschiedlicher Produkte und Software-Guidelines innerhalb eines Verantwortungsbereichs unweigerlich.

Im Focus steht aber stets ein Kernbedürfnis des Schlüssel- oder Badgeträgers: alle Türen mit einem einzigen Medium öffnen zu können.

Da die unterschiedlichen Programmierframeworks untereinander nach wie vor nicht kompa-tibel sind, bleibt nur die Möglichkeit, auf dem Zutrittsmedium mit einem Segment je Produkt zu arbeiten. Die unterschiedlichen Systeme könnten auch durch ein komplett neues System ersetzen werden, welches von Grund auf neu konzipiert, beschafft und installiert wird. Doch welches Unternehmen wendet diese Kosten auf? Entweder fehlt schlicht das Geld oder die Budgetverantwortlichen erkennen die Komplexität der Verwaltung verschiedener Systeme nicht und lehnen eine entsprechende Investition ab.

Ein Endanwender mit Badgelesern verschiedener Hersteller kämpft also mit folgenden Problemen:

- Verschiedene proprietäre Segmente auf ein Medium bringen
- Verschiedene proprietäre Verwaltungsapplikationen betreiben und miteinander vernetzen.
- Entweder die Prozesse den Programmierphilosophien der Hersteller anpassen oder auf Leistungsmerkmale einzelner Philosophien verzichten.
- Verstehen aller unterschiedlichen Philosophien, um das Maximum an Nutzen herauszuziehen.
- Steigende Komplexität im Gesamtsystem, mit entsprechend höherer Fehleranfälligkeit.

Abhilfe schaffen

Wie lässt sich verhindern, dass der Überblick im Gesamtsystem verlorengeht und das System nicht mehr korrekt funktioniert? Zunächst muss dafür gesorgt werden, dass die Anzahl unterschiedlicher Systeme nicht weiter anwächst.

Eine Möglichkeit hierfür sind langfristige Rahmenverträge mit möglichst wenigen Herstellern. Natürlich lässt sich das nicht in jedem Unternehmen einfach so durchführen, aber es ist zumindest eine prüfenswerte Alternative.

Eine andere Möglichkeit wäre eine Standardsegmentierung mit mehreren proprietären Segmenten und ausschliesslich

kompatiblen Produkten zu erstellen. Die Herausforderung besteht in diesem Ansatz darin, die richtigen Programmierphilosophien zu wählen. Darüber hinaus müssen immer noch je System eine Verwaltungsapplikation betrieben und mit anderen vernetzt werden. Für bundesnahe Betriebe steht diese Möglichkeit aus rechtlicher Sicht kaum zur Disposition (Öffentliches Beschaffungsrecht mit gleichen Chancen für alle potentiellen Lieferanten).

Beide Varianten wurden in der Vergangenheit angewendet. Gerade für grössere Firmen, Unternehmen mit besonderen Anforderungen an die Sicherheit und/oder komplizierten Strukturen ist allerdings keine dieser Varianten ideal.

Ein neuer Ansatz

Diese Unzufriedenheit machte sich im Verlauf der letzten Jahre bei einer steigenden Anzahl von Endanwendern bemerkbar. Immer mehr Sicherheitsverantwortliche wünschen sich eine Segmentierung, die mit den Badgelesern möglichst aller Hersteller kompatibel ist. Es gab denn auch verschiedene Bemühungen, einen solchen Standard zu entwickeln. Allerdings verliefen diese Bemühungen allesamt erfolglos.

Im Oktober 2015 trafen sich 13 Vertreter von verschiedenen Schweizer Endanwendern, um einen weiteren Versuch zu starten, ein herstellerneutrales Standardsegment zu entwickeln.

Dieser Ansatz wurde allerdings relativ schnell zu Gunsten des bereits existierenden Standards der OSS-Association e.V. verworfen. Der sogenannte OSS-SO erfüllte bereits in der ersten Version die wesentlichsten Anforderungen, wovon sich die Endanwender verschiedentlich überzeugen konnten.

Nun ging es darum, die bestehenden Verbesserungspotentiale des neuen Standards zu benennen und bestmöglich abzuschöpfen. Hierfür schlossen sich die Endanwender in der «Interessengemeinschaft Offline Standard iGOS» zusammen. Dabei wurde bewusst darauf verzichtet, sich in einem Verein oder einer sonstigen Organisation zusammenzuschliessen. So kann die höchstmögliche Flexibilität in Bezug auf aktive Beteiligung gewährleistet werden und es bestehen keinerlei Verpflichtungen.

Die iGOS wählte anschliessend einen Consultant, der dem Verein OSS beitrat und die Interessen der Endanwender im Entwicklungsprozess einfliessen liess. Dieser Ansatz trug bereits erste Früchte und heute steht eine verbesserte Version der Standards zur Verfügung.

Weitere Auskünfte zur Interessengruppe sind im Internet unter www.offline-standard.ch zu finden. Für Auskünfte steht Fabian Lange (fabian.lange@sbb.ch) gerne zur Verfügung.

Weitere Informationen zum aktuellen Standard OSS-SO (inkl. Gewisser technischen Dokumentationen) und zur OSS-Association e.V. finden sich unter www.oss-association.com.

Seit dem ersten Workshop ist der Kreis von interessierten Endanwendern immer grösser geworden, was von allen Beteiligten sehr begrüsst wird. Alle interessierten Unternehmen sind weiterhin herzlich eingeladen, an einem der kommenden Workshops teilzunehmen, ihre Bedürfnisse zu formulieren oder sich einfach mit anderen Endanwendern auszutauschen.

Fazit

Der Standard OSS ist aus zwei Gründen der bislang erfolgreichste Versuch, einen herstellerneutralen Standard für das Zutrittsmanagement im Bereich Offline-RFID zu erarbeiten. Einerseits haben sich einige renommierte Hersteller zusammengesetzt und ein Produkt entwickelt, das «Hand und Fuss» hat. Andererseits bieten die Endanwender mit einigen gestarteten und diversen geplanten Projekten für die Produzenten den nötigen finanziellen Anreiz, dieses Produkt auch tatsächlich zu entwickeln. Aufgrund der Tatsache, dass nicht jeder Endanwender separat mit seinen Herstellern das Gespräch sucht, wird auch eine gezieltere Weiterentwicklung ermöglicht.

Natürlich besteht momentan noch Entwicklungspotential. Sei es in der Anzahl Anbieter von marktfähigen Produkten oder im Bereich der technischen Möglichkeiten. Dank der koordinierten und konstruktiven Zusammenarbeit aller Beteiligten ist die Chance aber gross, dass sich hier ein weiterer, lang erwarteter Standard weiterentwickelt und schlussendlich etabliert.

Autor

Fabian Lange
Leiter
Schliess- und
Zutrittskontroll-
systeme
SBB AG

CYBERSICHERHEIT

Szenario basierte Trainings (War Game) als Baustein zur Erhöhung der Cybersicherheit

Einleitung

In den letzten Jahren entstand durch das Internet ein technologisch geprägter gesellschaftlicher Wandel, welcher nicht mehr aufhaltbar ist. Getrieben durch Digitalisierung, Automatisierung und Vernetzung wurden immer mehr Lebensbereiche sowie Geschäftsprozesse miteinander vernetzt. Dies hat zu einer Technologiespirale geführt, die immer schneller neue Technologien und Nutzungskontexte hervorbringt. Dadurch entsteht ein vielfältiges und lukratives Betätigungsfeld für kriminelle Aktivitäten im und durch das Internet. Viele Studien belegen den dadurch entstandenen volkwirtschaftlichen Schaden, jedoch sind für die Schweiz solche Erhebungen nicht vorhanden.

Die Professionalisierung der Täter führt zu immer neuen Angriffsmethoden und die Schäden auf der einen Seite sind die Gewinne auf der anderen Seite. Insbesondere Unternehmen und Behörden sind in den Fokus der Kriminellen gerückt. Egal ob Cybercrime, Cyberspionage und Cybersabotage, die Motivation der Angreifer ist hoch und die Ziele sind lohnend. Da die technischen Komponenten und IT-Infrastrukturen der meisten Unternehmen und Behörden häufig unsicher sind und ausnutzbare Schwachstellen aufweisen, werden diese für Straftaten missbraucht. Die IT-Systeme sind meistens nicht das Ziel, sie sind das Mittel zum Zweck und werden dazu benutzt, Daten und Informationen zu entwenden, diese zu manipulieren oder Systeme nachhaltig zu stören. Bei Cyberangriffen steht immer ein Täter und somit eine Straftat im Vordergrund, daher müssen bei Cyberangriffen neben den technischen auch nicht-technische Aspekte berücksichtigt werden.

Cyberangriffe können als Massenphänomen oder als gezielter Angriff einem sogenannten «targeted attack» durchgeführt werden. Bei Massenphänomenen handelt es sich meistens um Cybercrime im engeren Sinne[1]. Bei gezielten Angriffen haben die Angreifer immer häufiger auch Cyberspionage[2], zur verdeckten Informations- und Datengewinnung oder Cybersabotage[3] zum Stören oder Zerstören strategischer IT-Systeme von Kritischen-Infrastrukturen zum Ziel. Welche Angriffsmethode von den Tätern angewandt wird, hängt vom übergeordneten Ziel des Cyberangriffs ab.

Bevor wir uns dem Szenario basierten Training als Baustein zur Erhöhung der Cybersicherheit zuwenden, nehmen wir eine Begriffsdefinition und Abgrenzung zwischen Informationssicherheit, IT-Sicherheit und Cybersicherheit vor, damit ein einheitliches Verständnis der Begriffe entsteht.

Begriffsdefinitionen und Abgrenzung zur Cybersicherheit

Wenn nach Cybersicherheit im Internet gesucht wird, gibt es zahlreiche Treffer und eine grosse Anzahl von unterschiedlichen Begriffen und Begriffsdefinitionen, die alle zumeist die Vertraulichkeit, Integrität und Verfügbarkeit von Informationen, Daten und Systemen beschreiben. So ist die Rede von Informationssicherheit, Datensicherheit, Datensicherung, Datenschutz, IT-Sicherheit, Computersicherheit, Cybersicherheit und noch vielen weiteren Begriffen. Eine nähere Betrachtung und Definition dieser Begriffe zeigt jedoch, dass oft eine Falschverwendung und Überdefinition von Begriffen herrscht. Es gibt zu viele Begriffe, die sich überschneiden, gemeinsame Schnittstellen haben und häufig vermischt werden.

Es ist daher wichtig in einem ersten Schritt die korrekten Begriffe und Begriffsdefinitionen darzustellen. Die Autoren fokussieren dabei auf 3 zentrale Begriffe, unter denen die zahlreichen weiteren Begriffe subsumiert werden können. Diese sind Cybersicherheit, Informationssicherheit und IT-Sicherheit, die ebenfalls fälschlicherweise oft einander gleichgestellt werden, da sie stark voneinander abhängen und Wechselwirkungen haben. Ein

1 Bei Cybercrime spricht man von Cybercrime im engeren und im weiteren Sinne. Unter Cybercrime im engeren Sinn werden alle Straftaten gefasst, die sich gegen Computersysteme, Netzwerke und Daten durch das Internet richten oder nur damit durchführen lassen (DDoS Attacken, Trojaner wie WannaCry, Locky, TeslaCrypt). Cybercrime im weiteren Sinne umfasst der Begriff aller Straftaten, die über oder durch Dienste im Internet durchgeführt werden können (Betrugsarten im Internet – eCommerce-Fraud, CEO-Betrug, etc.).

2 Bei Cyberspionage handelt es sich wie bei der klassischen Spionage um die verdeckte Informations- und Datengewinnung, mit dem Unterschied, dass bei der Cyberspionage die Gewinnung von Informationen, welche in Computersystemen oder Datenbanken gespeichert sind, im Vordergrund stehen. Bei der Cyberspionage geht es darum, einen Wettbewerbsvorteil (Industriespionage) oder einen staatlichen Wirtschaftsvorteil (Wirtschaftsspionage) zu erlangen (z.B. Deutscher Bundestag, RUAG, Abhörskandal der Iran-Atomgesprächen in Genf, etc.).

3 Bei der Cybersabotage geht es um störende oder zerstörende Angriffe auf strategische Ziele zumeist bei Kritischen-Infrastrukturen. Bei einem Sabotageangriff ist es wichtig zu verstehen, was das eigentliche Ziel des Angriffs ist und ob die angegriffene Infrastruktur das direkte Ziel oder nur eine Teilkomponente in der zu sabotierenden Wertschöpfungskette ist. (Ukrainischer Stromerzeuger, Hochofen in Deutschland)

einheitliches Verständnis und eine klare Abgrenzung der Begriffe ist elementar für die Definition der Massnahmen zur Erhöhung der Sicherheit.

Abgrenzung der Begriffe

Viele Unternehmen auf der Anbieter- als auch auf der Anwenderseite stellen die Cybersicherheit häufig der Informationssicherheit und/oder der IT-Sicherheit gleich. Durch die zunehmende Digitalisierung und Vernetzung der Systeme und Netzwerke ist jedoch festzustellen, dass ein reiner IT-Ansatz nicht zielführend ist und die Cyberproblematik deutlich über den IT-Ansatz hinausgeht und sich daher auch von der Informationssicherheit abgrenzt.

Cybersicherheit	Technische und organisatorische Massnahmen zum Schutz der jeweiligen Organisation gegen kriminelle Handlungen (Straftaten) durch Missbrauch der Informationstechnologie (z.B. Cyberstrategie, Risikomanagement, Lagebild, Strafverfolgung).
Informationssicherheit	Technisch und organisatorische Massnahmen zum Schutz von geschäftsrelevanten und personenbezogenen Daten und Informationen, sowie zur Erfüllung regulatorischer Auflagen (z.B. Privacy, Compliance, GDPR).
IT-Sicherheit	Massnahmen und Sicherheitstechnologien zum Schutz der IT Infrastrukturen (z.B. Identity and Access Management, SIEM, End-point Security, ISMS, ISO 27000)

Tabelle: Begriffsdefinitionen

Die Informationssicherheit dazu gehören die Daten im Kontext (Informationen), und die IT-Sicherheit (dazu gehören die technischen Infrastrukturen und Schutzmechanismen für Arbeitsplatzcomputer, Rechenzentren, Server, Netzwerke, etc.) sind eine Untermenge der Cybersicherheit, die Cybersicherheit als solche ist viel komplexer, da sie der letzte Schutzanker ist, wenn die technischen Sicherheitsmassnahmen durch Angreifer massiv gestört oder ausser Kraft gesetzt werden. Zusammen bilden die Informationssicherheit und die IT-Sicherheit die Grundlage für einen sicheren IT-Betrieb gegenüber Ausfälle, Defekte, Fehlkonfigurationen, usw. Darüber hinaus sollen die Informationssicherheit und IT-Sicherheit die Hürden für Angreifer höher legen, damit Missbrauch und Manipulationen vermieden werden. Zusätzlich ist zu berücksichtigen, dass bei der Cybersicherheit immer eine Straftat durch einen innovativen und motivierten Straftäter zu Grunde liegt, der ein strategisches Ziel verfolgt, das über die reine technische Dimension deutlich hinausgeht. Oft ist das Ziel auch die jeweiligen Geschäftsmodelle zu stören und deshalb sollten vor einem Cyberangriff zudem Massnahmen zum Schutz der jeweiligen Geschäftsmodelle getroffen werden. Cyberrisiken und Bedrohungen können nicht nur mit technischen Sicherheitsmassnahmen bekämpft werden, sondern sollten zwingend auch nicht-technische, physische, personelle und organisatorische Mittel zum Schutz des Gesamtunternehmens beinhalten. Zudem ist das Unternehmen unter Umständen zur Tat- und Täterermittlung auf externe Hilfe, wie polizeiliche oder nachrichtendienstliche Unterstützung sowie zusätzlichem IT-Fachwissen und Forensik angewiesen.

Auswirkungen sind bei Cyberangriffen höher

Im Gegensatz zum Cyberangriff ist häufig bei klassischen IT-Vorfällen eine eins-zu-eins-Wiederherstellung im Rahmen der allgemeinen Business Continuity Planung möglich. In einer ersten Betrachtung sind die Auswirkungen in beiden Fällen gleich (Ausfall der geschäftsrelevanten Systeme), jedoch sind bei einem Cyberangriff die Wiederherstellungszeiten und die damit verbundenen Kosten deutlich höher, da externe Schnittstellen (Strafverfolgung) und Experten (Forensik) eingebunden werden sollten, damit eine Wiederholung des letzten Angriff vermieden werden kann. Dazu müssen möglicherweise die Hersteller der betroffenen Systeme und Komponenten Fehlerbereinigungen, Updates oder gänzlich neue Systeme zur Verfügung stellen. Stehen diese nicht kurzfristig zum Einsatz bereit, müssen zusätzliche Sicherheitstechnologien in Betracht gezogen werden. Dieses kann unter Umständen noch längere Zeiten beanspruchen und führt direkt zu zusätzlichen Ressourcen und Budget Aufwendungen.

Szenario Basiertes Training (War Game)

Ein wichtiger Lösungsansatz zur Erhöhung der Cybersicherheit ist es ein Planspiel oder eine sogenannte strategische Simulation auf Basis eins reellen und kundenindividuellen Szenarios durchzuführen. Hierbei werden die Fach- und Führungskräfte unter Zeitdruck vor Entscheidungen und Maßnahmen gestellt, um eine Unternehmens- oder Behördenkrise durch Cyberangriffe zu vermeiden und diese mit geeigneten Massnahmen so schnell wie möglich zu beenden. Durch aufeinander aufbauende Eskalationen führt das Szenario zu relevanten Fragestellungen bei drohenden Cyberkrisen. Durch das Planspiel können Rückschlüsse darauf gezogen werden, welche strategischen, organisatorischen, personellen und technischen Maßnahmen getroffen werden sollten, damit Cyberangriffe mit geringen Auswirkungen überstanden werden können oder es erst gar nicht zur Cyberkrise kommt. Es geht dabei nicht um ein technisches Verständnis, sondern um den Erkenntnisgewinn wie Cyberangriffe ablaufen, welches die Methoden und Ziele der Täter sind, welches die Massnahmen der Schadensbegrenzung sind und wer bei welcher Problemstellung helfen kann (Behörden, Polizei, externe Dienstleister, usw.). Zudem können auf Basis der Ergebnisse geeignete präventive und stabilisierende Massnahmen identifiziert, geplant und umgesetzt werden.

Szenario basierte Trainings haben sich als wirksames Instrument zur Identifikation von technischen und organisatorischen Schwachstellen sowie den kritischen Geschäftsprozessen erwiesen. Dadurch wird ersichtlich, welche konkreten präventiven, reaktiven und stabilisierenden Massnahmen auf Basis des zugrundeliegenden Szenarios ergriffen werden sollten. Auch wird ersichtlich, dass die Massnahmen der Informationssicherheit und IT-Sicherheit für Cyberangriffe häufig falsch eingeschätzt, meistens nicht ausreichend sind und durch zusätzliche Massnahmen ergänzt werden sollten, um die Sicherheit im

gesamten Unternehmen oder einer Behörde sicherzustellen. Darüber hinaus können die Ergebnisse als Grundlage für die Entwicklung einer allumfassenden Cyberstrategie dienen und priorisieren in welche relevanten Sicherheitstechnologien und Ressourcen investiert werden sollte.

Szenario basierte Übungen sollten im zeitlichen Verlauf weiterentwickelt und an die neuen Gegebenheiten angepasst werden, dabei sind Veränderungen im Geschäftsmodell, neue Technologien, geostrategische Veränderungen als auch die Wettbewerbssituation zu beachten.

Fazit

Cyberbedrohungen sind komplex und betreffen die jeweilige Organisation über alle Geschäftsbereiche hinweg. Wer die Cyberbedrohungen erkennt, sich auf entsprechende Szenarien vorbereitet, diese übt und geeignete Massnahmen ergreift, ist auf den Ernstfall vorbereitet. Dadurch wird die Cybersicherheit nachhaltig erhöht. Sie sollten das Bewusstsein für Cybersicherheit im Rahmen einer «Sicherheitskultur» entwickeln und geeignete Kontrollmechanismen etablieren. Die thematische Wichtigkeit von Cybersicherheit steigt, da die schnell wachsende Anzahl vernetzter Informationssysteme und Netzwerke einer steigenden Anzahl von Schwachstellen gegenübersteht und die Bedrohungen durch Straftäter immer größer werden und damit das Schadensausmass stetig steigt. Cybersicherheit ist zunehmend ein Qualitätskriterium, welches nur erreicht werden kann, wenn alle technischen und organisatorischen Massnahmen zusammenwirken und diese in der Unternehmensstrategie verankert sind. Die Durchführung von Simulationsübungen/War Games sind ein «Best Practice» für Staaten und Behörden (incl. Strafverfolgung, Krisenmanagement und Verteidigung), internationale Organisationen, IT-Industrie und Anwender, um die Cybersicherheit nachhaltig zu erhöhen.

Autoren

Michael Bartsch
Geschäftsführer

Stefanie Frey
Geschäftsführerin

DEUTOR
Cyber Security Solutions Switzerland GmbH

E-GOVERNMENT

E-Government stärkt den Staat

Ein durchgängig umgesetztes E-Government vereinfacht das Leben der Bürgerinnen, Bürger sowie der Unternehmen und entlastet die Verwaltung. Die Nutzerinnen und Nutzer erhalten Behördenantworten im Idealfall innert Sekunden und die Verwaltung kann sich in einer zunehmend vernetzten Welt auf Steuerungsaufgaben konzentrieren. So stellt E-Government sicher, dass die Schweiz auch in Zukunft eine moderne und anerkannte Verwaltung hat.

Seit Jahren steht E-Government, also die elektronische Verwaltung und ihre Leistungen weit oben auf der Prioritätenliste des Bundes, der Kantone und der Gemeinden. Verschiedene Initiativen und Vorhaben wurden – zum Teil mit viel Geld – umgesetzt, um den Bürgerinnen und Bürgern wie auch den Unternehmen Behördenleistungen elektronisch anzubieten.

Beim E-Government geht es allerdings nicht nur um Vereinfachungen und mehr Flexibilität für die Bürgerinnen, Bürger und Unternehmen. Es geht ebenso um die Modernisierung der Verwaltungstätigkeit: E-Government eröffnet die Möglichkeit, die elektronisch erhaltenen Daten innerhalb der Verwaltung automatisiert zu verarbeiten. Das heisst, dass elektronische Gesuche nicht jedes Mal durch einen Fachexperten geprüft werden müssen, sondern auf Basis von vordefinierten Regeln und dank Mustererkennung mit Analytics automatisiert verarbeitet werden – sofern kein Problem vorliegt. Somit wird die Behördenantwort, zum Beispiel die Steuerverfügung, der Bürgerin oder dem Bürger innerhalb von Sekunden nach der (elektronischen) Einreichung automatisiert zugestellt. Die Entlastung ist nicht nur für die Bürgerinnen und Bürger resp. die Unternehmen substanziell, sondern auch für die Verwaltung, welche so Ressourcen für neue Aufgaben zur Verfügung hat. Zudem stehen die entsprechenden Daten dank durchgängigen digitalen Prozessen auch für Analysen und Auswertungen zur Verfügung – ein zentraler Vorteil in einer Zeit, da Steuerungsinformationen in einer zunehmend komplexen und vernetzten Welt immer wichtiger werden.

Der Weg dorthin führt über grössere und kleinere Verbesserungen in folgenden drei Bereichen: Zugang zu Leistungen für die Nutzerinnen und Nutzer, Bereitstellung von Leistungen durch die Behörden und verwaltungsinterne Verarbeitung der Gesuche.

Zugang zu Leistungen

Die Benutzerinnen und Benutzer erwarten denselben einfachen Zugang zu elektronischen Behördenleistungen, wie sie ihn aus der täglichen Erfahrung mit den grossen Anbietern im Internet kennen. Das heisst, dass die Webseiten der Behörden grafisch ansprechend, einfach verständlich und kontextabhängig dargestellt werden müssen. Eine Bürgerin oder ein Bürger möchte sich für den Antrag einer Fristverlängerung für die Steuererklärung nicht durch einen Dschungel verwirrend dargestellter und unverständlich beschriebener Behördenleistungen kämpfen. Die relevanten Behördenleisten sollen übersichtlich, leicht verständlich und kontextabhängig dargestellt sein. Dabei kann zum Beispiel der Bezug zur Lebenssituation (Familie mit Kindern, Wohnortwechsel, Arbeitsbewilligung etc.) hergestellt oder nach Leistungen für natürliche oder juristische Personen gefiltert werden.

Mit der neuen SwissID steht ein Loginsystem bereit, welches sowohl für privatwirtschaftliche Leistungen (aktuell bei der Post, in Zukunft auch bei der SBB und anderen) wie auch für Behördenleistungen genutzt werden kann. Aus Sicht der Bürgerinnen und Bürger stellt dies eine grosse Erleichterung dar, da ein separates kantonales Login und somit ein spezieller Username/Passwort für Behördenleistungen entfällt. Auch mit einem solchen Login-System ist der Datenschutz sichergestellt: Alle Fachdaten verbleiben in der Fachapplikation und ob eine Benutzerin oder ein Benutzer eine Leistung tatsächlich beziehen oder auf Daten zugreifen darf, wird durch die Fachlösung geregelt, welche die Leistung bereitstellt.

Bereitstellen von Leistungen

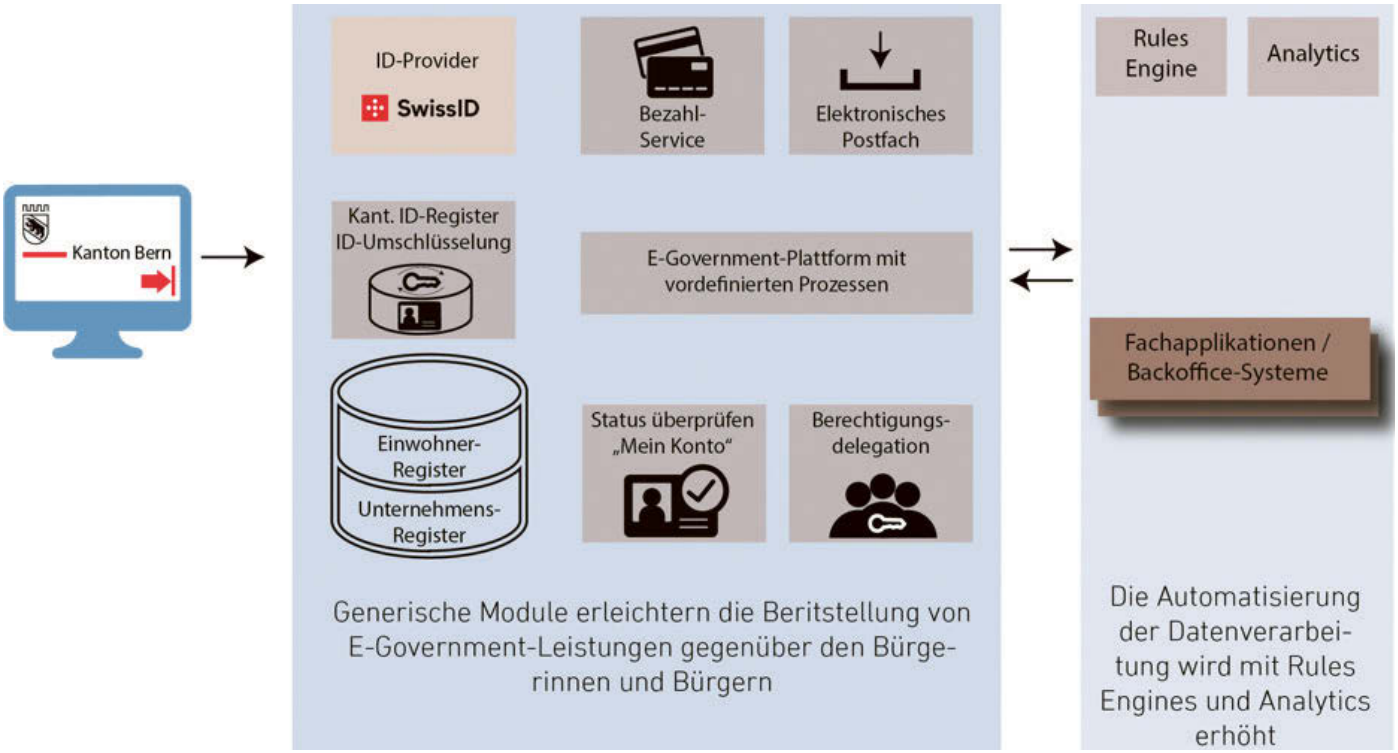
Moderne Lösungen stellen allgemein nutzbare Dienste als generische Services zur Verfügung. Solche Dienste sind beispielsweise ein Bezahlservice für die Onlinezahlung der Gebühren, ein Service für die Rechteverwaltung und Delegation (damit beispielsweise der Garagist das Auto seines Kunden beim Strassenverkehrsamt vorführen kann), ein elektronisches Postfach (damit der Behördenentscheid elektronisch zugestellt werden kann) etc. Dabei werden nach Möglichkeit auf dem Markt bestehende Services wie das SwissID-Login, bestehende Bezahldienste und das elektronische Postfach der Post eingebunden.

So wird die Breitstellung von elektronischen Dienstleistungen für die einzelnen Amtsstellen vereinfacht, da sie die allgemeinen Dienste nicht mehr selber konzipieren und umsetzen müssen, sondern bestehende Services einbinden.

Verwaltungsinterne Verarbeitung

Die verwaltungsinterne Verarbeitung ist das zentrale Element eines modernen E-Government-Systems. Um verwaltungsintern die Vorteile von E-Government nutzen zu können, müssen elektronisch erhaltene Anfragen der Bürgerinnen, Bürger und Unternehmen durchgehend digital und so weit wie möglich automatisiert verarbeitet werden. So kann der Nutzerin oder dem Nutzer im Idealfall innert Sekunden eine Antwort zugestellt und der Aufwand auf Behördenseite reduziert werden.

Für die kostengünstige und zukunftssichere Umsetzung bedarf es einer Daten- und Prozessplattform, welche es ermöglicht, Daten jeglicher Art aufzubereiten und zu verarbeiten. Bei der Verarbeitung wer-



E-Government-Plattform mit generischen Services ermöglicht die einfache Anbindung von Fachapplikationen

den drei Ansätze kombiniert: Einerseits wird mit Regeln die formale Richtigkeit sowie die Einhaltung von fixen Regeln (insbesondere von rechtlichen Vorgaben) geprüft. Komplexere Konstellationen werden mit Analyticsansätzen (beispielsweise Mustererkennung) analysiert. Fälle, welche durch das Regelwerk und die Analyticsanalyse als korrekt respektive unproblematisch beurteilt werden, werden automatisch verarbeitet. Die anderen Fälle werden den Fachexperten zur Bearbeitung vorgelegt. Dem Fachexperte werden die für die jeweilige Aufgabe relevanten Daten (beispielsweise Regelverletzungen, relevante Abschnitte aus einem Schreiben, Daten aus dem Fachsystem) situativ und rollen- resp. berechtigungsbasiert angezeigt.

Durch dieses System wird die verwaltungsinterne Verarbeitung deutlich erleichtert und beschleunigt. Fachexperten werden von aufwendigen Routinearbeiten entlastet und können sich auf Arbeiten konzentrieren, bei denen sie ihre Kompetenzen optimal einsetzen können.

Die Resultate der einzelnen Prozessschritte sowie der Prozessfortschritt werden gespeichert. Dies ermöglicht Auswertungen für die Prozessoptimierung sowie die Fortschrittsanzeige der Dossierbearbeitung gegenüber den Bürgerinnen und Bürgern. Zudem können die Daten analysiert und zu relevanten Steuerungsinformationen aufbereitet werden.

Fazit

E-Government und die damit einhergehende Modernisierung der Verwaltungstätigkeit sind zentrale Elemente für die Anerkennung des Staates. Nur ein Staat, welcher sich entsprechend den gesellschaftlichen Entwicklungen und technologischen Möglichkeiten weiterentwickelt, kann seine Rolle als zentrale regulative und ausgleichende Vertrauensinstanz auch in Zukunft aktiv und glaubhaft wahrnehmen. Dabei schafft E-Government nicht nur echten Mehrwert für Bürgerinnen, Bürger und Unternehmen, sondern führt zu Effizienzgewinnen in der Verwaltung, welche für neue Aufgaben eingesetzt werden können. Insbesondere im Bereich der Steuerung werden in unserer zunehmend vernetzten und komplexen Welt die Aufgaben zunehmen.

Ein starker politischer Wille mit klaren Bekenntnissen zu E-Government geben den Bürgerinnen und Bürgern sowie den Unternehmen die Legitimität, elektronische Behördenleistungen einzufordern und sind der Verwaltung gegenüber ein klares Signal, dass die Leistungserbringung modernisiert werden muss – eine unabdingbare Voraussetzung für ein auch in Zukunft effizientes, effektives und vertrauenswürdiges Staatswesen.

Über den Autor

Thomas Alabor leitet das Solution Engineering der Bedag Informatik AG, welches zur Aufgabe hat, neue Lösungen zu konzipieren, innovative Ansätze zu testen und die Kunden bei der Problemlösung zu unterstützen. Davor leitete er grosse Organisations-, IT- und Changeprojekte in der öffentlichen Verwaltung (Bund und Kanton).

queoflow

INDIVIDUELLE SOFTWARE – LUXUS PUR? MIT UNS NICHT!

Sichern Sie sich Wettbewerbsvorteile durch individuelle Softwarelösungen: Seien Sie Ihren Konkurrenten eine Nasenlänge voraus, indem Sie exakt auf Ihre Bedürfnisse abgestimmte Software einsetzen und sich nicht den Prozessen von Standardsoftware beugen.

Die optimale Kombination von Standardkomponenten mit individueller Software ist nicht nur effizient sondern auch hochgradig flexibel und bildet Ihr bestehendes Geschäftsmodell 1:1 ab. Mehr Details lesen Sie in unserem Whitepaper.

Durch das Scannen des QR-Codes oder über bit.ly/whitepaper-luxus-pur gelangen Sie zum Download des Whitepapers. Viel Spass bei der Lektüre!

T +41 32 625 60 00
info@queo.swiss
www.queo.swiss

DIGITALISIERUNG UND HR

Digitalisierung – Erfolgsfaktor Mensch!

Erst der Mensch macht digitale Transformation möglich

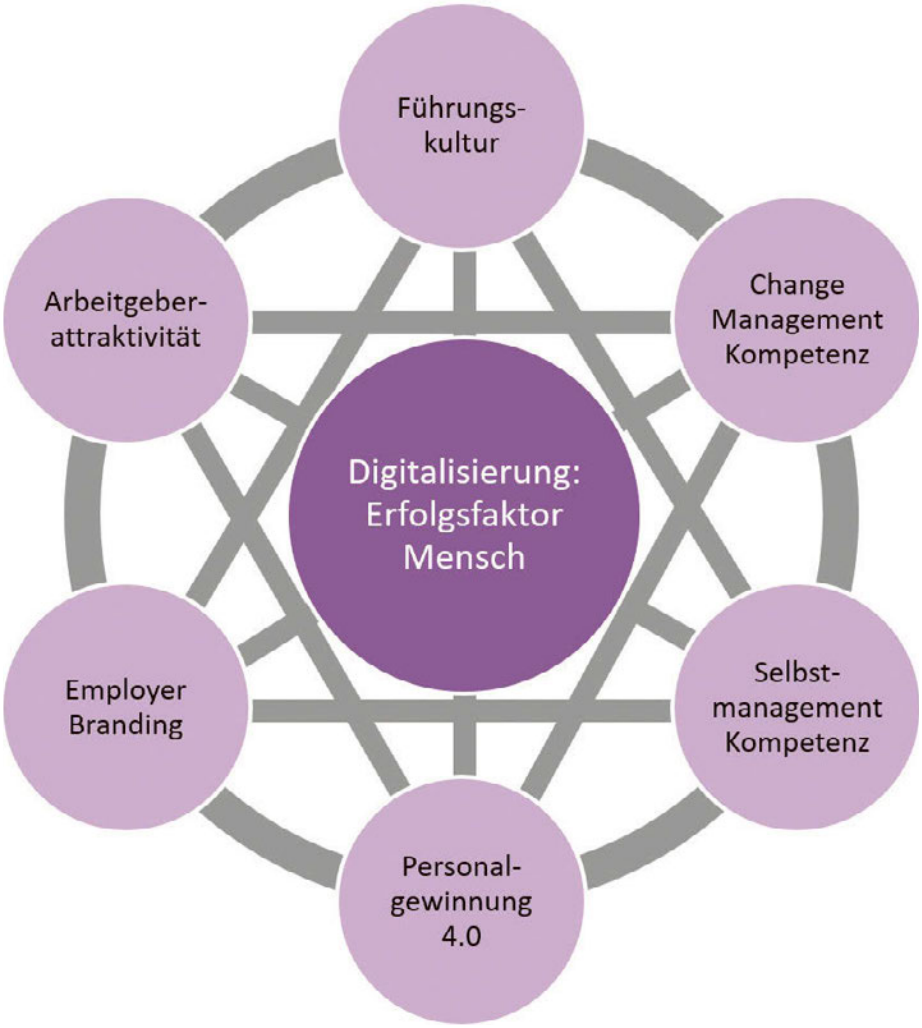
Digitalisierung ist in aller Munde. Es scheint, als ob das Thema in unserer privaten und beruflichen Lebenswelt angekommen ist und uns die mediale Präsenz des Schlagworts mit jedem weiteren Artikel sagen möchte: Aufgepasst – da kommt etwas ganz Grosses auf uns zu! Wie der Weg in die digitale Zukunft gelingt, bleibt Stand heute weitgehend unbeantwortet.

Der Begriff Digitalisierung beschreibt in seiner Verwendung meistens vor allem technische Neuerungen oder die Automatisierung von Abläufen und Vernetzung von Daten. Dabei wird häufig ausgeblendet, dass der Mensch mit seinen nicht automatisierbaren Eigenschaften der eigentliche Schlüssel für eine gelingende digitale Transformation darstellt. Schliesslich trifft er Entscheidungen, führt andere Menschen, setzt Ziele und schlichtet Konflikte. Dies wird auch in Zukunft so sein.

Digitalisierung ist Chance und Bedrohung zugleich. Sie erfordert praktisch von allen Menschen und Unternehmen eine Verhaltensanpassung. Die innovativen Startups, welche häufig als vorbildhafte Beispiele der digitalen Revolution gezeigt werden, weil sie mit alternativen Formen der Zusammenarbeit experimentieren, verleiten zum Glauben, dass digitale Transformation mit dem richtigen Spirit schnell gelingt. Allerdings sind die wenigsten Unternehmen in der Schweiz innovative Startups mit einem digitalen Selbstverständnis. Die Mehrheit der Führungskräfte und Mitarbeitenden arbeitet in klassischen Unternehmen und nimmt die Digitalisierung der Geschäftswelt eher als Bedrohung denn als Chance wahr. Damit Unternehmen die Möglichkeiten, welche sich durch die Digitalisierung eröffnen, auch realisieren und Risiken frühzeitig abwenden können, müssen Betroffene den Wandel verstehen, aktiv mitgestalten wollen und dies dann auch tatsächlich gemeinsam tun. Gerade in angestammten Traditionsbetrieben oder noch eher analog funktionierenden Unternehmenskulturen geschieht dies selten von selbst, sondern bedarf einer aktiven, umfassenden und umsichtigen Auseinandersetzung mit dem Thema «Digitalisierung – Erfolgsfaktor Mensch». Kohler & Partner hat ein Modell entwickelt, welches sechs Themenfelder hervorhebt, die für einen erfolgreichen Wandel in Bezug auf die Digitalisierung von zentraler Bedeutung sind.

Arbeitgeberattraktivität

Neue Technologien und andere Wertvorstellungen haben unser Arbeitsverhalten verändert. Junge Generationen werden als Digital Natives beschrieben. Sie sind mit smarten Geräten aufgewachsen und kennen die Schreibmaschine nur noch aus dem Museum. Flexible Arbeitsmodelle (z.B. Teilzeitarbeit) und Arbeitsformen (z.B. Home Office, Co-Working-Space) werden als Selbstverständlichkeit und unverhandelbare Voraussetzung betrachtet. Doch viele Unternehmen betrachten neue Arbeitsformen und -modelle eher skeptisch und rücken nur ungern ab von Arbeitsmodalitäten, die sich in Vergangenheit bewährt haben. Doch vor dem Hintergrund des Wettbewerbs um Talente, gut ausge-



bildete Spezialisten und Mitarbeitende mit einer inhärenten «Digitalisierungs-DNA» wird die bewusste Gestaltung der Arbeitgeberattraktivität auch auf anderen Ebenen immer wichtiger.

Employer Branding
Das Image eines Unternehmens als Arbeitgeber ist häufig geprägt durch Medien, Erfahrungen von Mitarbeitenden sowie Produkteigenschaften und die damit verbundene Wahrnehmung der Konsumenten. Ein einzigartiges Arbeitgeberprofil und dessen Kommunikation auf Kanälen, welche auf die Zielgruppe abgestimmt sind, bietet gerade für KMU ein riesiges Potenzial. Und dies bedeutet in unserer heutigen Zeit, immer mehr auch digital zu kommunizieren.

Personalgewinnung 4.0
Viele Bewerber machen im Prozess der Personalgewinnung immer wieder dieselben Erfahrungen: Auswahl lediglich nach klassischen Selektionskriterien und mehrwöchiges Warten auf eine Antwort. Es ist an der Zeit, die Perspektive des Bewerbers einzunehmen und damit die Möglichkeit zu nutzen, die sogenannte Candidate Experience optimal zu gestalten. Nur wer sich bereits im Prozess der Personalgewinnung verstanden und abgeholt fühlt, wird überhaupt einen neuen Arbeitsvertrag eingehen und die Stelle motiviert und mit vielen neuen Ideen antreten. Ohne professionelle Gestaltung der Personalgewinnung auf Augenhöhe wird es Unternehmen zukünftig nicht mehr gelingen, die am Arbeitsmarkt knappen und vielseitig umworbenen Mitarbeitenden mit «Digitalisierungs-DNA» für sich zu gewinnen.

Führungskultur
Führung in Zeiten neuartiger Arbeitsformen und -modelle erfordert ein angepasstes Führungsverhalten sowie Vertrauen. Wie führe ich mein Team, wenn es sich sowohl aus langjährigen Mitarbeitenden als auch aus Digital Natives zusammensetzt, wenn also erfahrene und unerfahrene Teammitglieder gemeinsam an einem Projekt arbeiten? Wie treffe ich Entscheidungen, ohne genügend Informationen zu haben, diese aber gar nicht mit angemessenem Aufwand beschaffen kann? Wie führe ich Teammitglieder in Teilzeit oder im Home Office? Und kann ich auch als Führungskraft einzelne Mitarbeitende wirkungsvoll coachen?

Change Management Kompetenz
Veränderungen sind für viele Mitarbeitende häufig schmerzhaft. Ein Schlüssel, Veränderungen erfolgreich zu begegnen und sie als Chance zu sehen, liegt in der gemeinsamen und proaktiven Arbeit an Veränderungsthemen. Die meisten Menschen sind sich bewusst, dass es Veränderungsbereitschaft braucht. Doch mangelnde Fakten zu Kontext und Ziel aufseiten der Mitarbeitenden, geringes Wissen zu Change Management bei Führungskräften sowie fehlende bewusste Entwicklung der Veränderungsfähigkeit führen oftmals zu einem Klima der Ablehnung, wenn sich Wandel abzeichnet. Kompetente Change Manager holen deshalb Sorgen und Bedürfnisse frühzeitig ab und gestalten den Veränderungsprozess partizipativ, denn digitale Transformation bedeutet permanente Veränderung. Es ist daher zentral, dass Unternehmen ihre Führungskräfte und Mitarbeitenden diesbezüglich befähigen.

Selbstmanagement Kompetenz
Die Digitalisierung bringt für Mitarbeitende grosse Herausforderungen wie z. B. eine höhere Informationsdichte und -geschwindigkeit, permanente Erreichbarkeit sowie die Kommunikation auf unterschiedlichsten, analogen und digitalen Kanälen. Dies verstärkt tendenziell den Druck und erhöht die Gefahr von Überlastung. Damit wird es immer wichtiger, eigene Grenzen und Ressourcen zu kennen und frühzeitig Gegensteuer zu geben, falls sich die Belastung dauerhaft negativ auf das persönliche Wohlbefinden auswirkt. Auch der Arbeitgeber sollte sich fragen, wie er optimale Arbeitsbedingungen schaffen kann, damit der individuell empfundene Stresslevel keine ungesunden Formen annimmt.

«Ja» zur Digitalisierung – und loslegen!
Die Digitalisierung ist in vollem Gange. Der Trend hin zu Automatisierung und Vernetzung wird sich weiter verstärken und unseren Alltag durchdringen. Dies wirkt sich bereits heute disruptiv auf unser Zusammenleben aus. Digitalisierung verspricht Mehrwert für uns als Individuen, aber auch für Unternehmen und die Gesellschaft insgesamt. Unternehmen werden die Chancen der Digitalisierung jedoch nur nutzen können, wenn Führungskräfte und Mitarbeitende sich aktiv damit auseinandersetzen und sich fragen, was dies für das eigene Unternehmen bedeutet und an welchen Punkten sie beginnen, den Wandel aktiv mitzugestalten. Wo setzen Sie an?

Autoren

Sandra Kohler

Christopher Schneider

BE ADVANCED

Mit dem Blick von Aussen die Welt erobern

Seit rund einem Jahr bietet be-advanced das KMU-Coaching für Berner KMU in Zusammenarbeit mit dem Coaching-Netzwerk platinn an. KMU mit Innovationsvorhaben können dabei von Rat und Tat durch einen erfahrenen Experten profitieren – ein Angebot mit grossem Mehrwert, wie der Fall von Payrexx aus Thun zeigt.

Wer sich im Online-Shop des FC Thun einen Fanartikel kaufen will, hat nicht nur die Wahl zwischen Trikots, Sweatshirts, Baseball-Caps und Wintermützen, sondern auch ob er oder sie, mit Visa, Mastercard, Postcard oder auf Rechnung bezahlen möchte. Was vom User innert weniger Clicks abgewickelt werden kann, ist im Hintergrund alles andere als unkompliziert. Verschiedene Zahlungsmittel verlangen im online Bereich nach verschiedenen Plugins, was insbesondere bei kleinen Firmen mit beschränkten Ressourcen schon den einen oder anderen Software Ingenieuren an den Rand der Verzweiflung gebracht hat. Wenn denn ein Software Ingenieur zur Verfügung steht!

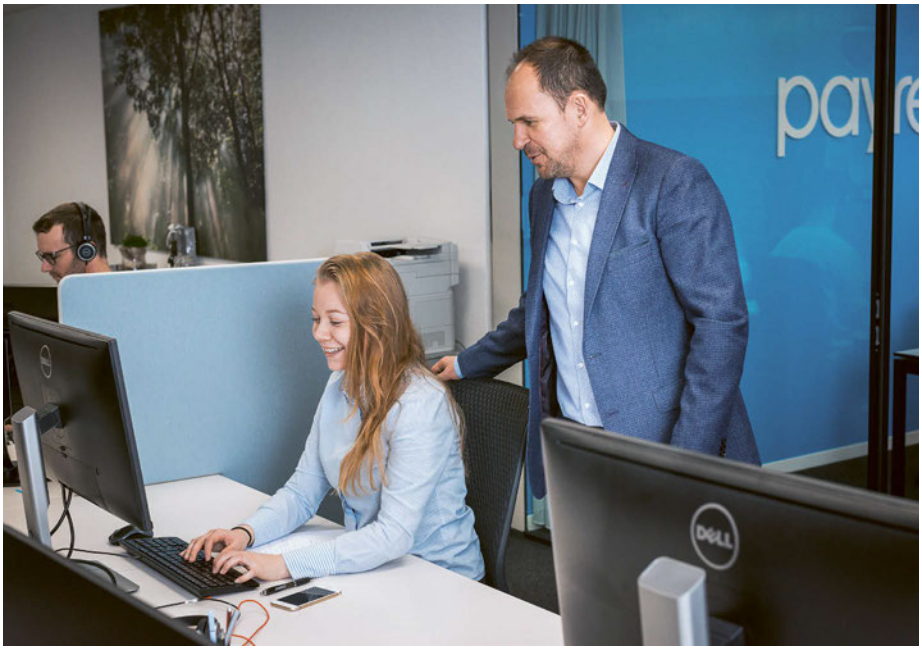
Das Problem zur Geschäftsidee gemacht

«Ich habe bereits mehrfach miterlebt, wie die Integration verschiedener Zahlungssysteme zur mühsamen Arbeit wird», erklärt Serien-Unternehmer Ivan Schmid. Was bei früheren Firmengründungen ein Problem war, macht er mit seinem in Thun angesiedelten Unternehmen Payrexx nun zur Tugend. Das Angebot von Payrexx ist ein sehr einfaches Online Payment Tool, welches erlaubt, auf einer Website verschiedene Bezahlmöglichkeiten zu akzeptieren. Kunden können damit direkt einen eigenen kleinen Webshop aufbauen, ohne separate Software. Ob Kleinstunternehmen oder Grosskonzern: mit wenigen Klicks können Produkte, Dienstleistungen oder Spendenprojekte in einem Webshop mit individuellem Design aufgelistet und verkauft werden – und all das mit nur einem Plugin.

Der T-Rexx unter den Anbietern

Was im beschaulichen Thun sein Zuhause hat, soll dereinst das einfachste und bekannteste Online Payment Tool der Welt werden. Der Name ist Programm: Pay steht für bezahlen «und Rexx, wie T-Rexx. Es soll etwas ganz Grosses darstellen», so Ivan Schmid. Dass er hoch hinaus will – und kann – hat der Unternehmer bereits bewiesen. Der findige Thuner hat mit Astalavista, Comvation und Hotelcard bereits mehrere Firmen zum Erfolg geführt.

Zwar könne man in der Schweiz als Firma wachsen, aber nicht schnell genug, erklärt Ivan Schmid. Bald sei klar geworden: eine Internationalisierungsstrategie



muss her! Doch wie gelingt Payrexx als kleiner Firma mit wenig Ressourcen der globale Coup und der damit verbundene Wachstumsschub? Ein Mittagessen mit seinem ehemaligen Studienkollegen Markus Binggeli, seines Zeichens Fachmann im Online Marketing Bereich bei Netzpuls und akkreditierter Platinn-Coach, kam da gerade richtig. «Ich wusste, dass Payrexx eine Wachstumsstrategie ins Auge fasst – da habe ich Ivan von der Möglichkeit eines Platinn Coachings erzählt».

Dem Gesagten folgen Taten: Wird im Kanton Bern ein platinn Coaching beantragt und genehmigt, fungiert be-advanced als Vermittler. Den Bedürfnissen und thematischen Schwerpunkten entsprechend, werden KMU und Coach zusammengeführt. In diesem Fall war Markus Binggeli mit seinem Marketing Know-How die offensichtliche Wahl.

Zusammen eine Strategie ausgearbeitet

Dreimal hat sich Markus Binggeli mit Ivan Schmid zwischen August und Dezember getroffen. Sich die Problemstellungen angehört, eine ABC-Kunden-Analyse erstellt. «Daraus haben wir eine Internationalisierungsstrategie abgeleitet, die wir jetzt anwenden können», so Ivan Schmid.

Das Platinn Coaching habe ihm sehr wichtige Erkenntnisse gebracht. «Die Gespräche waren spannend und förderlich», und haben den Weg für konkrete Massnahmen geebnet. «Ich bin total begeistert. Als kleine Firma haben wir nicht allzu viele Ressourcen. Und dennoch brauchen wir Leute, die mitdenken.» Den wohl grössten Vorteil des Coaching Angebots sieht Ivan Schmid in der externen Perspektive: «Es ist extrem wertvoll, solch eine Aussenansicht und neue Methoden kennenzulernen. Wir haben zusammen einen Vorschlag ausgearbeitet.»

In 16 weitere Länder vorstossen

Und was steht bei Payrexx konkret als nächstes an? «Bis Jahresende möchten wir in 16 weiteren Ländern Fuss fassen», erklärt Ivan Schmid. Wobei Fuss fassen heisst, für jedes Land einen Country Manager aufzustellen und über Online Kanäle relativ schnell weiterzukommen. «Die einzelnen Marketingstrategien für diese Zielländer sind wir zurzeit am ausloten», führt Schmid weiter aus.

Der Ressourcenknappheit entgegenwirken

Gleichzeitig sieht er sich mit Herausforderungen konfrontiert, etwa in Form regulatorischer Hürden. «Zum Beispiel müssen wir Finanzintermediär werden und das höchste Level einer schwierigen PCI-DSS Zertifizierung erreichen.» Das braucht Zeit und stiehlt dem kleinen Unternehmen viele Ressourcen. Um dem entgegenzuwirken und weiterhin von der Aussenperspektive von Markus Binggeli profitieren zu können, sind Coach und Kunde nun im Begriff bei platinn eine dritte Phase mit Fokus Online-Strategie zu beantragen. «Im Rahmen unserer Internationalisierungsstrategie möchten wir eine Marketingstrategie für die einzelnen Märkte entwickeln», erklärt Ivan Schmid.

**** Das Coaching ist für Berner KMU mit einem Innovationsvorhaben teilweise kostenlos. Interessiert?
Weitere Informationen und Kontaktdaten finden Sie auf **www.be-advanced.ch** und auf **http://www.platinn.ch/ger/**

TCBE.CH NEWS

Übersicht über die zahlreichen tcbe.ch Events

Jubiläumsanlass
Am 29. November 2017 liessen wir zusammen mit Ihnen die Korken knallen und haben auf unseren runden Geburi angestossen! Besonders gefreut hat uns die zahlreiche Teilnahme von Ihnen, geschätzte Mitglieder. So knackten wir an diesem Abend zusammen die 100er-Marke! Nebst den beiden spannenden Podiumsdiskussionen verzauberte uns Dottore Antonio Superbuffo Caradonna mit seiner atemberaubenden Darbietung. Ein spezieller Dank geht an unsere Sponsoren ADVIS, Puzzle ICT und Predata, welche den Anlass unterstützten. Ebenso bedanken wir uns bei der Cinématte für die vorzügliche Bewirtung – das war äusserst lecker. Das grösste MERCI geht aber an Sie, geschätzte Mitglieder des tcbe! Sie liessen den Abend zu etwas ganz Besonderem werden! Wir freuen uns zusammen mit Ihnen auf die nächsten 20 Jahre – die gemeinsame Reise geht weiter!

Digitalisierung – der echte Wandel findet abseits der Technik statt!
Am Donnerstag, 22. März 2018 begrüsste das neu gewählte Vorstandsmitglied Sandra Kohler von Kohler & Partner im Impact Hub 17 Teilnehmer zum Event «Digitalisierung – der echte Wandel findet abseits der Technik statt». Während den rund 2 ½ Stunden legte Sandra Kohler und ihr Team den Fokus auf den «Erfolgsfaktor Mensch», der in der Digitalisierung einen entscheidenden Punkt einer erfolgreichen Umsetzung darstellt. Am anschliessenden Apéro fanden weitere interessante und spannende Diskussionen zu diesem Thema statt.

Scratch Einführungskurs – Programmieren für Kinder und Jugendliche
Der Präsident des tcbe.ch, Matthias Stürmer, organisierte bereits drei sehr erfolgreiche Scratch Einführungskurse. Zusammen mit seinem 11-jährigen Sohn Lionel zeigte er jeweils während rund 5 Stunden auf spielerische Art, wie mit der Programmiersprache «Scratch» Computer-Programme funktionieren. Dabei wurden lustige Spiele, mathematische Aufgaben sowie Simulationen geschaffen. Der nächste Scratch Kurs findet in Zusammenarbeit mit dem Fäger am 9./10. August 2018 statt und ist bereits ausgebucht. Falls Sie Interesse an einem Kurs haben, melden Sie sich per Email an info@tcbe.ch.

Ordentliche Generalversammlung des tcbe.ch am Mittwoch, 14. März 2018
Pünktlich um 16.30 Uhr begrüsste Matthias Stürmer, Präsident des tcbe.ch, die rund 50 Teilnehmenden zur diesjährigen GV des tcbe.ch im Haus der Universität in Bern. Gleich zu Beginn hörten die Teilnehmenden spannende Referate über die DSGVO und DSG-Revision für Schweizer Unternehmen im digitalen Umfeld und wie be-advanced die Berner Bären zum Tanzen bringen möchten.

An der anschliessenden ordentlichen Generalversammlung stimmten die Mitglieder geschlossen der Jahresrechnung 2017, dem Budget 2018 und den Statutenänderungen zu. Einstimmig wählte die Anwesenden den bisherigen Vorstand sowie fünf neue Vorstandsmitglieder. Herzlichen Dank für Ihr Vertrauen in den tcbe.ch. Wir freuen uns auf ein spannendes neues Vereinsjahr.

Digital Morning – Augmented- und Virtual-Reality im Bau
Full House am 1. Digital Morning des tcbe.ch im Impact Hub Bern. Oliver Bachofen (B+S Ingenieure AG) und Ueli Gfeller (Bau-Spektrum AG) zeigten spannende Einblicke und vermittelten praxisnahes Grundlagewissen zu BIM (Building Information Modelling). Beim anschliessenden Networking zMorge konnten die Teilnehmerinnen und Teilnehmer mithilfe der HoloLens und dem HTC Vive in die Welt der Augmented- und Virtual-Reality eintauchen. Herzlichen Dank für die zahlreiche Teilnahme und den spannenden Anlass.

Geschäftsstelle
Seit Januar 2018 unterstützt Rebeca Sanchez als Office Managerin den Vorstand des tcbe.ch. Sie arbeitet jeweils Mittwochs und Donnerstagnachmittag und ist unter der Email Adresse rebeca.sanchez@tcbe.ch erreichbar. Mit ihrer Anstellung wurde die Zusammenarbeit für die Sekretariatsführung mit dem Handels- und Industrieverein des Kantons Bern per 31.12.2017 beendet. Wir danken an dieser Stelle dem HIV für ihr Engagement und die geleistete Arbeit.

Neu befindet sich die Geschäftsstelle des tcbe.ch im Impact Hub Bern. Die Adresse lautet:

tcbe.ch – ICT Cluster Bern, Switzerland
c/o Impact Hub Bern
Spitalgasse 28
CH-3011 Bern

Jubiläumsveranstaltung – 20 Jahre TCBE vom 8.11.2017 (Cinématte Bern)

Über den tcbe.ch

Digitalisierung als Chance

Die Digitalisierung erfasst die Wirtschaft und Gesellschaft in ihrer ganzen Breite. Die Schweiz ist dank hervorragender Basisinfrastruktur und ihrer allgemein hohen internationalen Wettbewerbsfähigkeit gut für die digitale Transformation gerüstet. Allerdings gilt es daneben Rahmenbedingungen zu schaffen, die die digitale Innovation fördern und nicht behindern.

Der tcbe.ch für die digitale Hauptstadtregion Schweiz

Der tcbe.ch – ICT Cluster Bern, Switzerland wurde 1996 gegründet um die Informations- und Kommunikationstechnologie (ICT) in der Region Bern zu stärken. Heute ist der tcbe.ch mit über 240 Mitgliedern ein Zusammenschluss von Unternehmen, Behörden, Bildungsinstitutionen und Verbänden zur Förderung der Digitalisierung in der Hauptstadtregion Schweiz (Kantone Bern, Freiburg, Neuenburg, Solothurn und Wallis). Ziele des tcbe.ch sind der Wissenstransfer zwischen Hochschulen und Praxis, die Aus- und Weiterbildung, die regionale ICT-Förderung sowie das Networking im Rahmen der zahlreichen Anlässe des Vereins.

Als Mitglied des tcbe.ch profitieren Sie von den folgenden Vorteilen

- Vergünstigte Teilnahme an Digitalisierungs-Anlässen des tcbe.ch und an Anlässen von Mitgliedern und Partnerorganisationen
- Möglichkeit zur Bekanntmachung von eigenen Anlässen, Weiterbildungsangeboten und Stellenausschreibungen betreffend Digitalisierung im monatlichen tcbe.ch-Newsletter
- Auflistung der Firmen oder Organisation im Mitgliederverzeichnis inkl. Logo und Link
- Jährliches Fachmagazin FOCUS mit Beiträgen zu aktuellen Digitalisierungs-Themen
- Exklusive Versicherungsangebote im Bereich ICT und Haftung in Zusammenarbeit mit der Funk Insurance Brokers AG
- Vergünstigte Mitgliedschaft beim Verein ICT Berufsbildung Bern

Mitgliedschaft

Mitglieder des tcbe.ch entrichten einen einmaligen Eintrittsbeitrag sowie einen jährlich wiederkehrenden Mitgliederbeitrag. Anbieter, welche die gesetzlichen Ausbildungskriterien zwar erfüllen, aber keine Auszubildenden beschäftigen, entrichten einen zusätzlichen Solidaritätsbeitrag von CHF 50.00

Eintrittsbeitrag bzw. jährlicher Mitgliederbeitrag

- Organisationen mit weniger als 25 Mitarbeitenden: CHF 175.00
- Organisationen mit 25–100 Mitarbeitenden: CHF 350.00
- Organisationen mit mehr als 100 Mitarbeitenden: CHF 800.00
- Einzelmitgliedschaft: CHF 125.00
- In Ausbildung (Lehre, Erststudium usw.): CHF 20.00

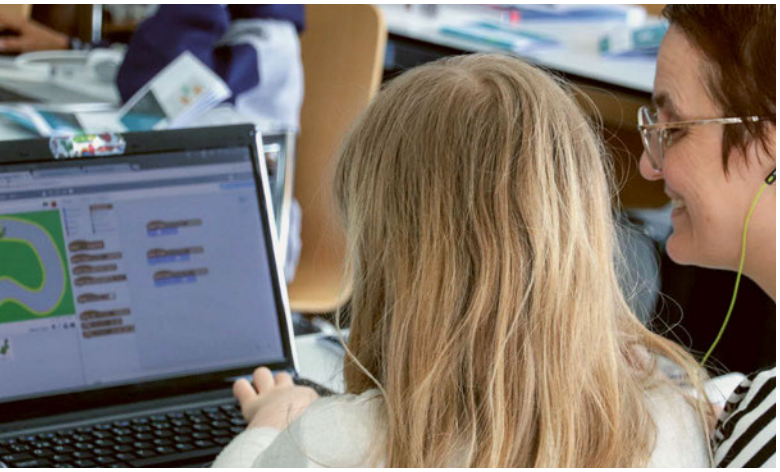
Die Mitgliedschaft kann auf der tcbe.ch Website unter www.tcbe.ch/mitglieder/neumitgliedschaft.html abgeschlossen werden. Alle Mitglieder werden mit Adresse und Logo auf der Website www.tcbe.ch/mitglieder veröffentlicht.

Rückblick Chapter Solothurn 2017

- Wachstum auf 31 Mitglieder
- Stabiles Netzwerk zwischen Firmen, Behörden und Hochschulen (HFTM, FHNW, VSIA)
- Rekrutierungsevent «Sprungbrett Solothurn» mitinitiiert
- Studie zum Thema «Digitale Maturität» in Zusammenarbeit mit FHNW
- Zahlreiche Events für Mitglieder organisiert:
  - Neue Plattform «Füürobe Bier» eingeführt
  - GetTogether mit Solothurner Spitäler im Herbst
  - Etablierte Plattform «Business Breakfast» weiter geführt
  - Präsentation der Resultate der Studie «Digitale Zukunft» als Highlight

Digitalisierung
Erfolgsfaktor Mensch –
Der echte Wandel findet abseits der Technik statt 22.03.2018
(Impact Hub Bern)

Scratch Einführungskurse für Kinder und Jugendliche vom 27.01.2018 und 14.04.2018 (Uni Bern)



GV vom vom 14.02.2018 (Haus der Universität Bern)

Digital Morning
Augmented- und Virtual Reality im Bau
vom 28.03.2018 (Impact Hub Bern)

TCBE VORSTAND

Vorstand

Der Vorstand des tcbe.ch präsentiert sich seit der Generalversammlung vom 14. März 2018 wie folgt:

Dr. Matthias Stürmer
Präsident tcbe.ch
ICT Cluster Bern, Switzerland

Diego Schmidlin
Vizepräsident tcbe.ch
VBS/FBU CISO

Sandra Kohler
Kohler & Partner

Andreas Dürsteler
Swisscom AG

Martin Frieden
Gibb

Raphael Reber
Impact Hub Bern

Sarah Pfeiffer
Puzzle GmbH

Dr. Christoph Zimmerli
Kellerhals Carrard

Reto Brechbühl
queo swiss GmbH

Stefan Otziger
Wirtschaftsbeauftragter der Stadt Thun

David Caliesch
Regions- und Wirtschaftszentrum Oberwallis AG

Beat Rutishauser
Blue Line Consulting GmbH

Prof. Dr. Andreas Spichiger
Berner Fachhochschule

Roman Kurzo
T-Systems Schweiz

Raphael Karlen
MAK Consulting AG

Wir schaffen gute Rahmenbedingungen für die Berner Unternehmen!

Die Kraft der Wirtschaft.

Unsere politischen Schwerpunkte:

- Bildung stärken,
- Verkehrserschliessung verbessern,
- Steuern senken,
- Bürokratie abbauen.

Wir arbeiten partnerschaftlich, vertrauenswürdig und lösungsorientiert.

Jetzt Mitglied werden!

HANDELS- UND INDUSTRIEVEREIN DES KANTONS BERN
Berner Handelskammer

Handels- und Industrieverein des Kantons Bern
www.bern-cci.ch