NUMMER 2
2019

abraxas magazin

Für die digitale Schweiz.

IT-Sicherheit
Wie schütze ich meine Daten?

Schutz und Schirm

Liebe Leserin, lieber Leser

Die Medienberichte über Cyberattacken auf Schweizer Unternehmen hielten uns diesen Sommer in Atem. IT-Security ist auch gemäss Marktbefragungen und Analysen von Expertinnen und Experten das grosse Branchen-Thema, welches die kommenden Jahre prägen wird.

Sicherheit ist für uns aber nicht nur ein Modebegriff, sondern ein wesentlicher Teil unseres Dienstleistungsversprechens. Tag für Tag setzen sich unsere Mitarbeitenden engagiert ein für eine digitale Schweiz – mit Sicherheit.

So liegt es auf der Hand, dass wir in dieser Ausgabe unseres Magazins thematisch auf Nummer sicher gehen: In diesem Heft finden Sie Entwicklungen, Empfehlungen und Experten zu Cybersecurity. Ich wünsche Ihnen eine spannende Lektüre.

Laufend neue Beiträge finden Sie übrigens auf abrax.as/magazin. Ein Besuch lohnt sich also mit Sicherheit.

Reto Gutmann
CEO
Abraxas Informatik AG

04

↘ **FOKUS** Sicherheit.
Wo stehen wir? Wohin gehen wir? Das Abraxas-Magazin beleuchtet das Thema IT-Security aus verschiedenen Perspektiven.

16

↘ **DER DIGITALE MENSCH** auf dem Kasernenhof: Lokaltermin beim Kommandanten des Cyber-Lehrgangs der Schweizer Armee.

21

↘ Mit Sicherheit up to date! In der Rubrik **ABRAXAS AKTUELL** erfahren Sie mehr zu unserem Angebot und unserem Engagement für die digitale Schweiz.

27

↘ Sicherheit auf den Punkt gebracht: In der Rubrik **CARTOON** zeichnet Corinne Bromundt die digitale Schweiz.

Sicher mobil unterwegs!
Laufend aktuelle Inhalte finden sich im digitalen Magazin.

abrax.as/magazin

Ohne Sensibilisierung keine IT-Sicherheit

Ganze Städte sind inzwischen von Erpresser-Software lahmgelegt worden. Diese Ransomware hat auch die Schweiz erreicht. Schutzlos ist aber niemand den Machenschaften der Cyber-kriminellen ausgeliefert.

Autor Volker Richert **Illustration** Geraldine Hasler

Viele der derzeitigen Cyber-angriffe versuchen die Schwachstelle Mensch auszunutzen.

Es war nicht zuletzt das erste iPhone vor rund 12 Jahren, mit dem die Digitalisierung in einem zuvor unbekannten Ausmass Unternehmen wie Behörden neue Chancen eröffnete. Die seither sich über immer mehr Anwendungen erstreckende Mobilität oder die wachsende Nutzung von Cloud-Lösungen eröffneten Möglichkeiten der ICT-Nutzung, auf die heute kaum mehr verzichtet werden kann. Für Franz Grüter, Co-Präsident der aus allen Parteien zusammengesetzten Parlamentarischen Gruppe Digitale Nachhaltigkeit (Parldigi), ist klar, dass die Digitalisierung «Prozesse nicht nur effizienter macht, sondern in vielen Bereichen sogar einen zusätzlichen Nutzen für Bürger und Unternehmen stiftet». Zur Illustration verweist er darauf, «wie viel einfacher eine digitale Steuerabrechnung ist oder der Austausch mit der Zollverwaltung, sobald auch deren Prozesse vollständig digitalisiert sind».

Franz Grüter, Co-Präsident der Parlamentarischen Gruppe Digitale Nachhaltigkeit (Parldigi)

«Digitalisierung macht nicht nur Prozesse effizienter, sondern stiftet in vielen Bereichen sogar einen zusätzlichen Nutzen für die Bürger; dabei ist die IT-Sicherheit zentral.»

Demokratie in Gefahr?

Allerdings ist für die Parldigi auch klar, dass mit dieser Entwicklung die Gefahren des Missbrauchs zugenommen haben. Die IT-Sicherheit ist zentral, so Grüter mit dem Hinweis auf «höchst sensible Daten der Behörden». Dramatisch wären die Auswirkungen, wenn etwa beim elektronischen Stimmkanal die Vertraulichkeit und das Stimmgeheimnis nicht jederzeit gewährleistet wären: «Unsichere Systeme hätten fatale Folgen, das würde die Grundwerte unserer Demokratie infrage stellen.»

Max Klaus, stellvertretender Leiter der Melde- und Analysestelle Informationssicherung (Melani) des Bundes

«Der Grossteil der Cyberangriffe richtet sich nicht gezielt gegen einzelne Branchen oder Unternehmen respektive Behörden. Gemeinden und Städte sind grundsätzlich den gleichen Gefahren ausgesetzt wie die Privatwirtschaft oder Privatpersonen.»

Beim Informatiksteuerungsorgan des Bundes (ISB) teilt man zwar diese Einschätzung, ergänzt aber, dass «für alle Betreiber von IT-Infrastrukturen in erster Linie im Wandel der Technologie» die Herausforderung besteht. «Das Internet der Dinge oder ‹Bring your own device› stellen alle IT-Betreiber vor Fragen, mit denen man sich vor einigen Jahren noch gar nicht befassen musste», erklärt Max Klaus, stellvertretender Leiter der Melde- und Analysestelle Informationssicherung (Melani) des Bundes, auch im Namen des ISB. Zu beachten sei dabei, dass der «Grossteil der Cyberangriffe sich nicht gezielt gegen einzelne Branchen oder Unternehmen respektive Behörden richtet». Gemeinden und Städte sind grundsätzlich den gleichen Gefahren usgesetzt wie beispielsweise auch die Privatwirtschaft oder Privatpersonen, so Klaus weiter.

Entführer und Erpresser im Cyberraum

Wie weit Cyberkriminelle zu gehen bereit sind, haben zuletzt bösartige Angriffe durch Erpresser-Software gezeigt. So warnte gerade erst im September das eng mit Melani verbundene Computer Security Incident Response Team des Bundes (GovCERT.ch) vor solcher Ransomware. Cyberkriminelle hatten gefälschte E-Mails im Namen der Eidgenössischen Steuerverwaltung genutzt, um Fragen zur Steuererklärung beantwortet zu bekommen. Würde darauf eingegangen, so die Warnung, werde von den Angreifern beispielsweise via Teamviewer versucht, die Kontrolle über den Rechner zu erlangen.

Meist erfolgen die Angriffe via E-Mail, die in der Regel über einen Link auf eine bösartige Webseite oder einen schädlichen Dateianhang verfügt. Aber längst werden im sogenannten Darknet auch Zugänge zu bereits infizierten Rechnern verkauft. Oder Kriminelle scannen das Internet nach offenen VPN- und Terminal-Servern, um dann Zugriff auf sie durch automatisiertes, wahlloses Ausprobieren von Passwörtern oder Schlüsseln zu erhalten.

Lösegeld in Millionenhöhe

Welcher Schaden am Ende angerichtet werden kann, zeigten gerade die letzten Monate. Erfolgreich durchgeführte Erpressungsangriffe hatten Gemeinden und Städte in den USA genauso zu verzeichnen wie namhafte Unternehmen in der Schweiz. Dabei traf es die Rothenburger Auto AG Group genauso wie den Gebäudetechnik-Spezialisten Meier Tobler oder den Hersteller von Industrieminералien Omya im aargauischen Oftringen. So ausgelöste Betriebsunterbrüche hatten allein für Meier Tobler oder die US-Stadt Baltimore Millionenschäden zur Folge.

Zwar geht es den Cyberkriminellen bei ihren Angriffen in der Regel um Geld. Doch ist die Motivlage nicht immer klar. Neben der Übernahme der Systeme oder Datendiebstahl kann Schadsoftware auch zur Spionage genutzt werden. Weltweit Schlagzeilen machten die Angriffe auf die Schweizer Rüstungsschmiede Ruag oder auf das bundeseigene Labor Spiez. Wie einfach solche Angriffe zum Teil funktionieren, zeigen Fälle in Basel und St. Gallen, wo Schüler Rechner von Lehrern kaperten, um an Prüfungsfragen zu gelangen. Und während der diesjährigen Lehrabschlussprüfungen legte Ransomware auch grosse Teile des Kantonalen Gewerbeverbands St. Gallen lahm.

Daniel Nussbaumer, Präsident der Swiss Internet Security Alliance

«Eine der grössten Gefahren – ob für Verwaltungen oder Unternehmen – ist der Faktor Mensch.»

Faktor Mensch als Schwachstelle

Nicht ohne Grund betont Daniel Nussbaumer, der Präsident der Swiss Internet Security Alliance (SISA), denn auch, dass «eine der grössten Gefahren – ob für Verwaltungen oder Unternehmen – der Faktor Mensch» ist. Bei der SISA, welche von namhaften Vertretern der Wirtschaft ins Leben gerufen wurde, um die Schweiz zum sichersten Internet-Land der Welt zu machen, konstatiert man, dass viele der derzeitigen Angriffe versuchen, diese Schwachstelle auszunutzen.

Der Klick auf ein Phishing-Mail eines vermeintlichen Bekannten, das unter anderem wie eine Kalendereinladung oder ein Video-Link aussehen kann, ermöglicht das Eindringen der Malware. Es seien oft einfache Tipps zu berücksichtigen, wie man sie mit der Kampagne iBarry anbiete, um den Schutz der IT-Infrastruktur zu erhöhen und die Bürger für Online-Betrüger und ihre Methoden zu sensibilisieren», so Nussbaumer.

Bruno Baeriswyl, Datenschutzbeauftragter des Kantons Zürich

«In vielen Fällen werden Budgets für grosse Digitalisierungsprojekte gesprochen, ohne dass angemessene Ressourcen für den Datenschutz und die Datensicherheit bereitgestellt werden.»

Der Zürcher Datenschutzbeauftragte Bruno Baeriswyl betont hingegen die mit der Digitalisierung wachsende Komplexität und die damit auch zunehmenden Risiken. Dieser Risiken bewusst sei sich «nur der kleinere Teil der Gemeinden und Städte». Seriöse Risikoanalysen oder Datenschutzfolgeabschätzungen fänden oft nicht statt und Transparenz über die Risiken fehle, konkretisiert Baeriswyl. IT-Security-Verantwortliche seien nicht festgelegt und die politische Führung nicht in die Verantwortung einbezogen. Zudem würden «in vielen Fällen Budgets für grosse Digitalisierungsprojekte gesprochen, ohne dass angemessene Ressourcen für den Datenschutz und die Datensicherheit bereitgestellt werden».

Verteidigungslinien im Cyberkrieg
Peter Kölsch, als Bereichsleiter Informatik für die IT der Stadt Wetzikon verantwortlich, ist noch nicht in die Fänge der Kriminellen geraten.

Peter Kölsch,
Bereichsleiter
Informatik
der Stadt Wetzikon

> «Die Sensibilisierung für die Gefahren der Cyberkriminalität gelingt am besten, wenn man sie möglichst praktisch bewusst machen kann.»

Auch er weiss aber, dass diese Ruhe trügerisch sein kann. Zu den umfangreichen Massnahmen, die die Stadt getroffen hat, gehört unter anderem, dass alle Hardware «kastriert» worden ist, wie er sagt. Über eine Citrix-basierte Infrastruktur würden alle Mitarbeitenden Daten aus einem Rechenzentrum (RZ) nutzen, das gelte auch für mobil genutzte private Devices. Nur eines sei pro Mitarbeiter zugelassen. Lokale Verzeichnisse, Laufwerke sowie USB-Sticks sind so im Homeoffice unterbunden. Zudem habe man das städtische WLAN vom öffentlichen getrennt. Und wer remote arbeiten wolle, müsse eine 2-Faktor-Authentifizierung nutzen. Kölsch verweist zudem auf die enge Kooperation mit dem RZ-Betreiber RIZ (Regionales Informatikzentrum). Dort sei eine restriktive Nutzung von Applikationen implementiert. Zudem würde die Konfiguration lokaler Firewall-Richtlinien Angriffsmöglichkeiten reduzieren und die komplette Übernahme der Domäne und deren Systeme genauso erschweren, wie weitere Sicherheitsmechanismen die Weiterbewegung der Angreifer im Netzwerk sehr aufwendig machen würden.

Generell, so Kölsch, sei Wetzikon technisch auf Cyberangriffe vergleichsweise gut vorbereitet. Das ändere aber nichts daran, dass der Mensch weiterhin eine Schwachstelle bleibe. Nicht jedes Mail müsse geöffnet werden. Und manche Aufgaben wie die Bildschirmsperre beim Verlassen des Büros und das Schliessen der Tür müssten einfach manuell ausgeführt werden. Die zentralste Aufgabe der IT-Security sei deshalb, die Mitarbeitenden zu sensibilisieren. Dabei habe er die Erfahrung gemacht, dass dies am besten gelingt, wenn man die Gefahren der Cyberkriminalität möglichst praktisch veranschaulichen kann.

Das müssen Gemeinden für ihre IT-Security tun

Grundsätzlich sind die gängigen technischen Schutzmassnahmen wie beispielsweise Firewall, Antivirus, Updates, Datensicherung und E-Mail-Verschlüsselung zwingend umzusetzen.

Zugriffe über ein Netzwerk auf Internetdienste möglichst mit einer 2-Faktor-Authentifizierung schützen.

Sichere Passwörter mit mindestens 12 Zeichen benutzen und diese regelmässig ändern. Zudem sind verschiedene Passwörter für verschiedene Zwecke zu nutzen.

Organisatorisch sollte unter anderem überall mit BCM (Business Continuity Management) ein «Notfallplan» implementiert sein, der sicherstellt, dass auch bei einem Ausfall der IT weitergearbeitet werden kann.

Zudem ist es geboten, via «Access Management» genau festzulegen, wer in der Verwaltung welche Rechte in der IT hat.

Da die Cyberkriminellen immer öfter gezielt einzelne Mitarbeiter angehen und auskundschaften wollen, ist Sensibilisierung in Sachen IT-Security unumgänglich. Jeder in der Gemeinde sollte sich klar darüber sein, dass sein Verhalten wesentlich über die IT-Risikominimierung entscheidet.

Mehr erfahren:
Unser Experte erklärt
E-Mail-Verschlüsselung.

abrax.as/secure-mail

So schützen Sie Ihre Organisation vor Cyberkriminellen

Verheerende Cyberattacken auf Unternehmen und Verwaltungen nehmen zu und zeigen auf, wie wichtig der Schutz der eigenen IT-Infrastruktur ist. Weil IT-Sicherheit vielfach immer noch kostenintensiv ist, vernachlässigen vor allem kleinere Organisationen dieses Risiko. Dabei gibt es eine einfache, günstige und sichere Lösung, nämlich IT-Sicherheit von Spezialisten als Service zu beziehen.

Autoren Elisa Signer, Gregor Patorski **Bild** Dominique Vernier

Die heutige Bedrohungslage durch Cyberkriminalität stellt Führungskräfte nicht vor die Frage ob, sondern wann die eigene Organisation angegriffen wird. Auch diesen Sommer fielen in der Schweiz einige namhafte Unternehmen Cyberattacken zum Opfer. Die neuartigen Risiken sind gross, die Verluste können sich auf mehrere Millionen belaufen. Der finanzielle Schaden geht zudem einher mit einem erheblichen Reputationsverlust des Unternehmens, vor allem wenn sensitive Daten gehackt werden. Ausserdem kann es zu Produktionsausfällen und zum Unterbruch von Geschäftsprozessen kommen, wenn der Zugriff auf die eigenen Daten verloren geht.

Sensibilisieren, Blockieren und Überwachen

Doch wie können sich Verwaltungen und Unternehmen vor diesen neuen Risiken schützen? Bisherige Massnahmen wie die Sensibilisierung von Mitarbeitenden durch Awareness-Schulungen und immer stärkere technische Firewalls

In fünf Schritten zum optimalen Schutz

Zuerst wird die bereits vorhandene Sicherheitsstruktur identifiziert und ergänzt, damit in einem zweiten Schritt Schutzmassnahmen ergriffen werden können. Dieses Schutzdispositiv erkennt dank diversen Logs und Big-Data-Analysen allfällige Cybergefahren. Ist ein Angriff einmal erkannt, erfolgt die Reaktion unter Anweisung und Begleitung von Security-Analysten. Nach dem Angriff ist vor dem Angriff: Die Systeme werden wiederhergestellt und der Schutz weiter optimiert.

reichen bei den heutigen Angriffsmöglichkeiten alleine nicht mehr aus, weil man davon ausgehen muss, dass die Bedrohung sich schon innerhalb der Firewall in der eigenen Infrastruktur befinden kann. Was es braucht, ist ein internes Sicherheitsdispositiv, das mittels implementierter Sensoren und Big-Data-Analysen eine 7×24-Rundum-Überwachung ermöglicht. Diese Früherkennung erlaubt es, Eindringlinge zu bekämpfen und der Gefahr für ein nächstes Mal vorzubeugen.

Die Lösung: IT-Sicherheit als Service

Hier bietet sich der Bezug eines Security Operations Center (SOC) als Service an, der es Unternehmen erlaubt, ihre IT-Sicherheit kostengünstig an einen Schweizer IT-Spezialisten auszulagern. Abraxas hat sich der Sicherheit der digitalen Schweiz verschrieben. Wir unterstützen unsere Kunden dabei, ein individuelles Sicherheitskonzept zu erarbeiten, die Bedrohungslage zu identifizieren und am Ende das entsprechende Sicherheitsdispositiv auch umzusetzen. Unsere Kunden profitieren zusätzlich von unserer umfassenden Supportorganisation und dem Know-how unserer Security-Spezialisten. Der SOC-Service von Abraxas befähigt Unternehmen dazu, die cyberkriminelle Bedrohung auf einfache Art und Weise zu überwachen, ihr vorzubeugen, sie zu bekämpfen und schliesslich auch zu eliminieren.

SOC im Detail

Beim Abraxas SOC-Service schützt eine ausgeklügelte Sensorik im Zusammenspiel mit qualifizierten Security-Analysten vor Cyberangriffen. Das technologische Herzstück des SOC ist ein «Security Information & Event Management»-System (SIEM) unseres Partners Hacknowledge, das mögliche Cyberattacken erkennen kann. So werden aus unzähligen Events ernst zu nehmende Security Alerts herausgefiltert. Zur Verdeutlichung: Von wöchentlich geloggten 3 Milliarden Events eines Beispiel-Unternehmens werden durch vordefinierte Filter gut tausend davon als Alerts eingestuft, von denen dann drei als Incidents mit negativem Impact für die Organisation qualifiziert werden. Die SOC-Analysten von Abraxas liefern dann den Kunden professionelle Handlungsempfehlungen zum Umgang mit diesen Incidents. Mit einer umfassenden Support-Organisation kann Abraxas allen Kunden – wenn gewünscht – eine 7×24-Überwachung sicherstellen.

Mehr Informationen
zum Abraxas SOC-Service.

abrax.as/soc

Mann auf Mission

Gespräch mit Anton Brauchli, Solution Architect bei Abraxas

Man hat den Eindruck, Cyberattacken häufen sich. Wohin geht der Trend?

Brauchli: Die Tendenz ist klar: Cyberangriffe werden immer ausgeklügelter und Cyberkriminelle wissen sich immer besser zu verstecken. Deshalb braucht es eine ebenso professionell organisierte Abwehr aus Security-Spezialisten und Sensorik, um diese in Schach zu halten.

Sind Schweizer Unternehmen und die öffentliche Hand gegen Cyberangriffe gewappnet?

Brauchli: Natürlich hat die Sensibilisierung zugenommen. Wir stellen aber fest, dass viele Organisationen die Bedrohung unterschätzen. Das geht teilweise bis zum bewussten Wegschauen mit der Begründung, dass dies neben den hohen direkten Kosten auch Folgeaufwände für die Behebung von Security-Lücken verursacht. Die Risiken sind aber sehr real: Das reicht von Haftungsfragen über Imageschäden bis hin zu finanziellen Schäden durch Produktionsausfälle.

Was empfehlen Sie Organisationen, die über kein grosses Budget verfügen?

Brauchli: Um eine Organisation besser zu schützen, braucht es Security-Spezialisten. Die gibt es aber nicht in dieser Zahl auf dem Markt – schon gar nicht in der Schweiz. Auch deshalb wird sich der Bezug eines SOC-as-a-Service durchsetzen. Sich externe Hilfe zu holen und die Dienstleistung zu beziehen, wird für die allermeisten Unternehmen der richtige Weg sein. Abraxas gibt mit diesem neuen Service Unternehmen und Organisationen einen wirksamen Schutzschild an die Hand. Damit können sie ihre IT-Sicherheit kostengünstig, massgeschneidert und sicher auslagern.

Grossumzug für mehr Sicherheit

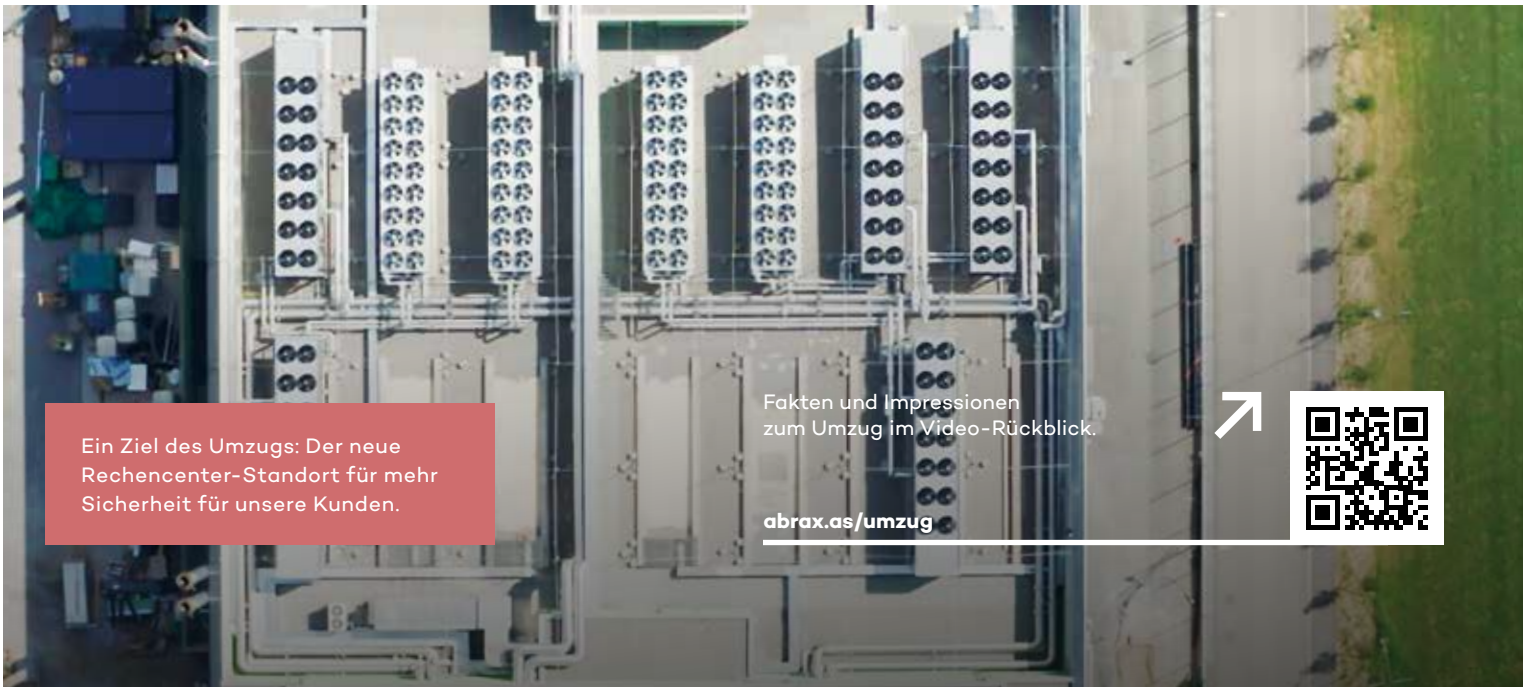
Diesen Sommer hatte Abraxas eine logistische Herkulesaufgabe zu meistern. Vom 1. bis zum 4. August wurden die beiden St. Galler Rechenzentren konsolidiert. Im Zentrum stand dabei stets die Sicherheit der Kundendaten.

Autor Gregor Patorski **Bild** Signorell Film

Seit der Fusion Ende Mai 2018 verfügt Abraxas über vier Datacenter. Deren Konsolidierung wurde als grosses Synergiepotenzial identifiziert: In mehreren Zügeletappen werden die Rechenzentren an zwei Standorten zusammengelegt. Am verlängerten Nationalfeiertags-Wochenende ging die sechste Tranche des Umzugs über die Bühne. Diese hatte den grössten Impact auf unsere Kunden: 182 Gemeindeverwaltungen in vier Kantonen mit insgesamt 35 Fachapplikationen waren betroffen. Die Herausforderungen bei Planung, Vorbereitung und Koordination allein für dieses Wochenende waren gewaltig: Insgesamt standen über 50 interne und externe Mitarbeitende für Aus- und Einbau, Transport und Testing im Einsatz. Bei Abschluss des Projekts Mitte 2020 werden insgesamt 900 Systeme in 10 Tranchen gezügelt worden sein.

Angebot für die Zukunft

Der Aufwand und die Mühen lohnen sich: Die neuen Datacenter sind nach Tier-IV-Standard gebaut und Tier-III-zertifiziert, das heisst, sie bieten eine hohe Ausfallsicherheit dank kompletter Redundanz aller Komponenten wie Server, Strom, Klima und Versorgungswege. Bei Stromausfall kann dank Notstromdiesel neu eine Autonomiezeit von 48 Stunden geboten werden – statt zuvor 90 Minuten. Auch Georedundanz ist dank der Distanz von 27 Kilometer Luftlinie zwischen den beiden Standorten gegeben, welche im Katastrophenfall eine verbesserte Sicherheit gewährleistet. Die Kunden profitieren darüber hinaus von einer technischen und personellen 7×24-Stunden-Security-Überwachung, welche vor Ort geboten wird. Last, but not least kann Abraxas dank dem neuen Datacenter-Setup eine umweltfreundliche, grüne Datenhaltung dank besserer Energieeffizienz anbieten.



Ein Ziel des Umzugs: Der neue Rechencenter-Standort für mehr Sicherheit für unsere Kunden.

Markus Röösli

54, Polizeihauptmann und Chef IT-Steuerung der Kantonspolizei Zürich, ist beruflich und privat am Puls des Digitalen. Die Kapo Zürich ist Abraxas-Kunde seit über 15 Jahren.

Interview Daniel Slongo

Wo und wie sind Sie beruflich und privat «digital»?

Markus Röösli: Wir realisieren und betreiben Informatiklösungen, die – insbesondere in der Kommunikation – der gemeinsamen Datenverwaltung und dem Datenaustausch zur Erfüllung von Polizeiaufgaben dienen. Ziel ist es, dass wir die Polizeiarbeit und deren Wirkung unterstützen und verbessern können. Als Pikettoffizier der Kantonspolizei Zürich nutze ich diese Informatikmittel auch selber im Einsatz. Ich bediene mich in fast allen Lebenslagen regelmässig der heutigen Möglichkeiten der digitalen Welt. So auch im Privaten, wenn ich beispielsweise auf dem Rennvelo mit Pulsuhr und Wattmessgerät unterwegs bin. Damit kann ich die Daten im Anschluss analysieren und das Training optimaler steuern.

Welchen Nutzen sehen Sie in der Digitalisierung?

Markus Röösli: Die Digitalisierung erspart uns bei zahlreichen Tätigkeiten im Alltag viel Zeit und Geld. Sie bringt uns einen ungeheuren Effizienzgewinn. Diese zusätzliche Zeit können wir für unsere eigenen Bedürfnisse einsetzen. Zudem erschliesst sie uns Möglichkeiten, von denen wir ohne sie nicht mal zu träumen wagen. In allen Lebenslagen – von der Schule über den Gesundheitsbereich bis hin zur Kommunikation – können dank der Digitalisierung Leistungen erbracht werden, die bis vor wenigen Jahren noch undenkbar waren.

Wie begegnen Sie Herausforderungen und Gefahren im digitalen Raum?

Markus Röösli: Die Digitalisierung hat natürlich auch grosse Tücken: Aufgrund der vielen Möglichkeiten, die sich uns 24 Stunden am Tag bieten, kommen wir nicht mehr zur Ruhe. Statt mit der gewonnenen Zeit etwas Tempo rauszunehmen, arbeiten wir noch mehr, erledigen vieles parallel und geben selbst in unserer Freizeit zusätzlich Gas. Dieser Gefahren sollten sich alle bewusst werden und im eigenen Einflussbereich dagegenhalten. Als Polizeikorps sind wir heute in beiden Welten gefordert, in der realen und in der virtuellen. Die grundsätzlichen Arbeiten sind ähnlich strukturiert, unterscheiden sich aber in der Art und Weise sehr stark. Und die Anforderungen an jene Personen, die Polizeiarbeit in diesen Welten verrichten, unterscheiden sich ebenfalls sehr stark.

Welche Trends in Sachen Sicherheit beobachten Sie online und offline?

Markus Röösli: Im Kleinen habe ich das Gefühl, dass wir im virtuellen Raum viel sorgloser mit unseren «Wertgegenständen» umgehen als in der realen Welt. Wie sagt man so schön: «Das grösste IT-Sicherheitsrisiko arbeitet zwischen Bildschirm und Tastatur!» Auf der einen Seite müssen wir uns wohl immer noch an den virtuellen Raum gewöhnen und uns mit den notwendigen Sicherheitsmassnahmen vertraut machen. Auf der anderen Seite legt die Digitalisierung auch ein Tempo vor, bei dem wir fast nicht mithalten können. Trotzdem müssen wir uns dieser Herausforderung stellen. Denn entschleunigen oder gar aufhalten können wir die Digitalisierung wohl nicht.

Was sind Ihre Wünsche an die Digitalisierung der Gesellschaft?

Markus Röösli: Ich wünsche mir, dass trotz allem Fortschritt mit der Digitalisierung die Menschen nicht auf der Strecke bleiben: Erstens besteht die Gefahr, dass jene Menschen, die nicht mitmachen können oder wollen, systematisch und nachhaltig ausgegrenzt werden. Dies kann zu gesellschaftlichen Problemen führen, die den Nutzen der Digitalisierung wieder stark infrage stellen. Und zweitens bin ich der Meinung, dass das reale soziale Umfeld eines Menschen etwas vom Wichtigsten ist, was unsere Gesellschaft überhaupt ausmacht. Dies sollte jeder Einzelne, jede Einzelne von uns bedenken, wenn in allen Lebenslagen digital kommuniziert wird. Ansonsten vereinsamen Leute, obwohl sie Tausende von virtuellen Freunden haben.

Monat für Monat mehr Antworten in der Rubrik «5 Fragen an» im digitalen Magazin.

abrax.as/5-fragen

«Sicherheit ist ein gutes Gefühl im Bauch»

Beide sind Profis, was IT-Security angeht: Peter Müntener, Sicherheitsbeauftragter des Kantons St. Gallen, und Michael Dobler, Chief Information Security Officer bei Abraxas. Im Doppel-Interview suchten wir vergebens nach ihren Sicherheitslücken.

Interview Gregor Patorski **Bild** Florian Brunner

Sie führen beide «Sicherheit» in Ihrer Berufsbezeichnung. Wie würden Sie Ihre Aufgabe in einem Satz beschreiben?

P. Müntener: Meine Aufgabe ist die zentrale Informationssicherheit im Kanton St. Gallen – im Spannungsfeld zwischen Kunden in den kantonalen und kommunalen Behörden und den verschiedenen Leistungserbringern.

M. Dobler: Ich sehe mich als Bindeglied zwischen Management und Technik. Ich muss zwischen diesen beiden Anspruchsgruppen vermitteln, damit Risiken verstanden, richtig adressiert und auch Sicherheitsmassnahmen umgesetzt werden.

Mit welcher Herausforderung werden Sie beim Übersetzen dieser technischen Sprache am häufigsten konfrontiert?

M. Dobler: Aus meiner Sicht ist es diese Vermittlerrolle: Mit dem Management rede ich in Risiken, Schadensausmass, Eintrittswahrscheinlichkeiten. Mit der Technik in Regeln, Accounts, technischen Erfordernissen.

P. Müntener: Ich sehe mich manchmal als eine Art Maler, der einen Bau- oder Architekturplan so visualisiert, dass der Kunde es verstehen kann. In der Zusammenarbeit mit Michael machen wir eine technische Zeichnung, für die Kunden zeichne ich «Blumenwiesen» mit allem, was da kreucht und fleucht und für ihn von Belang sein könnte. Das Sichtbarmachen der Sicherheitsanforderungen ist oft ein schwieriges Thema.

Die Medienberichte des vergangenen Sommers vor Augen, hat man den Eindruck, dass Cyberangriffe auf Unternehmen in der Schweiz zugenommen haben. Müssen wir in Zukunft verstärkt mit solchen Fällen rechnen?

M. Dobler: Das wird sich häufen. Es ist der Trend, immer schneller Geräte wie Smartphones und Pads auf den Markt zu werfen mit teilweise unreifer Software. Daneben haben wir eine CPU-Architektur – die nicht mehr angefasst worden ist, seit man sie erfunden hat – mit bekannten Schwachstellen. Ich habe also unreife Software auf verletzlicher Hardware. Diese Kombination ermöglicht es Angreifern, Angriffe zu fahren.

P. Müntener: Einerseits gibt es immer mehr Software und Hardware, die verletzlicher sind. Zudem sind die Geräte immer mehr vernetzt, was mit der 5G-Technologie noch stärker zunehmen wird. Dies erhöht einfach das Potenzial für gefährliche Angriffe. Ausserdem ist es ein lukratives Geschäft. Es ist zum Businessmodell geworden und offensichtlich verdient man viel Geld damit.

Wenn solche Cyberangriffe immer mehr und immer ausgeklügelter werden, dann stellt sich die Frage: Was kann ich jetzt dagegen machen? Wie kann ich mein Unternehmen dagegen schützen?

M. Dobler: Einerseits kann ich technisch aufrüsten: Ich kann mit einem SOC/SIEM alle meine Systeme und Anwendungen genauer betrachten, Logfiles auswerten, mein Netzwerk kennen und so auch Anomalien erkennen. Andererseits kann ich unternehmensintern mit Aware-

Zwei Profis, was IT-Security angeht: Peter Müntener (l.) und Michael Dobler (r.).

ness-Kampagnen arbeiten wie beispielsweise Phishing-Tests, Schulungen, Quiz. Und drittens sich vorbereiten, was man macht, wenn es passiert. Denn passieren wird es. Die Frage ist nicht ob, sondern wann es einen trifft.

P. Müntener: Awareness ist etwas vom Wichtigsten, denn der Mensch ist nach wie vor das schwächste Glied. In die Sicherheitstechnologie kann man je nach Risikoabschätzung mehr oder weniger Geld investieren. Aber häufig wird viel zu wenig in die Mitarbeitenden investiert. Letzthin hat mir zwar ein Mitarbeiter gesagt, er glaube, er sei jetzt übersensibilisiert. Aktuelle Ereignisse zeigen, dass man nie zu viel sensibilisiert hat. Es gibt Leute, die sind sehr vorsichtig im Umgang mit sicherheitsrelevanten Informationen, und andere, die gehen mit ihren persönlichen Daten und teilweise auch mit Geschäftsdaten eher etwas unbedachter um.

Was erwarten Sie von der Abraxas als Partner?

P. Müntener: Gute Services zu marktentsprechenden Preisen sowie ein proaktives, unkompliziertes und kundenorientiertes Handeln. All das muss Hand in Hand gehen. Und schlussendlich muss ich dem Partner vertrauen können, dass er seinen Job, den er im Hintergrund macht, gut macht.

Was wünschen Sie sich in der Zusammenarbeit mit Kunden?

M. Dobler: Ich würde mich gern mit mehr Kunden austauschen können, so wie wir das beispielsweise mit dem Kanton St. Gallen haben, wo wir sehr offen über Sicherheit und Herausforderungen reden. Das hilft auch im Verständnis für den Kunden. Für uns ist vielleicht ein System einfach nur ein System unter vielen, aber es könnte der Lebensnerv des Kunden sein. Das will ich stärker merken. Diese Erkenntnis hilft beim Definieren und Gewichten von Risiken und Massnahmen.

P. Müntener: Dieser offene Austausch ist wichtig. Einen Sparringspartner zu haben auf der anderen Seite, jemanden herausfordern zu können: «Ist das nicht ein Problem? Können wir da nicht miteinander etwas verbessern?» Hier habe ich mit Abraxas sehr gute Erfahrungen gemacht und das schätze ich natürlich.

Das komplette Interview im digitalen Magazin.

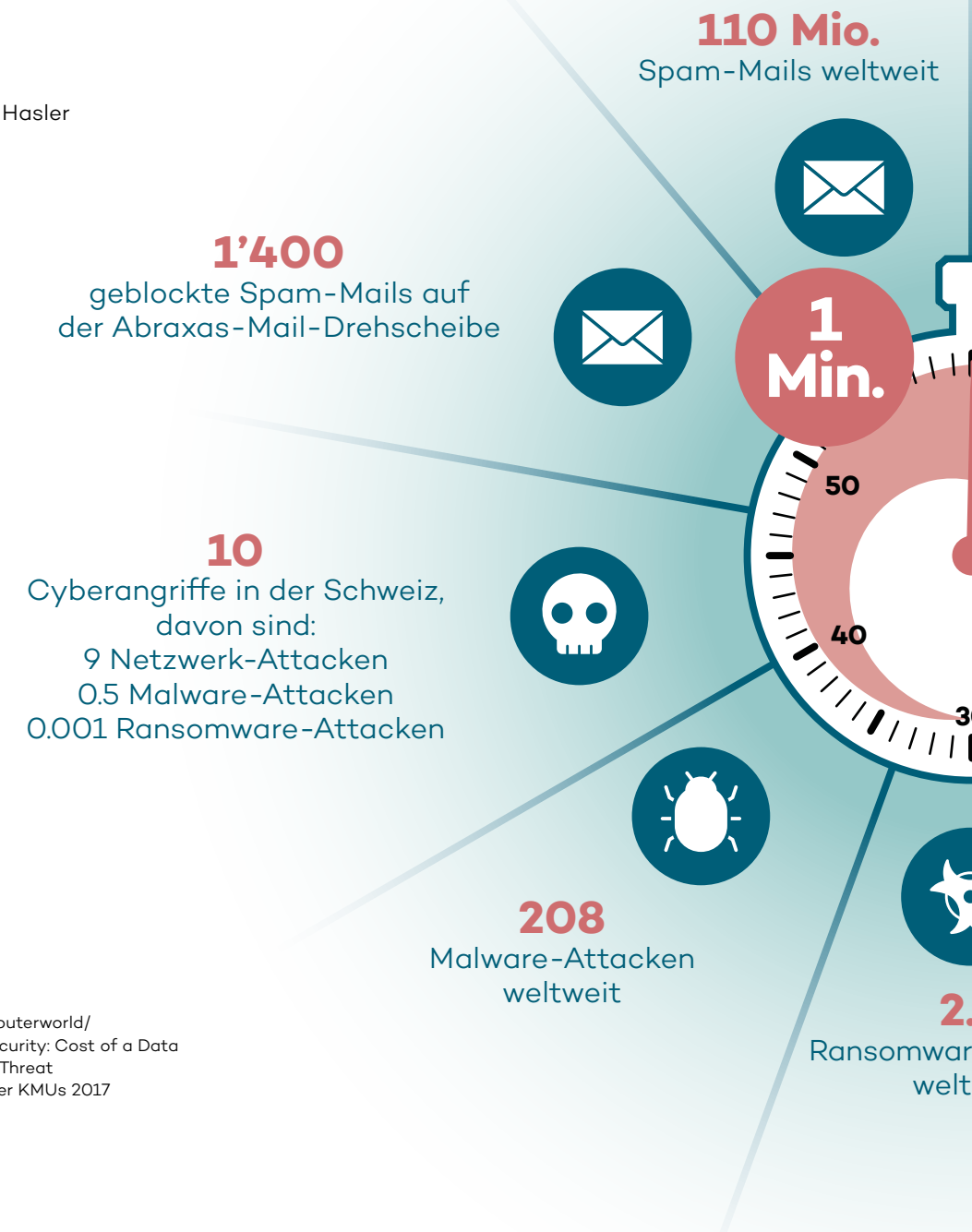
abrax.as/security-interview

Die Bits des Bösen: Was Cyberkriminelle pro Minute verursachen

Sie sind die Nepper, Schlepper, Bauernfänger des digitalen Zeitalters: Hacker, Spammer, Cyber-Phisher. **Was und wie viel Böses richten sie in einer Minute Internet an?** Und wie viel Schaden wird dadurch verursacht? Ziemlich viel, wie ein Blick auf neues Zahlenmaterial zeigt. Was übrigens aktuelle Daten zu Cyberkriminalität in der Schweiz angeht, fischt man – noch – grösstenteils im Trüben. Die Cybercrime-Statistik des BfS ist für kommendes Jahr angekündigt.

Grafik Dominique Vernier, Geraldine Hasler

Autor Gregor Patorski



Alle Angaben pro Minute

Quellen: → RiskIQ: Evil Internet Minute 2019 → Computerworld/ Symantec: Schweizer Security Barometer → IBM Security: Cost of a Data Breach Report 2019 → Symantec: Internet Security Threat Report 04/19 → gfs-zürich: Cyberrisiken in Schweizer KMUs 2017

17’700 $
durch Phishing verursachter finanzieller Schaden weltweit

2.9 Mio. $
betragen die Einnahmen von Hackern und Spammern weltweit

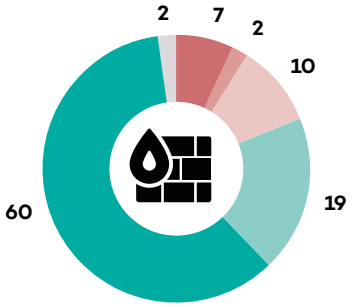
22’184 $
durch Ransomware verursachte Verluste weltweit

62’000
Phishing-Mails weltweit

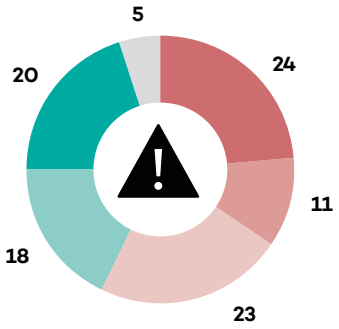
.8
e-Attacken
weit

Wie schützen sich Schweizer KMUs?

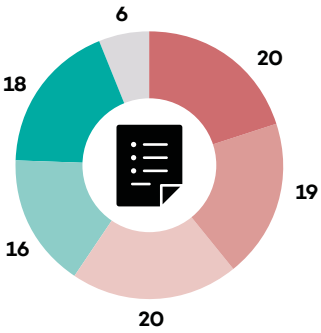
Cyber-Grundschutz (Firewall, Backup etc.)



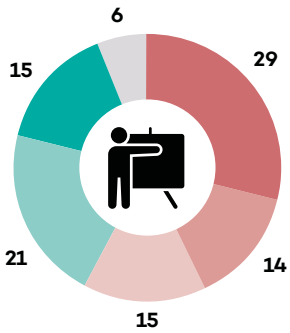
Cyberattacken erkennen (Log-Files)



Cyberattacken managen (Notfall-Pläne)



Cyber-Awareness (Mitarbeiter-Trainings)



Alle Angaben in Prozent

Massnahme gar nicht umgesetzt | voll und ganz umgesetzt | keine Antwort

«Digitale Sicherheit fängt bei jedem selber an»

Beschäftigt man sich mit dem Thema Sicherheit, ist es naheliegend, die Armee in die Überlegungen mit einzubeziehen. Und es bietet sich an, die Elektronische Kriegsführung und den 2018 neu geschaffenen Cyber-Lehrgang genauer unter die Lupe zu nehmen.

Autor Daniel Slongo **Bilder** Sandro Breu

Der Schulkommandant der Elektronischen Kriegsführungs-Schule 64 (EKF S 64) der Schweizer Armee lädt zum Ortstermin in der Kaserne Jassbach. Oberst im Generalstab Patrik Anliker ist in der EKF S 64 für die Ausbildung der Funkaufklärer und seit 2018 für die Durchführung des Cyber-Lehrgangs der Schweizer Armee verantwortlich. Um die Einsatzfähigkeit und Handlungsfreiheit jederzeit und in allen Lagen sicherzustellen, muss die Armee fähig sein, Cyber-Bedrohungen zu erkennen, sich vor Angriffen zu schützen und diese nötigenfalls abzuwehren. Im Konfliktfall kommt die Fähigkeit hinzu, mit Cyber-Aktionen militärische Operationen zu unterstützen. Denn der Schulkommandant stellt klar: Die Cyber-Thematik durchdringt alle Bereiche der Armee und der Verwaltung.

Von 0 auf 100 in einem Jahr

Um die Sicherheit im Cyberraum zu gewährleisten, braucht es entsprechend ausgebildetes Personal. Der Cyber-Lehrgang bildet für die Armee einen wichtigen Meilenstein im Rahmen der Umsetzung des Aktionsplans für Cyber-Defense des Eidgenössischen Departements für Verteidigung, Bevölkerungsschutz und Sport (VBS) vom November 2017. Dieser ist auf die Nationale Strategie zum Schutz der Schweiz vor Cyberrisiken abgestimmt, die unter anderem festhält, dass jeder Akteur im Cyberraum selbst für den Schutz vor und für die Bewältigung von Cyberangriffen zuständig ist. Armeeangehörige für diese speziellen Funktionen auszubilden, lautete 2017 denn auch der Auftrag an den Schulkommandanten Anliker. In nur fünf Monaten wurde dieser Cyber-Lehrgang konzipiert und auf die Beine gestellt. Er ist schweizweit auf grossen Anklang gestossen.

Win-win-win-Situation

Die Miliz und der Nutzen des Lehrgangs für Wirtschaft und Armee standen bei der Konzeption des Lehrgangs im Zentrum. Anliker umschreibt es so: «Es ist eine Win-win-win-Situation: für den Armeeangehörigen, die Armee und die Wirtschaft. Die Armee kann vom Vorwissen der jungen Rekruten profitieren und bildet sie im Cyber-Lehrgang aus. In ihrem Arbeitsalltag bringen sie ihr militärisch erworbenes Wissen gewinnbringend zum Nutzen der Wirtschaft ein und bringen ihre zivile Erfahrung später in den Wiederholungskursen wieder in den militärischen Cyber-Alltag ein.» Ein einfaches, aber überzeugendes Konzept. Damit aber noch nicht genug: Die Armeeangehörigen schliessen den Cyber-Lehrgang mit einer höheren Berufsprüfung, dem «Cyber Security Specialist» mit eidgenössischem Fachausweis, ab.

Weitermachen ist Pflicht

Das Interesse am Cyber-Lehrgang ist angesichts der Attraktivität und Modernität sehr gross. «Es braucht viel Zeit, um die Inhalte in der gewünschten Tiefe zu vermitteln. Darum werden die Interessenten selektioniert und jeder Lehrgangsteilnehmer muss sich verpflichten, sich mindestens zum Wachtmeister weiterbilden zu lassen», erklärt der Oberst. Denn der Cyber-Lehrgang dauert nicht 18 Wochen wie eine Rekrutenschule, sondern 40 Wochen. Eine strenge Selektion sei nötig, betont Anliker. Zum einen könne so die Qualität der Absolventen hochgehalten werden und zum anderen sei es wichtig, die richtigen Leute für diese verantwortungsvollen Funktionen zu selektionieren.

Patrik Anliker

Patrik Anliker, 1967, ist verheiratet und hat drei Kinder. Seine Ausbildung hat er beim damaligen Festungswachtkorps (FWK) absolviert. Nach mehreren Jahren als Verteidigungsattachéassistent und stellvertretender Attaché absolvierte er den Diplomlehrgang an der ETH und ein EMBA an der HTW in Chur. 2003 trat er ins Instruktionskorps der Armee ein. Nach verschiedenen Kommandierungen und Lehrgängen im In- und Ausland übernahm er 2017 das Schulkommando der EKF S 64.

> «Es ist eine Win-win-win-Situation: für den Armeeangehörigen, die Armee und die Wirtschaft.»

Konvention mit sich selber

Ob es nicht eine Herausforderung sei, junge Menschen, Digital Natives, in seiner Schule zu Geheimhaltung und verantwortungsbewusstem Bewegen im digitalen Raum zu bringen? Der Schulkommandant bestätigt. Anliker setzt hier untypisch für militärische Angelegenheiten auf das Prinzip der Selbstverantwortung und auf das Prinzip der «Konvention mit sich selber», wie er es nennt. «Jeder muss sich selber bewusst sein, was er wie und wo veröffentlichen und von sich preisgeben will. Sei dies auf den sozialen Medien, im Internet oder im unendlichen Universum von Big Data mit Apps, die Einkaufsgewohnheiten, Gesundheitsdaten und vieles mehr sammeln.»

Oberst im Generalstab Anliker lebt dieses Prinzip auch bei sich selber. Er verschliesst sich den sozialen Medien nicht, denn das sei heute fast nicht mehr möglich. Doch er nutzt sie sehr vorsichtig und achtet sehr genau darauf, was für Beiträge er veröffentlicht.

Segen und Gefahr der Digitalisierung

Viele Bereiche des Lebens werden dank der Digitalisierung einfacher, effizienter und schneller. Auf der Schattenseite stehen aber die Verletzlichkeit, die Verwundbarkeit und die Abhängigkeit, welche die Digitalisierung mit sich bringt. Gerade in der immer stärker werdenden Tendenz, die Vernetzung mobil zu machen, also «durch die Luft zu transportieren», sieht Anliker eine grosse Angriffsfläche und grosses Missbrauchspotenzial. «Alles, was frei durch die Luft transportiert wird, kann mit einfachen Mitteln von irgendjemandem aufgefangen werden.» Gäbe es all diese digitalen Möglichkeiten nicht, müsste man sich auch nicht vor dem Missbrauch schützen, und dann bräuchte es auch den Cyber-Lehrgang nicht. Anliker bewegt sich beruflich und privat immer auf dem schmalen Grat von Segen und Fluch der Digitalisierung. Aus gutem Grund verhält er sich sehr vorsichtig im digitalen Raum: Jede Woche erhält er mehr oder weniger dubiose E-Mails, die er nicht öffnet. Er ist sich bewusst, dass er als Kommandant der EKF-Schule und als Kommandant des Cyber-Lehrgangs im digita-

len Glashaus sitzt und dass er ein gesuchtes Ziel – eine lohnende Trophäe – für jeden Hacker darstellt. Paranoid wird der 52-jährige Oberst darum aber nicht. «Ich weiss, wie ich mich schützen kann, und bin bestrebt, meinen digitalen Datenfussabdruck möglichst klein zu halten.»

> «Alles, was frei durch die Luft transportiert wird, kann mit einfachen Mitteln von irgendjemandem aufgefangen werden.»

Eigenverantwortung im Umgang mit Daten

Aber trotz allen systemischen Schutzmechanismen liegt es am Ende in der Verantwortung jedes Einzelnen, wie er selber mit dem Schutz seiner persönlichen Daten umgeht. Und da schliesst sich der Kreis zur Konvention mit sich selbst wieder. Das System kann die Daten noch so gut zu schützen versuchen; wenn jemand wissentlich oder unwissentlich diese Daten preisgibt, ist jede systemische Schutzmassnahme wirkungslos.

Als lebenserfahrener Berufsoffizier ist sich Anliker auch bewusst, dass man in der Abwehr – im Speziellen auch in der Cyber-Abwehr – der Entwicklung immer einen Schritt hinterherhinkt. Die Angriffe und Möglichkeiten werden immer vielfältiger, die technischen Tools für Cyberattacken können immer einfacher beschafft werden und sind immer einfacher zu bedienen. Er gibt sich da realistisch: «Wir können nicht vorhersagen, was morgen passieren wird. Aber mit den geeigneten Massnahmen und der nötigen Aufmerksamkeit ist präventiv schon viel gemacht.» Das stellt hohe Anforderungen an das Erkennen und an den Schutz der eigenen Systeme.

Digitalisierung weiter vorantreiben

Als Kommandant der EKF-Schulen und des Cyber-Lehrgangs hat Anliker tiefen Einblick in die digitalen Gefahren, die täglich lauern. Er hat auch tiefe Einblicke in die Möglichkeiten, wie man Systeme hacken kann und unbemerkt an Daten und Systeme kommen kann. Trotzdem verschliesst sich Anliker der digitalen Entwicklung nicht. Im Gegenteil. Dort, wo die Digitalisierung einen Mehrwert bringt, will er sie auch effizient und vehement vorangetrieben wissen. Aber immer mit dem Primat, dass der Schutz vor Missbrauch und die entsprechenden Massnahmen prioritär mitentwickelt werden. Als Bürger und Privatperson bleibt er auch überzeugt, dass die Digitalisierung viel Gutes bringt und dass man noch viel mehr Effizienz herausholen kann und muss. Bei der aktuellen Diskussion um autonomes Fahren fügt Anliker beispielsweise an, dass nicht nur die autonom fahrenden Autos entwickelt werden sollen, sondern auch die notwendigen Strassen dazu. So, dass die Autos auch untereinander oder mit der Strasse kommunizieren können. So liessen sich Stau und Stosszeiten enorm verringern. Aber im gleichen Atemzug fügt der Berufsoffizier an, dass diese Systeme auch wieder gut vor Missbrauch geschützt werden müssen und die Sicherheit als oberste Priorität gewährleistet bleiben muss.

Schutz der Systeme und Daten

Darin sieht Anliker die nächsten Schritte der Digitalisierung. Die Systeme müssen geschützt werden und der Missbrauch erschwert werden. Egal ob WLAN, 5G oder Internet of things. Alles ist für jedermann aus der Luft greifbar, und das macht es verwundbar. Und der Schutz fängt bei jedem persönlich an. Bei seiner Konvention mit sich selber und der Selbstverantwortung. Patrik Anliker fasst am Ende des Gesprächs seine digitalen Selbstschutztipps zusammen: «Erstens nichts von sich in den sozialen Medien oder in der Cloud preisgeben, was man nicht mit allen teilen könnte. Zweitens den eigenen digitalen Fussabdruck möglichst klein halten. Drittens die eigenen elektronischen Geräte so einstellen, dass die Gefahr eines unbemerkten Zugriffs minimiert werden kann. Und viertens aufmerksam und alarmiert sein auf Ungereimtheiten in Mails und zugestellten Anhängen und Dokumenten.»

> «Die Systeme müssen geschützt und der Missbrauch erschwert werden.»

Dieser Besuch beim digitalen Menschen Oberst im Generalstab Patrik Anliker hat das Bild eines differenzierten, aufgeschlossenen, aber vorsichtigen Schweizer Bürgers und Soldaten gezeichnet. Auch beim Autor hat der Besuch einen bleibenden Eindruck hinterlassen: Seither bleiben auf dem Smartphone WLAN- und Bluetooth-Funktion grundsätzlich ausgeschaltet und werden nur eingeschaltet, wenn ein bekanntes, gesichertes Netz zur Verfügung steht und die Funktion benutzt wird.

Das ausführliche Porträt im digitalen Magazin.

abrax.as/der-digitale-mensch

Mit strammem Schritt in die digitale Zukunft.

Die Idee hinter dem Projekt «Face Cartography» war, sich selber als Fotograf aus dem Spiel zu nehmen. Die hochauflösenden Bilder wurden von einem Industrieroboter aufgenommen und setzen sich aus über 600 Einzelaufnahmen und 900 Millionen Pixeln zusammen. Fotograf: Daniel Boschung.

Weitere Bilder des Monats finden Sie in der gleichnamigen Rubrik im digitalen Magazin.

abrax.as/bild

Abraxas Aktuell

Transformation mit Abraxas

Als Verwaltung die Chancen der Digitalisierung nutzen

Wir begleiten unsere Kunden auf dem Weg zur digitalen Verwaltung. So nutzen sie die Chancen und finden die passenden Lösungen für die Bedürfnisse ihrer Zielgruppen. (Bild: Shutterstock)

Die Digitalisierung ist eine Herausforderung für Verwaltungen. Sie schafft aber auch neue Chancen. Abraxas ist in der Schweiz ein **Pionier in der Digitalisierung** von Verwaltungen. Unsere Erfahrung zeigt: Die erfolgreiche digitale Transformation basiert auf einer optimalen Kombination von der Gestaltung von Geschäftsprozessen und dem Einsatz moderner und geeigneter Technologien.

Abraxas hat rings um die digitale Verwaltung mehrere Chancenfelder ausgemacht. Wir unterstützen unsere Kunden dabei, diese **Chancen** zu packen: Erstens sorgen effiziente Prozesse für mehr freie Ressourcen und erleichtern die tägliche Arbeit. Zweitens führen benutzerfreundliche Anwendungen zu produktiveren und zufriedeneren Mitarbeitenden. Drittens tragen unsere integrierten Gesamtlösungen zu einem Full-Service-Public für die Bevölkerung bei. Zu guter Letzt legen unsere **Lösungen** die Basis für ein grosses Vertrauen der Bürgerinnen und Bürger in eine sichere digitale Verwaltung.

Unsere Kunden spiegeln dieses Vertrauen auch uns gegenüber. Verwaltungen aller drei Staatsebenen setzen auf die Dienste von Abraxas, welche alle **Zielgruppen** mitdenken. Auf kommunaler Ebene zum Beispiel vertrauen insgesamt 184 Gemeinden auf die Lösungen von Abraxas. Per 1. Januar 2020 kommen die vier Gemeinden Neerach ZH, Fischenthal ZH, Rebstein SG und Surses GR hinzu.

Lernwerkstatt im Fokus

Riesenplakat rockte den LEO

Während zweier Wochen im Oktober zierte ein Riesenplakat die Fassade des «Leopard»-Gebäudes, des Hauptsitzes der Abraxas in St. Gallen. Das Motiv rockte und rückte für den Verein «IT rockt!» den Ostschweizer IT-Nachwuchs ins Licht der breiten Öffentlichkeit. Eines der neuen Motive der **«IT rockt!»-Kampagne** inszeniert gleich Erfolgsfaktoren des IT-Standortes St. Gallen: Teamwork und Nachwuchsförderung. Als treffendes Sujet zeigt es die Lernwerkstatt der Abraxas.

Abraxas ist ein Ausbildungsbetrieb aus Überzeugung und engagiert sich in der beruflichen Grundbildung für IT-Fachkräfte. Wir beschäftigen permanent mindestens 30 Lernende mit Fachrichtungen in der Informatik.

Gemeinsam rockt IT! Video zur Plakat-Aufrichte: abraxas.ch/012

Wir sind #TeamAbraxas!
(Bild: Florian Brunner)

Ausbruch aus dem Papier

Neues Lernen dank «Base4Kids 2»

Am 14. Oktober war es so weit: Im Rahmen des «Base4Kids 2»-Projekts für das Schulamt der Stadt Bern wurden 6300 iPads an Schülerinnen und Schüler ausgehändigt. Neugierige Kinderhände und begeisterte Jugendliche nahmen die Geräte entgegen, gespannt auf die **neue Welt des Lernens,** zu welcher Abraxas und Umsetzungspartner in den letzten Monaten die Basis gelegt haben.

«Base4Kids 2» ist in vielen Belangen ein hochkomplexes Projekt: Vereinfacht gesagt, erhalten die 22 Volksschulen der Stadt Bern eine Lösung, welche **sowohl Applikationen als auch Infrastruktur** umfasst. Einerseits erhalten Schulverwaltung, Lehrpersonen, Schülerinnen und Schüler (SuS) und deren Eltern Zugriff zu einem umfassenden Lernportal (Moodle, Mahara) inklusive Chat (Mattermost) und Datenablage (Nextcloud). Andererseits werden ihnen auch insgesamt 7780 iPads als Endgeräte zur Verfügung gestellt. Diese setzen sich aus 1430 Lehrpersonen-iPads und 6350 SuS-iPads zusammen.

Die Technologie ist aber nur eine Seite des Projekts. Sie ist einzig der Katalysator, welcher eine neue Art des Lernens und der Wissensvermittlung ermöglichen kann. Während Jahrhunderten wurde Wissen auf dem Medium Papier vermittelt. «Base4Kids» befreit das Lernen aus dem Papier und schafft eine multimediale **Lernumgebung,** welche die **individuellen Bedürfnisse** der Schülerinnen und Schüler stärker berücksichtigt und die Didaktik auf ein neues Niveau heben kann.

Case-Video: Ausbruch aus dem Papier. abraxas.ch/013

Neuer Vertrag und neue Funktionen

Mit KOMPASS erfolgreich unterwegs

Mit KOMPASS bietet Abraxas eine Gesamtlösung für Berufsbildungsämter, die in enger Zusammenarbeit mit der Interessengemeinschaft Informatik im Berufsbildungswesen (IGIB) entwickelt wurde. Der September brachte zwei richtungsweisende Entwicklungen: Zum einen konnte ein **neuer Rahmenvertrag** unterzeichnet werden. Dieser beinhaltet sowohl Lizenz, Wartung und Weiterentwicklung von KOMPASS bis Ende 2027 als auch den Betrieb bis Ende 2023 für die Kantone Appenzell Innerrhoden, Appenzell Ausserrhoden, Graubünden, Luzern, St. Gallen, Schaffhausen, Solothurn, Thurgau und Zürich sowie das Fürstentum Liechtenstein. Zum anderen wurde

Zufriedene Vertreter der IGIB und von Abraxas beim Vertragsabschluss: Elias Mayer, Peter Baumberger, Andres Meerstetter, Curdin Tuor, Markus Zollinger und Marcel Wissmann (v.l.). (Bild: zvg)

die **Inbetriebnahme der Lehrbetrieb-Services** gefeiert. Damit können KOMPASS-Prozesse aus den Ämtern hin zu den Lehrbetrieben und Lernenden verlängert werden. So können z. B. Lehrverträge online abgeschlossen oder auch der Lehrstellennachweis online gepflegt werden.

Produktportfolio

Elektronische Betreibung, eine Erfolgsstory

Gemäss den aktuellsten Zahlen des Bundesamts für Justiz wurden 2018 rund 1.68 Mio. Betreibungsbegehren über den digitalen Standard eSchKG abgewickelt. Dies entspricht rund 55 % aller Betreibungen in der Schweiz. Der Standard vereinfacht also ganz offensichtlich die Kommunikation zwischen Gläubigern und Betreibungsämtern. Dank der laufenden Integration des eSchKG-Standards in alle betroffenen Abraxas-Applikationen für Finanz-, Steuer- und Betreibungsämter können Betreibungsmassnahmen **einheitlich und ohne Medienbrüche** abgewickelt werden. Wie der Betreibungsprozess bei teilnehmenden Gemeinden verschlankt und effizienter wird, berichten uns Vertreter von Betreibungs-, Finanz- und Steueramt im Interview – zu lesen im digitalen Magazin.

Drei Herren vom Amt: eSchKG-Interview und -Video. abraxas.ch/014

Rollin' all over Europe

Über 1'000 Clients für Hoval

Der Outsourcing-Auftrag für den Heizungs- und Klimaspezialisten Hoval war eine internationale **Premiere für Abraxas:** Zum ersten Mal überhaupt wurde damit in der EU ausgerollt. Der Rollout führte das Projekt an insgesamt 25 Standorte in 13 Ländern.

Abraxas. Für das digitale Europa. Mit Sicherheit. (Bild: zvg)

Auf ihrer Tour durch Europa rollten die insgesamt drei Teams mit jeweils sieben Personen zunächst durch die Schweiz, Frankreich, Liechtenstein, Italien, Grossbritannien, Deutschland. Den Abschluss bildete dann der Osten des Kontinents mit Rollouts in der Slowakei, in Polen, Tschechien, Bulgarien, Kroatien und Rumänien. Insgesamt umfasste der Auftrag über **1'000 Clients sowie 145 Monitore.** Am Schluss ging es plötzlich ganz schnell – nach einer Gesamtlaufzeit von fast drei Jahren fand das Projekt Anfang Oktober sein Ende: In nur 5 Wochen wurden die letzten 6 Länder ausgerollt.

Speziell herausfordernd waren bestehende Clients, welche während der Betriebszeiten am Arbeitsplatz der Hoval-Mitarbeitenden neu aufgesetzt werden mussten, was das Rollout-Team bravourös meisterte und die **Professionalität von Abraxas im IT-Outsourcing** unter Beweis stellte: Aufgrund des minutiösen Rollout-Konzeptes beider Partner konnte die Neuinstallation inklusive aller Applikationen innert zweier Stunden erbracht werden. Neue Clients wurden innert 30 Minuten ausgerollt. So wurde die Ausfallzeit auf ein Minimum reduziert. Inklusive Vorbereitung, Koordination, Installation, Schulungen und Reisetätigkeiten hat das Projekt mehr als 5'500 Stunden beansprucht.

Mehr über das Outsourcing-Angebot erfahren. abraxas.ch/015

Herbst-Fachveranstaltung 2019

Digitalisierung: Zukunft hat längst begonnen

An der Abraxas Herbst-Fachveranstaltung **im Würth Haus Rorschach** führte Peter Baumberger, stv. CEO, durch die wichtigsten News aus dem Unternehmen. Unter anderem informierte er über die Mehrprodukte-Strategie im Bereich Finanzen und kündigte die neue Produktelinie VOTING an, welche das bewährte WABSTI ablösen soll. Informationen zum neuen Kundenportal, zur Krisen- und Service-Kommunikation rundeten den ersten Teil der Veranstaltung ab.

Nach dem Plenum verteilten sich unsere Gäste auf diverse spannende Fachforen. Darin erhielten sie Antwort und Auskunft zu Produkten und Entwicklungen in den Bereichen Neue Arbeitswelt, Finanzen, Betreibungsamt, Einwohner, Bildung und Abacus. Eines unter vielen vorgestellten Beispielen war der **Secure Mailhub Service** von Abraxas. Mit dieser Dienstleistung können unsere Kunden ihre Mails mit sensiblen Daten sicher austauschen und einfach handhaben. E-Mail-Sicherheit bedeutet dabei Vertraulichkeit, Integrität und Nachweisbarkeit.

Fazit: Die **Digitalisierung** der öffentlichen Verwaltung sollte kein Thema für eine mehr oder weniger weit entfernte Zukunft mehr sein. Sie findet bereits **heute im Hier und Jetzt** statt. Abraxas unterstützt, berät und begleitet öffentliche Verwaltungen und Unternehmen auf diesem Weg.

Engagierte Diskussionen im Würth Haus Rorschach. (Bild: Dominique Vernier)

Fachveranstaltungs-Rückblick in Text und Bild. abraxas.ch/016

QR-Rechnung ab Mitte 2020

Mit Abraxas gelingt die Umstellung

Am 30. Juni 2020 macht die Schweiz einen weiteren grossen Schritt in Richtung vollständig digitale und medienbruchfreie Rechnungsverarbeitung: Im Schweizer Zahlungsverkehr wird die QR-Rechnung eingeführt. Sie ersetzt die altbekannten roten und orangen Einzahlungsscheine. Ab diesem Zeitpunkt können theoretisch alle 600'000 Akteure **QR-Rechnungen** an ihre Kunden **verschicken.** Daher müssen alle Rechnungsempfänger auch in der Lage sein, eingehende **QR-Rechnungen** zu **empfangen** und mit ihrem Kreditorenprozess zu verarbeiten.

Mit Abraxas sind unsere Kunden bestens vorbereitet: QR-Rechnungseingänge werden ab dem 30. Juni 2020 unterstützt. Ab dem 31. Dezember 2020 sind alle Fachlösungen dann auch in der Lage, QR-Rechnungen zu erstellen und sowohl zentral als auch lokal zu drucken.

Laufend mehr News finden Sie in der Rubrik «Abraxas Aktuell» des digitalen Magazins.

abrax.as/aktuell

6 Ideen zur Digitalisierung

Die zwei letzten Legislaturperioden sind – in Sachen zukunftsfähiger Digitalisierung – verloren. Sechs Ideen zur Besserung.

1. Abschaffung der Massenüberwachung

Mittel der Massenüberwachung wie das minutiöse Festhalten aller Bewegungs- und Kontaktdaten der Bevölkerung (Gesetz zur Überwachung auf Vorrat BÜPF) und die Stichwort- respektive Mustersuche in Datenströmen (Geheimdienstgesetz NDG) müssen abgeschafft werden. Sie verletzen eklatant unsere Privatsphäre und stellen ein grosses Sicherheitsrisiko dar: Für Kriminelle eignen sich die eingesammelten Daten zum grossflächigen Identitätsdiebstahl. Sie sind deshalb auch potenzielles Erpressungsmaterial.

2. Beendigung der Internetzensur

Mit dem Geldspielgesetz wurde erstmals eine schweizweite Zensurinfrastruktur errichtet. Bereits wurden im Fernmeldegesetz neue Netzsperren gegen verbotene Pornografie beschlossen. Weitere Begehrlichkeiten von Staat (zwecks «Sicherheit») und Wirtschaft (zwecks Marktabschottung) sind absehbar. Das staatlich angeordnete Fälschen des Internets – nichts anderes ist diese Zensur – schafft zudem Sicherheitsrisiken, die es Kriminellen und Geheimdiensten einfacher machen, die Menschen in der Schweiz auszutricksen.

3. Ausbau des Datenschutzes

Das Datenschutzgesetz von 1992 befindet sich gegenüber der Datenschutzgrundverordnung (DSGVO) der EU im Hintertreffen. Die laufende Revision ist umstritten. Was sie wirklich bringt, ist noch offen. Am wichtigsten wäre es, sehr hohe Bussen für grössere Datenschutzverletzungen zu verhängen. Dies schafft Anreize, mehr in sichere und dezentralisierte IKT zu investieren. Auch muss geboten werden, den Datenschutz, wenn immer möglich, technisch durchzusetzen (Grundsätze von «Privacy by Design» und «Privacy by Default»).

4. Bildungsoffensive auf allen Ebenen

An Schulen muss die Digitalisierung fächerübergreifendes Thema werden: Nicht nur Chancen, auch Risiken müssen thematisiert und den Jugendlichen direkt gezeigt werden (z. B. Visualisierung von Tracking und Zeigen unverschlüsselter Datenströme). An Berufsbildungs- und Hochschulen müssen IKT-Studierende in sicherem und privatsphärefreundlichem Programmieren ausgebildet werden, um von vornherein schwere Patzer bei Konzeption und Umsetzung von Soft- und Hardwareprojekten zu vermeiden.

5. Public Money – Public Code

Die Bundesverwaltung und die Kantone sollten ihre Software quelloffen und mit urheberrechtlichen Freiheiten für alle lancieren, damit Misskonzeptionen früh erkannt werden und alle mitwirken können. Gerade bei kritischen Infrastrukturen von E-Government und E-Health (z. B. dem Elektronischen Patientendossier) ist maximale Transparenz geboten, um Fehlfunktionen und Sicherheitslücken offen auszuräumen, aber auch, um den Einbau von Hintertüren zu erschweren, die andernfalls zum Beispiel einen Datenabfluss erleichtern würden.

6. Unabhängigkeit von Konzernen und Grossmächten

Zusammen mit europäischen Partnern muss die Schweiz Milliarden in die Hände nehmen, um transparente Hardware (sogenannte Open-Hardware) zu fördern: Nicht nur beim viel diskutierten 5G (danach: 6G), auch bei Endgeräten – von Handys über Internet-of-Things-Geräte bis hin zu Servern – ist sehr klar absehbar, dass die Wahrscheinlichkeit direkter Fremdkontrolle – durch Hintertüren in der Hardware – immer weiter zunimmt. Schliesslich sind alle in der Schweiz eingesetzten Kernkomponenten direkt oder indirekt aus China oder den USA – beides Staaten mit erheblichen Angriffskapazitäten. Damit machen sich nicht nur Bürgerinnen und Bürger, sondern auch staatliche Stellen und Unternehmen – wegen der zunehmenden Digitalisierung – immer weiter auf Knopfdruck erpress- und angreifbar.

Hernâni Marques

ist Computerlinguist, Soziologe und Neuroinformatiker, Vorstandsmitglied des Chaos Computer Club Schweiz (CCC-CH) und Mitglied im Stiftungsrat der p≡p foundation. Er hilft mit, technische Werkzeuge zu erstellen, Privatsphäre wiederherzustellen und setzt sich politisch für Privatsphäre, Meinungsäusserungs- und Informationsfreiheit ein.

↘ Das Abraxas-Magazin lädt Gastautorinnen und -autoren dazu ein, pointiert zu Aspekten der Digitalisierung Stellung zu nehmen. Die Texte geben die Ansichten und Meinungen der Autorinnen und Autoren wieder und können von der Position von Abraxas abweichen.


BROMUNDT

abraxas

www.abraxas.ch/magazin

Impressum → magazin → Das Abraxas-Magazin für die digitale Schweiz →
Herausgeber: Abraxas Informatik AG, St. Leonhard-Strasse 80, 9001 St. Gallen → Auflage: 2500 Exemplare → redaktionelle Mitarbeit: alea iacta & Richert Media → Gestaltung: schalter&walter → Druck: Typotron