tribune

Das Magazin mit unternehmerischen Visionen

Ausgabe 4
November 2022

Digitale Identifikation

Roger Thiriet
Medienschaffender
Schriftleiter «tribune»
thiriet@bluewin.ch

«Die Zeit ist reif für die digitale Signatur als neuer Unterschrifts-Standard!» konstatierte unlängst der Architekt und damalige Verwaltungsrat der Vischer Architekten AG Basel Lukas Stutz in einer Publikation der Initiative be-digital der Handelskammer beider Basel. Und schlug vor, dass die «tribune» die Rahmenbedingungen für diese Art elektronischer Identifikation aus rechtlicher Sicht darlegt. Ein Jurist aus unserer Redaktionskommission hat diese Anregung aufgenommen.

«E-Voting schadet unseren demokratischen Werten nicht!», ist die Staatsschreiberin des Kantons Basel-Stadt überzeugt. Und äussert sich in dieser Nummer unserer Publikation über diesen und andere Aspekte der elektronischen Stimmabgabe bei Wahlen und Abstimmungen, deren Entwicklung und Einführung nach einer dreijährigen sicherheitsbedingten Pause nicht nur in Basel-Stadt zur Zeit wieder Fahrt aufnehmen.

«Cyber Security muss 365 Tage im Jahr ein Thema sein!» mahnt im dritten Beitrag der aktuellen Ausgabe unseres Magazins für unternehmerische Visionen der Chief Technology Officer eines in uptown Basel ansässigen ICT-Dienstleistungsunternehmens. Und legt dar, weshalb nicht alle Bedenken gegenüber der digitalen Identifikation unbegründet sind, mit den richtigen Sicherheitsvorkehrungen aber ausgeräumt werden können.

Die «tribune»-Redaktionskommission wünscht anregende Lektüre!

handelskammer beider basel

Jubiläumsstiftung
des Bankhauses La Roche & Co

Advokatenkammer Basel
Basellandschaftlicher Anwaltsverband

Digitale Signatur – Möglichkeiten und Grenzen

lic. iur. Roman Felix, Advokat
Enderle Felix Haidlauf Schmid
Advokatur und Notariat
felix@advokatur.ch

Elektronisch unterschreiben – das hört sich verlockend an. Die digitale Signatur kann erhebliche Vorteile bringen. Gleichzeitig ist vielerorts ein vages Gefühl der Unsicherheit wahrnehmbar. Sind derart unterzeichnete Dokumente wirklich rechtsgültig? Welche Art der Signatur wird dafür benötigt?

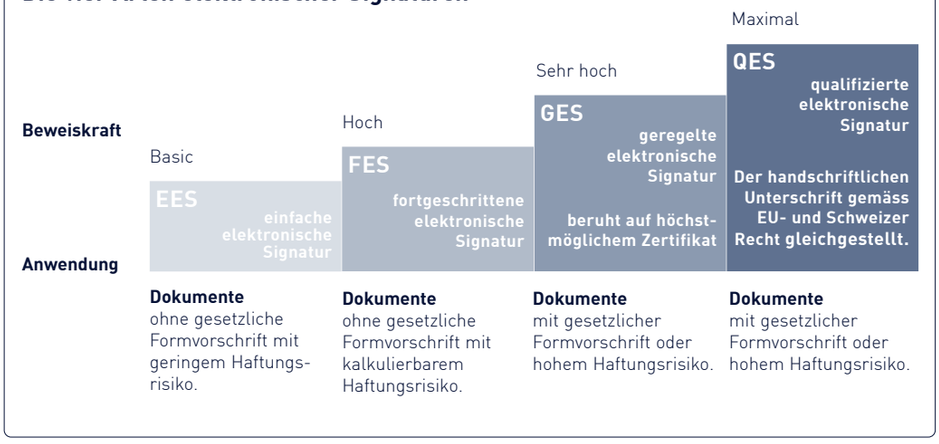
Die elektronische Signatur kann den Geschäftsalltag erheblich erleichtern. Sie macht den postalischen Austausch von Originaldokumenten überflüssig, Verzögerungen entfallen. Es werden weniger physische Papierdokumente benötigt, der Zeitaufwand für die Verfolgung und Ablage und die damit zusammenhängenden Kosten lassen sich deutlich reduzieren, der Zugriff ist zu jeder Zeit an jedem Ort möglich.

Gesetzliche Grundlagen vorhanden

Die gesetzlichen Grundlagen wurden mit dem Bundesgesetz über die elektronische Signatur (ZertES) und zugehöriger Verordnung bereits per 1. Januar 2005 in Kraft gesetzt. Trotz dieser Zeitspanne werden E-Signaturen noch immer zurückhaltend verwendet. Das mag daran liegen, dass die E-Signatur relativ teuer sein kann und eventuell auch die Hürde der aufwändigen physischen Identifikation genommen werden muss. Das wiederum kann Unternehmen davon abhalten, ihren Kunden die sicherste E-Signatur anzubieten. Zentral dürfte jedoch die weit verbreitete Unsicherheit sein, welche Rechtsgeschäfte mit der E-Signatur tatsächlich rechtsgültig abgeschlossen werden können.

> «Der Begriff der digitalen Signatur ist in der Schweiz deckungsgleich mit demjenigen der elektronischen Signatur.»

Die vier Arten elektronischer Signaturen



Die QES ist der höchste verfügbare E-Signatur-Standard mit maximaler Sicherheit und Beweiskraft

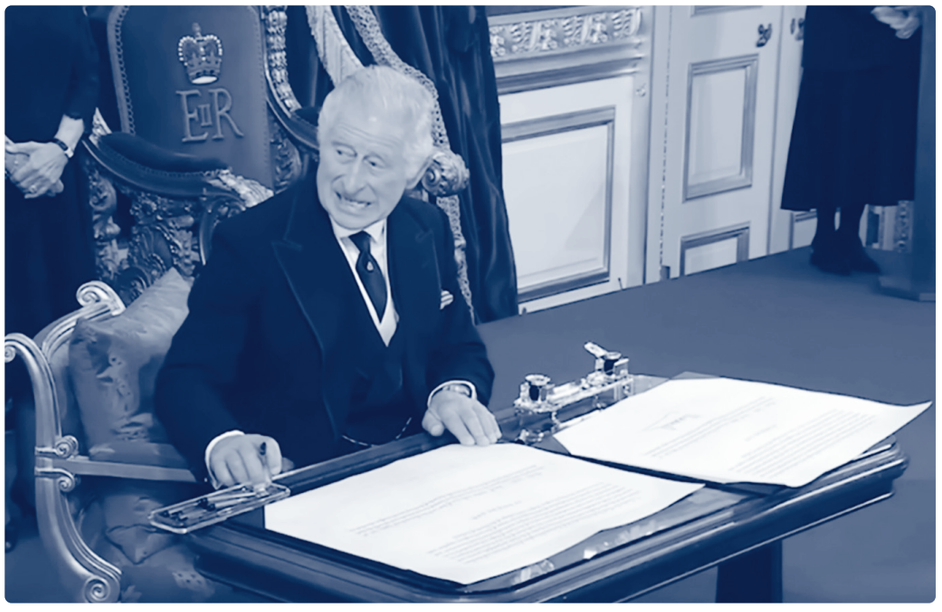
Arten der elektronischen Signatur

Vorweg: Der Begriff der «digitalen Signatur» ist in der Schweiz deckungsgleich mit demjenigen der «elektronischen Signatur». Innerhalb dieser Oberbegriffe sieht das ZertES vier verschiedene Arten von Signaturen vor. Die simpelste Form ist die einfache elektronische Signatur (EES), wie man sie etwa von PDF-Readern kennt. Damit wird die Integrität des Dokumentes sichergestellt, nachträgliche Änderungen lassen sich einfach erkennen. Die fortgeschrittene elektronische Signatur (FES) ermöglicht zusätzlich eine eindeutige Identifikation des Inhabers. Dabei handelt es sich zumeist um eine Zwei-Faktor-Authentisierung, wie etwa bei heutigen Zahlungsaufträgen an die Bank. Eine rechtsgültige Verifizierung der Identität des Inhabers findet hier allerdings nicht statt. Deutlich weiter geht die qualifizierte elektronische Signatur (QES). Es erfolgt eine Identifikation mittels amtlichen Ausweises durch einen anerkannten Anbieter eines Zertifizierungsdienstes. Zusätzlich wird ein Zeitstempel ausgestellt. Mittels der QES kann damit Integrität und Authentizität eines Dokumentes zu einem bestimmten Zeitpunkt von jedermann und jederzeit online überprüft werden (validator.ch). Schliesslich sieht das Gesetz als vierten Standard die geregelte elektronische Signatur (GES) vor, welche auf dem höchstmöglichen Zertifikat beruht, das auch auf juristische Personen ausgestellt werden kann. Die GES ist in Bezug auf die Sicherheit beziehungsweise Beweiskraft zwischen FES und QES anzusiedeln.

Anwendungsbereiche

Das ZertES regelt nur die Anforderungen an die Zertifikate und deren Anbieter. Wann aber welche Art von Signatur im jeweiligen Kontext erzeugt werden muss, um die gewünschte Rechtswirkung zu erzielen, lässt sich daraus nicht entnehmen. Massgebend hierfür sind die Bestimmungen des Schweizerischen Obligatio-

nenrechts (OR). Danach bedürfen Verträge zu ihrer Gültigkeit nur dann einer besonderen Form, wenn das Gesetz eine solche vorschreibt und können folgerichtig auch mündlich oder sogar konkludent abgeschlossen werden (Art. 11 und 1 OR). Ein Arbeitsvertrag kommt damit auch dann



zustande, wenn er bloss mündlich oder per E-Mail abgeschlossen worden ist, was aus Gründen der Rechtssicherheit und Beweiskraft natürlich nicht zu empfehlen ist. Gleiches gilt, wenn der Arbeitsvertrag mit einer einfachen (EES) oder fortgeschrittenen (FES) Signatur unterzeichnet wird, was die Beweiskraft doch erheblich verbessern kann.

Anders sieht es aus, wenn von Gesetzes wegen das Formerfordernis der Schriftlichkeit besteht. Gemäss Art. 13 OR muss ein Vertrag diesfalls die Unterschrift aller zu verpflichtenden Personen tragen, die Unterschriften sind gemäss Art 14 Abs. 1 OR eigenhändig zu leisten. In Absatz 2 wird nun aber festgehalten, dass der eigenhändigen Unterschrift die qualifizierte elektronische Signatur (QES) gleichgestellt ist. Daraus folgt, dass bei allen Verträgen mit gesetzlich vorgeschriebener Schriftlichkeit ausschliesslich die QES verwendet werden kann. Dies gilt zum Beispiel für Forderungsabtretungen, Schenkungsversprechen, Kreditaufträge, Erbteilungsverträge oder auch Pfandverträge. Auch im Bereich des Arbeitsrechts gilt teilweise das Erfordernis der Schriftlichkeit, unter anderem für besondere Arbeitsverträge (Lehrverträge, Verträge über Leih- und Temporärarbeit et cetera) oder für die Vereinbarung eines Konkurrenzverbotes. In all diesen Fällen führt nur die qualifizierte elektronische Signatur zum Ziel, der Gebrauch aller anderen Signaturarten führt hier unweigerlich zur Ungültigkeit.

«Die Einführung der elektronischen Signatur erfordert gute Vorbereitung.»

Was geht nicht?

Auch für die grundsätzliche Gleichstellung der qualifizierten elektronischen Signatur mit der eigenhändigen Unterschrift gilt: Abweichende gesetzliche oder vertragliche Regelungen (Art. 16 OR) bleiben vorbehalten. So kann die QES dann nicht benutzt werden, wenn der Gesetzgeber weitere Erfordernisse definiert hat. Das gilt insbesondere für Vorgänge, die gemäss Gesetz einer qualifizierten Schriftform bedürfen. Die Qualifikation liegt dabei in zusätzlich zu erfüllenden Kriterien, so etwa die Formularpflicht im Mietrecht für die vermieterseitige Kündigung oder die Mitteilung von Mietzinserhöhungen, ebenso das Erfordernis der Eigenhändigkeit beim Testament und bei der Bürgschaft. Ausgeschlossen ist die Anwendung einer elektronischen Signatur natürlich auch im Bereich der öffentlichen Beurkundung, der strengsten gesetzlichen Form der qualifizierten Schriftlichkeit (Grundstücksgeschäfte, Ehe- und Erbverträge und so weiter).

Fazit

Die Einführung der elektronischen Signatur erfordert gute Vorbereitung; rechtliche Beratung ist ratsam. Und im Zweifelsfall: Vor dem Rechtsöffnungsrichter ist eine bloss als PDF eingescannte Schuldanerkennung mit Unterschrift noch immer besser, als ein vom Richter nicht sogleich überprüfbares (unqualifiziertes) Zertifikat. Deshalb: Wenn schon eine elektronische Signatur, dann die qualifizierte (QES).

lic. iur. Roman Felix
ist Advokat und Partner von Enderle Felix Haidlauf Schmid, Advokatur und Notariat in Reinach. Er vertritt den Basellandschaftlichen Anwaltsverband in der Redaktionskommission der «tribune».

Schadet E-Voting der Demokratie?

lic. iur. Barbara Schüpbach-Guggenbühl
Staatsschreiberin des Kantons Basel-Stadt
Leiterin der Staatskanzlei
barbara.schuepbach@bs.ch

Mit dem E-Voting, dem Abstimmen und Wählen auf elektronischem Weg, beschäftigt sich die Politik seit über 20 Jahren. Bereits im Jahr 2000 hat das eidgenössische Parlament den Bundesrat beauftragt, die Vorbereitungen für eine elektronische Stimmabgabe in der Schweiz voranzutreiben. Im Juni 2002 ergänzte es das Bundesgesetz über die politischen Rechte; es erlaubt seit 2003 E-Voting. Zu den Vorreitern auf dem neuen, dritten Abstimmungs- und Wahlkanal gehört der Kanton Basel- Stadt; federführend ist dessen Staats- kanzlei mit ihrer Leiterin, Staatsschreiberin Barbara Schüpbach-Guggenbühl. «tribune» sprach mit ihr über den aktuellen Stand der Dinge im Kanton und wie sich E-Voting ihrer Ansicht nach auf unser Demokratieverständnis und -verhalten auswirkt.

Frau Schüpbach, wann hat der Kanton Basel-Stadt mit E-Voting begonnen?
Im Oktober 2008 hat der Grosse Rat die gesetzliche Grundlage für das elektronische Wählen und Abstimmen geschaffen. Ab 2009 konnten dann baselstädtische Auslandschweizerinnen und Auslandschweizer und ab 2016 auch Menschen mit Behinderungen elektronisch abstimmen und wählen. Damit haben wir gute Erfahrungen gemacht; so kamen durchschnittlich 60 Prozent der Stimmabgaben aus dem Ausland über diesen dritten Weg der Stimmrechtsausübung.

Dennoch haben Sie ihn 2019 wieder geschlossen. Weshalb?
In jener ersten Phase ging es darum, in einigen Kantonen im kleinen Massstab zu testen, ob und wie E-Voting alltagstauglich gemacht und auf breiter Ebene eingeführt werden kann. Da ging es auch immer wieder um Fragen der verwendeten Technik und vor allem der Sicherheit. Unser Partner in diesem Bereich war zuletzt die Schweizerische Post. Deren System hat anfänglich den hohen Anforderungen entsprochen; bei einer Weiterentwicklung kam es dann aber 2019 zu systemischen Schwächen.

Worin bestanden diese Probleme?
Beim ersten eingesetzten System war die Stimmabgabe nur individuell verifizierbar. Wer elektronisch abstimmte oder wählte, konnte sich selber vergewissern, ob seine Stimme in der elektronischen Urne angekommen war. In einem weiteren Schritt sollte nun die Stimmabgabe auch universell verifizierbar gemacht werden; will heissen, unabhängige Prüferinnen und Prüfer hätten zusätzlich unter der Anleitung der Staatskanzlei und der Wahrung

> «E-Voting ist wesentlich komplexer als E-Banking.»

des Stimmgeheimnisses überprüfen können, ob das System Manipulationen festgestellt hat. Tests haben dann aber gezeigt, dass die universelle Verifizierbarkeit noch ungenügend umgesetzt war. Deshalb hat die Post 2019 einen Marschhalt eingeschaltet. In der Folge wurde das Projekt insgesamt neu ausgerichtet, seitens Bund und in Absprache mit den Kantonen.

Wieso ist der Vorgang so kompliziert?
E-Voting ist wesentlich komplexer als andere digitale Anwendungen. Beim E-Banking etwa müssen ja nicht nur Sie allein geschützten Zugriff auf Ihr Konto haben; auch die Bankmitarbeitenden können und dürfen Einsicht nehmen. Das Bankgeheimnis teilen also mindestens zwei; das ist beim Stimmgeheimnis anders. Dieser zentrale Wert unserer Demokratie ist unantastbar und muss auch beim E-Voting hundertprozentig garantiert bleiben. Deshalb werden bei der Erfassung und der Auswertung des Stimmverhaltens Daten von Personen getrennt. Die digitale Umsetzung dieser Schritte, die so genannte Kryptografie beherrschen nur wenige Spezialisten. Das neue System der Post setzt nun die vollständige Verifizierbarkeit des Stimm- und Wahlvorgangs um.

Und was bedeutet diese Neuausrichtung konkret?
In der ersten Phase, also bis 2019, mussten sich die Kantone bezüglich Sicherheit des Systems auf die Aussagen der Systemanbieter verlassen. Mit der Neuausrichtung wurde die Systembewilligung dem Bund übertragen. Er hat die gesetzliche Grundlage neu gelegt und die Bundesverordnung dazu komplett neu geschrieben. Auf fachlicher Ebene wird das E-Voting kontinuierlich durch unabhängige Experten begleitet, der Quellcode ist publiziert und die Post muss jeden Entwicklungsschritt ins öffentliche Schaufenster eines «Bug Bounty»*-Prozesses stellen. Wichtig zu verstehen ist, dass dieses «friendly hacker»-Community-Programm der Post nicht eine einmalige Sache ist, sondern ständig weitergeführt wird. Damit wird auch der Weiterentwicklung des Systems und der Angriffsmöglichkeiten Rechnung getragen. Je nach Schweregrad der gefundenen Fehler wird eine Prämie von bis zu CHF 250'000 ausbezahlt. Was den Zeitplan betrifft, befindet sich die Post nun im Schlussspurt; das System sollte Ende Jahr bereitstehen.

Welche Argumente werden gegen E-Voting ins Feld geführt?
Was die Diskussion schwierig macht, ist die technische Dimension. Je weniger man weiss im Bereich der Kryptographie, desto vagere Bedenken werden vorgebracht. Interessanterweise hat die Sicherheitsdiskussion so lange keine Rolle gespielt, als es nur um das E-Voting-Privileg für Auslandschweizer Stimmberechtigte ging. Erst als man dann von einem dritten ordentlichen Stimmkanal für die ganze Bevölkerung zu sprechen begann, kamen Befürchtungen auf, E-Voting würde das demokratische System verfälschen; als ob eine Auslandschweizer-Stimme weniger wert wäre als eine aus dem Gundeli. Immer wieder vorgebracht wurden auch die von Donald Trump reklamierte «gestohlene Wahl» oder die kolportierte

* Bug-Bounty-Programm: Von Unternehmen, Interessenverbänden, Privatpersonen oder Regierungsstellen betriebene Initiativen zur Identifizierung, Behebung und Bekanntmachung von Fehlern in Software unter Auslobung von Sach- oder Geldpreisen für die Entdecker (siehe auch Beitrag auf den Seiten 6/7).

Einflussnahme von russischen Hacker-Kollektiven. Wieder andere befürchten Leaks bei den Druckereien der Wahl- und Abstimmungsunterlagen, denn das ist der einzige Ort, wo Namen und Adressen von Stimmberechtigten tatsächlich mit den E-Voting-Codes zusammengeführt werden. Solche Stimmen – konstruktive wie kritische – haben wir gehört und in die Neuausrichtung integriert.

Das Video der Bundeskanzlei erklärt die Massnahmen für ein sicheres E-Voting in der Schweiz.

Wie sieht der Zeitplan für die Wiedereinführung von E-Voting in Basel-Stadt aus?
Bereits 2017 hat der Grosse Rat einen Kredit von 5,9 Millionen Franken gesprochen, um E-Voting für alle Stimmberechtigten des Kantons einzuführen und den Betrieb über zehn Jahre zu finanzieren. Dieses Geld liegt bereit. Sobald der Bund eine Bewilligung zur definitiven Einführung des neuen, verbesserten Systems erteilt hat, können wir das neue System wieder einsetzen. Bis zu den Nationalratswahlen 2023 soll der elektronische Kanal für stimmberechtigte Baslerinnen und Basler im Ausland und Menschen mit Behinderungen wieder offen sein. Und später können wir dann bis maximal 30 Prozent der Basler Stimmbevölkerung auf diesem Weg abstimmen und wählen lassen.

Weshalb diese Beschränkung?
Mit dieser Obergrenze für den einzelnen Kanton – gesamtschweizerisch werden gar nur 10 Prozent zugelassen werden – haben die eidgenössischen Räte die politische Befürchtung aufgenommen, wonach eine elektronische Stimmabgabe der Gesamtheit oder einer Mehrheit der Stimmberechtigten eine demokratische Ausmarchung verfälschen könnte. Sie gehen davon aus, dass bei einem «Deckel» von knapp einem Drittel bei einem eventuellen Versagen des elektronischen Systems immer noch so viele Stimmen brieflich oder persönlich abgegeben werden, dass aus ihnen ein repräsentatives und somit gültiges Resultat ermittelt werden könnte. Ich teile diese Überlegung nicht: Das Ergebnis eines Urnengangs muss in seiner Gesamtheit stimmen, Extrapolieren ist nicht zulässig. In Basel-Stadt sollte E-Voting 2019 flächendeckend als dritter Stimmkanal eingeführt werden; der Stimmrechtsausweis für alle drei Abstimmungswege war schon vorbereitet. Dann hat aber die Post ihr System zur Überarbeitung zurückgezogen. Beim Neuanfang werden wir wegen der 30 Prozent-Hürde ein Anmeldeverfahren einführen müssen.

«Ich bin überzeugt, dass E-Voting unseren demokratischen Werten nicht schadet.»

Aber wie gesagt, die Ausdehnung auf 30 Prozent der hier wohnenden Stimmbevölkerung ist erst der übernächste Schritt.

Lohnt sich der Aufwand dafür überhaupt?
Ich bin überzeugt, dass er es tut. Erstens investieren wir in die Zukunft. Wer die Entwicklung der online verfügbaren Dienstleistungen in den letzten Jahren verfolgt hat, kann nicht daran vorbeisehen. Sich am Abend noch schnell einloggen und abstimmen? Das wird so selbstverständlich, wie wenn man vor dem Frühstück noch ein paar Schuhe ordert, beim Lunch per E-Banking die Monatszahlungen erledigt und vor dem Einschlafen das SBB-Ticket für den nächsten Tag kauft. In fünf Jahren ist das Stimmcouvert vielleicht das letzte Couvert, das wir im Briefkasten finden. Übersehen wir es dann nicht einfach? Und zweitens können wir die Erkenntnisse und Erfahrungen aus dem E-Voting-Prozess in andere Prozesse wie E-Collecting, also das Sammeln von gültigen Unterschriften für Initiativen und Referenden, einfliessen lassen. Aber zu diesem Thema müssten wir ein separates Interview führen.

Sie befürchten also keine Abwertung der Demokratie durch das E-Voting?
Ich bin überzeugt, dass E-Voting unseren demokratischen Werten nicht schadet. Die Meinungsbildung in einem demokratischen Prozess findet nach wie vor statt, aber vor allem die Jüngeren nutzen dafür andere Kanäle, Stichwort Social Media. Und da soll es der Demokratie schaden, wenn man auf jenem Handy, wo man die ganzen Informationen gesammelt hat, auch seine Stimme abgeben kann? Immer vorausgesetzt natürlich, dass die Stimmabgabe sicher ist, von niemandem verfälscht und von niemandem eingesehen werden kann.

Vielen Dank, Frau Schüpbach, für dieses Gespräch.

Interview Roger Thiriet

lic. iur. Barbara Schüpbach-Guggenbühl
studierte Jurisprudenz an den Universitäten von Basel und Neuchâtel. Von 2000 – 2004 war sie Geschäftsleiterin des Verfassungsrats des Kantons Basel-Stadt, anschliessend von 2004 – 2008 2. Ratssekretärin des baselstädtischen Kantonsparlaments. Seit 2009 ist sie Staatsschreiberin des Kantons Basel-Stadt und Leiterin der Staatskanzlei. Von September 2016 bis September 2022 präsidierte sie zudem die schweizerische Konferenz der Staatsschreiberinnen und -schreiber.

«Cyber Security muss 365 Tage im Jahr ein Thema sein!»

Mathias Bücherl
Chief Technology Officer
Axians IT Services AG
mathias.buecherl@axians.com

In der 1. Industrienacht der Regio Basel gehörte das IT/OT Security Operations Center (SOC) des ICT-Dienstleistungsunternehmens Axians in uptownBasel bei Arlesheim zu den meistbesuchten Attraktionen. In einer hochmodernen Kommandozentrale, die an diejenige des Raumschiffs Entreprise erinnert, sorgen hier hoch qualifizierte Informatikerinnen und Informatiker rund um die Uhr für den Schutz von Unternehmensnetzwerken vor Hackerangriffen. «tribune» hat dort den Mann getroffen, der für den Aufbau und den Betrieb dieses Zentrums mitverantwortlich zeichnet.

Mathias Bücherl, was ist Ihr Kerngeschäft als Chief Technology Officer?
Axians Cyber Security bietet sogenannte Managed Security Services an. In diesem Bereich überwachen und schützen wir Systeme nach dem Prinzip «Identify – Protect – Detect – Respond – Recover». Wir *identifizieren* Datenbestände und die Risiken, denen sie ausgesetzt sind. Dann fragen wir uns, wie die Daten *geschützt* werden müssen. Auf Stufe *Detect* sorgen wir dafür, dass wir schnellstmöglich merken, wenn ein Schaden droht. Dann wird reagiert – *Respond* –, und schliesslich geht es um die *Wiederherstellung* des Normalzustands. Wir bieten unseren Kunden so eine Rundummöglichkeit, sich zu schützen.

Was geht hier in diesem Raum vor?
Das SOC kümmert sich um die Bereiche Detect, Respond und Recover. Hier sammeln unsere Analystinnen und Analysten Daten aus den Unternehmensnetzwerken unserer Kunden. Sie sehen auf den Bildschirmen sofort, wo ein unvorhersehbares Ereignis eintritt und agieren dann wie die Piloten von Flugzeugen in einer aussergewöhnlichen Lage: Sie arbeiten eine Checklist ab, um die Störung zu beseitigen und den Normalzustand wieder herzustellen. Danach folgt die Aufarbeitung. Was ist passiert? Weshalb ist es dazu gekommen?

«Cyber Security ist in erster Linie ein Gedankenweg.»

Und wie kann das Unternehmen solche Zwischenfälle künftig verhindern? Das ist unser Job im SOC im Rahmen von Managed Services: Wir machen unsere Kunden sicherer in allen Belangen der Informatik und der Informationstechnologie.

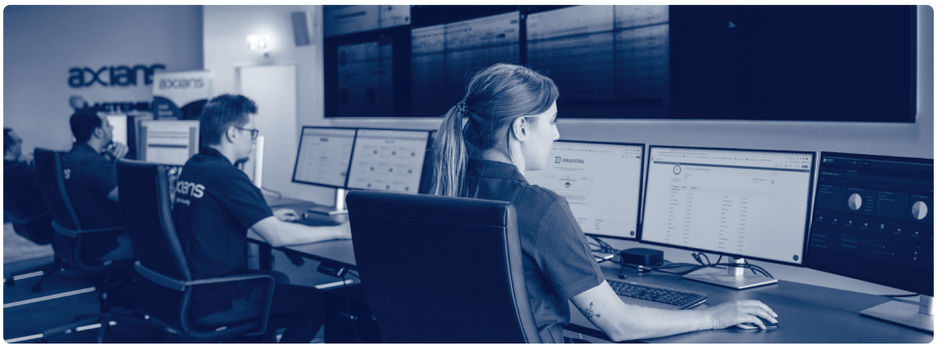
Beziehen die Kunden Sie von Anfang an mit ein? Oder werden Sie erst zu Hilfe gerufen, wenn «das Triebwerk schon brennt»?
Letzteres kommt leider sehr häufig vor. Dann übernimmt das Incident Management aus dem Bereich Response. Diese Feuerwehr rückt aus, im besseren Fall, wenn das Flugzeug noch in der Luft ist, und gibt den Piloten beziehungsweise den IT-Fachleuten der Kunden Anweisungen, wie es sicher gelandet werden kann. Im schlechteren Fall, wenn der Absturz Tatsache ist, setzen unsere Fachleute die noch vorhandenen Bruchstücke so gut wie möglich wieder zusammen und retten, was noch zu retten ist.

Welche Fehler führen hauptsächlich zu IT-Problemen in Unternehmen?
Das Internet und ganz speziell die E-Mail-Kommunikation sind Einfallstore in jedes System. Ungeschützt machen sie Angreifenden Datendiebstahl und Sabotageakte leicht. Mit dieser Tatsache beschäftigen sich viele Mitarbeitende kaum und leider auch Führungskräfte oft zu wenig. Sie wissen zwar um die Problematik, aber sie verschliessen die Augen, nicht selten, weil Sicherheit im Netz nicht gratis zu haben ist. Das Risiko wird unterschätzt – frei nach dem Motto «Uns kann das nicht passieren» – oder allenfalls an eine Versicherung delegiert. Ein Unternehmen muss aber nicht nur das Risiko erkennen – und ein solches ist immer da! – seine Führung muss es auch richtig einstufen und frühzeitig die richtigen Massnahmen einleiten. In dieser Verpflichtung sind Geschäftsführung und Verwaltungsräte. Wenn diese nach eingehender Prüfung zum Schluss kommen: «Okay – es gibt Cyberangriffe, aber ich akzeptiere das Risiko» – dann ist das ein mögliches «Mindset». Mit anderen Worten: Cyber Security ist in erster Linie ein Gedankenweg; erst danach eine technische Herausforderung.

Hat sich dieses Mindset in letzter Zeit verändert?
Der Geschäftsbereich Cyber Security wächst in der Tat, und dies sicher auch, weil die feindlichen Angriffe auf Netzwerke zunehmen. Das Umdenken ist in vollem Gang; in den letzten Jahren haben viele Unternehmen gemerkt und teilweise auch schmerzlich erfahren müssen, dass sie die Augen nicht mehr vor der Gefahr verschliessen und vor allem Security nicht länger mit Safety gleichsetzen können. Safety im Sinn von Betriebssicherheit steht bei allen Unternehmen zuoberst auf der Checklist, weil sie wissen: Eine

Über Axians

Axians ist die globale Marke für ICT von VINCI Energies und beschäftigt 12'500 Spezialistinnen und Spezialisten in 27 Ländern weltweit. Axians Schweiz ist ein agiles Unternehmensnetzwerk aus spezialisierten ICT-Dienstleistern und Softwareherstellern an über 20 Standorten in allen Schweizer Sprachregionen. Das IT/OT Security Operations Center (SOC) von Axians befindet sich im neuen Kompetenzzentrum für Industrie 4.0 «uptown Basel» am Schorenweg in Arlesheim.



unsachgemäss installierte oder bediente Stanzmaschine kann einen Menschen seinen Arm kosten. Im Cyber Security-Bereich fehlt dieses Verständnis häufig. Ein Netzwerkkabel sieht halt nicht so gefährlich aus wie eine Kreissäge, aber es kann eine ganze Produktion lahmlegen. Und während der Safety-Punkt nach der sicheren Installation der Maschine und der Abgabe von Helmen ans Personal meist abgehakt werden kann, ist Cyber Security nie erledigt.

Was können Ihre Spezialisten retten, wenn nichts mehr geht in einem Firmennetz?
Das ist stark abhängig davon, wie das Unternehmen auf einen solchen Fall vorbereitet ist. Das nennen wir Business Continuity Management beziehungsweise Desaster Recovery. Da geht man zum Chef und fragt: «Hast du diese Pläne? Ist dir bewusst gewesen, dass das passieren kann?» Viele Unternehmen machen zwar Backups, aber sie testen sie nicht. Oder sie haben keine Dokumentation erstellt und alles Wissen ist ausschliesslich im Kopf einer einzelnen IT-Fachkraft abgespeichert. Ein solcher Wiederaufbauprozess ist um vieles leichter, wenn sich jemand schon vorher Gedanken darüber gemacht hat. Sonst wird die Bewältigung eines solchen Desasters schwierig bis unmöglich. Vor diesem Fall stehen wir oft im Bereich Cyber Security. Und da möchte ich an die Unternehmen appellieren: Es ist weder ein extrem schwieriges noch ein komplexes technisches Thema. Aber man muss sich ihm öffnen und sich mit ihm befassen.

Wie sieht die Interaktion zwischen den Angreifern und Ihnen als Verteidiger aus?
Das ist ein ständiges Wettrüsten. Wir auf unserer Seite halten uns über Taktiken und Techniken der Angreifenden auf dem Laufenden, auch mit Mitteln der künstlichen Intelligenz. Weiter stellen wir sogenannte «Honeypots» in ein Netzwerk; das sind Systemteile, die viele Schwachstellen aufweisen. Mit einem solchen Honigtopf provozieren wir einen Angriff auf ein System, das natürlich isoliert ausserhalb des Unternehmens liegt, damit nichts passieren kann. So lernen wir die Methoden der Angreifer kennen und merken, wenn sich ein Ernstfall anbahnt. Eine weitere Möglichkeit ist die Analyse von bereits erfolgten Angriffen auf andere Unternehmen; da tauschen wir uns regelmässig mit anderen Spezialisten aus.

> «Auch unsere Branche leidet unter einem Mangel an Fachkräften.»

Gibt es die einhundertprozentige Sicherheit im Cyber-Space?
Nein. Was vom Menschen geschaffen wird, ist fehlerhaft und angreifbar. Es gibt 365 Tage im Jahr neue und andere Möglichkeiten, ein IT-System anzugreifen. Kein Spezialist und schon gar kein Laie kann also sagen, dass der Cyber Security-Job für dieses Quartal erledigt sei und das Thema in zwölf Monaten wieder auf die Traktandenliste komme. Wer aber sein Mindset justiert und erkannt hat, dass Cyber Security eine 365-Tage-im-Jahr-Aufgabe ist, der kommt mit seiner IT-Sicherheit nahe an die 100 Prozent heran.

Gibt es genügend Spezialisten, die sich auf diese komplexen Aufgaben verstehen?
Auch unsere Branche leidet unter einem Mangel an Fachkräften. Das hat auch damit zu tun, dass man ein Konzept zuerst von Grund auf verstehen muss, bevor es sicherer gemacht werden kann. Mit anderen Worten: Cyber Security ist eine zusätzliche Stufe der Ausbildung. Deshalb bleiben viele Nachwuchsinformatiker bei der Anwendungsentwicklung. Sie haben ein abgeschlossenes Studium und eine Stelle in einem gut bezahlten Beruf auf sicher: Weshalb soll sich da einer – oder eine – noch ein weiteres Studium obendrauf packen? Apropos «eine»: In der Informatik finden wir gerade einmal 14 Prozent Frauen. Bei der Personalrekrutierung setzen wir daher stark auf Diversität, nicht nur was das Geschlecht betrifft. Wir akquirieren auch talentierte und motivierte Leute aus völlig fachfremden Gebieten. Nicht selten finden wir dabei Köpfe, die «out of the box» denken können und völlig neue Ideen einbringen.

Vielen Dank, Herr Bücherl, für dieses Gespräch.

Interview: Roger Thiriet

Mathias Bücherl
ist Chief Technology Officer von Axians IT Services AG. Er verfügt über langjährige Erfahrung im Bereich Managed Cyber Defense und Security Operation und hat in dieser Eigenschaft das Security Operations Center von Axians in Basel/Arlesheim aufgebaut. Neben seinem beruflichen Engagement ist er als Dozent für Cyber Security an der Hochschule Luzern und der Dualen Hochschule Baden-Württemberg DHBW in Stuttgart tätig.

Digitale Identifikation

Im World Wide Web finden sich zu allen drei Themenkomplexen der vorliegenden «tribune» zahlreiche Informationen.

Digitale Signatur
Wer Dokumente digital signieren möchte, braucht in erster Linie eine entsprechende Software für seine elektronischen Devices. Am mangelnden Angebot in diesem Bereich kann es nicht liegen, dass die digitale Unterschrift die Geschäftswelt erst zögernd erobert. Aus der langen Liste von Anbietern im Netz hier drei Links zu Seiten mit weiterführenden Informationen und Software-Angeboten.

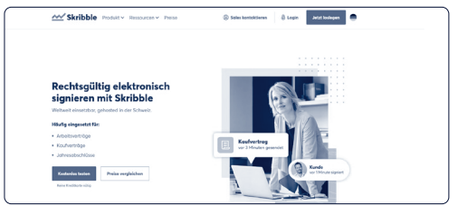
- Easy Software
  www.easy-software.com
- Adobe Sign
  www.adobe.com/ch_de/sign
- Skribble
  www.skribble.com

E-Voting
Auch zum Thema E-Voting haben die Stellen, die sich vertieft mit der Entwicklung und der Förderung des Abstimmens und Wählens auf elektronischem Weg befassen, einiges publiziert. Hier drei Links zu entsprechenden Hintergrundinformationen aus Bund und Kantonen sowie der Schweizer POST.

- Bundesverwaltung
  www.bk.admin.ch/bk/de/home/politische-rechte/e-voting/ueberblick.html
- DIE POST
  www.post.ch/de/geschaeftsloesungen/e-voting
- Basel-Stadt
  www.digitale-mitbestimmung.bs.ch

Cyber Security
Dass Sicherheit eines der ganz grossen Themen im Cyber Space ist, verwundert nicht. Auf nationaler Ebene befassen sich unter anderem folgende Sites der Bundesverwaltung, der Stiftung digitalswitzerland und der Schweizerischen Bankiervereinigung vertieft mit dem Thema:

- Nationales Zentrum für Cybersicherheit NCSC
  www.ncsc.admin.ch/ncsc/de/home.html
- Verband und Stiftung digitalswitzerland
  www.digitalswitzerland.com
- Schweizerische Bankiervereinigung
  www.swissbanking.ch/de/themen/digitalisierung-innovation-cyber-security
- Handelskammer beider Basel
  www.be-digital-basel.ch/angebote/cyber-security-checkup/



Fotos/Bilder: Seite 3: https://www.youtube.com/watch?v=HhV2082VhPA; Seite 5: Video der Bundeskanzlei: https://www.youtube.com/watch?v=qTzZXI-z7b8

AZB
CH-4010 Basel
P.P. / Journal
Post CH AG

tribune

IMPRESSUM Nummer 4/2022, erscheint viermal jährlich.

HERAUSGEBER: Handelskammer beider Basel (info@hkbb.ch), Advokatenkammer Basel, Basellandschaftlicher Anwaltsverband (maier@svwam.ch) grosszügig unterstützt von der Jubiläumsstiftung La Roche & Co
REDAKTION: Dr. Philip R. Baumann, lic. iur. Roman Felix, Dr. iur. Alexander Filli,
lic. phil. I Jasmin Fürstenberger, MLaw Andrea Tarnutzer-Münch, lic. phil. I Roger Thiriet
LAYOUT: Elmar Wozilka, Handelskammer beider Basel, Druck: bc medien ag, Münchenstein
gedruckt in der Schweiz
ADRESSE: «tribune», St. Jakobs-Strasse 25, Postfach, 4010 Basel,
Telefon: +41 61 270 60 55, Telefax: +41 61 270 60 05, E-mail: info@hkbb.ch
«tribune» ist eine offizielle Publikation der herausgebenden Organisationen für deren Mitglieder.
Der Abonnementspreis ist im Mitgliederbeitrag inbegriffen. Für Nichtmitglieder kostet das Jahresabonnement CHF 20.–.