ti&m special

Digital Trust 2024

Wie digitalisiert man Vertrauen?

Thomas Wüst, CEO und Gründer der ti&m AG

Liebe Leserin Lieber Leser

Digital Trust, also Vertrauen im digitalen Raum, ist das Thema des vorliegenden ti&m special. Um den Wert von Vertrauen in einer digitalen Welt zu verstehen und zu bemessen, müssen wir uns nur vor Augen halten, dass Vertrauen die Basis jeglicher sozialen und wirtschaftlichen Interaktion ist – seit jeher und von unserem ersten Lebenstag an. Ob in der Familie, im Freundes- oder Kollegenkreis – Vertrauen entsteht aus einer Mischung aus Emotionen, Verhaltensmustern und Regeln, die die Qualität einer solchen Interaktion bestimmen.

Als Teil eines Systems, wie z. B. einem Unternehmen oder sogar einem Staat, baut man wiederum Vertrauen zu anderen Systemen auf. Dieses Vertrauen basiert auf den gleichen oben aufgeführten Komponenten – Emotion, Verhalten, Regeln – wobei die Gewichtung sich von der Emotion immer weiter in Richtung Regeln verschiebt, je grösser und anonymer das System wird.

Digitale Transaktionen sind emotionslos

Eine digitale Basistransaktion kennt nun aber keine Emotionen oder moderierende Massnahmen. Das heisst, Vertrauen basiert hier ausschliesslich auf Regeln und dem Wissen, dass diese Regeln auch eingehalten werden. Eine digitale Transaktion enthält genau drei Komponenten, die durch digitale Technologien und Protokolle realisiert werden müssen:

1. *Wer ist mein Gegenüber?*
2. *Sind die empfangenen Informationen auch genau die, die versendet wurden?*
3. *Kann ich zu dieser Transaktion verbindlich meine Zustimmung geben?*

Diese drei Komponenten sind dann auch genau diejenigen, in denen in den letzten Jahren auf dem Weg vom Informations- zum Transaktions-Internet die grössten Entwicklungen zu verzeichnen sind und die z. B. von der Europäischen Union in ihrer eIDAS-Verordnung vorangetrieben werden. Von der Online-Identifikation und der Herausgabe einer robusten und sicheren digitalen Identität über digitale Siegel bis hin zur digitalen Signatur sind hier vertrauensbildende Lösungen entstanden und werden weiterhin entwickelt. Effektive Krypto-Algorithmen, aber auch neue Usability-Ansätze machen die Kommunikation, die Daten und damit die digitalen Transaktionen immer sicherer und fördern die Akzeptanz beim Benutzer. Der Übertrag von digitalen Werten ohne Intermediäre wurde durch die Blockchain-Technologie möglich, womit ein wichtiger Baustein für das von einigen bis anhin nur erträumte Metaverse geschaffen wurde.

Die Herausforderungen wachsen mit der technischen Entwicklung

Trotzdem sind wir noch weit entfernt von einer jederzeit sicheren und vertrauenswürdigen digitalen Welt. Eine wirklich sichere, die Bürgerinnen und Bürger und ihre Daten respektierende digitale Identitätslösung ist weltweit immer noch die Ausnahme (die Schweiz ist mit ihrem derzeitigen Entwurf zur E-ID sicher auf einem guten Weg). Die künstliche Intelligenz stellt uns vor ganz neue Vertrauensfragen: Wenn wir nicht einmal mehr theoretisch nachvollziehen können, wie Aussagen entstehen und Entscheidungen gefällt werden, wie sollen wir darauf vertrauen, was wahr ist oder fake? Und was passiert, wenn in sechs bis zehn Jahren die neuen Quantencomputer unsere gesamte Krypto-Maschinerie in Frage stellen? Wie gehen wir als Organisationen mit der stetig wachsenden Menge an Daten um, so dass wir ein (ebenfalls ständig wachsendes) Regelwerk einhalten und trotzdem den Wert dieser Daten konstruktiv nutzen? Und wie bereiten wir all diese neuen Technologien und daraus resultierenden Anwendungsfälle so auf, dass sehr breite Benutzergruppen daraus einen Nutzen ziehen können?

Daran arbeiten wir bei ti&m

Genau diese multidisziplinären Herausforderungen sind es, die uns als Beraterin, Designer und Ingenieurin bei ti&m motivieren und antreiben. So sind wir mit unserer Mobile- und E-Banking-Lösung und unserer patentierten Online Identification im sensitiven Bankenumfeld mit führenden Produkten am Markt. Gemeinsam mit Swisscom haben wir mit «Swisscom Sign» den De-Facto-Standard in der Schweiz

bei der qualifizierten elektronischen Signatur (QES) entwickelt. Und unsere 2-Faktor-Authentisierungslösung ermöglicht bereits seit vielen Jahren zahlreichen Kunden einen benutzerfreundlichen und sicheren Zugang zu den digitalen Dienstleistungen unserer Bankenkunden. Diese Angebote sind wichtige Bestandteile unseres umfassenden «Digital Trust Frameworks», welches sich von Governance und Beratungsthemen wie Information Security Risk Management, Self Sovereign Identity oder Compliance & Ethics über Produkt- und Servicekomponenten wie Onboarding, MFA und Signing bis hin zum SOC-/SIEM-as-a-Service und IT-Grundschutz im Bereich der Managed Services erstreckt. Mit dem ständigen Ausbau dieses Frameworks adressieren wir das Thema «Digital Trust» auf allen Ebenen unserer Wertschöpfungskette – ganz wie Sie es vom Partner Ihres Vertrauens in der digitalen Transformation erwarten dürfen.

Ich lade Sie ein, über diese und weitere Lösungen mit uns ins Gespräch zu kommen. Und es sind natürlich wieder die zahlreichen Artikel von kompetenten Autorinnen und Autoren aus der Praxis und aus der Forschung, die uns neue und vielfältige Perspektiven auf das Thema «Digital Trust» eröffnen. Ich hoffe, Sie geniessen die Lektüre und bekommen interessante Anregungen für Ihre tägliche Arbeit.

Mit vertrauensvollen Grüssen,

Thomas Wüst

Herausgeber: ti&m AG, Buckhauserstrasse 24, 8048 Zürich, Schweiz
Publikation: ISSN 2235-7971
Redaktion: Thomas Wüst, Leunita Saliji, Pascal Wild, Mathias Liechti
Gestaltung/Produktion: ti&m AG **Auflage:** 1'500 Exemplare
Druck und Distribution: Multicolor Print AG

Lesen Sie weitere spannende Artikel zum Thema «Digital Trust» online in unserem Blog!

Lukas Ruf, Group CISO, Migros-Genossenschafts-Bund

Gregor Hofer, Leiter Fähigkeitsentwicklung Cyber Raum, Schweizer Armee

Dominika Blonski, Datenschutzbeauftragte des Kantons Zürich

ti8m.com/blog

Digitale Innovation durch Vertrauen stärken

Digital Trust // In der heutigen Ära der allgegenwärtigen digitalen Transformation kann die Bedeutung von Vertrauen nicht hoch genug eingeschätzt werden. Durch die Priorisierung sicherer und geschützter Technologien sowie einer verantwortungsvollen Governance können wir eine vertrauenswürdigere digitale Landschaft schaffen.

Jüngste Umfragen von KPMG und die öffentliche Debatte zeigen eine weit verbreitete Skepsis gegenüber künstlicher Intelligenz und anderen Technologien. 61 Prozent der Befragten gaben an, dass sie künstlichen Intelligenzsystemen misstrauen. Je nach Land lag der Anteil der KI-Skeptiker bei bis zu 84 Prozent (Finnland). Der daraus resultierende Rückgang von Digitalisierungsprojekten und der Technologieakzeptanz wirft die Frage auf: *Wie können wir digitales Vertrauen gewinnnen und aufrechterhalten?*

Ebenso sehen sich Unternehmen und staatliche Organisationen mit Bedenken externer Stakeholder wie Kunden, Geschäftspartnern und Regulierungsbehörden sowie interner Stakeholder wie Mitarbeitenden, Risiko- und Compliance-Spezialistinnen und -Spezialisten oder dem Verwaltungsrat bezüglich der Risiken ihrer KI-Systeme konfrontiert. Typischerweise beziehen sich die Bedenken auf Fairness, Genauigkeit, Sicherheit, Datenschutz und Compliance. Die Folgen sind verzögerte oder sogar gescheiterte Innovationsprojekte, längere Markteinführungszeiten und eine langsame Akzeptanz neuer Technologien.

Diese Skepsis beschränkt sich nicht nur auf KI und ist kein neues Phänomen. Bspw. hat die Schweiz vor wenigen Jahren das E-ID-Gesetz abgelehnt, weil die Öffentlichkeit der Technologie und der Art und Weise, wie sie eingesetzt und betrieben werden sollte, nicht vertraute. Bedenken hinsichtlich Datenschutz und Transparenz wurden vor und nach der öffentlichen Abstimmung intensiv diskutiert. Ist dieses mangelnde digitale Vertrauen gerechtfertigt? Man könnte dies angesichts der hohen Anzahl an gemeldeten Problemen hinsichtlich der Zuverlässigkeit digitaler Systeme sowie der hohen Anzahl der in der Schweiz und im Ausland erscheinenden Medienberichten annehmen.

Warum Digital Trust wichtig ist

Wenn unsere Brücken mit der gleichen Qualität gebaut würden wie einige der digitalen Produkte und Dienstleistungen, die uns Nutzerinnen und Nutzern präsentiert werden, würden wir diese nicht überqueren. Sie würden zu wackelig und unsicher aussehen. Leider geniessen digitale Bastlerinnen und Bastler, die diese unzuverlässigen Produkte und Dienstleistungen entwickeln, allzu oft einen Wettbewerbsvorteil, da sie scheinbar die erwartete Funktionalität und Features zu einem niedrigeren Preis und/oder mit kürzerer Markteinführungszeit liefern, während sie bei Sicherheit und anderen Qualitätsaspekten Abstriche machen.

Allzu oft werden wir uns als Konsumentinnen und Konsumenten dieser Abstriche erst bewusst, wenn das Äquivalent zu einer einstürzenden Brücke aufgetreten ist – typischerweise begleitet von einer Mitteilung des verantwortlichen Unternehmens oder der öffentlichen Einrichtung, dass dieser Vorfall überraschend kommt.

Dies ist kein nachhaltiger Ansatz. Das Vertrauen der Kunden, Geschäftspartner, Regulierungsbehörden und der Öffentlichkeit zu gewinnen und aufrechtzuerhalten, wird zunehmend wichtig für den Erfolg digitaler Produkte und Dienstleistungen und die Akzeptanz neuer Technologien im Allgemeinen.

Was ist Digital Trust?

In einem kürzlich in Zusammenarbeit mit dem WEF[1] verfassten Bericht hat KPMG digitales Vertrauen wie folgt definiert: Digital Trust ist die Erwartung, dass digitale Technologien und Dienstleistungen und die Organisationen, die sie bereitstellen, die Interessen aller Beteiligten schützen und gesellschaftliche Erwartungen und Werte wahren. Die zwei Schlüsselkomponenten des digitalen Vertrauens:

1. Sichere und geschützte Technologien, widerstandsfähige Infrastrukturen

Digitale Produkte und Dienstleistungen müssen auf einem soliden Fundament basieren, das sicherstellt, dass Daten vertraulich bleiben und nicht manipuliert werden können; dass Produkte und Dienstleistungen den Nutzerinnen oder Nutzern oder der Umwelt keinen Schaden zufügen; und dass Produkte und Dienstleistungen widerstandsfähig gegen störende Ereignisse sind, einschliesslich menschlicher Fehler, (Cyber-)Angriffe usw.

2. Verantwortungsbewusste Nutzung

Jede Technologie, sei es ein Messer oder ein digitales System, kann zum Guten oder zum Schlechten verwendet werden. Daher ist es entscheidend, dass digitale Produkte und Dienstleistungen unter einer Governance bereitgestellt werden, die sicherstellt, dass die Nutzerinnen und Nutzer verantwortungsvoll bedient werden, d. h. aufrichtig, ethisch und transparent.

Ein Differenzierungsmerkmal für digitale Produkte und Dienstleistungen «Made in Switzerland»?

Vertrauenswürdigkeit sollte als Qualitätsmerkmal behandelt werden und kann als Differenzierungsmerkmal für Produkte und Dienstleistungen dienen. Viele erfolgreiche Schweizer Unternehmen in verschiedenen Branchen haben dies erkannt und rechtfertigen damit ihre Premium-Preise. Allerdings bedeutet die Tatsache, dass ein Produkt oder eine Dienstleistung «Swiss made» ist, nicht unbedingt, dass es vertrauenswürdig ist. Insbesondere für digitale Produkte und Dienstleistungen gibt es mehr als genug Fälle, die das Gegenteil bewiesen haben und in die Medien gelangt sind. Um das Vertrauen der Nutzerinnen und Nutzer zu gewinnen und nachhaltig davon zu profitieren, sollten Entwickler und Anbieter digitaler Produkte und Dienstleistungen einen aktiven Ansatz verfolgen:

Digitale Produkte und Dienstleistungen sollten bereits ab der Designphase („trustworthiness-by-design") mit Vertrauenswürdigkeit im Hinterkopf und konkreten Anforderungen an Sicherheit, Zuverlässigkeit, Verantwortlichkeit, Aufsicht sowie einer ethischen und verantwortungsvoller Nutzung entwickelt werden.

Vertrauenswürdige digitale Produkte und Dienstleistungen sollten durch das Engagement und die Kommunikation mit den Stakeholdern entwickelt und betrieben werden. Der Nachweis der eigenen Ansprüche kann erbracht werden, indem Produkte und Dienstleistungen von sachkundigen, unabhängigen Dritten überprüft werden. Dies kann die Einhaltung von Standards und bewährten Verfahren in Form von Zertifikaten und SOC-2-Bescheinigungen umfassen, die von vertrauenswürdigen Organisationen ausgestellt werden.

Die Entwickler und Anbieter solcher Produkte und Dienstleistungen sollen auch von ihren ***Lieferanten und Ökosystemen*** dieselben hohen Standards einfordern.

Das Wissen und das Verständnis von Käufern und Beschaffungsorganisationen sowie von Gesetzgebern und der breiten Öffentlichkeit sollte gefördert werden. Branchenverbände können hierbei eine wichtige Rolle spielen.

Unsere Entscheidungen bestimmen, ob Digital Trust die Aufmerksamkeit erhält, die sie verdient

Als Käufer und Verbraucher digitaler Produkte und Dienstleistungen sind unsere Entscheidungen entscheidend, um den Übergang zu einer vertrauenswürdigeren digitalen Umgebung zu unterstützen und zu beschleunigen. Wir müssen unter die Motorhaube schauen, um Anbieter und Entwickler herauszufordern und Digital Trust zu einem Teil unserer Anforderungen bei der Beschaffung oder dem Nutzen digitaler Dienstleistungen und Produkte zu machen. Oft müssen wir bereit sein, dafür einen anfänglichen Aufpreis zu zahlen, aber diese Investition kann sich schneller als erwartet auszahlen: In Form einer beschleunigten Markteinführung, reibungsloserer Projektabwicklung und geringeren Kosten bei der Bewältigung von Vorfällen.

Letztendlich liegt es in der Verantwortung von uns allen, die Transparenz einzufordern, die notwendig ist, um informierte Entscheidungen zu treffen. Wir sollten Dienstleistungen und Produkte von denjenigen Organisationen und Technologie-Ökosystemen kaufen und konsumieren, die in der Lage sind aufzuzeigen, dass sie unser Vertrauen verdienen. ●

Dr. Matthias Bossardt

Leiter Cyber & Digital Risk Consulting und Partner, KPMG Schweiz

Als Partner und Leiter des Cyber & Digital Risk Consulting bei KPMG Schweiz berät Matthias Bossardt seine Kunden im vertrauenswürdigen, verantwortungsvollen und sicheren Umgang mit Daten und digitalen Technologien.
Er ist Mitglied des globalen Trusted AI Steering Committee von KPMG. Er leitete die Arbeitsgruppe Cybersecurity von economiesuisse und ist Mitglied des Cyber Advisory Board der Schweizerischen Akademie der Technischen Wissenschaften (SATW).
2016 wurde er von der Bilanz zu einem der 100 einflussreichsten Digital Shapers der Schweiz gewählt. ***kpmg.com***

1 https://www3.weforum.org/docs/WEF_Earning_Digital_Trust_2022.pdf

Macht DeFi Banken als Intermediäre obsolet?

Decentralized Finance // Ein stabiles, funktionierendes Finanzsystem ist essenziell für Wirtschaft und Wohlstand. Bisher haben die Banken eine entscheidende Rolle darin übernommen. Bleibt das so?

Das Finanzsystem sorgt dafür, dass die verschiedenen Marktteilnehmer an ihr Geld kommen: Privatpersonen möchten Geld sparen oder anlegen; Unternehmen benötigen Eigen- oder Fremdkapital, um ihre Produktion auszubauen. Auch der Staat ist ein wichtiger Marktteilnehmer, sei es als Anleger oder Kreditnehmer. Wie wichtig das Vertrauen in ein funktionierendes Finanzsystem ist, zeigt sich, wenn es nicht mehr da ist. Die negativen Auswirkungen von Finanzkrisen auf die Realwirtschaft, bspw. durch den Rückgang von Investitionen, können schwerwiegend sein und es kann lange dauern, bis das Vertrauen wieder hergestellt ist. Oftmals braucht es zusätzliche vertrauensbildende Massnahmen in Form staatlicher Garantien und Krediten oder von Regulierung. Die Allokation von Geld erfolgt auf verschiedene Arten, wobei Banken und Börsen die traditionellen Kanäle darstellen. Ergänzend bieten Peer-to-Peer-Plattformen und Decentralized Finance (DeFi) vergleichsweise neuartigere Alternativen.

Banken und Börsen

Banken bringen Anleger (oder Kreditgeber) und Kreditnehmer zusammen und führen verschiedene Funktionen wie die Fristen- und Grössentransformation aus. Dabei werden typischerweise kurzfristige und kleine Anlagen in langfristige und grössere Kredite transformiert. Zusätzlich dienen Banken als Risikopuffer zwischen Kreditnehmern und Kreditgebern. Das heisst, dass bei einem Ausfall des Kredites der Verlust bei der Bank und nicht beim Anleger liegt. Damit Banken diese Risiken tragen können, müssen sie ihre Geschäfte mit Eigenmitteln unterlegen und unterstehen spezifischen Regulierungen. Zu Problemen kommt es, wenn Anleger das Vertrauen in eine Bank verlieren und ihr Geld abheben möchten, da die Bank durch die Fristentransformation nicht fähig ist, alle Forderungen sofort zu begleichen. Diese «Bank Runs» können zu einer Kettenreaktion im Finanzsystem führen: Die Insolvenz einer Bank kann bei anderen Finanzdienstleistern zu negativen Konsequenzen führen, was sich wiederum auf andere Finanzdienstleister sowie Kundinnen und Kunden auswirkt. Diesen Dominoeffekt gilt es zu verhindern.

Auch Börsen sind wichtige Knotenpunkte im Finanzsystem. Sie bieten einen zentralen Markt, wo Geld beispielsweise in Form von Eigenkapital (Aktien) oder Fremdkapital (Obligationen) transferiert wird. Börsen ermöglichen es Anlegern, bspw. in Unternehmen zu investieren, und unterstützen so den Kapitalfluss in der Wirtschaft. Dabei findet keine eigentliche Fristen- oder Risikotransformation statt. Börsen sind üblicherweise reguliert, was auf die Anleger vertrauensfördernd wirkt. Allerdings bleiben die Risiken gegenüber dem Emittenten beim Anleger. Börsen und die entsprechenden Clearing- und Settlement-Infrastrukturen werden häufig unter dem Begriff Finanzplatzinfrastruktur zusammengefasst, die ebenfalls einer speziellen Regulierung und Aufsicht untersteht.

Peer-to-Peer-Plattformen

Peer-to-Peer-Plattformen bieten eine Alternative zu traditionellen Finanzierungswegen wie Banken und Börsen, indem sie Kapitalsucher direkt mit Kapitalgebern verbinden. Sie sind für Kapitalsucher wie bspw. Firmen einfacher zugänglich als Börsen und eignen sich besonders für die Aufnahme kleinerer Beträge. Anleger können direkt investieren, ohne die Nutzung von kostenpflichtigen professionellen Brokerdienstleistungen in Anspruch zu nehmen. Die nicht oder weniger regulierten Peer-to-Peer-Plattformen sind volumengemessen insgesamt weniger bedeutend als die traditionellen Börsen und vor allem im Primärmarkt und weniger im Sekundärmarkt tätig.

Ähnlich wie bei Banken und Börsen ist es auch bei Peer-to-Peer-Plattformen essenziell, dass Anleger und Kreditnehmer auf die Integrität der Betreiber vertrauen können. Diese müssen gewährleisten, dass Transaktionen fair und transparent ablaufen und dass die sichere Verwahrung der Mittel sichergestellt ist.

Decentralized Finance (DeFi)

Die Verschmelzung des traditionellen Finanzwesens mit der Distributed-Ledger-Technologie (Blockchain) wird häufig unter dem Begriff «Decentralized Finance» zusammengefasst. DeFi zielt unter anderem darauf ab, traditionelle Finanzdienstleistungen ohne zentrale Vermittlungsinstanzen wie Banken, Börsen oder Peer-to-Peer-Plattformen anzubieten. Anleger und Kreditnehmer transferieren ihre Finanzmittel also direkt und selbstständig über eine Blockchain. Die angebotenen Produkte und Dienstleistungen basieren dabei auf intelligenten Verträgen, sogenannten Smart Contracts, wo definierte Regeln automatisch und autonom durchgesetzt werden. Diese Regeln werden auf der Blockchain gespeichert, was ein Paradigmenwechsel in Bezug auf das Vertrauen in entsprechende Finanztransaktionen mit sich bringt: Während im traditionellen Finanzwesen das Vertrauen in die Funktion der zentralen Institutionen wie Banken, Börsen oder Peer-to-Peer-Plattformen im Vordergrund steht, basiert das Vertrauen in DeFi-Systeme auf der Sicherheit und Transparenz der zugrunde liegenden Blockchain-Technologie.

Braucht es in Zukunft noch Banken?

Banking oder Finanzdienstleistungen als regulierte, risikotragende Intermediäre nehmen wichtige Funktionen für die Realwirtschaft ein und wird es wahrscheinlich auch in Zukunft aus folgenden zwei Gründen geben:

1. *Banken, zentrale Plattformen und Märkte gab es auch in der Vergangenheit in Koexistenz. DeFi stellt eine weitere Möglichkeit zur Allokation von Finanzmitteln dar, wird die bestehenden Systeme aber wahrscheinlich nicht ablösen, sondern sie ergänzen. Durch DeFi erhalten die Anleger und Kreditnehmer für gewisse Finanzprodukte und -dienstleistungen eine Alternative zu den traditionellen Kanälen und werden basierend auf ihren Präferenzen und ihrem Vertrauen das entsprechende Angebot auswählen. Es sind auch nicht alle Produkte und Dienstleistungen auf allen Kanälen verfügbar.*

2. *Nicht alle Teilnehmer wollen und können alle ihre Finanztransaktionen selbständig auf der Blockchain durchführen und brauchen Unterstützung. Diese Unterstützung suchen sie teilweise wiederum bei Banken, die als vertrauenswürdige Intermediäre agieren und dabei sowohl traditionelle als auch Blockchain-basierte Finanzdienstleistungen anbieten können. Auch gibt es Mischformen wie zum Beispiel zentrale Börsen auf der Blockchain.*

Traditionelle Finanzintermediäre werden wohl auch in Zukunft das Vertrauen von Kundinnen und Kunden geniessen. Allerdings: Es gibt eine (wachsende) Gruppe von Personen, die die Transparenz, Effizienz und Autonomie der Blockchain schätzen und der Technologie grösseres Vertrauen entgegenbringen als dem etablierten und regulierten Finanzsystem. ●

Thomas Ankenbrand

Head of the Competence Center for Investments, IFZ

Thomas Ankenbrand hat ein Lizenziat der HSG und einen Doktortitel der Universität Lausanne. Derzeit forscht er im Bereich FinTech und Investment Management an der Hochschule Luzern. Zu seinen Schwerpunkten gehören die Anwendung von KI, Agent based Modeling (ABM), Decentralized Finance (DeFi) und Quantum Computing in Finanzmärkten.

Denis Bieri

Dozent, IFZ

Denis Bieri hat an der Universität Basel promoviert und ist derzeit Dozent an der Hochschule Luzern. Sein Forschungsschwerpunkt liegt im Bereich der Finanzdienstleistungen, mit speziellem Fokus auf Finanztechnologien (FinTech).

hslu.ch/ifz

Krypto als Wegbereiter von Digital Trust

Dr. Luka Müller

Mitgründer MME und Sygnum Bank AG

Dr. Luka Müller ist Experte in den Bereichen FinTech und RegTech, Gründungspartner von MME sowie Mitgründer und Verwaltungsratspräsident der Sygnum Bank AG. Zudem ist er Mitgründer der daura AG und der KYC Spider AG, die sich mit digitalen Assets, Share Tokenisation und Digital Compliance beschäftigen.

mme.ch / sygnum.com

Distributed Ledger // Kryptowährungen werden oft im Kontext von Spekulation und Geldwäscherei erwähnt. Die zentrale Bedeutung der ihr zugrunde liegenden Technologie für vertrauenswürdige digitale Informationen und Funktionen (Digital Trust) geht dabei verloren. Ein Blick in die Geschichte des Wertpapiers veranschaulicht die Bedeutung des Standes der Technik für die Entwicklung der Form und der Rechtskonzepte von vertrauenswürdigen Informationen von der Urkunde bis hin zu Digital Trust.

Schon im Imperium Romanum waren Urkunden beliebt, um rechtsverbindliche Inhalte festzuhalten. Eine Urkunde belegt die Echtheit und die Richtigkeit des Inhaltes auf Papier. Nach dem damaligen Stand der Technik bestand dieser Träger aus Pergament und später aus Papier. Mit der Zunahme des Handels im späten Mittelalter wuchs das Bedürfnis nach einer weiteren Funktion der Urkunde. Mit ihr sollte ein Recht nicht nur verbindlich festgehalten, sondern auch mobilisiert werden: Durch Übergabe einer Urkunde von Person zu Person (peer to peer). Es entwickelte sich das Konzept des Wertpapiers.

Nach dem heute noch geltenden schweizerischen Rechtsverständnis ist ein Wertpapier eine Urkunde, mit der ein Recht derart verknüpft ist, dass es ohne die Urkunde weder geltend gemacht noch übertragen werden kann. Der Besitz des Papiers ist Ausweis für die Geltendmachung des Rechts und die Übertragung des Besitzes ist die Voraussetzung für die Übertragung des Rechts.

Zentrale Rechner und das Vertrauen in deren Betreiber

Die Verbreitung des Wertpapieres begann im 16. Jahrhundert und erlebte eine erste Blüte anfangs des 20. Jahrhunderts. Millionen von Urkunden mussten physisch eingelagert und ausgetauscht werden. Bald zeigten sich die Grenzen der Mobilisierungsfunktion des Wertpapiers. So gründeten Schweizer Banken 1970 ein Gemeinschaftsunternehmen, die Schweizerische Effekten-Giro AG (SEGA – Vorgängerin der heutigen SIX Group AG), zur zentralen Verwahrung der physischen Aktienzertifikate. Bei dieser sogenannten mediatisierten Wertpapierverwahrung musste der Titel zur Übertragung des Rechts fortan nicht mehr physisch geliefert werden. Das Wertpapier wurde durch die Verwahrung immobil gemacht und die Übertragung des Rechts erfolgte nur noch mittels Gutschriften (Buchungen). Diese Buchungen wurden mit der fortschreitenden Digitalisierung auf den zentralen Rechnern von Banken und Verwahrern erfasst. Es wurde der erste Grundstein für das digitale Erfassen, Halten und Übertragen eines Rechtsanspruches gelegt. Eine zentrale digitale Datenbank war und ist heute noch der «Gralshalter» für die Urform von Digital Trust.

Die Bedeutung des Standes der Technik

Die Geschichte des Wertpapiers ist geprägt vom Bemühen der Marktteilnehmer und des Gesetzgebers, das Eigentum am Papier und das damit verknüpfte Recht zivilrechtlich bestmöglich zu schützen und gleichwohl eine sichere Übertragung auch bei hohen Volumen und vielen Marktteilnehmern sicherzustellen. Dabei sind die im Verlauf der Zeit entwickelten Rechtskonzepte immer auch im Kontext des jeweiligen Standes der Technik zu verstehen. Im Zentrum stand und steht dabei die Frage, welchen digitalen Informationen und Funktionen man vertrauen kann. Dieser Stand der Technik entwickelte sich seit dem Anfang des 21. Jahrhunderts rasant und beeinflusste auch die nächste Stufe der Evolution von Digital Trust.

Mit der Einführung des sog. Registerwertrechtes (Art. 973d OR) im Jahr 2021 manifestierte der Schweizer Gesetzgeber eine erstaunliche Offenheit für einen neuen Stand der Technik. Das neue Registerwertrecht fusst auf der Erkenntnis, dass es heute technisch möglich ist, digitale Funktionen so zu programmieren und so zuverlässig auf digitalen Infrastrukturen zu betreiben, dass sie als Informationsträger funktional mit einer Urkunde bzw. einem Wertpapier vergleichbar sind. Rechtlich relevante Informationen können mit dieser Technologie unveränderlich eingetragen und ausschliesslich für den Berechtigten oder die Berechtigte zur Übertragung verfügbar gemacht werden. Der oder die Berechtigte kann sich dadurch auch gegenüber dem Schuldner und Dritten als Inhaber oder Inhaberin des Rechts ausweisen. Der Schweizer Gesetzgeber hat damit ein Rechtskonzept für eine wichtige Anwendung von Digital Trust geschaffen.

Um möglichst technologieneutral zu bleiben, fasste der Gesetzgeber diese digitalen Funktionen und Infrastrukturen unter dem Begriff der «Technologie der verteilten Register» zusammen. Es fallen darunter Technologien, die auch als Blockchain oder Distributed Ledger Technology (DLT) bekannt sind. Blockchain-Protokolle wie z. B. das Bitcoin-Protokoll ab 2009 und das Ethereum-Protokoll ab 2015, die oft nur als «Krypto» abgewertet werden, enthalten diese Funktionen. Was ebenfalls in der Berichterstattung über Krypto bislang untergeht, ist der Umstand, dass diese Protokolle seit der Einführung ununterbrochen und präzise wie ein Schweizer Uhrwerk laufen. Gerade darin liegt neben der Funktionalität die Radikalität dieser Protokolle: Sie funktionieren zuverlässig und sicher als dezentrale Systeme. Diese Protokolle sind heute Stand der Technik und das «Papier» der Zukunft. Sie sind die Wegbereiter für die Weiterentwicklung von Digital Trust, nicht nur im Bereich der Wertpapiere, sondern auch bei anderen Anwendungen wie Zertifikate, Warenpapiere, Ausweise, etc.

Der Kreis schliesst sich

Dank der «Technologie der verteilten Register» können mit diesem neugeschaffenen Rechtskonzept des Registerwertrechts Rechte sicher digital mobilisiert werden. Damit kann digital das ermöglicht werden, was früher durch direkte physische Übergabe einer Urkunde oder Buchung durch einen lizenzierten Intermediär möglich war. Die Herausgabe, das Halten und das Übertragen von digitalen mobilisierten Rechten wird wieder ohne Intermediäre möglich. Der Kreis schliesst sich.

Der Schweizer Gesetzgeber hat nicht geschlafen. Er hat das Potenzial der «Technologie der verteilten Register» erkannt und neben Papier und zentralen Datenbanken neu digitale Funktionen als Informationsträger und Anwendungsform von Digital Trust zur Mobilisierung eines Rechts zugelassen. Dank Digital Trust und einem wachen Gesetzgeber erlebt das Wertpapier in seiner Ursprungsfunktion einen zweiten Frühling. Einer neuen Ära der digitalen Mobilisierung von Rechten und rechtlich relevanten Informationen mit einer zum Teil neuen Rollenverteilung der verschiedenen Marktakteure wird der Weg bereitet. Es eröffnen sich neue Möglichkeiten, Produkte und Dienstleistungen für Userinnen und User zu entwickeln, die immer digitaler agieren und deren Bedürfnis nach sicheren und richtigen digitalen Informationen ungebrochen ist. Diese neue Ära kann sich in der Schweiz in einem bereits gut regulierten Rechtsraum entfalten. Selbstverständlich wird es dennoch notwendig sein, an gewissen Stellschrauben zu drehen. Diese sind aber mit Bedacht und am richtigen Ort anzuziehen. ●

Foto: mme

Vertrauen als Schlüssel zum Erfolg

Innovator of Trust // In unserer vernetzten und digitalen Welt spielt Vertrauen eine zentrale Rolle. Als innovative und verantwortungsbewusste Anbieterin von Digital-Trust-Produkten und -Services ist es Swisscom ein grosses Anliegen, die letzte Vertrauensmeile in der Digitalisierung zu erschliessen.

«On the Internet, nobody knows you're a dog.»

– Peter Steiner

Dieses berühmte Zitat des US-Karikaturisten Peter Steiner bringt auf den Punkt, wie einfach es ist, sich im digitalen Raum hinter einer Maske zu verstecken und so die wahre Identität zu verschleiern. Die Grenzen zwischen digitaler und physischer Realität verschwimmen immer stärker. Vertrauen als Grundlage für ein funktionierendes Miteinander nimmt in unserer digitalen Gesellschaft – unabhängig, ob privat oder geschäftlich – einen immer wichtigeren Stellenwert ein. Mit der weltweit fortschreitenden Vernetzung steigt gleichzeitig die Gefahr von gezieltem Missbrauch: Cyberkriminalität, Datenmissbrauch und Identitätsdiebstahl sind schmerzliche Realitäten, mit denen wir uns auseinandersetzen müssen.

Der Cyber Security Threat Radar 2024 von Swisscom zeigt, dass sogenannte AI-Based Attacks diese Entwicklung weiter beschleunigen. Die wachsende Gefahr im Netz spiegelt sich auch in den Zahlen des Bundesamts für Cybersicherheit (BACS) wieder: Die Gesamtzahl der beim BACS eingegangenen Meldungen ist 2023 mit knapp 50'000 Eingängen im Vergleich zum Vorjahr um 30 Prozent gestiegen.

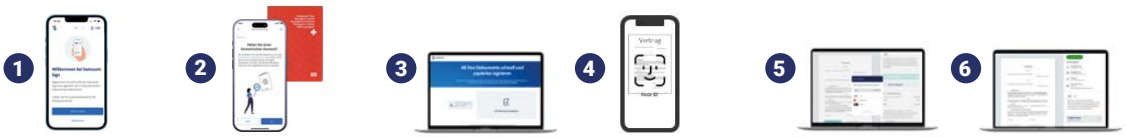
Identität, Integrität und Verbindlichkeit: die Säulen des expliziten Trusts

Damit der Vertrauensverlust im digitalen Raum verhindert werden kann, ist die Etablierung einer Vertrauensebene (engl. Trust Layer) in Kombination mit weiteren Sicherheitskomponenten im Internet essenziell. Dabei ist das Zusammenspiel der sogenannten impliziten und expliziten Vertrauenselemente zentral. Der implizite Trust umfasst verschiedene Cybersicherheitsmassnahmen, um die digitale Infrastruktur und Daten vor Bedrohungen wie Hacking, Malware, Phishing und Diebstahl zu schützen. Der Begriff expliziter Trust beschreibt Handlungen, die bewusst darauf abzielen, Vertrauen zu schaffen und diese aufrechtzuerhalten, beispielsweise die Freigabe verifizierter Informationen durch den Nutzer oder die Nutzerin oder die Signierung und Versiegelung von Dokumenten. In einer digitalen Welt ist dabei das transaktionale Vertrauen von zentraler Bedeutung. Darunter wird das Vertrauen im Rahmen einer digitalen Interaktion bzw. Transaktion zwischen zwei oder mehreren Parteien verstanden. Es setzt sich aus den drei Säulen Identität, Integrität und Verbindlichkeit zusammen, welche übrigens auch in der Offline-Welt zur Anwendung kommen.

Identität: Mit wem habe ich es zu tun?

Digitale Identitäten sind das Rückgrat einer prosperierenden digitalen Gesellschaft und zentral für die Zukunft. Zurzeit fehlt der Schweiz eine eindeutige Identifikationsgrundlage im digitalen Raum. Swisscom begrüsst deshalb einen möglichst zeitnahen Einsatz der Schweizer E-ID. Zudem betreibt Swisscom diverse Projekte im Bereich der digitalen Identitäten, insbesondere mit dem Self-Sovereign Identity-Ansatz (SSI). Ziel ist es, für unsere Business- und für unsere Privatkunden verständliche und Mehrwert stiftende Anwendungsprojekte zu etablieren, in denen die Nutzerinnen und Nutzer zu jedem Zeitpunkt die Kontrolle über ihre Daten behalten.

In wenigen Schritten zu Swisscom Sign



1. **Download My Swisscom App**
2. **Digitales Onboarding**
   Check!
   Person wurde eindeutig identifiziert
3. **Dokument hochladen**
4. **Signieren / Authentifizieren**
   Check!
   Rechtsgültige Signatur (QES)
5. **Bezahlen**
6. **Dokument verarbeiten**
   Check!
   Integrität der Dokumente validierbar

Jetzt kostenlos für Swisscom Sign registrieren!
sign.swisscom.ch/sign

Orts- und zeitunabhängig ohne Stift und Papier signieren
Die QES ersetzt die handschriftliche Unterschrift und ist in der Schweiz und Europa gültig. Swisscom Sign kann von Privatpersonen, Firmen, Vereinen oder Stiftungen genutzt werden und ist als API-Integration für grosse Organisationen und Softwareanbieter erhältlich. Dokumente können gemeinsam mit anderen Personen signiert werden.

Integrität: Sind die übermittelten Informationen echt?
Integrität steht für die Unveränderlichkeit von Informationen. Diese ist ebenfalls entscheidend für das Vertrauen in digitale Transaktionen. Immer besser werdende Deep Fakes erschweren es, Falschinformationen zu erkennen. Auch hier nimmt der dezentrale SSI-Ansatz eine entscheidende Rolle ein. Dieser erlaubt es, in Zukunft digitale Originale wie Nachweise, Dokumente, Zeugnisse etc. auszustellen, deren Echtheit digital verifiziert werden kann.

Verbindlichkeit: Ist die formale Verbindlichkeit gegeben?
Verbindlichkeit bezeichnet die verlässliche und rechtliche Bindung der digitalen Willensäusserung. Nur die qualifizierte elektronische Signatur (QES) ist gemäss CH- und EU-Gesetz der handschriftlichen Unterschrift gleichgestellt. Swisscom bietet mit Swisscom Sign eine einfache und sichere Möglichkeit, die QES zu nutzen. Die QES stellt durch die «Versiegelung» die Integrität eines Dokuments sicher. Eine nachgängige Anpassung des Dokuments wäre bei einer Überprüfung in einem Signatur-Validator erkennbar. Neben der Zeit- und Kosteneffizienz bringt die QES viele weitere Vorteile. Mehr zu Swisscom Sign in der Infobox.

Swisscom als treibende Kraft zur Etablierung von Digital Trust

Neue Technologien wie ChatGPT & Co. sind in der Gesellschaft angekommen und beschleunigen die Digitalisierung enorm. Gleichzeitig fordern sie auch die Glaubwürdigkeit von Informationen heraus. Digital Trust ist in der vernetzten Welt essenziell, da nur mit seiner Hilfe die letzte digitale Vertrauenslücke geschlossen werden kann. Ohne diesen Schritt bleiben Medienbrüche bestehen, welche für Kunden und für Anbieter zu negativen Effekten führen. Swisscom als vertrauenswürdige und sicherere Partnerin möchte in diesem Bereich Verantwortung übernehmen und eine führende Rolle einnehmen, um den Herausforderungen der Gesellschaft, Wirtschaft und des öffentlichen Sektors bestmöglich zu begegnen. Als «Innovator of Trust» setzt sich Swisscom mit innovativen Ansätzen auseinander und bringt mit ihrer Expertise Vertrauen in Form integrierter Lösungen an den Markt. ●

Andreas Tölke
Head FinTech & Digital Trust, Swisscom

Andreas Tölke, seit 2020 bei Swisscom, ist verantwortlich für FinTech & Digital Trust. Zuvor war er in verschiedenen Führungspositionen bei der Credit Suisse tätig. Er begann seine berufliche Laufbahn beim Industrieunternehmen Georg Fischer in Schaffhausen und ist Mitgründer eines Medien-Start-ups. Er studierte Betriebswirtschaft an der ZHAW School of Management and Law und hält einen Executive MBA der Universität St.Gallen.

«Ein wissensbasiertes Umfeld und die Förderung der Adaption durch Unternehmen sind entscheidend für das Vertrauensökosystem»

E-ID // 2026 kommt die E-ID. In Partizipationsmeetings des Bundes haben sich private und staatliche Akteure wie die Digital Identity & Data Sovereignty Association (DIDAS) eingebracht und Anforderungen und Ausgestaltung diskutiert. Wir haben mit dem Präsidenten Daniel Säuberli über die künftige E-ID und die ihr zugrunde liegende Vertrauensarchitektur gesprochen.

Herr Säuberli, wie zufrieden sind Sie mit der Ausgestaltung der neuen E-ID?
Die Einführung der E-ID ist ein entscheidender Schritt für die digitale Transformation in der Schweiz. Sie bildet eine solide Grundlage für die sichere, digitale Verifizierung von Identitäten. Da sie ein solch wichtiger Baustein darstellt, ist es zentral, Anforderungen, Ausführung und Weiterentwicklung partizipativ zu erarbeiten. Vertrauenswürdige Infrastrukturen sind sehr komplex, daher ist es wichtig, unterschiedliche Kompetenzen in einem Team zusammenzubringen. Das Projekt wurde vom Bund unter der Leitung des Bundesamts für Justiz mit viel Weitsicht entwickelt, Datenschutz- und Sicherheitsbedenken wurden von Anfang an sehr ernst genommen und im Design berücksichtigt. Ich bin zufrieden mit der Ausgestaltung und noch glücklicher, wenn wir einen definitiven Startpunkt für das Vorhaben gefunden haben. Die E-ID ist ein Musterbeispiel, mit welchem Mindset komplexe Projekte des Bundes in Zukunft angepackt werden sollten.

Sehen Sie Schwachstellen? Gibt es Aspekte, die anders hätten gestaltet werden sollen?
Obwohl wir bei Themen wie Kryptographie und Sicherheit mittlerweile sehr weit sind, ist jede technologische Lösung immer ein Kompromiss zwischen Benutzerfreundlichkeit und Sicherheitsanforderungen. So war zum Beispiel bis anhin das datensparsame Teilen von Attributen und die Verhinderung von Korrelation nur schwer unter einen Hut zu bringen. In diesem Bereich wurden Fortschritte gemacht, die berücksichtigt werden können. Deshalb ist es wichtig, Umsetzungsbestimmungen flexibel zu halten, um Verbesserungen systematisch und kontinuierlich einpflegen zu können.

«Die Implementierung der E-ID muss flexibel bleiben, um kontinuierlich Verbesserungen zu ermöglichen.»

Es gibt die Befürchtung der Überidentifikation: Für Alltagsgeschäfte müssen sich Konsumenten online ausweisen, was bis jetzt nicht der Fall ist. Der Bund will dem mit einer schwarzen Liste begegnen. Was hat es damit auf sich?
Die Möglichkeit für datensparsames Teilen von Informationen ist eine hervorragende Eigenschaft der zukünftigen E-ID. Damit kann ich sicherstellen, dass nur die Daten geteilt werden, die ich als Halter der E-ID aktiv freigebe. Die Vertrauensinfrastruktur verhindert nicht, auch komplett anonym oder pseudonym aufzutreten, während gleichzeitig selektiv Attribute oder Teile davon auf ihre Authentizität überprüft werden. Diese Eigenschaft haben wir bei der heutigen physischen Identitätskarte nicht: Beim Vorzeigen gebe ich alle darauf enthaltenen Informationen preis. Versucht ein Anbieter im digitalen oder physischen Raum trotzdem, bei einem Proof Request – beispielsweise bei der Verifikation des Mindestalters für einen bestimmten Service – Informationen von der E-ID abzufragen, die für den Geschäftsfall nicht benötigt werden, kann ich das rapportieren. Solche selbstregulierenden Mechanismen im Ökosystem zu ermöglichen, indem man sie auch in der Governance verankert, ist sehr wichtig. Genau wie klare Massnahmen bei Missbrauch.

Können Sie uns die Vision der Vertrauensarchitektur hinter der neuen E-ID erläutern?
Die Vision besteht darin, ein sicheres und zukunftsfähiges digitales Ökosystem zu schaffen, das allen Beteiligten einen Mehrwert bietet. Dank der E-ID können über die Vertrauensinfrastruktur Identitätsverifizierungen stattfinden, sie kann aber auch dazu verwendet werden, unterschiedliche digitale Nachweise oder authentische Datenpakete verifizierbar zu machen. So kann beispielsweise ein Impfnachweis, ein Arztrezept, ein Lieferschein oder ein Vermögensnachweis von der Bank elektronisch verifizierbar gemacht werden, um Prozesse automatisch und datenschutzfreundlich abzuwickeln. Das Ökosystem muss durch die Förderung von Innovation und die Schaffung eines Wissensumfelds vorangetrieben werden, um Unternehmen zu unterstützen und Experimente zu ermöglichen. Da sind wir noch nicht weit genug.

Wie weit ist die technische Ausgestaltung dieser Architektur bereits geklärt, und inwieweit sind Sie als Verein in diese Ausgestaltung einbezogen?
DIDAS ist wie alle anderen über die Partizipationsmeetings des Bundes in die Gestaltung der digitalen Vertrauensinfrastruktur involviert, hat sich jedoch als Think-Tank darüber hinaus als Kompetenzzentrum für die Vertrauensinfrastruktur etablieren können. Wir sind bei der inhaltlichen Standardisierung der sektoralen Ökosysteme für Ambitionsniveaus 1– 3 tief involviert. Um sicherzustellen, dass die Bedürfnisse aller Stakeholder berücksichtigt werden, verfolgen wir genau, wie die Strukturen mit unserem Input weiterentwickelt werden. ▶

Daniel Säuberli

Präsident DIDAS

Daniel Säuberli ist Mitgründer und Präsident der Digital Identity and Data Sovereignty Association (DIDAS) und bringt seine umfangreiche Erfahrung an der Schnittstelle von Geschäftsstrategie und Technologie in die Förderung digitaler Identität und Datensouveränität ein. Er ist seit über 25 Jahren in verschiedenen Organisationen, von Start-ups bis zu multinationalen Konzernen wie IBM, tätig und sieht die digitale Identität als unverzichtbaren Baustein für eine vertrauensvolle und automatisierte Welt, in der Individuen nachhaltig die Kontrolle behalten.

Die **Digital Identity & Data Sovereignty Association (DIDAS)** ist eine schweizerische Non-Profit-Organisation, die sich der Förderung sicherer digitaler Identitäten und der Datensouveränität widmet. Ziel von DIDAS ist es, ein vertrauenswürdiges, sicheres und inklusives digitales Ökosystem in der Schweiz zu schaffen, welches die Kontrolle über persönliche Daten stärkt und die digitale Autonomie der Bürger fördert. Die Organisation engagiert sich in der Entwicklung von Standards und Technologien für digitale Identitäten und arbeitet mit verschiedenen Stakeholdern zusammen, darunter Regierungen, der Privatwirtschaft und zivilgesellschaftlichen Gruppen. DIDAS beteiligt sich aktiv an internationalen Diskussionen und Initiativen, um interoperable, grenzüberschreitende Lösungen zu fördern. Über ihre Plattform bietet DIDAS regelmässig Workshops und Seminare an, um das Bewusstsein und das Verständnis für digitale Identitäts- und Datenschutzthemen zu erhöhen. Als Brückenbauer in der digitalen Welt unterstützt DIDAS die Schweiz dabei, eine führende Rolle in der digitalen Transformation einzunehmen und technisch fortschrittliche und sozial verantwortliche Lösungen zu entwickeln. DIDAS finanziert sich ausschliesslich über Mitgliederbeiträge.
didas.swiss

«Die E-ID erlaubt es auch in Zukunft, anonym oder pseudonym aufzutreten. Wichtig für das entstehende Ökosystem sind selbstregulierende Mechanismen in der Governance und klare Massnahmen bei Missbrauch.»

Wie engagiert sich DIDAS bei der Entwicklung dieser Vertrauensarchitektur?
Durch unsere Arbeit mit verschiedenen Stakeholdern tragen wir dazu bei, die Grundlagen für ein digitales Ökosystem zu schaffen, das Vertrauen und Sicherheit in der digitalen Welt fördert. Beispiel Portabilität und Interoperabilität: Verifiable Credentials wie die E-ID können dezentral über verschiedene Systeme und Plattformen hinweg genutzt werden, was ihre Einbindung in bestehende und neue Systeme erleichtert. Dies fördert die Kompatibilität und Flexibilität bei der Technologiewahl des Bundes und des privaten Sektors – und auch die Umsetzung des «Once-Only»-Prinzips. Also des Prinzips, bestimmte Informationen nur einmal erfassen zu müssen, sodass sie wiederholt verifizierbar geteilt und durch einen Verifikator vertrauenswürdig überprüft werden können.

Könnte E-Voting irgendwann Teil dieser Vertrauensarchitektur sein?
Wie die Identifikation müssen Wahlen und Abstimmungen für alle Bevölkerungsgruppen, digital oder physisch einfach und barrierefrei zugänglich sein. Ich glaube, E-Voting hat generell das Potenzial, den Prozess zu vereinfachen und zu modernisieren. Die Wahlbeteiligung, speziell bei der jüngeren Generation, könnte gestärkt werden. Die Vertrauensinfrastruktur und Verifiable Credentials können da eine Rolle spielen, beispielsweise bei der Identitätsverifikation, bei der Stimmabgabe oder bei der Wahlberechtigung.

«Die E-ID kann dezentral über verschiedene Systeme und Plattformen genutzt werden. Das fördert die Kompatibilität und Flexibilität bei der Technologiewahl für Bund und Private, und unterstützt die Umsetzung des ‹Once-Only›-Prinzips.»

Und wie steht es um digitale Signaturservices? Könnten diese in die Architektur der E-ID integriert werden?
Digitale Signaturservices sind eine logische Erweiterung der digitalen Identitätsinfrastruktur. Ob diese von Drittanbietern oder vom Bund erbracht werden, kann man getrost dem Markt überlassen. Was ich als aktiver Nutzer gerne sehen möchte, ist eine benutzerfreundliche Integration von Signaturservices in meine Abläufe im Unternehmen oder als Privatperson.

Die E-ID soll auch in der EU anerkannt werden. Wie sehen Sie die Interoperabilität mit anderen Rechtsräumen, insbesondere im Hinblick auf die eIDAS-Verordnung?
Die Interoperabilität mit der EU und anderen Rechtsräumen ist entscheidend für die nachhaltige Nutzung der E-ID und weiterer digitaler Nachweise. Beispielsweise unterscheidet eIDAS nicht zwischen der Identifikation von natürlichen und juristischen Personen, das E-ID-Gesetz beinhaltet dagegen nur natürliche Personen. Wir müssen auf funktionaler und auf technologischer Ebene Wege finden, Interoperabilität und die hohen Datenschutzanforderungen der Schweizer Infrastruktur sicherzustellen. Es gibt gute Lösungswege, die aber kontinuierlich weiterentwickelt werden müssen.

Wie sehen Sie die Möglichkeit, die E-ID ohne physische Identitätsprüfung zu erhalten? Gibt es digitale Onboarding-Möglichkeiten?
Ja, die gibt es. Es soll ein digitales Onboarding geben, das einen Moment-Abgleich mit den beim Fedpol hinterlegten Eigenschaften des Passfotos mit den im Onboarding-Prozess der E-ID gesammelten Daten ermöglicht. Das E-ID-Team hat dazu eine Ausschreibung publiziert. Meines Wissens soll auch eine Ausstellung im Passbüro möglich sein. Ausgestellt wird die E-ID immer in die Wallet des Bundes und allenfalls parallel in weitere elektronische Brieftaschen. ●

Wir kümmern uns um die Identifikation. Und den Rest.

ti&m Online Identification

Als Experte für Online-Identifikation wissen wir, dass die Identifikation nur ein Teil der User Journey ist. Deshalb unterstützen wir unsere Kunden nicht nur bei der nahtlosen Implementierung unserer Lösung ti&m Online Identification. In enger Zusammenarbeit mit den Kunden können unsere UX-Experten, Prozessberater und Softwareentwickler alle Teile der Journey optimieren und ein einmaliges Onboarding-Erlebnis kreieren.

swisscom · Vontobel · VermögensZentrum · Credit Suisse · Obwaldner Kantonalbank

Martin Unterbäumen, Head Client Engagement, informiert Sie gern:
+41 44 497 75 00 oder ti8m.com/online-id

ti&m

«Wer sich schon jetzt mit den Möglichkeiten der E-ID auseinandersetzt, wird 2026 einen Wettbewerbsvorteil haben»

Self-Sovereign Identity // Missbrauch und Diebstahl von Identitäten im Internet sind eine wachsende Bedrohung. Die Schweiz und die EU treiben die Entwicklung einer dezentralen digitalen Identität voran: gesetzliche Grundlagen werden geschaffen, technologische Diskussionen geführt. Von Désirée Heutschi wollen wir wissen, welche Massnahmen Unternehmen und Behörden jetzt ergreifen sollten, um sich auf die Einführung sicherer digitaler Identitäten vorzubereiten.

Désirée Heutschi

Geschäftsleitungsmitglied Orell Füssli AG & VR/Co-CEO von Procivis AG

Désirée Heutschi ist seit 2020 Geschäftsleitungsmitglied bei der Orell Füssli AG und Verwaltungsrätin bei Procivis AG sowie seit 2023 Co-CEO von Procivis. Sie verfügt über langjährige Erfahrungen in der Softwareindustrie und Innovation und hält einen Executive Master of Business Law (Universität St.Gallen).

Frau Heutschi, einer deutschen Studie zufolge hat bereits jeder Zehnte Erfahrung mit Identitätsdiebstahl gemacht. Sie sind mit physischen und digitalen Identitätslösungen gut vertraut. Was sagen Sie zu diesen Zahlen?

Diese Zahlen überraschen mich nicht. Gesetzlich wurde reagiert: In der Schweiz gilt einerseits der Identitätsmissbrauch seit 2023 als Straftatbestand, andererseits wird mit dem künftigen E-ID-Gesetz eine wichtige Grundlage für eine sichere, vom Staat herausgegebene digitale Identität geschaffen. Parallel dazu hat die EU mit der «eIDAS 2.0»-Verordnung die Mitgliedstaaten verpflichtet, E-ID-Wallets für ihre Bürgerinnen und Bürger bereitzustellen. Beides soll 2026 umgesetzt werden.

18 Monate sind keine lange Zeit. Wie bereiten wir uns vor?

Wir brauchen Technologielösungen, die uns Sicherheit geben, damit wir dem virtuellen Gegenüber vertrauen können. Diese müssen den Schweizer und europäischen Richtlinien entsprechen, denn Landesgrenzen werden bei digitalen Identitäten und Nachweisen kaum eine Rolle spielen. Wir haben in den letzten eineinhalb Jahren ein einzigartiges Produkt entwickelt, das alle bisher bekannten Anforderungen an eine Technologielösung erfüllt und heute implementiert werden kann. Behörden und Unternehmen sollten jetzt beginnen, ihre Systeme für die Einführung der E-ID vorzubereiten, damit sie die Vorteile sofort nutzen können.

Wie soll die technologische Umsetzung dieser Richtlinien funktionieren?

Mit dem Konzept der selbstverwalteten Identität, englisch Self-Sovereign Identity. Denn digitale Nachweise oder Verifiable Credentials sind mehr als nur digitale Pendants zu physischen Dokumenten. Sie enthalten Informationen, sogenannte Attribute, die die Nutzer selektiv und gezielt teilen können. Sie können beispielsweise für sichere Berechtigungen für Mitarbeitende oder effiziente Überprüfungen der Kreditwürdigkeit eingesetzt werden. Die Nutzer behalten die Hoheit über ihre Daten und können nachvollziehen, welche Attribute sie wann mit wem geteilt haben. Im Gegensatz zu herkömmlichen zentral verwalteten Systemen erhält kein Dritter Informationen über die Verwendung.

Sie leiten die Unternehmensentwicklung der Orell-Füssli-Gruppe und sind Co-CEO des Tochterunternehmens Procivis, einer Anbieterin für Technologielösungen für digitale Identitäten und Nachweise. Wie passen diese Rollen zusammen?

Eines der Kerngeschäfte von Orell Füssli ist Sicherheit. Wir sind langjährige Vertrauenspartnerin von Staaten in der Herstellung physischer Vertrauensdokumente wie Banknoten, dem Schweizer Pass und Führerausweisen. Procivis ergänzt das Portfolio um digitale Identitäten und Nachweise. Wir haben eine neue zukunftsweisende Softwarelösung entwickelt, über die Nachweise wie eine E-ID, ein digitaler Führerausweis oder andere digitale Nachweise ausgestellt, geprüft und gespeichert werden können. Diese Software bieten wir Behörden und Unternehmen an.

Warum sollten sich Behörden und Unternehmen für die Lösung von Procivis entscheiden?

Es gibt viele technische Diskussionen rund um Protokolle, Formate und Standards, mit denen die meisten Institutionen nichts anfangen können. Daher warten viele darauf, dass sich die EU beziehungsweise der Bund technisch entscheidet. Wir haben mit Procivis One eine eigene Pionierlösung entwickelt, die multiprotokollfähig ist, den aktuellen Regularien in der Schweiz und in der EU entspricht und flexibel auf künftige Entwicklungen angepasst werden kann. Sie entspricht den SSI-Vorgaben und stellt die Datenhoheit bei den Nutzern sicher. Procivis One kann schon heute eingesetzt und von unseren Kunden autark betrieben werden – hochperformant und skalierbar für Millionen Nutzer und Nachweise.

Welche anderen Nachweise könnten denn in den nächsten Jahren relevant werden?

Es gibt in der Schweiz drei verschiedene Ambitionslevel: Level 1 ist die digitale Identität per se, Level 2 sind staatlich regulierte Nachweise wie Führerausweis, Strafregisterauszug oder Diplome, Level 3 sind alle anderen digitalen Nachweise wie Berechtigungs- und Mitgliedsausweise. Potenzielle Anwendungsfälle sind praktisch endlos vorhanden.

Was würden Sie unseren Leserinnen und Lesern raten?

Ich bin davon überzeugt, dass Institutionen, die sich bereits jetzt auf die Einführung der E-ID in der Schweiz beziehungsweise eIDAS 2.0 in der Europäischen Union vorbereiten, einen Wettbewerbsvorteil gegenüber anderen haben werden. Sie sollten sich überlegen, welche Prozesse effizienter oder neu gestaltet werden können und welche Auswirkungen dies auf die bestehende IT-Infrastruktur hat. Parallel dazu sollte die technologische Implementierung beleuchtet werden, damit die zukünftige Umsetzung vereinfacht wird. ●

Orell Füssli ist eine Pionierin im Bereich Sicherheit und Bildung. Als führende Systemanbieterin für Sicherheitstechnologien und Identifikationssysteme und als langjährige Partnerin von Staaten setzt Orell Füssli technologische Standards in analogen und digitalen Anwendungen. Im Bereich Bildung ist Orell Füssli mit ihren Verlagen aktiv und an Orell Füssli Thalia AG, der grössten Buchhändlerin der Schweiz, beteiligt. *orellfuessli.com*

Die Tochtergesellschaft **Procivis** ist eine etablierte Technologieanbieterin für digitale Identitäten in der Schweiz, die 2023 die neue Softwarelösung Procivis One für dezentrale digitale Identitäten und verifizierbare digitale Nachweise lanciert hat. *procivis.ch*

Foto: Orell Füssli

Warum Versicherungen jetzt in Tech & Data investieren müssen

Andy Maier

Verwaltungsrat, ti&m

Als CIO der AXA, von Zurich Financial und der Winterthur Versicherungen hat Andy Maier die Digitalisierung der Versicherungsbranche nachhaltig geprägt. Auch nach seiner Pensionierung im September 2023 ist der InsurTech-Experte als Senior Advisor weiterhin für die AXA tätig. Ausserdem ist er Mitglied des Verwaltungsrats der SOBRADO AG sowie Präsident der EcoHub AG und der noimos AG. Als Mitglied des Verwaltungsrats unterstützt er ti&m bei der strategischen Entwicklung des Bereichs «Insurance».
ti8m.com

InsurTech // Versicherungen müssen die Digitalisierung beschleunigen – aber dazu fehlen teilweise die Kompetenzen. Strategische Technologiepartner wie ti&m bringen das nötige Know-how in «Tech & Data»-Projekte, um die nächsten Schritte erfolgreich anzugehen.

Was wollen die beiden wichtigsten Anspruchsgruppen von einer Versicherung?

Sinn und Zweck einer Versicherung ist die Übertragung der finanziellen Aspekte eines Risikos von einer Person auf eine Versicherung. Dahinter steckt auch das soziale Prinzip, dass diese Risikoübertragung für die gleiche Risikoselektion für alle gleich viel kostet. Kunden erwarten im Schadenfall eine verbindliche, einfache und rasche Leistung. Investoren kaufen Aktien von Versicherungen wegen nachhaltigen und sicheren Dividenden. Die Geschäftsmodelle sind stabil und die Renditen sehr attraktiv.

Die digitalen Herausforderungen für Versicherungen

Das Kundenverhalten ändert sich. Junge Kunden sind weniger loyal. Vollständig digitale und flexible Produkte und Services sind ein Muss, genau wie Omnichannel für Advisory, Sales und Services. Interaktionen sollen häufiger, dafür digital und einfach erfolgen.

Der Markt setzt die Preise unter Druck. Neue Wettbewerber und Intermediäre kommen auf den Markt, die Preistransparenz wird detaillierter und einfacher für die Konsumenten. Die Vertriebskosten sind sehr hoch, die Produktivität der exklusiven Vertriebe und der Broker muss stark verbessert werden.
Die Abwicklung der Produkte muss einfacher, flexibler und digitaler werden.
Die Schadeninflation muss proaktiv mitigiert, die Schadenabwicklung den digitalen Anforderungen der Kunden gerecht werden.
Den Fachkräftemangel spürt man auch im Versicherungsgeschäft.

Die fünf Investitionsschwerpunkte

Die digitale Transformation ist kein Selbstzweck. Es müssen strategisch und nachhaltig digitale Capabilities aufgebaut werden, welche die Kundenanforderungen erfüllen:

Augmented Advisory: Der Vertrieb über Broker und Agenturen muss digital so unterstützt sein, dass sich alle auf den Beratungsprozess fokussieren können. Administration und Policierung werden vollständig automatisiert, die Beratung durch Copilot AI und Fragen zu Vertragsbedingungen durch LLM-Lösungen unterstützt. Beraterinnen und Berater haben eine 360-Grad-Sicht ihrer Kunden; zusätzliche Informationen liefern Beratungshinweise und proaktive Verkaufschancen.

Beyond Insurance: In Zukunft partizipiert eine Versicherung in verschiedenen Ökosystemen. Die Integration in Ökosysteme für Banking, Vorsorge, Home, KMU oder Health bieten Chancen für zusätzliche Kundeninformationen und Verkäufe. Differenzierende Partnerservices wie Präventionsservices erhöhen die Loyalität der Kunden.
Zero Ops: Operative Prozesse werden vollständig automatisiert. Es gibt sehr wenige manuelle Interventionen, und diese werden von AI augmentiert. Dokumente werden automatisch gelesen, Anliegen digital erkannt und verarbeitet; digitale Interaktionen mit den Kunden geschehen über ein sicheres Interaction Board. Oversight und Compliance werden definiert und automatisch sichergestellt.
Digital Products for Digital Natives: Versicherer haben einfache, modular kombinierbare Produkte mit verständlichen Leistungsversprechen und abrufbare Services. Deckungsüberprüfung und Abwicklung im Schadenfall sind digitalisiert und mobilefreundlich dargestellt.
Open Pension: Finanzielle Transparenz bei der Altersvorsorge wird wichtiger: Allfällige Lücken müssen früher bemerkt und Vorschläge für die Sicherstellung der Lebensqualität im Alter erkannt und den Kunden digital und einfach erklärt werden.

Die zwölf Capabilities, um diese Ambitionen zu erreichen

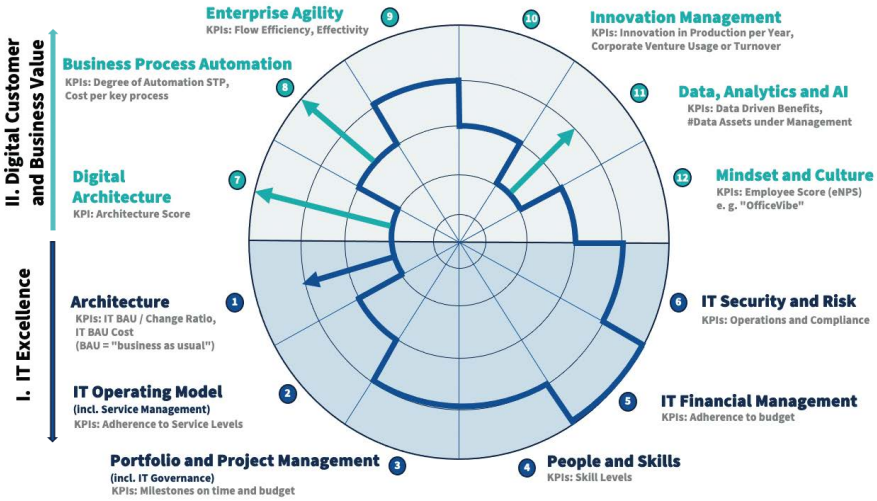
Um diese fünf Investitionsschwerpunkte zu entwickeln, müssen digitale Capabilities definiert und deren Maturität bestimmt werden:

IT Excellence

Das untere Segment im Radar (1 – 6) zeigt sechs fundamentale IT Capabilities. Dieses Fundament muss logischerweise eine gewisse Maturität erreichen, um darauf aufbauen zu können. Für diese Capabilities trägt die IT die Hauptverantwortung.

Digital Customer and Business Value

Die oberen sechs Capabilities (7 – 12) generieren indirekt Wert für Kunden und Investoren der Versicherung. Kundennutzen und unternehmerisches Wachstum gehen im digitalen Zeitalter Hand in Hand. Um diese Capabilities zu entwickeln, braucht es einen Co-Creation-Ansatz von Business und IT-Sponsoren. Versicherungen haben erkannt, dass die Entwicklung von digitalen Fähigkeiten strategisch sehr relevant und komplex ist. Investitionen in diese Capabilities steigen bereits heute, die Suche nach Fachkräften und kompetenten Partnern nimmt zu.



Der richtige Partner

Versicherungen werden nicht alles selbst stemmen können und sind auf gute Partner angewiesen, die Technologie- und Businesskompetenz in die Projekte bringen. ti&m besitzt die notwendigen Kernkompetenzen als «Tech & Data»-Partner, um Versicherungen bei den nächsten Schritten der digitalen Transformation zu begleiten.

Integration der gesamten Wertschöpfungskette

Eine der beiden wichtigsten Voraussetzungen für eine strategische und nachhaltige Partnerschaft ist die Fähigkeit, auf der gesamten «Klaviatur» spielen zu können: mit Consulting verschiedene Lösungsoptionen erarbeiten und beurteilen, Business-Anforderungen mitprägen und schnell ein MVP entwickeln. Mit Mobile, UX, Design Thinking etc. Methoden einbringen, die neue Perspektiven eröffnen. Security-Aspekte von Beginn weg in das Design integrieren. Und mit agilen Teams gemeinsam mit den Versicherern Produkte entwickeln und die Kernlandschaft erweitern.

Technologische Kernkompetenzen und Fachkräfte vor Ort

Diese vier Dimensionen sind die grössten Treiber für künftige Wertgenerierung:

Digital Architecture: Alle Versicherer werden investieren, um neue Anwendungen cloudnative zu entwickeln. Zweitens werden heutige Kernanwendungen auf die Cloud migriert und modernisiert. Heisst: Anwendungen werden modularisiert und virtualisiert, das Testing automatisiert, Infrastrukturkonfigurationen mit Software konfiguriert, Application Integration und Configuration Management mit Scripting automatisiert etc. Die Anforderungen dazu kommen aus schnelleren Entwicklungszyklen, aber auch aus Resilienz und Reversibilität.

Business Process Automation & Augmentation: Wie beschrieben werden die Versicherer in den nächsten zehn Jahren ihre heutigen Geschäftsmodelle digitalisieren. Die Produktivität der Beraterinnen und Berater und von Inhouse Operations muss durch Business Process Automation (BPA) massiv verbessert werden. Dazu benötigen Versicherer eine Taxonomie zu Prozessmanagement, Automatisierungsframeworks, Metriken für das Performancemanagement und Technologien für die Umsetzung. AI Analytics der Prozessdaten liefern zusätzliche Informationen.

Data, Analytics & AI: Data Governance, Data Management, Data Architecture, Master- und Metadaten-Management, Quality Management, Data Security & Privacy Management, Data Leakage and Lineage sowie Ethics & Compliance sind zwingende Voraussetzungen für analytische Regeln und Modelle. Natürlich braucht es auch moderne Technologien dazu – diese stellen die drei grossen Cloud-Hyperscaler bereit. Auf dieser Basis können wertsteigernde Modelle entwickelt und getestet werden. Die wichtigsten Anwendungsgebiete sind neben Customer 360° Use Cases in den Bereichen Risk Selection & Pricing, Claims Leakage & Fraud Prevention und Document Intelligence.

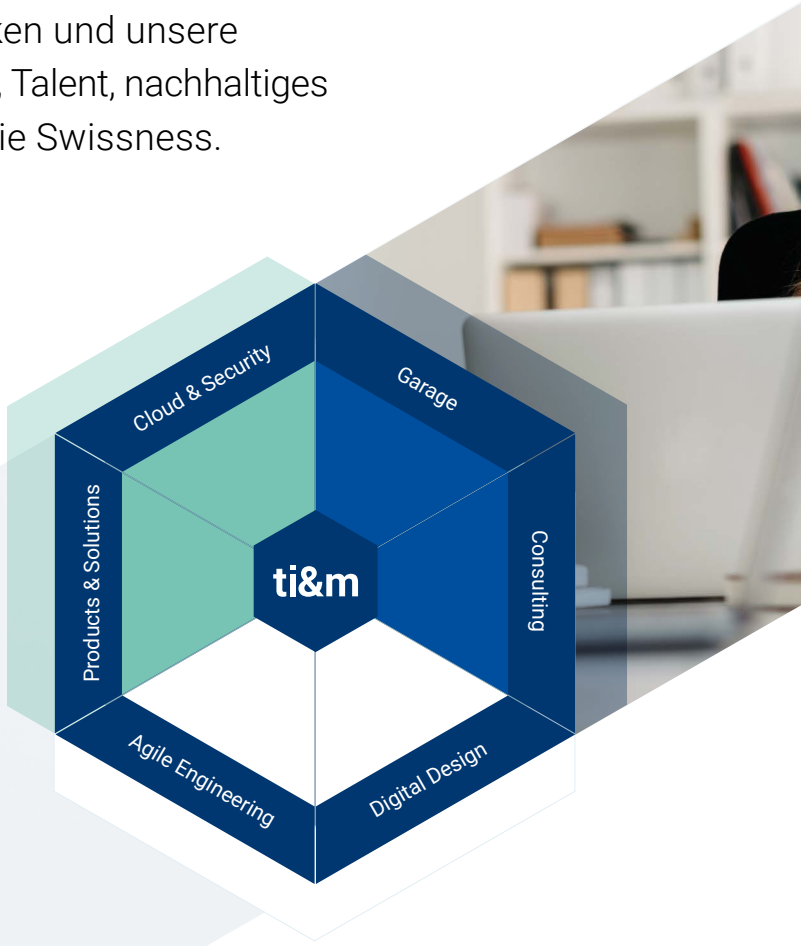
Security Technologies: Der Einsatz neuer Technologien bedingt moderne und robuste Sicherheitskonzepte.

Die Herausforderungen für Versicherer in Business und Technologie sind komplex. Es gilt, zusammen mit kompetenten IT-Partnern wie ti&m die strategischen Bedürfnisse zu analysieren, die notwendigen Tech & Data Capabilities zu identifizieren und Softwarelösungen zu entwickeln, die den Anforderungen der Kunden und der Mitarbeitenden gerecht werden. ●

Portrait: AXA

Wir digitalisieren Ihr Unternehmen

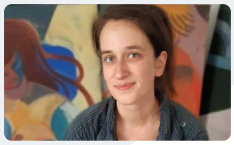
ti&m steht für technology, innovation & management. Wir sind Marktführer für Digitalisierungs- und Security-Produkte sowie Innovationsprojekte. In unseren sechs Niederlassungen beschäftigen wir aktuell über 600 Engineers, Designers und Consultants. Die Grundlage unseres Wachstums sind unsere Stärken und unsere Werte: Mut zur Innovation, Leidenschaft, Talent, nachhaltiges Wachstum, Respekt und Toleranz sowie Swissness.



Wir integrieren die gesamte IT-Wertschöpfungskette vertikal und entwickeln User-zentrierte Innovationen in unschlagbarer Time-to-Market.

Unsere Engagements

ti8m.com/hack-an-app



ti8m.com/art-at-work

ti8m.com/shake-the-lake

Vertrauen ist die Grundlage jeder Interaktion.

Mit dem Digital Trust Center haben wir bei ti&m die Kompetenz geschaffen, um holistisch alle Aspekte von Digital Trust in unseren Services, Produkten und Softwareentwicklungen zu integrieren. Unsere Expertinnen und Experten unterstützen Sie, sichere und vertrauenswürdige digitale Geschäftsräume zu schaffen, Risiken zu minimieren und sich gegen Cyberangriffe zu verteidigen. Damit Sie Ihr digitales Potenzial durch Innovationen und neue Geschäftsmodelle voll auszuschöpfen können.

Digital Trust Center

Cybersecurity

- Security Assessment
- Threat Modeling & Awareness Training
- Information Security Risk Management
- Threat & Vulnerability Management
- Ransomware Resilience
- Security Operation Center (SOC)
- CISO Services
- SIEM
- Public Cloud Platform Management

Datenschutz

- Online Identification
- Multi-Factor Authentication
- E-Signing
- Compliance & Ethics
- Quantum-Safe Cryptography
- Self-Sovereign-Identity & E-ID

Interoperabilität

- API Security & Consent Management
- SOC Integration
- SOC Connector

Auditability

- Trust Network & Token
- Signature Verification
- Transfer of Ownership

Leunita Saliji, Head Cloud & Innovation Hosting, informiert Sie gern: +41 44 497 75 00 oder *ti8m.com/security*

ti&m

So fördert das Bundesamt für Cybersicherheit die Resilienz

Cyberresilienz //
Die Cybersicherheit ist ein Thema, das unseren Alltag prägt und immer wichtiger wird. Aus diesem Grund hat der Bundesrat aus dem Nationalen Zentrum für Cybersicherheit per 1.1.2024 ein Bundesamt für Cybersicherheit (BACS) geschaffen. Was bedeutet dies und welche Veränderungen bringt dies mit sich?

Die Cybersicherheit hat in den vergangenen Jahren auf allen Ebenen stark an Bedeutung gewonnen. Sie ist ein zentraler Faktor für den Wirtschaftsstandort und für die Sicherheit der Bevölkerung im digitalen Raum. Sie spielt zudem eine wichtige Rolle in der nationalen und internationalen Aussen- und Sicherheitspolitik. Die Gewährleistung der Cybersicherheit ist deshalb zu einer unverzichtbaren Aufgabe des Bundes geworden. Mit der Überführung des Nationalen Zentrums für Cybersicherheit in ein Bundesamt wurde der wachsenden Bedeutung der Cybersicherheit Rechnung getragen. Der Kernauftrag des Bundesamtes ist jedoch gleichgeblieben. So ist das BACS weiterhin die erste Anlaufstelle für Wirtschaft, Verwaltung, Bildungseinrichtungen und die Bevölkerung bei Cyberfragen. Es ist verantwortlich für die koordinierte Umsetzung der Nationalen Cyberstrategie (NCS) und trägt durch seine operative Tätigkeit wesentlich zur Erhöhung der Widerstandsfähigkeit der Schweiz gegen Cyberangriffe bei.

Cyberbedrohungslage

Anhand der beim BACS eingehenden Meldungen aus der Bevölkerung und von Unternehmen sowie den Kontakten zu Betreibenden kritischer Infrastrukturen und einem sowohl nationalen als auch internationalen Netzwerk von Partnerorganisationen erhält das BACS eine gute

Florian Schütz

Bundesamt für Cybersicherheit (BACS)

Florian Schütz ist Direktor des Bundesamtes für Cybersicherheit (BACS). Er hat an der ETH in Zürich studiert und verfügt über einen Master in Computerwissenschaft sowie einen Master of Advanced Studies in Sicherheitspolitik und Krisenmanagement. In unterschiedlichen Positionen konnte er seine Expertise in der IT-Sicherheit ausbauen, u. a. bei Zalando in Deutschland.

ncsc.admin.ch

Hackerangriff auf Firma Xplain: Bericht des Bundesamtes für Cybersicherheit zur Datananalyse bit.ly/3QLCpmZ

Übersicht über die aktuelle Bedrohungslage im Cyberraum und kann dadurch zielgruppengerecht Informationen und Warnungen an die entsprechenden Empfängerkreise publizieren.

Das BACS nutzt die Erkenntnisse aus seiner operativen Tätigkeit zudem für Sensibilisierungsmassnahmen, die sich an Privatpersonen, Unternehmen und Behörden richten. Es koordiniert diese Anstrengungen mit zahlreichen Partnern wie beispielsweise der Schweizerischen Kriminalprävention (SKP) oder der Hochschule Luzern und führt landesweite Kampagnen durch. Alle Anstrengungen werden laufend ausgewertet und überprüft, damit sie hinsichtlich ihrer Realisierung und Wirksamkeit optimiert werden können.

Kritische Infrastrukturen schützen und Verwundbarkeiten reduzieren

Eine der Kernaufgaben des BACS ist die Unterstützung von Betreibenden kritischer Infrastrukturen beim Schutz vor Cyberbedrohungen. Hierzu stellt es Werkzeuge und Hilfsmittel zur Verfügung, welche die Cybersicherheit der Infrastruktur sowie ihrer Nutzerinnen und Nutzer erhöht. Dazu zählen beispielsweise technische Informationen zu IT-Infrastrukturen, welche für die Verbreitung von Schadsoftware oder das Betreiben von Phishing-Websites missbraucht werden. Das Computer Emergency Response Team (GovCERT) des BACS unterstützt Betreibende kritischer Infrastrukturen bei der Bewältigung von Cybervorfällen.

Seit Ende September 2021 ist das BACS ausserdem die offizielle Anlaufstelle zum Melden von Sicherheitslücken in der Schweiz und von MITRE als Autorisierungsstelle für die Vergabe von CVE-Nummern anerkannt. In dieser Funktion stellt das BACS für die ihm gemeldeten Schwachstellen die koordinierte Veröffentlichung sicher und leistet damit einen wichtigen Beitrag, damit das Ausnutzen dieser Schwachstellen möglichst vermieden werden kann.

Überblick Meldungseingang 2023

Im vergangenen Jahr hat das BACS, damals noch NCSC, insgesamt 49'380 Meldungen erhalten. Das entspricht einem deutlichen Anstieg von 30 Prozent gegenüber dem Meldeeingang im Jahr 2022. Nach wie vor belegen Meldungen zu verschiedensten Betrugsformen den ersten Platz (rund 30'000 Meldungen im letzten Jahr). Zu diesen Angriffsformen zählen beispielsweise angebliche E-Mails von Behörden, bei denen oft die Namen amtierender Bundesrätinnen und Bundesräte missbraucht werden. Die Betrüger wollen damit ihrer Nachricht mehr Glaubwürdigkeit verleihen. Weitere Beispiele sind angeblich nicht zustellbare Paketlieferungen, Anlagebetrug usw. Ausserdem beobachtete das BACS erste Angriffsversuche, bei denen offensichtlich künstliche Intelligenz zum Einsatz kam. Erwähnenswert sind ausserdem vereinzelt in Schweizerdeutsch verfasste Phishing-E-Mails. Dies war insbesondere beim Kleinanzeigenbetrug zu beobachten.

Angriffe mit Ransomware beschäftigen das BACS (respektive das damalige NCSC) seit einigen Jahren. Im Mai 2023 wurde ein IT-Dienstleister der Bundesverwaltung Opfer eines Ransomware-Angriffs. In der Folge wurden zuvor bei der Firma entwendete Daten im Darknet veröffentlicht. Davon betroffen waren auch Daten aus der Bundesverwaltung. Diese hat die veröffentlichten Daten umgehend analysiert und in der Folge einen ausführlichen Bericht über diese Datenanalyse veröffentlicht. Ebenfalls wurde eine Administrativuntersuchung eingeleitet, die Ende April abgeschlossen worden ist.

Derartige Angriffe auf Dienstleister zeigen deutlich auf, wie wichtig präventive Massnahmen gegen Cyberangriffe sind und welche zentrale Bedeutung dem nationalen und internationalen Austausch und der Kommunikation nach einem Cyberangriff zukommt. ●

«Es war nie geplant, die heutigen kryptographischen Verfahren zu ersetzen»

Kryptographie // Dank viel höherer Rechenleistung können Quantencomputer Aufgaben lösen, die heutige Computer überfordern. Die schlechte Nachricht: In naher Zukunft werden sie in der Lage sein, die heute gängigen Verschlüsselungsverfahren zu knacken. Was soll auf die heutigen Verfahren folgen? Wir haben mit Marc Stöcklin, Head of Security Research bei IBM in Rüschlikon, über den kommenden Q-Day gesprochen.

Dr. Marc Stöcklin

Head of Security Research, IBM Research Europe

Dr. Marc Stöcklin ist Principal Research Scientist und Leiter der Sicherheitsforschung bei IBM Research Europe – Zurich sowie globaler Co-Leiter für Quantum Safe Cryptography bei IBM.

research.ibm.com

Welche Verschlüsselungsverfahren gibt es?
Grundsätzlich gibt es zwei Verschlüsselungsverfahren, die symmetrische und die asymmetrische. Die symmetrische Verschlüsselung verwendet denselben Schlüssel zum Verschlüsseln und zum Entschlüsseln, was bedeutet, dass der Sender und der Empfänger den gleichen Schlüssel besitzen müssen. Dieses System hat den Nachteil, dass der gemeinsame Schlüssel über einen sicheren Kanal verteilt werden muss. Um diesen Nachteil zu umgehen, wurde in den 1970er Jahren die asymmetrische Verschlüsselung entwickelt. Sie verwendet ein Schlüsselpaar bestehend aus einem öffentlichen Schlüssel zum Verschlüsseln und einem privaten Schlüssel zum Entschlüsseln. Der öffentliche Schlüssel wird frei verteilt, während der private Schlüssel geheim bleibt. Dies ermöglicht eine sichere Kommunikation ohne die Notwendigkeit, einen gemeinsamen geheimen Schlüssel im Voraus auszutauschen. Das asymmetrische Verfahren schuf die Basis für den heutigen Informationsaustausch im Internet wie E-Banking usw. Für die Post-Quanten-Kryptographie ist eigentlich nur die asymmetrische von Bedeutung.

Wie funktioniert die asymmetrische Verschlüsselung?
Das asymmetrische Verschlüsselungsverfahren basiert auf schwierigen mathematischen Problemen. Also Problemen, die von einem Computer nicht in schneller Zeit gelöst werden können, bspw. die Faktorisierung von grossen Zahlen. Die Zahl 91 können auch wir als Menschen noch in die zwei Primfaktoren 13 und 7 zerlegen, Bei einer 600-stelligen Zahl braucht ein Computer Millionen von Jahren, weil es keinen schnellen Algorithmus dazu gibt. Auf dieser Einwegfunktion basiert die Sicherheit der Verschlüsselung: die Multiplikation ist einfach, aber die Faktorisierung, als die Zerlegung der Zahl in ihre Multiplikatoren, sehr schwierig. Die Faktorisierung einer grossen Zahl in Primzahlen, das sogenannte RSA-Verfahren, ist nur eines der möglichen Verfahren.

Warum stellen Quantencomputer eine Gefahr für diese Verschlüsselungsverfahren dar?
In den 90er Jahren entwickelte Peter Shor einen Algorithmus, mit dem ein Quantencomputer die Faktorisierung innerhalb von Stunden berechnen kann. Damals waren Quantencomputer nur Theorie, heute gibt es sie. Und sie werden immer leistungsstärker.

Ist die heute gebräuchliche Verschlüsselung also noch sicher?
Jein. Stand heute ist das RSA-Verfahren, das seit 50 Jahren angewendet wird, sicher. Aber durch die Zunahme der Rechenleistung werden Quantencomputer in der Zukunft in der Lage sein, Informationen, die heute mit diesen Verfahren geschützt sind, zu entschlüsseln.

Wann wird es so weit sein?
Es gibt verschiedene Schätzungen, aber genau kann es niemand sagen. Das National Institute of Standards and Technology (NIST) in den USA bspw. geht davon aus, dass es 2030 kryptographisch relevante Quantencomputer geben wird, die für die Kryptographie eine Gefahr darstellen. Es gab und gibt verschiedene Schätzungen, wie viele Quantenbits, kurz Qubits, es braucht, damit ein Quantencomputer den Algorithmus von Shor oder auch andere Algorithmen anwenden kann, die die Verschlüsselung knacken können. Anfangs wurde von Milliarden von Qubits ausgegangen, aber in den letzten Jahren hat sich sehr viel getan. Heute geht man von einer Grössenordnung von 10'000 Qubits aus. IBM hat letzten Herbst 1'100 Qubits erreicht. Die Zahl wird in den nächsten Jahren steigen, und irgendwann wird der Q-Day kommen. Heute haben wir auch das Problem, dass Quantencomputer und Qubits sehr fehleranfällig sind. Aber auch in diesem Bereich werden mehr Durchbrüche gemacht, um die Fehlerkorrektur oder Fehlerverringerung zu beschleunigen.

Welche neuen Verfahren, die einem Quantencomputer widerstehen, stehen zur Ablösung bereits zur Verfügung?
2022 hat das NIST im Rahmen eines mehrjährigen Wettbewerbs vier Algorithmen ausgewählt, die quantensicher sind: Zwei CRYSTALS-Algorithmen, CRYSTALS-Kyber und CRYSTALS-Dilithium, sowie FALCON und SPHINCS+. Noch in diesem Sommer wird das NIST die neuen Standards öffentlich publizieren. Dies werden die neuen Standards sein, um die digitale Welt für die nächsten Jahrzehnte sicher zu machen. An diesem mehrjährigen Wettbeweb konnte jeder teilnehmen, und Kryptographinnen und Kryptographen weltweit haben versucht, die eingegebenen Verschlüsselungsalgorithmen zu knacken. Logischerweise sind viele rausgeflogen, und am Ende hat das NIST die genannten vier Algorithmen ausgewählt, weil sie am sichersten und auch am praktikabelsten sind. Europa ist in diesem Bereich übrigens führend. Alle vier ausgewählten Verfahren sind primär von Instituten aus Europa entwickelt worden, drei der vier Algorithmen massgeblich von uns am IBM-Forschungslabor in Rüschlikon.

Für welche Bereiche werden die Algorithmen verwendet?
CRYSTALS-Kyber ist ein Algorithmus für den sicheren Schlüsselaustausch über einen öffentlichen Kanal. Er ersetzt bekannte Verfahren wie das Diffie-Hellman-Verfahren und ist im Gegensatz zu diesen sicher gegen Quantencomputer. Die drei anderen Algorithmen sind Verfahren für digitale Signaturen, um die Authentizität von Zertifikaten, Dokumenten, Softwareupdates usw. zu beweisen.

Ab wann und für wen gilt der neue NIST-Standard?
Standard heisst, dass man sich darauf einigt, wie man verschlüsselt und kommuniziert. Die US-Regierung macht das nicht nur für sich selbst, sondern für das gesamte Ökosystem, also auch für die Finanzindustrie und andere. Die US-Regierung hat in einer Roadmap festgelegt, wann und in welchen Anwendungen die neuen Algorithmen integriert werden müssen. Die Standards des NIST sind massgeblich für ganz viele Bereiche in den USA, haben aber auch eine weltweite Wirkung. Auch in Europa referenzieren Behörden auf das NIST. Die Standardisierung hat Signalwirkung: Die Verschlüsselung einer Lösung wird typischerweise zertifiziert. Softwarehersteller, die die US-Regierung und auch den US-Markt beliefern, müssen diese Zertifizierungen vorweisen. Die Käufer möchten nicht 20 verschiedene Algorithmen implementieren. Daher wird auch die Privatwirtschaft nachziehen, da Kryptographie überall eingesetzt wird und alle betroffen sind.

Haben IBM und die anderen Entwickler ein Patent auf ihre Algorithmen?
Nein. Eine der Vorgaben des Wettbewerbs war, dass die eingereichten Verfahren nicht mit Patenten belastet sein dürfen. Alle eingereichten Algorithmen sind öffentlich als Open Source verfügbar und müssen frei von Intellectual Property Rights sein. Es ist wichtig, dass die Algorithmen transparent für alle einsehbar sind und geprüft werden können.

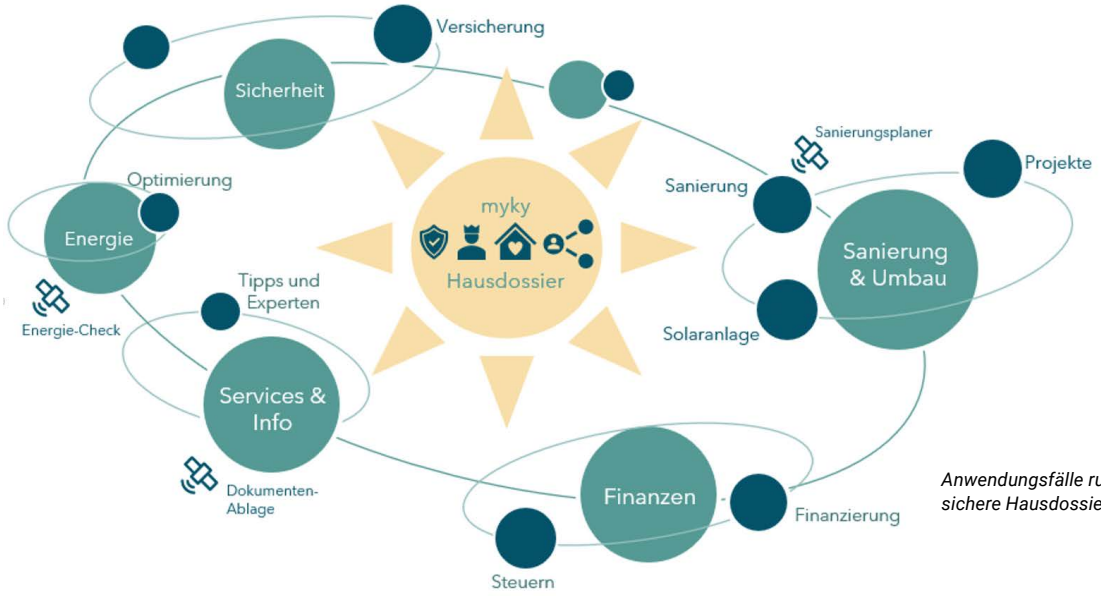
Wann findet die Ablösung der heutigen Verschlüsselungen durch die neuen Algorithmen statt?
Sie hat bereits angefangen. Bei IBM haben wir in unseren Grossrechnern schon 2022, vor der Bekanntgabe des NIST, die Algorithmen implementiert. Verschiedene Cloud-Provider bieten die Algorithmen an, im Google Chrome Browser sind sie schon integriert und Apple hat beim Sicherheitsupdate von iMessage im Februar bekannt gegeben, dass neu CRYSTALS-Kyber verwendet wird. Nun geht es darum, dass sich Unternehmen und Dienstleister auf diese Umstellung vorbereiten können. Es soll nicht so werden wie beim Jahr-2000-Problem. Damals hat man die Umstellung relativ spät gemacht und es ist sehr teuer geworden. Jetzt haben wir noch etwas mehr Zeit, aber es steht und fällt damit, ob wir es rechtzeitig angehen und ob es schlau geplant wird.

Wo sehen Sie die Schwierigkeiten beim Wechsel zu den neuen Verfahren? Ist der Aufwand gross?
Bis jetzt hat sich nie wirklich jemand viel Gedanken zu den verwendeten Kryptographien gemacht. Sie haben existiert, sie wurden eingesetzt. Niemand hat ein Inventar gemacht, wo welche Verfahren in der heute sehr komplexen IT-Umgebung angewendet werden, da nie geplant war, die Kryptographie zu ersetzen. Man muss zuerst verstehen, wie die relevanten Datenströme verschlüsselt sind. IBM unterstützt Organisationen bei der Umstellung: Wie bereitet man sich vor? Was soll priorisiert werden? Wie organisiert und orchestriert man das Ganze? Und wie stelle ich effizient über einen gewissen Zeitraum um, ohne dass es sehr viel Geld und Kopfschmerzen bereitet?

Die Umstellung ist sehr komplex, weil es in der heutigen IT-Landschaft viele Abhängigkeiten gibt. Eine Firma bezieht einen Grossteil ihrer Software oder zumindest Komponenten davon von verschiedenen Anbietern oder direkt aus der Cloud. Die Umstellung hat dadurch viele Abhängigkeiten, da die Systeme weiterhin miteinander kompatibel sein müssen. Bspw. muss eine Bank sicherstellen, dass die Umstellung nicht nur im E-Banking-Backend erfolgt, sondern dass auch alle Bankkunden, sprich die von ihnen verwendeten Browser, dazu in der Lage sind. Bei heutigen Initiativen, in denen Workloads in Clouds oder Container in Cluster verschoben werden, sollte die Quantum-Safe-Thematik von Anfang an integriert sein. Dies retrospektiv umzustellen ist viel komplexer und teurer. Hier gibt es das Konzept der Kryptoagilität, bei der Kryptographie nicht tief im Code eingebettet werden muss, sondern als Cryptography as a Service externalisiert wird. Somit kann Kryptographie besser und einfacher verwaltet und verwendet werden. Das BSI in Deutschland hat kürzlich eine Empfehlung zu Kryptoagilität publiziert, die Firmen als Leitfaden dient. ●

Ob wir bereit für den Q-Day sind, und in welchen Bereichen der Kryptographie bei IBM sonst noch geforscht wird, sagt Marc Stöcklin im zweiten Teil des Interviews.

Jetzt online weiterlesen:
ti8m.com/kryptographie



Anwendungsfälle rund um das sichere Hausdossier

Digital Trust und Datenaustausch im Ökosystem Wohnen

Digitale Ökosysteme // Eine zentrale Herausforderung für den Aufbau unternehmensübergreifender Customer Journeys sind verlässliche Daten, die jederzeit gut geschützt sind und möglichst einfach kontrolliert zwischen Unternehmen und Kunden geteilt werden können. Dieser Beitrag gibt Einblicke in das Thema am Beispiel des Start-ups myky. myky ist das sichere, persönliche und digitale Hausdossier für Immobilieneigentümer und ihr Schlüssel zu Tools, Tipps und einem Netzwerk, um das Eigenheim nachhaltig zu bewirtschaften.

Wohnen ist ein Grundbedürfnis jedes Menschen und rund um die Wohnsituation und die Immobilie gibt es unzählige Anwendungsfälle, in denen Unternehmen und Privatpersonen Daten benötigen und verarbeiten. myky hat sich in den letzten Monaten verstärkt mit der nachhaltigen Sanierung von Wohngebäuden auseinandergesetzt, daher nutzen wir dieses Beispiel für diesen Beitrag. Der Immobiliensektor ist ein wesentlicher Faktor für die Schweiz, um ihre CO_2-Ziele zu erreichen. Immobilien verursachen gemäss Bundesamt für Umwelt knapp ein Viertel der heutigen Treibhausgas-Emissionen und bieten viel Potenzial für Verbesserungen. Kundenbefragungen von myky zeigen, dass eine Sanierung für die Eigentümer eine komplexe Aufgabe ist, die sie nur angehen, wenn es für sie ökonomisch und ökologisch nachhaltig ist. Zentrale Herausforderungen sind unter anderem fehlende Daten zum aktuellen Zustand, das ideale Vorgehen und belastbare Hochrechnungen realistischer Fördermittel sowie die Kosten einer Sanierung.

Herausforderung Datenqualität

Es gibt viele Datenquellen rund um Immobilien. Neben den sukzessive ausgebauten öffentlichen Datenquellen bieten spezialisierte Datenprovider Informationen zu allen Objekten der Schweiz. Weitere mögliche Quellen sind Daten von Unternehmen, die für ihre Produkte und Dienstleistungen mit Immobiliendaten arbeiten wie z. B. Banken für die Vergabe von Hypotheken, Versicherungen für Gebäude- oder Hausratsversicherungen, Energieversorger, Handwerker sowie Bauunternehmer und Architekten. Diese Akteure haben eine isolierte Sicht auf die Immobilie, die oft auf den Zeitpunkt der letzten Transaktion/Interaktion mit den Hauseigentümern bezogen ist und in der Regel nur für ihre jeweiligen Themen «verläss-

Tiziano Lenoci

CEO myky AG

Tiziano Lenoci ist Betriebsökonom (MSc) und war vor der Gründung der myky AG Mitglied der Gruppenleitung der GVB Gruppe. Er war CEO der GVB Services AG und u. a. verantwortlich für das gruppenweite Marketing & Sales und Start-up-Investments.
myky.ch

Stefan Reitbauer

CEO NNH Holding AG

Stefan Reitbauer ist Wirtschaftsinformatiker und hat sich bereits in seiner Doktorarbeit an der HSG mit dem Thema Unternehmensnetzwerke auseinandergesetzt. Bevor er Ende 2022 als CEO der NNH startete, war er bei Swisscom u. a. Field CTO für Banking und Insurance.

liche» Daten umfasst. Sobald diese Unternehmen neue, «breitere» Anwendungsfälle bearbeiten, fehlt oft eine belastbare Datenbasis. So sind im Bereich der nachhaltigen Sanierung notwendige Informationen, bspw. zu Heizsystem, Gebäudevolumen oder Lageinformationen, oft veraltet, lückenhaft und nicht zentral verfügbar bzw. nutzbar.

myky als Schlüssel fürs nachhaltige Eigenheim – intelligent und sicher

Den besten, weil umfassendsten Zugang, zu den «richtigen» Informationen über eine Immobilie haben in der Regel die Hauseigentümer. In der Praxis werden diese Informationen heute oft physisch in Aktenordnern abgelegt. Die Vision von myky ist es, den Hauseigentümern eine Plattform bereit zu stellen, auf der sie die Informationen zu ihrer Immobilie geschützt digital ablegen und für konkrete Anwendungsfälle wie die Sanierung nutzbringend einsetzen können. Ein «intelligenter Assistent» soll den Eigentümern mit dem myky-Hausdossiers wertvolle Hinweise geben und sie auf Chancen und Risiken rund um ihre Immobilie aufmerksam machen.

Das Teilen von Daten

Im heutigen vernetzten Umfeld ist es unerlässlich, dass Datenplattformen nicht isoliert agieren, sondern nahtlos mit anderen Systemen und Partnern interagieren können. Ein wichtiger Pfeiler des myky-Hausdossiers ist, dass unter der Kontrolle, und nur mit Zustimmung des Hauseigentümers, Daten rund um seine Immobilie geteilt werden. Heisst: Sowohl der Hauseigentümer teilt nach Bedarf seine Daten rund um seine Immobilie, als auch die Unternehmen, mit denen der Hauseigentümer interagiert, stellen Daten für das Hausdossier bereit. Im Kontext der nachhaltigen Sanierung können Hauseigentümer Informationen zum aktuellen Gebäudezustand (Heizung, Isolation, etc.) und ihren Sanierungsplänen mit Banken, Handwerkern, Gebäude-Experten oder ihrer Gebäudeversicherung teilen. Im Gegenzug können die Unternehmen mit den Hauseigentümern Informationen zu ihrer Hypothek, dem Wert ihrer Immobilie, der Versicherungsdeckung oder auch konkrete Offerten zu ihren Wohnideen teilen. Im Idealfall arbeiten beispielsweise Handwerker direkt in separaten Projektbereichen des myky-Hausdossiers interaktiv mit den Hauseigentümern zusammen und entwickeln so das passende, finanziell optimierte Sanierungsvorhaben.

Google-basierte Plattform als technische Basis

In einer Ära, in der Daten das Herzstück vieler Unternehmen bilden, sind Sicherheit und Vertrauen in die Verwaltung dieser Daten von entscheidender Bedeutung. Das trifft insbesondere auf private, von Eigentümern erfasste Informationen rund um das Eigenheim zu. Hauseigentümer wie Unternehmen stehen vor der Herausforderung, solche Informationen umfassend zu schützen, während sie gleichzeitig die Möglichkeiten moderner Technologien nutzen und gut abgestützte, datenbasierte Entscheide treffen möchten. myky nutzt dafür eine von der NNH Holding aufgebaute Plattform. Diese Plattform wurde im Auftrag von 19 Kantonalbanken gemeinsam mit ti&m als Generalunternehmer als Implementierungs- und Betriebspartner umgesetzt. Die Vision von NNH ist, dass über die NNH-Plattform viele Unternehmen wie myky unternehmensübergreifende Customer Journeys rund um das Thema Wohnen effizient und sicher umsetzen können. Die NNH-Plattform basiert für zentrale Komponenten wie Datenverarbeitung und -analyse (u. a. BigQuery), Systemintegration (u. a. Apigee) und Security auf mächtigen Standard-Services der Google Cloud Platform (GCP). Wichtige Design-Kriterien der Plattform sind unter anderem:

- *Nutzung offener Standards und etablierter Produkte*
- *Profitieren von der Innovationskraft und dem Funktionsumfang einer führenden Cloud-Lösung durch konsequenten Einsatz von Google-Produkten*
- *Umsetzen von Best Practices wie z. B. Datenhaltung in der Schweiz, Customer Managed Encryption und Zero-Trust auch zwischen den Plattform-Komponenten.*
- *Definition von API-basierten Datenprodukten anstelle eines starren Immobilien-Referenzdatenmodells*

Auch unsere nächsten Anwendungsfälle setzen auf erweiterte Funktionen für das kontrollierte Teilen von Daten, das Ermöglichen datenbasierter Entscheidungen sowie flexible und sichere Interaktionen zwischen Unternehmen und Privatpersonen. Für ein nachhaltiges Eigenheim und damit einen Beitrag, die CO_2-Ziele zu erreichen. ●

Quelle Grafik: myky, 2024

Digital Trust bei ti&m: ein ganzheitlicher Ansatz

ti&m Digital Trust Center // Datenschutzverletzungen, Cyberangriffe, Fehlverhalten von Unternehmen: Fast täglich lesen wir von Vorfällen, die das Vertrauen in die digitale Welt erschüttern. Traditionelle Sicherheitsmassnahmen und Compliance-Standards allein reichen nicht aus, um die komplexen Anforderungen zu erfüllen. Mit unserem Digital Trust Center verfolgen wir einen ganzheitlichen Ansatz, der Vertrauen, Sicherheit und Technologie aufeinander abstimmt.

Unser Privat- und Geschäftsleben verschiebt sich immer mehr in den digitalen Raum, Transaktionen werden (fast) nur noch online abgewickelt, persönliche Informationen, von Steuererklärungen bis zu Kinderfotos, liegen irgendwo in einer Cloud. Klar also, dass für die Digitalisierung die gleiche Regel gilt wie für eine Bank: Vertrauen ist das höchste Gut. Weil digitales Vertrauen zum entscheidenden Wettbewerbsfaktor wird, ist ein umfassender Blick auf Digital Trust entscheidend, um den Ansprüchen und Herausforderungen nachhaltig gerecht zu werden..

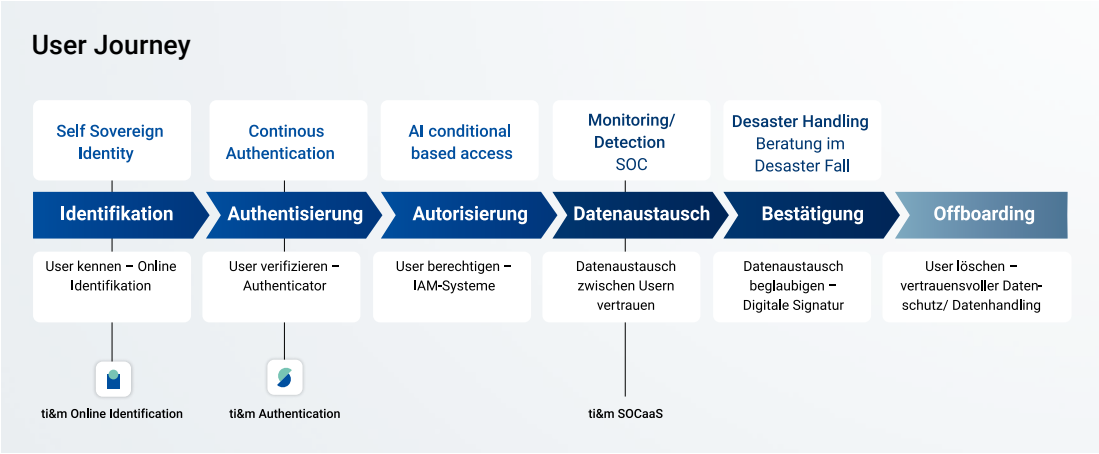
Blockchain, KI und Co. – die Hauptrolle spielt die Technologie

Der Technologie kommt im Digital Trust die entscheidende Rolle zu. Und diese Rolle ist durchaus ambivalent. Zwar bieten Innovationen wie Blockchain, künstliche Intelligenz oder IoT neue Möglichkeiten, das digitale Vertrauen zu stärken. Sie bieten aber auch neue Gefahren, das Vertrauen zu erschüttern, ob absichtlich durch Aktivitäten von Cyberkriminellen, oder unabsichtlich durch eine falsche Antwort eines intelligenten Chatbots aufgrund eines Bias. Unser Digital Trust Center integriert diese Technologien nahtlos in bestehende Infrastrukturen und Prozesse, und ermöglicht es Unternehmen, durch automatisierte Compliance-Checks, kontinuierliche Sicherheitsanalysen und massgeschneiderte Schulungen Risiken zu minimieren und das Vertrauen in die Stakeholder zu festigen.

Kompetenz entlang der gesamten User Journey

Durch die Integration von Technologie, Compliance, Governance und einer vertrauensvollen Unternehmenskultur können Unternehmen ein Fundament für digitales Vertrauen schaffen, das sie für die Herausforderungen der Zukunft rüstet. ti&m bietet eine umfassende Palette von aufeinander abgestimmten Services und Produkten, die Unternehmen dabei unterstützen, digitales Vertrauen aufzubauen und zu erhalten. Dank unserer langjährigen Expertise und Innovationskraft berät unser Digital Trust Center unsere Kunden bei der Umsetzung von sicheren Trust-Konzepten und entwickelt massgeschneiderte Lösungen, die die spezifischen Anforderungen und Herausforderungen unserer Kunden entlang der gesamten User Journey adressieren.

Um unsere Kunden gegen die stetig wachsende Zahl von Cyberbedrohungen und Angriffen zu schützen, entwickeln wir gemeinsam mit ihnen proaktive und effektive Sicherheitsstrategien. Wir entwickeln und implementieren für unsere Kunden sichere, digitale Plattformen und Infrastrukturen und helfen ihnen so, eine Resilienz gegen zukünftige Bedrohungen aufzubauen, und mit ti&m Online Identification, ti&m Authentication und SOCaaS (Security Operations Center as a Service) bieten wir bewährte Security- und Authentisierungsprodukte, die sich nahtlos in bestehende Lösungen integrieren lassen.



Durch die Kombination unserer Produkte und Services schaffen wir so eine robuste Sicherheitsumgebung, die digitales Vertrauen gewährleistet und es Unternehmen ermöglicht, ihre digitalen Geschäftsprozesse sicher und effizient zu gestalten. Dabei legen wir besonderen Wert auf die kontinuierliche Verbesserung und Anpassung unserer Lösungen an die sich verändernde Bedrohungslage.

Unsere Expertise und unser Engagement in der digitalen Sicherheit ermöglichen es Unternehmen, nicht nur ihre aktuellen Sicherheitsbedürfnisse zu erfüllen, sondern auch zukunftsorientiert und resilient zu agieren. So tragen wir massgeblich dazu bei, dass unsere Kunden im digitalen Zeitalter erfolgreich und vertrauensvoll agieren können. Wir unterstützen Unternehmen umfassend bei der erfolgreichen Gestaltung ihrer digitalen Transformation und tragen dazu bei, Vertrauen bei ihren Kunden, Partnern und Mitarbeitenden zu stärken.

Leunita Saliji

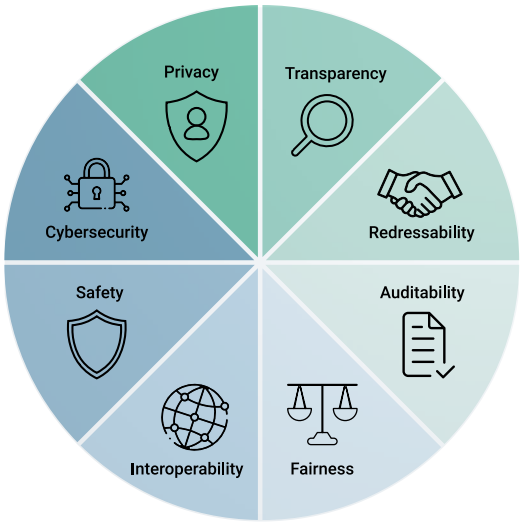
Head Cloud & Innovation Hosting, Mitglied der Geschäftsleitung

Leunita Saliji arbeitet seit über sechs Jahren bei ti&m und verantwortet seit Dezember 2023 den Bereich Cloud & Innovation Hosting bei ti&m. Davor war sie schon als Head Application Management und als Head Operations & Services Management in verschiedenen Führungspositionen bei ti&m tätig. Sie hat einen Master in Business Information Technology und doziert an der Fernfachhochschule Schweiz.

ti8m.com

Globale Perspektive und Kulturwandel

Das World Economic Forum bietet mit seinem Framework eine umfassende Orientierungshilfe für Unternehmen, um Digital Trust auf globaler Ebene zu verstehen und umzusetzen. Es umfasst Richtlinien zu Cybersecurity, Privacy, Transparency, Redressability, Auditability, Fairness, Interoperability und Safety und zeigt auf, wie das digitale Vertrauen in der gesamten Wirtschaft durch kollaborative Herangehensweisen gestärkt werden kann.



Allerdings: Um Digital Trust nachhaltig in einer Organisation zu verankern, braucht es mehr als nur Innovation, technologisches Know-how und die richtigen Massnahem in den Bereichen Cybersicherheit, Datenschutz oder Interoperabilität. Ohne Unternehmenskultur, in der Digital Trust, Transparenz, Ethik und Respekt fest verankert sind und von den Führungskräften jeden Tag vorgelebt wird, werden auch die durchdachtesten Massnahmen nicht die gewünschte Wirkung erzielen. Nur durch einen erfolgreichen Kulturwandel kann das Vertrauen der Mitarbeitenden und der Kunden nachhaltig gestärkt werden. ●

So schafft ti&m digitales Vertrauen

Authentication & Identification //
Mit unseren Produkten und Services unterstützen wir unsere Kunden entlang der gesamten IT-Wertschöpfungskette dabei, sichere und vertrauenswürdige digitale Geschäftsräume zu schaffen.

Cyberattacken haben nicht nur in der Schweiz stark zugenommen, sondern verursachen weltweit Schäden in Milliardenhöhe. Die weitverbreitete Phishing-Methode stellt nach wie vor eine effektive Methode für Cyberkriminelle dar, um an sensible Informationen zu gelangen. Ein angemessener Schutz bildet daher die Grundlage für den Erfolg und das Wohlergehen von Individuen, Unternehmen und Gesellschaften. Eine umfassende Sicherung sensibler Daten und ein ausreichender Schutz von komplexen Systemen, offenen Plattformen und innovativen Lösungen ist unerlässlich und gehört nicht zuletzt aufgrund der ständig wachsenden Bedrohungen zu den grundlegenden Säulen des digitalen Vertrauens.

Passwörter, die es nicht gibt, kann man nicht stehlen oder erraten

Zu den zentralen Massnahmen zur Verbesserung der digitalen Sicherheit gehört die passwortlose Authentifizierung, welche eine zukunftssichere Alternative zu herkömmlichen Passwörtern bietet. Ausgehend von der bekannten Verwundbarkeit von Passwortsystemen entwickelte und förderte ein branchenübergreifender Zusammenschluss von Organisationen und Unternehmen namens FIDO-Alliance (Fast Identity Online) weltweite Standards, um die Verwendung von Passwörtern zu reduzieren und sichere sowie benutzerfreundliche Lösungen zu fördern. Mit Passkeys, einer Erweiterung des FIDO2-Standards, wurde eine innovative Möglichkeit geschaffen, die Passwörter durch kryptografische Schlüsselpaare ersetzt. Anders als beim Passwort wird der private Schlüssel nie über das Netzwerk ausgetauscht und verlässt so niemals das Gerät (Smartphone oder ein anderes Hardware Token) oder das Ökosystem des Geräteherstellers. Entsprechend können diese im Gegensatz zu Passwörtern auch nicht abgefangen oder gestohlen werden.

Zukunftsfähiges Produkt mit «Schlüssel» zum Erfolg

Bereits 2013 setzte ti&m auf den Paradigmenwechsel in der sicheren Authentifizierung und ermöglichte ihren Kunden eine passwortlose und Phishing-sichere Alternative. Mit dem Produkt ti&m Authentication entwickelten wir eine benutzerfreundliche Authentisierungsplattform, welche den höchsten Sicherheitsstandards entspricht und auf der gleichen Technologie wie Passkey aufbaut. Früh erkannten wir den Mehrwert und das Potenzial dieser Technologie und erleichterten mit viel Digitalisierungserfahrung die wesentlichen Authentisierungshürden, ohne die Sicherheit zu kompromittieren. Eine nahtlose und einfache Integration in kundenspezifische Umgebungen bietet die notwendige Flexibilität eines lokalen Schweizer Produktes, egal ob in traditionellen Unternehmensnetzwerken, Cloud-Infrastrukturen

oder mobilen Anwendungen. Ein Wegweiser für die Entwicklung von sichereren, benutzerfreundlicheren und adaptiveren Authentifizierungslösungen in einer Welt, die sich den ständig ändernden Anforderungen anpassen muss.
Der wachsende Trend zur passwortlosen Authentifizierung und deren Vorteile in Bezug auf Sicherheit und Benutzerfreundlichkeit ist merklich zu spüren. Dennoch wird es wohl noch eine Weile dauern, bis die neue Technologie in unserem Alltag vollständig etabliert und akzeptiert wird. Als Experte für Cybersicherheit und Authentifizierungstechnologien können wir unsere Kunden umfassend beraten und realisieren massgeschneiderte Sicherheitslösungen mit der perfekten Balance zwischen Benutzerfreundlichkeit und höchsten Sicherheitsstandards.

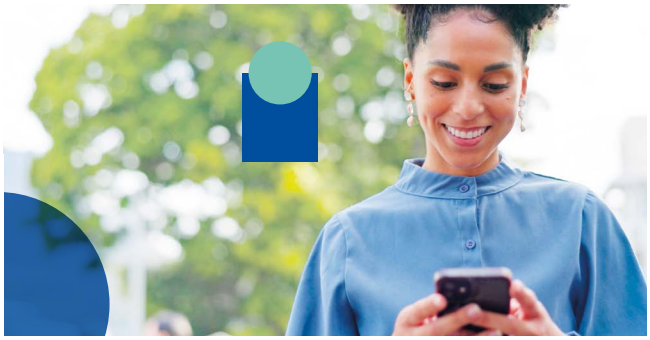
Philip Dieringer
Head Bern, ti&m
Ihr Experte für sichere Authentisierungen.

ti&m Online Identification

Jede Kundenbeziehung beginnt mit der sicheren Identifikation des Neukunden. Der Alltag ist schon kompliziert genug, und Kundinnen und Kunden haben keine Zeit (oder schlicht keine Lust), physisch in einer Filiale anzustehen oder sich online durch ein wenig intuitives Identifizierungsapp zu kämpfen, nur um ein neues Konto zu eröffnen.
Häufig wird erwähnt, Digitalisierung sei mehr als nur analoge Prozesse in die digitale Welt zu überführen. Es geht darum, gesamte Prozesse neu zu denken und in einer digitalen Lösung abzubilden, die zum einen Nutzerinnen und Nutzern dabei helfen, Leistungen schneller und unkomplizierter zu beziehen, und zum anderen Firmen von mühseligen und kostenintensiven administrativen Aufgaben befreit. Mit ti&m Online Identification bieten wir unseren Geschäftskunden genau das: Eine vollständig automatisierte Lösung, die es Neukundinnen und Neukunden erlaubt, sich jederzeit und von überall auf der Welt zu identifizieren und ein Konto zu eröffnen.

Mehr als nur Identifikation

Als Experte für Online-Identifikation wissen wir, dass die Identifikation nur ein Teil der User Journey und der im Hintergrund ablaufenden Prozesse ist. Deshalb unterstützen wir unsere Kunden nicht nur bei der nahtlosen Implementierung der ti&m Online Identification als White-Label-Lösung, sondern optimieren alle Teile der bestehenden oder neu geschaffenen User Journey und erhöhen so die Konversionsrate der Kundenonboardings. Gesamte Prozesse zu Ende denken heisst für uns auch, die Identifikation mit dem CRM oder weiteren Applikationen zu verbinden und nachgelagerte Services wie digitale Signaturen zu integrieren. So setzt Swisscom bei ihrem



neuen Signaturprozess «Swisscom Sign» auf ti&m Online Identification, um Kundinnen und Kunden rechtsgültig zu identifizieren und qualifizierte elektronische Signaturen auszustellen, die wiederholt für Vertragsabschlüsse und Transaktionen in der Schweiz und der EU genutzt werden können. Software Development Kits (SDKs) für Web und für mobile Plattformen (iOS und Android) ermöglichen die nahtlose Integration in unterschiedliche Umgebungen, genutzt werden kann der Identifikationsservice entweder On-Premises oder As-a-Service von ti&m.

Höchste Sicherheitsstandards

Sichere Authentisierungen wie wir sie mit ti&m Authentication anbieten oder eben Identifikationslösungen wie ti&m Online Identification sind wichtige Digital-Trust-Elemente. Sie ermöglichen es Nutzerinnen und Nutzern, sich jederzeit zu authentisieren, um auf Daten und Services zuzugreifen, oder rund um die Uhr ein neues Konto zu eröffnen, um eine neue Geschäftsbeziehung einzugehen und elektronische Signaturservices in Anspruch zu nehmen. Die mehrfach ausgezeichnete ti&m Online Identification ist FINMA-konform und erfüllt alle schweizerischen und europäischen Sicherheitsstandards wie ETSI oder eIDAS. Unser Dokumentenprüfsystem erkennt Identitätsausweise und Pässe aus über 40 Ländern und ist in der Lage, das bei der Identifikation verwendete Dokument sowohl durch die maschinenlesbare Zone (MRZ) als auch durch die visuelle Inspektionszone (VIZ) zu lesen.
Häufig ist die Identifikation der erste Kontakt einer Neukundin oder eines Neukunden mit den digitalen Services einer Organisation, entsprechend wichtig sind nutzerfreundliche Identifikations- und Onboardingprozesse, um positive Customer Journeys zu gestalten. Denn wie so häufig bei einer Reise ist der erste Schritt der wichtigste. Und der muss für Neukundinnen und Neukunden einfach, sicher und schnell sein.

Martin Unterbäumen
Head Client Engagement, ti&m
Ihr Experte für Online-Identifikationen.

KI – eine Vertrauensfrage?

Künstliche Intelligenz //
Wie fest wir KI vertrauen können, wird immer mehr zur Gretchenfrage des 21. Jahrhunderts.

Wohl alle von uns haben sich bei der Nutzung von Generative AI schon gefragt, ob man der Antwort trauen kann. Zum einen ist nicht klar, ob die zum Training verwendeten Daten wie Zeitungsartikel und Blogbeiträge faktisch korrekt sind, zum anderen stellt sich die Frage, wie viel Bias in den grossen Sprachmodellen steckt. Klar, wir alle wollen in unseren Antworten keinen Bias. Aber was ist ein Bias? Wer bestimmt eigentlich, was ein Bias ist? Vorurteile prägen uns als Individuen und als Gesellschaft und sind nun einmal Teil der Realität. Ein Beispiel: In Führungspositionen arbeiten mehr Männer als Frauen. Dass das nicht gut ist, sind wir uns wohl alle einig. Aber es ist die Realität. Soll Generative AI in ihren Antworten nun die Welt abbilden, wie sie ist, oder wie sie idealerweise sein sollte? Und wie sieht eine solche ideale Welt aus? Ist die Vorstellung, dass es gleich viele Frauen und Männer in Führungspositionen geben soll, nicht auch wieder ein Bias – wenn auch ein positiver? Es gibt verschiedene Initiativen, um bspw. durch AI Alignment gesellschaftliche Werte in grosse Sprachmodelle zu integrieren. Dies ermöglicht es Organisationen auch sicherzustellen, dass die verwendeten KI-Tools interne Geschäftsregeln und Complianceanforderungen erfüllen. Allerdings: Grosse Sprachmodelle ganz ohne Bias zu trainieren, wird kaum möglich sein. Denn wie bei Menschen gilt auch bei künstlicher Intelligenz: Im Lernen steckt auch immer ein Bias.

Obwohl alle grossen Sprachmodelle über ethische Sicherheitsvorkehrungen verfügen, ist in den Medien regelmässig über sogenannte Jailbreaks zu lesen. Beim Jailbreaking können durch spezifische Textaufforderungen die Richtlinien zur Inhaltsmoderation (z. B. bei den Themen Rassismus und Sexismus) umgangen werden. Im besten Fall sind die durch Jailbreaking provozierten Antworten einfach nur lustig, im schlechtesten Fall können die falschen (Preisangaben, verbindliche Zusagen) und rufschädigenden (Sexismus, Rassismus) Antworten für Firmen rechtliche und finanzielle Konsequenzen haben. Mit Guardrails (Leitplanken) wird versucht, die

Nutzung auf die vorgesehenen Bereiche zu limitieren und eine «Überlistung» des Chatbots zu verhindern. Mit Content-Filtern für die Fragen und die Antworten kann sichergestellt werden, dass keine unerwünschten Themen besprochen werden. Zudem kann es sinnvoll sein, dass grosse Sprachmodelle in ihren Antworten immer einen Disclaimer mitliefern, der darauf hinweist, dass die Antworten von der Nutzerin oder dem Nutzer überprüft werden sollten.

Auch das Problem der sogenannten Hallucinations, also das Generieren von falschen oder erfundenen Informationen aufgrund von Datenlücken, wurde noch nicht befriedigend gelöst. Datenlücken entstehen bpsw., weil die zum Training verwendeten Datensätze veraltet sind. Nutzt eine Organisation einen an ein LLM gekoppelten KI-Chatbot, können die verwendeten Daten Monate oder gar Jahre alt sein. Neue und spezifische Informationen über Produkte und Services fehlen, was zu falschen Antworten führt, die das Vertrauen von Kunden und Mitarbeitenden in die Technologie und schlussendlich in die Organisation untergraben. Diesem Problem kann mit Retrieval Augmented Generation (RAG) begegnet werden: RAG inkludiert aktuelle Informationen oder andere zusätzlichen Wissensquellen wie firmeninterne Daten, ohne dass grosse Sprachmodelle mit den neuen Datensätzen trainiert werden müssen. Man will die diversen Fähigkeiten der grossen Sprachmodelle nutzen, sich aber nicht auf deren «Wissen» verlassen. Weil viele Organisationen den durch KI generierten Antworten noch misstrauen, wird in die Prozesse häufig auch ein «human in the loop» eingebettet.

Eine weitere Herausforderung gibt es bei der granularen Berechtigung der Nutzerinnen und Nutzer. Nicht alle Mitarbeitenden oder Kunden sollen auf die gleichen, meist sehr sensitiven Daten zugreifen können. Es gilt, Wege zu finden, wie sensitive firmeninterne Daten so in Lösungen einzubetten, dass Mitarbeitende und Kundinnen und Kunden mit ihren Prompts nur Antworten erhalten, die auch für sie gedacht sind.

Wir bei ti&m sind überzeugt: KI kann ihr Potenzial nur entfalten, wenn es gelingt, sichere, vertrauenswürdige und ethische Lösungen zu schaffen. Denn KI ohne Digital Trust ist wertlos. ●

Lisa Kondratieva
Head AI & Digital Solutions, ti&m
Ihre Expertin für Artificial Intelligence und Digital Solutions.

Mit SBOM die Resilienz von IT-Services verbessern

Software Bill of Materials // Eine SBOM ist eine Liste aller Softwarekomponenten, Abhängigkeiten und Metadaten, die mit einer Anwendung verknüpft sind. Das Führen einer genauen «Zutatenliste» einer Software kann automatisiert werden und hilft, Anwendungen besser zu schützen.

Stephan Sutter

CTO Bern, ti&m

Stephan Sutter ist CTO des Standorts Bern. Er ist seit rund 23 Jahren als IT-Architekt und seit 16 Jahren in der ICT-Management-Beratung für Banken, Versicherungen und Verwaltungen tätig. Stephan Sutter ist Elektro-Ingenieur HTL in Industrie-Elektronik und Master of Science in Telematics (ICT) Management.

Um in einer Organisation die Auswirkungen von Software-Verletzlichkeiten (Vulnerabilities) besser zu verstehen, kann im Rahmen einer Übung ein Red Team gegen ein Blue Team antreten. Im Gegensatz zum Penetration Testing versucht bei diesem Ansatz das angreifende Red Team Lücken auszunutzen, während das Blue Team den Angriff mit Gegenmassnahmen und Security Services abwehrt. Die grosse Herausforderung ist, dass dem Red Team eine ausnutzbare Verletzlichkeit genügt, das Blue Team jedoch alle Verletzlichkeiten schützen muss.

Im Rahmen einer Studie untersuchte ein KI-Forschungsteam die Auswirkungen mehrerer Large Language Models (LLMS) und Open Source Vulnerability Scanners als Angreifer in Sandbox-Umgebungen. Das Ergebnis: GPT-4 konnte 87 Prozent der Lücken ausnutzen, die anderen LLMs und die Vulnerability Scanners 0 Prozent. Wurde die Verletzlichkeit als CVE-Beschreibung (Common Vulnerabilities and Exposures – Bekannte Schwachstellen und Anfälligkeiten) nicht genannt, fiel der Wert von 87 auf 7 Prozent. Die Studie zeigt, wie wichtig es ist, das Blue Team bei der Verteidigung gegen solche Angriffe zu unterstützen. Eine Möglichkeit besteht darin, Verletzlichkeiten mit SBOM so schnell wie möglich zu erkennen und zu beheben.

Das NIST definiert erstmals Minimalstandards an SBOM

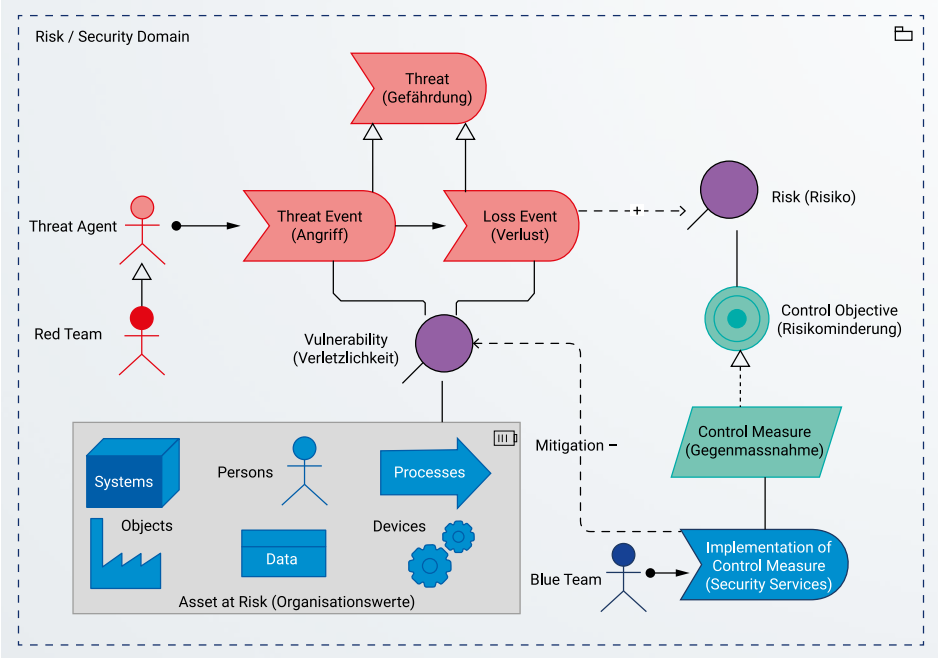
Das US-amerikanische National Institute of Standards and Technology (NIST) hat an einem dreitägigen Workshop mit 1400 Personen unter anderem SBOM verbindlich vorgeschrieben. Folgende Ziele sollen damit erreicht werden:

Alle an der Software-Lieferkette beteiligten Parteien entwickeln ein gemeinsames Verständnis für die Herausforderungen der Schwächen in Software im Sinne einer semantischen Interoperabilität.

Das Erkennen von Software mit Schwächen kann durch die Automatisierung von Tools und Prozessen einfacher und schneller erfolgen.

Bei einem höheren Automatisierungsgrad kann die Häufigkeit von Scans erhöht bzw. dem Risiko angepasst werden. Software, die direkt aus dem Internet verfügbar ist, wird häufiger geprüft als Software, die im Intranet von einem Team genutzt wird.

Software mit Verletzlichkeiten werden vom Vulnerability Management auf Ausnutzbarkeit geprüft und durch korrigierte Versionen ersetzt oder mit anderen Massnahmen geschützt.



Einfache Version des Risk and Security Archimate Metamodels

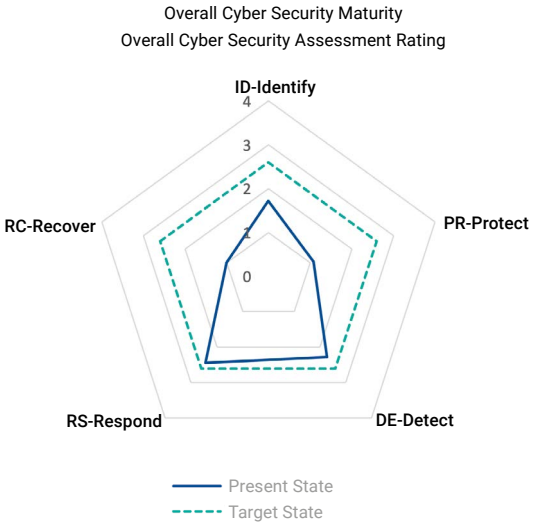
Alle Artikel können Sie auch online in unserem Blog lesen:
ti8m.com/blog

SBOM und der Fokus auf die Lieferkette stärkt das Blue Team. Verletzlichkeiten werden durch die Automatisierung schneller bekannt und die Zusammenarbeit mit den Partnern entlang der Lieferkette intensiviert, damit Verletzlichkeiten behoben werden können, bevor sie das Red Team ausnutzen kann.

Und die Schweiz?

Das Bundesamt für wirtschaftliche Landesversorgung empfiehlt im IKT-Minimalstandard (Informations- und Kommunikationstechnik) 2023 Massnahmen zur Verbesserung der IKT-Resilienz und bietet ein Assessmenttool, um die eigene Resilienz zu messen. Entscheidet sich eine Organisation, SBOM-basierte Prozesse einzuführen, werden folgende Bereiche verbessert:

Identifizieren (ID – Identify)
Erkennen (DE – Detect)
Reagieren (RS – Respond)



Das Assessmenttool des Bundesamt für wirtschaftliche Landesversorgung zeigt, wie SBOM die Security-Maturität verbessert.

In der Grafik ist das Ergebnis eines solchen Assessments zu sehen. Wir haben das Tool so ausgefüllt, dass die Wirkung einer SBOM-Einführung sichtbar wird: Ohne SBOM beträgt die Maturität 1 (partiell), mit SBOM beträgt sie 3 (wiederholbar). Eine Organisation, die ihre Maturität der SBOM-Verarbeitung automatisiert hat, erreicht in Detect und Respond annähernd den empfohlenen IKT-Mindeststandard. Identify verbessert sich, Protect und Recover müssen mit anderen Massnahmen adressiert werden.

Ein Tool wie SBOM kann die IKT-Resilienz einer Organisation massgeblich stärken. Dank der SBOM-Standardisierung und der Umsetzung in den Tools entlang der Software-Lieferkette wird das Blue Team im Beheben von Verletzlichkeiten unterstützt. Bestehende Tools können standardisierte SBOM aller Lieferanten automatisch verarbeiten, reduzieren so die manuellen Tätigkeiten und verschaffen dem Blue Team die Zeit, die Maturität weiterer Prozesse, welche die Resilienz verbessern, zu erhöhen.

«SBOM ist für eine effektive Verwaltung der Software-Lieferkette zwingend»

Das Information Service Center WBF ISCeco entwickelt, integriert und betreibt Fachanwendungen im Eidgenössischen Departement für Wirtschaft, Bildung und Forschung (WBF) und setzt seit kurzem auf SBOM. Wir haben mit Manuel Gysin, Teamleiter Software Engineering, über die Einführung und die Vorteile gesprochen.

Welches sind die grössten Herausforderungen im Managen der IT-Sicherheit, und welchen Beitrag kann SBOM leisten?
Moderne Software ist sehr komplex, oft umfasst sie hunderte von Drittanbieter-Komponenten. Diese Komponenten können sowohl in der Laufzeitumgebung als auch direkt in der Software eingebettet sein. Ohne eine genaue Übersicht ist es schwierig, auf CVE zu reagieren, da diese entweder unbekannt sind oder die Analyse jedes einzelnen CVE zu aufwendig ist. Es braucht ein Verständnis darüber, welche Komponenten tatsächlich verwendet werden, eine schnelle und automatische Reaktion auf neu entdeckte CVE, und es braucht auch eine Integration von Sicherheitsbewusstsein in den Entwicklungsprozess. Ein moderner, Toolchain-basierter DevSecOps-Ansatz ermöglicht die automatisierte Überprüfung von Software bei jedem Commit.

Warum haben Sie sich mit SBOM beschäftigt?
Der Anstoss kam durch die Diskussionen über deren Bedeutung und die zunehmende Forderung nach Transparenz in der Softwareentwicklung. In ihren Richtlinien verlangt die US-Regierung SBOM von ihren Lieferanten. Dies hat unsere Entscheidung, bei uns ebenfalls mit SBOM zu arbeiten, bestärkt. Kurz nach dem Entscheid aus den USA haben wir begonnen, SBOM in allen unseren internen Entwicklungsprojekten zu implementieren und von externen Lieferanten einzufordern.

Welche Prozesse unterstützt SBOM genau?
SBOM sind heute ein zentraler Auslöser für unseren «Security Incident Response»-Prozess. Interessanterweise entstand die Notwendigkeit für ein dediziertes Security Team genau durch die Einführung von SBOM, da wir zunächst nicht effektiv mit den Meldungen umgehen konnten. Dies zeigt, wie SBOM zur Sensibilisierung und Weiterentwicklung der organisatorischen Sicherheitskultur beitragen.

Wird SBOM auch bei uns bald zum Standard?
SBOM sind aus meiner Sicht unverzichtbar. Die Zeit zwischen der Entdeckung einer Schwachstelle und von Exploits, um diese Schwachstellen auszunutzen, ist heute extrem kurz. Die reaktive Überprüfung von Software auf Sicherheitslücken ist nicht mehr zeitgemäss. SBOM ermöglichen eine detaillierte «Zutatenliste» der Software, einschliesslich der Laufzeitumgebung, was eine ganzheitliche Sicht auf die Sicherheit bietet. Die zukünftige Entwicklung wird SBOM noch umfassender und serviceorientierter machen, von Netzwerkgeräten bis hin zu Softwarepaketen.

Welches sind die Erfolgsfaktoren für die Einführung von SBOM?
Wesentliche Erfolgsfaktoren umfassen klare Richtlinien und Standards, die Integration in bestehende Prozesse, den Einsatz von Automatisierungstools, umfassende Schulungen, Datensicherheit und Compliance, aktives Lieferantenmanagement, regelmässige Updates und die kontinuierliche Verbesserung durch Feedback.

Ist ein effektives Lieferkettenmanagement ohne SBOM überhaupt möglich?
Im Kontext der Sicherheit ist das Lieferkettenmanagement entscheidend, um Risiken zu minimieren, Compliance zu gewährleisten, Transparenz zu erhöhen, die Reaktionsfähigkeit auf Vorfälle zu verbessern, die Zusammenarbeit zu fördern und nachhaltige Sicherheitspraktiken zu entwickeln. SBOM spielen dabei eine zentrale Rolle, da sie Transparenz und detaillierte Informationen bieten, die für eine effektive Verwaltung der Software-Lieferkette unerlässlich sind. ●

Manuel Gysin

Teamleiter Software Engineering, ISCeco

Manuel Gysin ist seit über 20 Jahren in der IT-Branche tätig, u. a. als System- und DevOps Engineer und als Softwareentwickler. Er leitet das Engineering-Team für System- und Anwendungsentwicklung bei ISCeco und agiert auch als Scrum Master. Seine Expertise beinhaltet Cloud-Native-Lösungen, CI/CD-Prozesse, Open-Source-Technologien und Sicherheitslösungen.
isceco.admin.ch

Vertrauensraum Notariatswesen im digitalen Zeitalter

Notariatswesen // Sichere technologische Lösungen sind die Grundlage, um vertrauensbasierte Bereiche wie das Notariatswesen in den digitalen Raum zu überführen. Vor dem Hintergrund des Bundesgesetzes über die Digitalisierung im Notariat (DNG) wurden bereits bedeutende Schritte unternommen, um die Zugänglichkeit, Effizienz und Rechtssicherheit zu verbessern.

Pascal Wild

Head Consulting und Mitglied der Geschäftsleitung, ti&m

Nach seinem Wirtschaftsinformatikstudium an der Universität Zürich arbeitete Pascal Wild in verschiedenen Positionen im IT- und Finanzsektor, zuletzt als Mitglied der Geschäftsleitung bei Inventx, wo er für den Bereich Banking verantwortlich war.
Seit diesem Jahr leitet er das Consulting bei ti&m.
ti8m.com

Die korrekte, fälschungssichere und langfristige Sicherung von Urkunden wie Willenserklärungen, die sichere Aufbewahrung von Dokumenten und die korrekte Eintragung in entsprechende Register sind wichtige Funktionen, die Notariate wahrnehmen. Weltweit schreitet die Digitalisierung des Notariatswesens voran, und auch die Schweiz ist bemüht, dabei keine Ausnahme zu sein. Eine Übersicht zum Stand in der Schweiz und den wichtigsten rechtlichen Fragen:

Die technologischen Grundlagen

Die Digitalisierung im Notariatsbereich stützt sich auf mehrere Schlüsseltechnologien, die integral für die Transformation von analogen zu digitalen Prozessen sind:
Qualifizierte elektronische Signaturen (QES) ermöglichen die rechtsgültige Unterzeichnung elektronischer Urkunden.
Künstliche Intelligenz erhöht die Effizienz und Genauigkeit bei der automatischen Verarbeitung und Analyse von Dokumenten.
Plattform-Ökosysteme und Chatbots unterstützen die digitale Kommunikation und Interaktion und führen so zu besseren Kundenbeziehungen und effizienteren Prozessen.

Implementierungen und Entwicklungen in der Schweiz?

In der Schweiz zeigen verschiedene Kantone und Parteien Ansätze zur Digitalisierung:
Der Kanton St.Gallen arbeitet an der Einführung elektronischer Grundbuchgeschäfte und hat eine Übergangslösung mit gemischten Eingaben aus elektronischen Daten und Papierdokumenten vorgeschlagen. Diese Lösung soll die Vorteile der Digitalisierung nutzen, während die rechtliche Sicherheit gewahrt bleibt.
Der Kanton Wallis hat eine Plattform eingeführt, die eine direkte digitale Übertragung von Grundbuchdaten zwischen Notaren und Grundbuchämtern ermöglicht.
SIX Terravis ist eine Plattform, die den elektronischen Zugriff auf Grundbuchdaten ermöglicht, was die Abwicklung von Grundbuchtransaktionen beschleunigt und vereinfacht. Das System unterstützt Notare, Behörden, Hypothekarbanken und andere Beteiligte durch digitale Services, die Transaktionen sicher und transparent machen.

Globale Perspektiven und Vorbilder

Länder wie Frankreich und Österreich haben ihr Notariatswesen bereits vollständig digitalisiert und bieten wertvolle Einblicke in die Umsetzung und den Nutzen. Diese Länder nutzen fortschrittliche KI-Anwendungen und elektronische Dokumentenverwaltungssysteme, um den Notariatsdienst effizienter und sicherer zu gestalten.

Entwicklungen und Herausforderungen

Trotz der klaren Vorteile der Digitalisierung bestehen weiterhin Herausforderungen: Die vollständige Digitalisierung erfordert nicht nur die Implementierung von sicheren Technologien, sondern auch die Einhaltung strenger Datenschutzgesetze und die Anpassung bestehender regulatorischer Rahmenbedingungen.

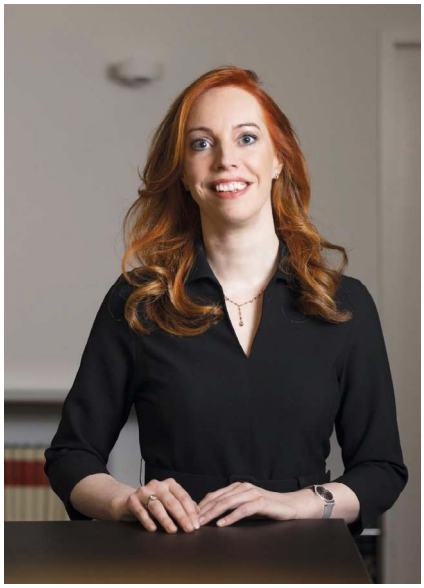
Vision für das digitale Notariat

«Wir digitalisieren bis 2027 die Geschäftsfälle im Notariatswesen und arbeiten so mit unseren Geschäftspartnern sicher und ohne Medienbrüche zusammen.» Dies ist die Vision des Schweizer Notarenverbandes vom Mai 2023. Die Zukunft des Notariats sieht eine umfassende digitale Umgebung vor, in der sämtliche Prozesse und Transaktionen digital abgewickelt werden. Im Fokus stehen hierbei die Geschäftsfälle Grundbuchgeschäfte, Handelsregistergeschäfte, Güter- und erbrechtliche Geschäfte sowie weitere notarielle Dienstleistungen.

Fazit: Die Digitalisierung im Notariatswesen bietet viele Vorteile wie eine höhere Effizienz, verbesserte Rechtssicherheit und einfachere Zugänglichkeit. Trotz bestehender Herausforderungen sind die Fortschritte in der Schweiz und anderen Ländern vielversprechend. Die kontinuierliche Entwicklung und Anpassung der Technologien und rechtlichen Rahmenbedingungen wird entscheidend sein, um die volle Bandbreite der Vorteile der Digitalisierung im Notariatswesen voll ausschöpfen zu können.

Rechtsanwältin Cornelia Stengel über Möglichkeiten und Grenzen der Digitalisierung.

«Digitale Register fördern Innovation – sowohl bei den technischen Lösungen als auch bei den Geschäftsmodellen, die sie ermöglichen»



Prof. Dr. Cornelia Stengel

Rechtsanwältin für Finanzmarkt- und Datenschutzrecht, Kellerhals Carrard

Cornelia Stengel ist Partnerin bei Kellerhals Carrard sowie Gastprofessorin und Leiterin des interdisziplinären #FinTank an der FHNW. Sie ist Geschäftsleitungsmitglied von Swiss Fintech Innovations (SFTI), Geschäftsführerin des Schweizerischen Leasingverbands (SLV) und Gast bei der Fachkommission Digitalisierung der Schweizerischen Bankiervereinigung (SBVg) und Verwaltungsrätin bei der St.Galler Kantonalbank.

kellerhals-carrard.ch

Ab 2027 sollen in der Schweiz Urkunden elektronisch erstellt und archiviert werden können. Gibt es aus juristischer Sicht noch Handlungsbedarf?

Das Bundesgesetz über die Digitalisierung im Notariat (DNG) schafft die Voraussetzungen dafür, dass öffentliche Urkunden in elektronischer Form erstellt und in einem zentralen vom Bund geführten digitalen Urkundenregister aufbewahrt werden können. Dieses Update der Infrastruktur ist ein wichtiger Schritt in die Richtung eines vollständig digitalisierten Geschäftsverkehrs. Es freut mich, dass die finale Fassung des Gesetzes die Grundvoraussetzungen technologieneutral formuliert und die detaillierten Ausführungsbestimmungen auf Verordnungsstufe geregelt werden. Das ermöglicht Flexibilität bei der Ausarbeitung der technischen Lösungen (vielleicht sogar gestützt auf die DLT-Technologie?) und erleichtert die fortlaufende Berücksichtigung des jeweiligen Stands der Technik. Bis ein vollständig digitalisierter Geschäftsverkehr möglich ist, gibt es allerdings noch Handlungsbedarf. So bleibt beispielsweise eine Fernbeurkundung erschwert, da in der Schweiz bislang eine zuverlässige digitale Form des Identitätsnachweises fehlt. Bis es eine elektronische ID gibt, müssen Urkundspersonen Alternativen finden, um sich von der Identität der Beteiligten zu überzeugen, z. B. beglaubigte ID-Kopien oder mittels QES signierte und live zugestellte ID-Kopien.

Distributed Ledger Technologien wie Blockchains scheinen wie geschaffen, um die Arbeit der Notariate zu übernehmen. Werden Notariate einer der Bereiche sein, die als erstes vollständig automatisiert und digitalisiert werden?

DLT würde sich auf jeden Fall für eine sichere, transparente und kostengünstige Erstellung und Aufbewahrung von digitalen Urkunden anbieten. Doch wie wir trotz Internet weiterhin E-Mails schreiben oder allenfalls prompten müssen, so ersetzt auch die Verwendung dieser Technologie für das Erstellen und Aufbewahren von Urkunden die Arbeit von Urkundspersonen keinesfalls. Denn neben dem reinen Erstellen und Aufbewahren von Urkunden kommt ihnen eine Vielzahl von Aufgaben zu, welche einen wichtigen Beitrag an die Rechtssicherheit und den Rechtsfrieden leisten. So muss der Inhalt z. B. von Kaufverträgen oder Ehe- und Erbverträgen weiterhin für den Einzelfall entworfen und/oder auf die Einhaltung mit dem Gesetz geprüft werden. Weiter liegt es in der Verantwortung der Urkundsperson, sicherzustellen, dass beim Abschluss von wichtigen Rechtsgeschäften wie Grundstückkauf oder Erbvertrag die beteiligten Parteien über den Inhalt und die Pflichten in Kenntnis sind und sich der Tragweite des jeweiligen Geschäfts bewusst sind. Diese wichtigen Funktionen kann ein digitales Register nicht übernehmen.

Seit letztem Sommer ist im Kanton Zürich das digitale Grundbuch online – im Kanton Bern sogar bereits seit Mitte 2020. Gibt es weitere digitale Register?

Gestützt auf eine Motion von Ständerat Beat Rieder laufen im Parlament zurzeit Bestrebungen, das Eigentumsvorbehaltsregister zu modernisieren. Gegenwärtig muss der Eigentumsvorbehalt in ein nicht digitales Register beim Betreibungsamt am (Wohn-) Sitz des Schuldners eingetragen werden. Bei einem (Wohn-)Sitzwechsel muss der Eintrag im Register des neu zuständigen Betreibungsamtes nachgeführt werden, um gültig fortzubestehen. Es ist klar, dass eine Revision nötig ist. Als Geschäftsführerin des Schweizerischen Leasingverbands setze ich mich allerdings an dieser Stelle für eine umfassendere Revision des Mobiliarsicherungsrechts und die Schaffung eines nationalen digitalen Mobiliarregisters[1] ein. Anstatt Grundstücke, die bekanntlich im Grundbuch eingetragen werden, könnten im Mobiliarregister bei Bedarf Rechte an Sachen, z. B. Eigentum oder Pfandrechte, eingetragen werden. Dies würde zusätzliche Möglichkeiten für die Eigentumssicherung schaffen und den Zugang zu Finanzierungen für KMU erleichtern bzw. vergünstigen. ●

1: leasingverband.ch/de/schweizerischer-leasingverband-slv/innovationen/mobiliarregister

Zukunftsgestaltung im SOC:

Die Transformation der Stellenprofile durch Infrastructure as Code und AI

Security Operations Center // Infrastructure as Code (IaC) und Artificial Intelligence (AI) sind mächtige Waffen gegen Cyberbedrohungen. Ihr Einsatz verändert das Profil der Mitarbeitenden im Security Operations Center (SOC).

In einer Ära, in der digitale Bedrohungen ebenso dynamisch sind wie die Technologien, die sie bekämpfen, stellt das Security Operations Center (SOC) die erste Verteidigungslinie gegen Cyberangriffe dar. Das SOC ist mehr als nur ein Überwachungszentrum; es ist das strategische Nervenzentrum für Sicherheitsintelligenz und -reaktion. Mithilfe von «Security Information and Event Management»-Systemen (SIEM) können diese Teams eine Vielzahl von Sicherheitsdaten aus diversen Quellen aggregieren, was ihnen eine 360-Grad-Sicht auf potenzielle Bedrohungen gewährt.

Von einem reaktiven zu einem proaktiven Ansatz

Diese kritischen Sicherheitsfunktionen haben im letzten Jahrzehnt einen enormen Wandel erfahren. Während SOC/SIEM-Spezialistinnen und -Spezialisten einst vorrangig auf die Erkennung und Meldung von Sicherheitsvorfällen fokussiert waren, hat sich der Schwerpunkt verlagert hin zu einem proaktiven und präventiven Ansatz. Technologien wie Machine Learning und Infrastructure as Code sind in den Vordergrund gerückt und stellen neue Anforderungen an die Stellenprofile. Diese technologische Revolution bedeutet, dass Sicherheitsexpertinnen und -experten heute nicht nur umfassende Kenntnisse in IT-Sicherheit benötigen, sondern auch die Fähigkeit, komplexe Algorithmen zu verstehen und anzupassen, eigene Sicherheitstools zu entwickeln und Infrastrukturen zu gestalten, die sich automatisch an die sich ständig ändernden Bedrohungslandschaft anpassen.

Ralph Keller

Head of SOC/SIEM, ti&m

Als Informatiker der ersten Stunde verfügt Ralph Keller über mehr als 20 Jahre Erfahrung in der IT-Branche, insbesondere bei IT-Dienstleistern und Managed Service Providern. Seit letztem Jahr leitet er das SOC/SIEM bei ti&m und verantwortet dessen Etablierung bei Kunden und Partnern. Darüber hinaus engagiert er sich privat in der Start-up-Szene und bringt sein Fachwissen als Dozent an verschiedenen Bildungseinrichtungen ein.

ti8m.com

Automatisierung verändert das Wesen des SOC

Die Automatisierung von Sicherheitsmassnahmen durch IaC erlaubt es, Sicherheitseinstellungen und -policies als Code zu definieren, wodurch die Implementierung von Sicherheitsstandards und die Reaktion auf Zwischenfälle beschleunigt werden. Diese Entwicklung verändert das Wesen des SOC, indem es Reaktionsfähigkeit mit Präzision kombiniert und das Bedürfnis nach Fachkräften schafft, die sich in der Programmierung ebenso zu Hause fühlen wie in der Sicherheitsanalyse.

SOAR verzahnt Sicherheit, Entwicklung und Betrieb

Mit der fortschreitenden Integration von SOAR (Security Orchestration, Automation and Response) können Reaktionsprozesse auf Vorfälle weiter optimiert werden. Die Konzeption von Playbooks, die automatisierte Workflows für häufige Bedrohungsszenarien definieren, erfordert ein tieferes Verständnis für den gesamten Lebenszyklus von Cyberangriffen. Gleichzeitig bedingt der DevSecOps-Ansatz eine noch engere Verzahnung von Sicherheit, Entwicklung und Betrieb, wodurch Sicherheitsexpertinnen und -experten zunehmend in Entwicklungsprozesse involviert werden.

Blicken wir in die Zukunft, so ist zu erwarten, dass die Verwendung von KI im SOC/SIEM-Umfeld weiter zunehmen wird. KI-Algorithmen, die in der Lage sind, aus Daten zu lernen und selbstständig zu agieren, werden die Art und Weise, wie Sicherheitswarnungen analysiert und gehandhabt werden, tiefgreifend verändern. Sie ermöglichen eine schnelle Identifikation von komplexen Angriffsmustern und stellen eine adaptive Reaktion auf die sich ständig wandelnde Taktik der Angreifer sicher. Doch nicht nur die Verteidigung, auch Angreifer rüsten auf und nutzen KI, um ausgeklügelte Cyberangriffe zu orchestrieren. Dies führt zu einem Wettrüsten in der Cyberwelt, in dem Sicherheitsexpertinnen und -experten fortwährend ihre Strategien anpassen und ihre Fähigkeiten weiterentwickeln müssen, um Schritt zu halten.

Weiterbildung der Sicherheitsteams als kritischer Erfolgsfaktor

Um in diesem hochdynamischen Umfeld erfolgreich zu sein, müssen Unternehmen in die Weiterbildung ihrer Sicherheitsteams investieren, besonders in den Bereichen KI und Machine Learning. Diese Expertinnen und Experten werden dann nicht nur als Reaktion auf Sicherheitsvorfälle agieren, sondern präventive Massnahmen entwickeln, die neue Angriffsvektoren antizipieren können. CI/CD-Pipelines (Continuous Integration/Continuous Deployment) und die Automatisierung von Prozessen helfen dabei, Qualität und Effizienz zu steigern und die Reaktionsfähigkeit zu beschleunigen. Dabei ist es wichtig, offene und flexible SIEM-Systeme zu nutzen, die Raum für Anpassungen und Erweiterungen bieten, wie es beispielsweise bei Open-Source-Lösungen wie Elastic der Fall ist.

Die neue Generation von SOC/SIEM-Spezialistinnen -und -Spezialisten muss daher ein breites Spektrum von Fähigkeiten und Wissen mitbringen. Von der Programmierung und Systemadministration über die Datenanalyse und -wissenschaft bis hin zum ethischen Umgang mit Technologie – all dies sind nun Schlüsselkomponenten für effektive Sicherheitsarbeit. Mit diesen Kenntnissen ausgestattet, können Sicherheitsteams nicht nur auf Bedrohungen reagieren, sondern diese voraussehen und präventiv handeln, um die Sicherheit und Resilienz ihres Unternehmens in einer unsicheren digitalen Welt zu gewährleisten. ●

Swiss Security Software. One you can trust.

ti&m Authentication

Swiss Security und Authentication Software: Von der Multi-Faktor-Authentifizierung bis zu Security Consulting bieten wir Produkte mit der perfekten Balance zwischen höchsten Sicherheitsstandards und Benutzerfreundlichkeit. Unsere langjährige Erfahrung in der Entwicklung und Anwendung von Sicherheitslösungen macht uns zum idealen Partner für alle Fragen rund um die Cybersicherheit.

Gutmann PRIVATE BANKERS · clevercircles · sanitas · Bank WIR · ti&m

Philip Dieringer, Head Bern, informiert Sie gern:
+41 31 960 15 55 oder ti8m.com/2fa

ti&m