CONCORDIA

Europas Cybersicherheit vernetzt sich

DSGVO

Benchmark und Wirtschaftsfaktor?

AUGMENTED REALITY

Mehr Durchblick beim Beschäftigtendatenschutz

Handelsblatt Journal

Eine Sonderveröffentlichung von Euroforum Deutschland

NOVEMBER 2019 | WWW.HANDELSBLATT-JOURNAL.DE

Cyb3r$EcUrity & Dat3n$(huTz

euroforum

Medienpartner

Handelsblatt

Substanz entscheidet.

Die Themen dieser Ausgabe

IMPRESSUM

Herausgeber
Euroforum Deutschland GmbH
Toulouser Allee 27
40211 Düsseldorf
Tel.: +49 (0)211.88743-3829
www.handelsblatt-journal.de

Projektleitung (V.i.S.d.P.)
Christiane Daners,
Euroforum Deutschland GmbH
christiane.daners@euroforum.com

Redaktionsleitung
Nicola Csepella,
Euroforum Deutschland GmbH
nicola.csepella@euroforum.com

Art Direction & Layout
EINRAUMBUERO, Köln
info@einraumbuero.de

Druck
Süddeutscher Verlag
Zeitungsdruck GmbH, München

Medienpartner
Handelsblatt
Substanz entscheidet.

IT-Sicherheit gemeinsam gewährleisten

von Horst Seehofer

Der Cyberraum ist weiterhin in hohem Maße gefährdet. Ob bei privater Nutzung, im Unternehmen oder in der Politik – wir alle sind auf eine funktionierende und sichere IT-Infrastruktur angewiesen. Der Ausfall von IT-Infrastrukturen – etwa infolge eines erfolgreichen Angriffs auf die Kritische Infrastruktur eines Krankenhauses – kann zu immensen wirtschaftlichen, gesellschaftlichen oder gar körperlichen Schäden führen

Damit solche Fälle gar nicht erst eintreten, müssen wir uns der Gefahren im digitalen Raum bewusst sein. Und wir müssen wissen, wie wir uns selbst vor diesen Gefahren schützen können, und welche Angebote der Staat dafür als Unterstützung anbietet.

Ein Vorfall, der große mediale Aufmerksamkeit bekam, war die unbefugte Veröffentlichung von teilweise sehr persönlichen Daten von Politikern und anderen Personen des öffentlichen Lebens zum Jahreswechsel 2018/2019. Dieses „Doxing“ führte uns die digitale Verwundbarkeit des Einzelnen wieder einmal deutlich vor Augen. Der schnelle Ermittlungserfolg sowie das effiziente Handeln der zuständigen Sicherheitsbehörden zeigten aber auch, dass wir mit diesen Behörden starke Partner an unserer Seite haben, die jeden Tag ihr Bestes geben, um uns vor neuen Bedrohungen in Verbindung mit der zunehmenden Digitalisierung zu schützen.

Cybersicherheit ist eine wesentliche Voraussetzung für das Gelingen der Digitalisierung. Wenn wir die Chancen der Digitalisierung voll ausschöpfen wollen, müssen wir die mit ihr verbundenen Risiken beherrschbar machen. Die Bürgerinnen und Bürger sowie die Wirtschaft erwarten von Staat und Politik zu Recht, dass sie die Herausforderungen der Digitalisierung meistern. Für diese Aufgabe müssen die zuständigen Behörden und Institutionen gut aufgestellt sein. Doch dies allein reicht nicht aus, um im Cyberraum dauerhaft ein hohes Schutzniveau zu gewährleisten. Vielmehr muss auch der Rechtsrahmen kontinuierlich überprüft und an neue Bedrohungen angepasst werden.

Die aus meiner Sicht notwendigen Anpassungen müssen insbesondere Verbesserungen für den Schutz der Verbraucherinnen und Verbraucher, der Kritischen Infrastrukturen sowie weiterer Wirtschaftszweige vorsehen. In diesem Zusammenhang ist geplant, ein einheitliches und freiwilliges IT-Sicherheitskennzeichen einzuführen. Dieses macht die IT-Sicherheitsfunktionen vor allem von Produkten im Verbrauchersegment erstmals für Bürgerinnen und Bürger sichtbar, so dass diese erkennen können, dass ihre Geräte die erforderlichen Sicherheitsfunktionen besitzen.

Im Bereich der Wirtschaft wollen wir die Pflicht ausweiten, Störungen von IT-Systemen zu melden und Mindeststandards einzuhalten. Auch Lieferanten von Hard- und Software nehmen wir in den Blick. Eine Störung in der Lieferkette kann sich schnell auf eine Kritische Infrastruktur ausweiten. Außerdem gibt es weitere Unternehmen, die Aufgaben wahrnehmen, an denen ein besonderes öffentliches Interesse besteht und deren Ausfall gravierende Folgen für die Gesellschaft haben kann.

Starke Behörden können IT-Sicherheit nicht allein gewährleisten. Lösungen werden nur erfolgreich sein, wenn alle gesellschaftlichen Gruppen gemeinsam daran arbeiten. Mit dem „Nationalen Pakt Cybersicherheit“, der die Akteure und Initiativen im Bereich der Cybersicherheit identifiziert und vernetzt, wird diese vertrauensvolle Zusammenarbeit zwischen Zivilgesellschaft, Wissenschaft, Wirtschaft und Staat weiter gestärkt.

Mit diesen Maßnahmen und Instrumenten, die der Staat für die Verbraucherinnen und Verbraucher und für die Wirtschaft bereithält, können wir Cybersicherheit gemeinsam gewährleisten.

Horst Seehofer, Bundesminister des Innern, für Bau und Heimat

„Cybersicherheit ist eine wesentliche Voraussetzung für das Gelingen der Digitalisierung.“

Foto: Henning Schacht | Icon: fm.stockers/shuttersock.com

Desinformation neu denken

Wie 2016 die Debatte prägte

von Dr. Julian Jaursch

Der Wendepunkt war das Jahr 2016: Damals dominierten Schlagzeilen zu „Fake News“ und ausländischer Wahleinmischung die politische Debatte zum Brexit-Referendum und dem US-Präsidentschaftswahlkampf. Das Gute daran war: Desinformationskampagnen, gerade in sozialen Medien, rückten in den Fokus der Öffentlichkeit. Doch leider schufen die speziellen Umstände von 2016 ein verzerrtes Bild von Desinformation, das bis heute die Debatte dazu prägt. Es wurden mehrere Schwerpunkte gesetzt, die auch politische Gegenmaßnahmen erschwert haben: der Fokus auf ausländische Wahlbeeinflussung, auf Inhalte (statt deren Verbreitung) und auf Selbstregulierung.

Falscher Fokus auf das Ausland

Zunächst ist eine Einordnung der Fokussierung auf ausländischen Einfluss wichtig. Zur Klarstellung vorab: Dass Staaten versuchen, Wahlen in anderen Ländern zu beeinflussen, ist eine Gefahr, die nicht unterschätzt werden sollte. Mittlerweile ist bekannt, wie stark Russland versuchte, in den US-Wahlkampf von 2016 einzugreifen. Solche Versuche müssen so gut es geht unterbunden werden. Doch leider entstand damals der Eindruck, dass Desinformation hauptsächlich dazu da sei, Wahlergebnisse zu manipulieren.

Das ist zu kurz gegriffen. Der US-Sonderermittler Robert Mueller selbst schreibt in seinem Bericht, dass Russland schon Jahre vor der Wahl in sozialen Netzwerken aktiv wurde. Und zwar nicht, um die Stimmabgabe zu beeinflussen, sondern um „politischen und gesellschaftlichen Zwietracht zu säen“. Bei Desinformation geht es also nicht unbedingt darum, Abstimmungen in die eine oder andere Richtung zu verschieben. Vielmehr sollen vorhandene Spaltungen in der Gesellschaft verstärkt werden und so das Vertrauen in demokratische Institutionen und Prozesse geschmälert werden. In den USA passierte dies zum Beispiel dadurch, dass sich aus Russland gesteuerte Social-Media-Profile als US-Aktivist:innen zu kontroversen Themen wie Rassismus, Polizeigewalt und Migration ausgaben und zu Protesten aufriefen – oft von beiden Seiten der Debatte, also etwa mit Protestaufrufen für und gegen Flüchtlinge. So verhärten sich soziale Spannungen und der demokratische Diskurs wird durch gegenseitiges Misstrauen und Polarisierung geschwächt, auch unabhängig von einer anstehenden Abstimmung.

Neben dem Fokus auf Wahlen ist es ebenfalls zu kurz gegriffen, sich ausschließlich auf staatliche Desinformation zu beschränken. Das ist ein weiterer Nebeneffekt der Diskussion von 2016. So entstand etwa zur Bundestagswahl ein Jahr später die Sorge, dass Russland auch in den deutschen Abstimmungsprozess eingreifen würde. Während es schwierig ist, dies kategorisch auszuschließen, so zeichnet eine umfangreiche Studie der Stiftung Neue Verantwortung doch ein ganz anderes Bild: Nicht staatliche Organisationen aus dem Ausland verbreiteten Desinformation im Vorfeld der Wahl, sondern inländische Personen und Gruppierungen – überwiegend aus dem rechtspopulistischen Umfeld. Auch dabei ging es nicht vornehmlich darum, das Abstimmungsverhalten zu beeinflussen. Wie in den USA waren kontroverse gesellschaftliche Themen, besonders Migration, Teil von Desinforma-

Illu: Alexander_P/shutterstock.com

tion. Als kurzes Zwischenfazit lässt sich sagen: Statt nur auf ausländische Wahlbeeinflussung muss sich das Augenmerk auch darauf richten, wie heimische Gruppierungen mit Desinformation gesellschaftliche Spaltungen ausnutzen.

Falscher Fokus auf die Inhalte

Zweiter Punkt: Eine der Reaktionen auf jegliche „unerwünschte“ Inhalte im Internet ist zunächst immer der Wunsch, diese Inhalte zu löschen. Bei vielen Inhalten gibt es für deren Löschung einen gesellschaftlichen Konsens und auch glasklare gesetzliche Regelungen. Dazu zählen etwa Kinderpornografie und gewalttätige oder gewaltverherrlichende Videos. Auf EU-Ebene gibt es dazu beispielsweise den Anspruch, terroristische Inhalte schnell von Plattformen zu entfernen. Unternehmen wie Facebook, Google, Twitter und YouTube sind mittlerweile recht versiert darin, solche Inhalte zu löschen. Selbst hier gibt es allerdings Abstufungen, was illegal ist und was nicht, und es kommt zu fehlerhaften Löschungen. Bei Desinformation wird diese Unterscheidung noch schwieriger: Desinformation bewegt sich oft in einem rechtlichen Grenzbereich, in dem unklar ist, welche Äußerungen von der Meinungsfreiheit gedeckt sind. Ein Ansatz wie im deutschen Netzwerkdurchsetzungsgesetz (NetzDG) ist daher für Desinformation ungeeignet. Das NetzDG zielt im Kern darauf ab, soziale Netzwerke, Suchmaschinen und Videoportale zu einer schnellen Löschung rechtswidriger Inhalte zu bewegen - unter Androhung hoher Strafen. Die Frage, welche Grenzen der Meinungsfreiheit von wem definiert und überwacht werden, ist bei einem Fokus auf einzelne Inhalte immer die Krux.

Sinnvoller wäre es, einen anderen Ansatz aus dem NetzDG näher zu verfolgen: Das Gesetz gibt vor, dass Unternehmen Ansprechpersonen benennen und Berichte zu ihren Löschungsmodalitäten veröffentlichen müssen. Idee dahinter ist es, für mehr Transparenz der unternehmensinternen Prozesse zu sorgen. Das NetzDG ist bei den Vorgaben für die Transparenzberichte zu vage, aber grundsätzlich könnte ein solcher prozessorientierter Ansatz die Verbreitungswege von Desinformation in den Blick rücken und nicht auf die Entfernung einzelner Inhalte setzen.

Denn irreführende und auch hetzerische Inhalte verbreiten sich besonders gut in sozialen Netzwerken und auf Videoportalen, in denen Aufmerksamkeitsmaximierung und fehlendes journalistisches Gatekeeping das Nachrichten- und Informationsumfeld bestimmen. Es bietet sich daher an, Nutzende in diesem digitalen Raum zu stärken, statt einzelne Inhalte zu löschen. Konkretere Vorschläge dazu gibt es etwa in Frankreich: Expert:innen schlugen dort der Regierung eine Aufsicht vor, die sie mit der des Finanzmarkts verglichen. Es solle nicht darum gehen, einzelne Finanzprodukte beziehungsweise einzelne Inhalte aus dem Verkehr zu ziehen, sondern für Compliance-Prozesse zu sorgen und diese zu beaufsichtigen, damit von vornherein Schaden von Menschen abgewendet wird.

Auch könnten Regeln zum Schutz der Privatsphäre helfen, weil die algorithmengesteuerte Anzeige und Sortierung von Nachrichten und Inhalten nur aufgrund einer umfassenden Datensammlung funktioniert. Wird diese eingeschränkt, könnte auch die Gefahr verringert werden, vornehmlich Inhalte angezeigt zu bekommen, von denen ein Algorithmus berechnet hat, dass sie möglichst viel Aufmerksamkeit erhalten. Im Zweifel sind das nämlich eher hasserfüllte und irreführende denn freundliche und wahre Posts. Gerade Gefühle der Wut führen nachgewiesenermaßen dazu, dass Inhalte geteilt und andere Ansichten abgelehnt werden.

Falscher Fokus auf Selbstregulierung

Nun zum letzten Punkt, der die Frage berührt, wer sich um die Aufsicht sozialer Netzwerke kümmert. Das NetzDG verdeutlicht die Einsicht vieler Politiker:innen, dass Selbstregulierung nicht mehr die Lösung sein kann. Das war aber lange die wichtigste Reaktion auf Desinformation. Paradebeispiel hierfür ist der EU-Verhaltenskodex mit selbstregulatorischen Maßnahmen. Der Verhaltenskodex weist erhebliche Schwächen auf, was die EU mittlerweile auch selbst so sieht. Problematisch ist insbesondere, dass er auf Freiwilligkeit beruht und keine Sanktionsmechanismen beinhaltet. Die negativen Folgen dieses Ansatzes lassen sich am Beispiel der öffentlichen Datenbanken für politische Werbung festmachen. Diese Werbedatenbanken sollten Journalist:innen, Forschenden und Interessierten einen Überblick zum Ausmaß und zur Ausrichtung politischer Werbung auf großen Plattformen liefern. Da die Datenbanken aber unvollständig und fehleranfällig waren, waren sie für die Forschung kaum zu benutzen. Dagegen konnte die EU aufgrund fehlender Sanktionsmöglichkeiten wenig unternehmen.

Gerade der Fall politischer Onlinewerbung offenbart, wie wichtig verbindliche Regeln und eine Aufsicht für große Unternehmen sind. Zwar ist die Gefahr von Desinformation über bezahlte politische Anzeigen in Deutschland noch überschaubar. Doch aus dem Mueller-Bericht ist ersichtlich, wie Werbeposts etwa auf Facebook genutzt werden können, um soziale Spaltungen zu betonen. Konkrete Vorschläge, wie mit politischer Werbung im Internet umgegangen werden könnte, gibt es: Zum Beispiel müsste klar erkennbar sein, wer wann wie mit viel Geld politische Online-Anzeigen geschaltet hat - und wer genau damit erreicht (und auch speziell nicht angesprochen) werden sollte. Solch detaillierte Regeln sind in Deutschland nicht vorhanden, auch wenn die Bundesländer das Thema politische Onlinewerbung in ihrer Reform der Medienaufsicht aufgreifen.

Insgesamt haben die Entwicklungen von 2016 einerseits also ein Bewusstsein für das Problem Desinformation geschaffen. Andererseits hat die damalige Schwerpunktsetzung den Umgang mit dem Problem verzerrt. Diese Schwerpunkte gilt es zu hinterfragen, um offen für neue Lösungsansätze zu sein.

„Statt nur auf ausländische Wahlbeeinflussung muss sich das Augenmerk auch darauf richten, wie heimische Gruppierungen mit Desinformation gesellschaftliche Spaltungen ausnutzen.“

Dr. Julian Jaursch ist Projektleiter „Stärkung digitaler Öffentlichkeit | Policy” beim Berliner Think Tank Stiftung Neue Verantwortung (SNV).

Die SNV möchte die Lücke in Fragen der Digitalisierung und neuer Technologien in der deutschen Think Tank-Landschaft füllen. Dafür bringen wir technisches Fachwissen und Expertise zu gesellschaftlichen und politischen Zusammenhängen in einer Organisation zusammen. Wir erarbeiten Analysen, entwickeln Handlungsempfehlungen für politische Entscheidungsträger:innen, führen Expert:innen-Workshops durch, laden zu öffentlich zugänglichen Fachdiskussionen ein und erklären Zusammenhänge und Hintergründe in den Medien.

www.stiftung-nv.de

Datenschutz bei der Deutschen Bahn

Helden on Tour

Chris Newiger ist seit fast zehn Jahren Konzerndatenschutzbeauftragte der Deutschen Bahn. An die oberste Datenschützerin eines Unternehmens mit derart vielen und sensiblen Kunden- und Mitarbeiterdaten hätten wir unzählige Fragen. Wir haben uns zunächst auf die mit dem höchsten Aktualitätsfaktor konzentriert, um uns dann von Frau Newiger in den Datenschutzkosmos der Bahn mitnehmen zu lassen.

Frau Newiger, die Deutsche Bahn hat sich mit ihrer neuen Dachstrategie „Starke Schiene“ viel vorgenommen. Bis 2030 sollen „für das Klima, für die Menschen, für die Wirtschaft und Europa“ u.a. die Passagierzahlen im Personenverkehr verdoppelt werden. Was bedeutet dies für Ihr Aufgabenfeld des Datenschutzes – wie können bzw. müssen Sie und Ihre Mitarbeiter da mit anpacken?

Der Datenschutz ordnet sich im Feld „Schlagkräftiger durch eine einfache Aufstellung, klare Abläufe und gemeinsames Anpacken“ ein. Hier geht es unter anderem um Prozessoptimierung, verbindliche Qualitätsvorgaben und gemeinsames Anpacken über Bereichsgrenzen hinweg für ein gemeinsames Ziel. Das bedeutet, dass wir konzernübergreifend noch stärker vor allem im Onboarding vertreten sein werden, um gerade unsere neuen Mitarbeiterinnen und Mitarbeiter von vornherein zu sensibilisieren. Natürlich bedeutet das auch eine stetige Weiterbildung und Weiterentwicklung unserer Datenschutzorganisation.

Sie erwähnen den einzelnen Bahn-Mitarbeiter als wichtiges Puzzlestück in Ihrem Konzept. Trotzdem kann es natürlich – wie zuletzt im Oktober in Düsseldorf, als Schichtpläne und Zahlungsaufforderungen in einem öffentlichen Papierkorb landeten – immer wieder zu Datenpannen aufgrund individueller Fehler kommen. Wie schaffen Sie und Ihr Team es, mit dem einzelnen Kollegen in Kontakt zu bleiben und den Datenschutz immer wieder auf die Tagesordnung zu bringen?

Die „Schwachstelle Mensch“ ist natürlich wie immer das größte Risiko, das man auch nie ganz auf Null bringen kann. Um unsere Mitarbeitenden in puncto Datenschutz zu sensibilisieren und up to date zu halten, setzen wir auf unsere Datenschutz-Community im Konzern.

Zentral unterstützt der Konzerndatenschutz mit knapp 40 Mitarbeitern die Konzernunternehmen bei der Einhaltung des Datenschutzes, um die persönli-

„Man kann sich an allen ein Beispiel nehmen, die auch die ethische Seite des Daten- bzw. Persönlichkeitsschutzes ernst nehmen und im Zweifelsfall über kurzfristig gedachte wirtschaftliche Interessen stellen."

Foto: Pablo Castagnola

Chris Newiger, Konzerndatenschutzbeauftragte der Deutschen Bahn

chen Daten unserer Kollegen und Kunden zu schützen. Die dezentrale Datenschutzorganisation sorgt mit rund 100 Kolleginnen und Kollegen vor Ort dafür, dass unsere Datenschutzpolitik in den einzelnen Konzernunternehmen umgesetzt und gelebt wird, ist also nah an jedem einzelnen dran.

Die Leitlinien entstehen in der Zentrale, wo beispielsweise auch Schulungsunterlagen und Handlungshilfen für die Beratung konzipiert werden. Zusätzlich sind wir in unserem Intranet mit einem gut besuchten Blog vertreten, mit dem wir uns direkt an unsere Mitarbeiterinnen und Mitarbeiter richten. Dort entsteht auch viel Austausch in den Kommentaren. Auch Awareness-Kampagnen an unterschiedlichen Standorten mit spielerischen Elementen sowie Give-Aways für die Kolleginnen und Kollegen fördern die positive Wahrnehmung des Datenschutzes. Wir sind durchaus weithin bekannt, das stelle ich immer wieder fest, wenn ich im Konzern unterwegs bin.

Man hört, dass Sie seit Ihrem Einstieg bei der Bahn ein für einen internationalen Konzern geradezu vorbildliches Datenschutz-Gebäude auch unter Einbezug anderer Governance- und Security-Einheiten errichtet hätten. Können Sie uns das große Ganze für Nicht-Konzernler herunterbrechen?

Wie schon skizziert haben wir vor rund 10 Jahren mit dem Aufbau der Datenschutzorganisation in ihrer heutigen Struktur begonnen. In diesem Jahr haben wir uns zu einer Neustrukturierung innerhalb des Konzerndatenschutzes entschieden, da die steigende Anzahl innovativer Geschäftsmodelle und intelligenter Datenverarbeitungen im Konzern eine schnelle, unkomplizierte datenschutzrechtliche Beratung erfordert. Deshalb haben wir innerhalb der Datenschutzorganisation ein Schnittstellenmanagement zwischen zentralem und dezentralem Datenschutz etabliert. Dies ermöglicht uns, konzernübergreifende Schwerpunktthemen gezielt zu identifizieren und die DB strategisch rechtssicher zu beraten.

Zusätzlich arbeiten wir natürlich bereichsübergreifend eng mit unseren themenverwandten Einheiten wie Compliance, Informationssicherheit/Cybersecurity, Konzernrevision und Konzernsicherheit zusammen. Aus der Zusammenarbeit mit Cybersecurity entstand bspw. die Awareness-Kampagne „Helden on Tour". Hierfür gehen wir – tatsächlich verkleidet als Helden und mit unseren Maskottchen im Gepäck – auf Tournee an verschiedene DB-Standorte, um so die Mitarbeitenden auf das wichtige Thema aufmerksam und neugierig zu machen. Aus der Zusammenarbeit mit den vier Bereichen ist zudem ein gemeinsamer Auftritt im konzernweiten Onboarding für neue Mitarbeiter entstanden, die so direkt von Beginn an mit dem Thema Datenschutz vertraut werden sollen. In den neuen Willkommenspaketen sind wir mit einem Eintrag im digitalen Bahn-ABC unter „D wie Datenschutz" sowie mit Webcam-Covern zum Abdecken der Laptop-Webcams vertreten.

Da Sie vom stetigen Wandel infolge technischer Entwicklungen sprechen: Wer oder was sind fachliche Vorreiter, an denen Sie sich orientieren? An welchen Nationen, Personen, Unternehmen oder Einrichtungen kann man sich in Sachen Datenschutz ein Beispiel nehmen?

Wir sind natürlich mit vielen anderen Playern im Austausch – ich persönlich sogar schon seit 1997 in diversen Arbeitskreisen der deutschlandweiten Datenschutz-Community. Damals habe ich vor allem die Deutsche Telekom für ihre Vorreiterrolle und organisierte Vorgehensweise bewundert. Die Datenschutzorganisationen von Deutscher Bahn und Deutscher Telekom arbeiten bis heute eng zusammen. Allerdings haben wir bei der DB auch eine vertrauensvolle Zusammenarbeit mit den jeweiligen Aufsichtsbehörden für den Datenschutz in den verschiedenen Bundesländern etabliert. Der Austausch inspiriert und hilft beiden Seiten, einander zu verstehen. Dabei sind wir immer im Bestreben, die besten Lösungen für die Betroffenen zu finden. Bei Konferenzen ergeben sich auch immer wieder interessante Gespräche und Einblick in die Erfahrungen anderer. Grundsätzlich kann man sich an allen ein Beispiel nehmen, die vor allem auch die ethische Seite des Datenschutzes bzw. des Persönlichkeitsschutzes ernst nehmen – und sie im Zweifelsfall dann eben auch über unmittelbare und kurzfristig gedachte wirtschaftliche Interessen stellen.

Und wie sieht es bei Ihnen ganz persönlich aus? was schätzen Sie besonders an Ihrem Arbeitsplatz, der Sie jetzt ja immerhin schon fast zehn Jahre halten konnte?

Im Grunde schätze ich immer noch das Gleiche, was mich vor zehn Jahren dazu bewogen hat, das Angebot der Deutschen Bahn anzunehmen – ich konnte und sollte von Grund auf eine neue Datenschutzorganisation und -kultur im Konzern gestalten. Das war von Anfang an eine sehr große Aufgabe, die ich auch nur mit vielen anderen gemeinsam stemmen konnte. Kolleginnen und Kollegen aus dem Konzern, aber auch viele, die von „draußen" kamen. Es wurde weder mir noch sonst jemand in meinem großen Team an irgendeinem Tag langweilig. Irgendwas ist immer (lacht). Die Vielfalt der Anfragen und Aufgaben im Datenschutz in einem so breit aufgestellten und internationalen Konzern ist unbeschreiblich. Und die neuen Themen gehen uns auch nicht aus – Stichwort Digitalisierung. Einer meiner Kollegen im Team hat mal vor Jahren gesagt: Ich will immer vor der Welle sein. Das ist unser Motto geblieben. Das begeistert uns immer noch und – was vielleicht am Schönsten zu beobachten ist – auch all die jungen Kolleginnen und Kollegen, die immer wieder neu zu uns stoßen. Das macht mir einfach Freude.

ADVERTORIAL

Cybersicherheit braucht verifizierbare Fakten

vs148/shutterstock.com

von Jörg-Alexander Albrecht

Digitalisierung verändert unser Leben und unsere Wirtschaft. Damit sie erfolgreich gelingt, müssen wir alle gemeinsam eines sicherstellen: Cybersicherheit.

Manche denken, sie kennen die Lösung. Handelsbeschränkungen sollen es richten. Doch diese widersprechen den Werten der internationalen Geschäftswelt, stören den fairen Wettbewerb und schaden den Interessen der europäischen und globalen Verbraucher. Sie bilden einen gefährlichen Präzedenzfall und schon morgen könnte es wieder die europäische Wirtschaft treffen.

Fakten sind alternativlos. Mit Blick auf die aktuelle Diskussion um 5G und Sicherheit setzen die deutsche und viele andere europäische Regierungen auf einen objektiven und evidenzbasierten Ansatz, bei dem die Sicherheit der Mobilfunknetze im Vordergrund steht. Der Kern dieses Ansatzes ist, dass Sicherheitsprinzipien auf verifizierbaren Fakten basieren müssen. Verifizierungen unterliegen einheitlichen Standards. Nur so schaffen wir Cybersicherheit. Vor diesem Hintergrund begrüßt Huawei den aktuellen Entwurf des Kataloges von Sicherheitsanforderungen in Deutschland, der mit genau diesem Ansatz die 5G-Netze sicherer macht.

Um die technischen Herausforderungen rund um Cybersicherheit effektiv angehen zu können, sollten wir auch technische Mittel nutzen. Dafür bedarf es einer systematischen Cybersicherheit-Governance, die auf einheitlichen Standards und unabhängigen Verifizierungen beruht - anstatt auf Emotion und Spekulation. Dafür sind gemeinsame Anstrengungen von Regulatoren, Standardisierungsgremien, Unternehmen und Wissenschaft notwendig. Insbesondere bei folgenden Punkten:

1. Sicherheit muss messbar sein.

Nur dann ist sie auch beherrschbar. Dafür bedarf es einheitlicher Sicherheitsstandards. Huawei ist mit Regulatoren, Netzbetreibern und Standardisierungsgremien im engen Austausch, um eine Vereinheitlichung von Sicherheitsstandards zu fördern. Wir leisten einen wesentlichen Beitrag zu den Sicherheitsstandards der 3GPP, einer weltweiten Kooperation von Standardisierungsgremien für die Standardisierung im Mobilfunk. 2018 hat Huawei dort 464 5G-Sicherheitsvorschläge eingereicht, von denen 227 angenommen wurden.

2. Verifizierung muss unabhängig sein.

Die ITK-Wirtschaft muss sich noch stärker öffnen, um Einblicke in ihre Produkte zu ermöglichen. Nur so lässt sich prüfen, ob die vorher vereinbarten Sicherheitsstandards eingehalten worden sind. Vor einem Jahr hat Huawei dafür in Bonn das Security Innovation Lab für Produktverifizierungen und einen vertieften fachlichen Austausch unter anderem gemeinsam mit dem BSI eröffnet. Ein weiteres Transparenz-Center gibt es in Brüssel. Mittlerweile haben mehrere Router- und Switch-Produkte BSI CC- und NDcPP-Zertifikate verliehen bekommen. Darüber hinaus betreibt Huawei das Internal Cybersecurity Lab, das Produkte völlig unabhängig von Geschäftsinteressen verifiziert, bevor sie auf den Markt gebracht werden dürfen.

3. Zusammenarbeit macht uns stark.

Nicht nur Huawei setzt seit vielen Jahren auf verschiedene Zulieferer, Produktionsstandorte und Logistikanbieter aus mehreren Ländern und Regionen. Auch viele andere Unternehmen der ITK-Branche setzen auf globale Lieferketten. Vor diesem Hintergrund müssen Politik und Zertifizierungsstellen verschiedener Länder zusammenarbeiten, um Anforderungen an Zertifizierungen international zu harmonisieren. Nur so kann ein effizienter Zertifizierungsmechanismus für die globale Wirtschaft geschaffen werden.

4. Vertrauen erarbeiten wir uns hart.

Huawei gehört einzig seinen Mitarbeitern, sie sind die alleinigen Teilhaber und bestimmen den Kurs des Unternehmens. Aus der Zusammenarbeit unserer Mitarbeiter mit ihren Kunden erwächst die Erfahrung: Wenn die Kunden unseren Produkten nicht vertrauen, haben diese auch kaum Chancen, sich auf den Märkten zu behaupten. Der oben genannte Dreiklang aus Standardisierung, Verifizierung und Zertifizierung erhöht Sicherheit und schafft damit genau dieses Vertrauen. So wird messbar, dass bei Huawei Vertrauen fundamentales Eigeninteresse und damit Grundgedanke jedes Geschäftsprozesses ist.

Jörg-Alexander Albrecht,
Director Corporate Affairs,
HUAWEI TECHNOLOGIES Deutschland GmbH

Seit 32 Jahren vertrauen unsere Kunden überall auf der Welt unseren Produkten und Services. In Deutschland sind wir seit 18 Jahren im Markt aktiv. Mit mehr als 400 Forschern in Deutschland investiert Huawei in lokale Forschung und Entwicklung mit Schwerpunkten in der Anwendung von 5G, vernetzten Fahrzeugen und smarter Fertigung.

www.huawei.com/de

„Der Dreiklang aus Standardisierung, Verifizierung und Zertifizierung erhöht die Sicherheit und schafft Vertrauen."

HUAWEI

ADVERTORIAL

Prävention und Reaktion – aber richtig

Who is Danny/shutterstock.com

von Michael Sauermann und Barbara Scheben

Cyber-Risiken sind allgegenwärtig und finden sich beinahe täglich in den Medien. Unternehmen müssen sich vermehrt mit der digitalen Bedrohungslage auseinandersetzen. Es wäre jedoch ein Irrglaube zu meinen, Unternehmen könnten präventiv und ausnahmslos alle erforderlichen Maßnahmen treffen, um niemals durch einen Cyber-Angriff getroffen zu werden. Dafür ist die Vielfalt der Attacken auf die digitale Angriffsfläche zu groß.

Prävention

Gleichzeitig sind die Unternehmen allerdings sehr wohl gefragt, stets vorauszudenken, um möglichen Angriffen vorzubeugen und den Aggressoren extrem hohe Hürden zu setzen. Und so werden heutzutage beispielsweise immer modernere Technologien wie maschinelles Lernen für die Angriffsfrüherkennung eingesetzt – ähnlich einer Wettervorhersage. Cyber-Kriminelle sind jedoch dynamisch und entwickeln ihre Taktiken und Schad-Codes ständig weiter. Ihre „Tools, Tactics and Procedures“ (TTPs) unterstützen Aggressoren dabei, neue Methoden zu entwickeln und unentdeckt zu bleiben (so gewünscht).

Reaktionsstrategien

Aber nicht nur Angreifer werden immer effektiver – auch die Verteidigung und entsprechende Reaktionsmechanismen entwickeln sich fortwährend weiter. Eine effektive Cybersecurity-Aufstellung beinhaltet daher eine Berücksichtigung von sowohl präventiven als auch detektiven und reaktiven Maßnahmen zu gleichen Teilen. Die aktuelle KPMG e-Crime-Studie 2019[1] belegt, dass die Reaktionsstrategie für Unternehmen zunehmend in den Fokus rückt, um auf den Ernstfall vorbereitet zu sein.

Mit der adäquaten Reaktion auf IT-Sicherheitsvorfälle tun sich Unternehmen jedoch immer noch schwer, was oftmals in der Vielfalt der zu berücksichtigenden Themen und deren Abhängigkeiten voneinander begründet liegt. IT, Information Governance, Datenschutz und Krisenmanagement – diese und weitere Themen müssen im Ernstfall zwingend berücksichtigt und gekonnt gesteuert werden. Wenn beispielsweise Verantwortlichkeiten und Rollen nur ungenügend definiert sind, wird auch die effektive Reaktion auf einen IT-Sicherheitsvorfall, wie beispielsweise bei einem Datenleck, nicht gelingen.

Pflichtbestandteile einer Reaktionsstrategie umfassen

- die Definition von Incident Response-Prozessen,
- die Ausarbeitung von Runbooks,
- ein Krisenmanagement bzw. die Auswahl von externen Dienstleistern für Incident Response, Forensic, Rechtsberatung und Cybersecurity sowie
- eine Krisenkommunikationsstrategie.

Sollen im Fall eines Datenlecks beispielsweise Kunden und Mitarbeiter die Möglichkeit haben, sich bei Ihrer Hotline zu melden? Bei einem Datenverlust von beispielsweise mehreren hunderttausend Datensätzen kann das Ihr Call-Center schnell zum Erliegen bringen.

Datenschutz

Ebenfalls nicht unberücksichtigt bleiben darf in diesem Zusammenhang der Datenschutz: Spätestens seit Wirksamwerden der DSGVO im Mai 2018 rücken datenschutzrechtliche Konsequenzen im Zusammenhang mit Cyber-Risiken in den Fokus der Unternehmen. Nicht nur potenzielle Bußgelder, sondern auch mögliche Reputationsschäden und Vertrauensverluste seitens der Kunden und Mitarbeiter stellen beachtliche Unternehmensrisiken dar. Was ist zu tun, um diesen Risiken wirksam zu begegnen?

Das Fundament für präventive Risikominimierungsmaßnahmen bildet die Implementierung eines Datenschutz-Management-Systems. Dazu gehören u. a. die Implementierung von wirksamen technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der personenbezogenen Daten sowie ein Prozess zum Umgang mit Datenschutzverstößen. Erstere können restriktive Berechtigungskonzepte sowie die Pseudonymisierung oder Verschlüsselung personenbezogener Daten beinhalten.

Hat sich ein Cyber-Angriff bereits realisiert, ist ein unternehmensweit bekannter Prozess zum Umgang mit potenziellen Datenschutzverstößen elementar. Dieser interne Melde- und Prüfprozess hat insbesondere die Meldung an die Aufsichtsbehörde innerhalb von 72 Stunden nach Bekanntwerden sowie die evtl. erforderliche Benachrichtigung der Betroffenen sicherzustellen.

Wirksame und effektive Abwehrmaßnahmen sowie entsprechende Reaktionsmechanismen auf Cyber-Angriffe sind auch unter Berücksichtigung des Datenschutzes stetig zu überprüfen, fortzuentwickeln und bei Bedarf anzupassen, um den potenziellen Schaden sowohl für das Unternehmen als auch für die betroffenen Personen zu minimieren.

www.kpmg.de

Michael Sauermann,
Head of Forensic Technology,
KPMG AG

Barbara Scheben,
Head of Data Protection,
KPMG AG

„Spätestens seit Wirksamwerden der DSGVO rücken datenschutzrechtliche Konsequenzen im Zusammenhang mit Cyber-Risiken in den Fokus der Unternehmen.“

[1] https://home.kpmg/de/de/home/themen/2019/07/e-crime-in-der-deutschen-wirtschaft-2019.html

Das Potenzial der Digitalisierung nutzen … aber sicher!

von Dr. Igor Podebrad

Absolute Sicherheit vor Angriffen aus dem Netz gibt es nicht. Cybersecurity kann jedoch die Risiken eines Angriffs und dessen negative Folgen minimieren. Ziel der Sicherheitsmaßnamen ist es daher, die Resilienz beziehungsweise Widerstandsfähigkeit des Unternehmens vor Cyberangriffen zu erhöhen. Mit einer guten Firewall ist es aber nicht getan. Das Thema umfasst die IT-Technologie und -Infrastruktur, die Software-Anwendungen, das Knowhow des IT-Personals und nicht zuletzt den einzelnen Mitarbeiter oder Anwender – also allgemein den Faktor Mensch. Und das schwächste Glied in dieser Kette bestimmt dabei das allgemeine Sicherheitsniveau.

Der Schutz gegen Cyberkriminalität beginnt deshalb damit, Verständnis für die Gefahren beziehungsweise Risiken zu entwickeln, auf die sich Unternehmen im Zuge der Digitalisierung einstellen müssen. Technische Maßnahmen wie ein Basisschutz – Passwortsicherung, Zwei-Faktor-Absicherung für alle Fernzugänge, Firewalls, Virenscanner, Updates und Backups – sind nahezu in allen Unternehmen vorhanden. Dieser Mindeststandard erweist sich aber angesichts der ständigen Weiterentwicklung auf der Seite der Angreifer als nicht ausreichend. Die IT-Technologie und -Infrastruktur sowie die Software-Anwendungen müssen daher permanent kontrolliert beziehungsweise aktualisiert werden.

Achtung Mensch: Das schwächste Glied in der Kette!

Ebenso wichtig wie die Sensibilität der Führungskräfte für das Thema Cybersecurity ist die Unternehmenskultur der Firma und die Aufmerksamkeit ihrer Mitarbeiter. Cyberkriminelle nutzen immer häufiger die Schwachstelle Mensch für ihre Zwecke. Social Engineers spionieren das persönliche Umfeld ihres Opfers aus, täuschen Identitäten vor oder nutzen Verhaltensweisen wie Hilfsbereitschaft und Autoritätshörigkeit aus, um geheime Informationen zu erlangen oder den Mitarbeiter unwissentlich betrügerische Zahlungsaufträge auslösen zu lassen. Häufig dient Social Engineering dem Eindringen in ein fremdes Computersystem, um vertrauliche Daten einzuse-

Illu: Sky vectors/shutterstock.com

Prof. Dr. Igor Podebrad,
Group Chief Information Security Officer,
Commerzbank AG

„Banken kommt beim Schutz ihrer Kunden vor kriminellen Angriffen über das Netz eine Schlüsselrolle zu. Für die Commerzbank ist das ein zentrales Thema.“

hen; man spricht dann auch von Social Hacking. Die Vielzahl an vernetzten Geräten und digitalen Kanälen macht es ihnen vergleichsweise leicht, die vorhandene Sicherheitstechnik zu umgehen. Das führt dazu, dass nahezu alles ein potenzielles Ziel ist und eröffnet den (Cyber-)Kriminellen nie dagewesene Einfallstore. In einer vertrauensvollen und wertschätzenden Unternehmenskultur muss jeder Mitarbeiter bei seinem Chef oder Geschäftsführer rückfragen können, wenn er scheinbar von diesem eine Mail mit einer ungewöhnlichen Bitte bekommen hat.

Schadenshöhe unbekannt

Laut der Cyber-Sicherheits-Umfrage des BSI waren 2017 rund 70 Prozent der Unternehmen in Deutschland Opfer eines Cyberangriffs. Ungefähr die Hälfte dieser Angriffe war erfolgreich, wobei jeder zweite erfolgreiche Angriff mit Produktions- beziehungsweise Betriebsausfällen verbunden war. Es ist davon auszugehen, dass diese Zahlen nur den unteren Rand darstellen. Bei Cyberkriminalität gibt es eine signifikante Dunkelziffer, da Unternehmen Angriffe entweder gar nicht erkennen oder aber aus Sorge um ihre Reputation nicht melden.

Die Schätzungen zu den Kosten von Cyberkriminalität fallen sehr unterschiedlich aus, was auf eine schwache Datenlage, die große Dunkelziffer sowie eine fehlende einheitliche Systematik zur Bestimmung der Kosten zurückzuführen ist. Außerdem sind nicht alle Bestandteile eindeutig zu quantifizieren. Die Kosten eines einstündigen IT-Ausfalls belaufen sich laut einer Umfrage des Marktforschungsunternehmens Techconsult unter deutschen Mittelständlern auf durchschnittlich 41.000 Euro. Schwieriger ist allerdings die Quantifizierung von Imageschäden nach einem Cyberangriff. Als Schadenshöhe für die Gesamtwirtschaft in Deutschland geht das Bundesamt für Verfassungsschutz von jährlich ungefähr 50 Milliarden Euro aus. In diesen Werten sind allerdings nicht die Verluste an Kunden und Reputation enthalten.

Eine andere Größenordnung weisen die Schäden der Attacke durch die Schadprogramme WannaCry oder NotPetya auf. NotPetya verursachte weltweiten Schäden von rund 10 Milliarden US-Dollar. Allein bei den Logistikunternehmen Fedex und Maersk verursachte der Angriff laut Unternehmensangaben jeweils Kosten von ungefähr 300 Millionen US-Dollar. So mussten bei Maersk 4.000 Server, 45.000 Computer und 2.500 Applikationen reinstalliert werden.

Banken kommt beim Thema Cybersecurity eine Schlüsselrolle zu

Banken kommt beim Schutz ihrer Kunden vor solchen kriminellen Angriffen über das Netz eine Schlüsselrolle zu. Für die Commerzbank ist das ein zentrales Thema.

Niemand kennt unsere Kunden so gut wie wir. Unsere Aufgabe ist es, dieses Wissen noch besser im Sinne der Kunden zu nutzen. Wir hatten immer schon extrem große Datenmengen zu Kunden, Zahlungsströmen und Volkswirtschaften. Bislang konnten wir diese Daten nur begrenzt für die Kunden nutzbar machen. Das ändert sich: Mit den neuen technischen Möglichkeiten können wir extrem große Datenmengen verarbeiten und analysieren. In Echtzeit. Dadurch erkennen wir noch früher, was unsere Kunden brauchen und wie wir ihnen gezielt weiterhelfen können, wenn sie das wünschen. Doch es geht nicht nur darum, die Chancen der technologischen Entwicklung zu nutzen. Unsere gesellschaftliche Aufgabe ist es auch, auf die Risiken hinzuweisen.

Der Schutz vor Cyberangriffen muss entlang der gesamten Liefer- beziehungsweise Wertschöpfungskette gedacht werden. Denn mit zunehmender Vernetzung zwischen den Lieferanten und Herstellern reicht ein hohes Schutzniveau bei einem Unternehmen nicht aus, wenn ein Zugang ins System über die schlechter gesicherte IT eines Lieferanten möglich ist. Daher erfordert Cybersecurity auch eine Zusammenarbeit und Abstimmung mit anderen Unternehmen. Darauf legen wir als Bank sehr großen Wert. In unsere Risikomanagement-Bewertung fließt die „Cyber Hygiene“ unserer Kunden mit ein. Sprich, unser Risikomanagement bewertet den Kunden nach seinem ganzheitlichen Schutz vor Cyberangriffen.

Mittelständische Unternehmen werden laut Bitkom-Studie besonders oft Opfer von digitaler Kriminalität. Hier haben es die Täter oft auf deren Daten abgesehen. Der Datendiebstahl kann Kundendaten betreffen oder sensibles Firmenwissen wie z.B. Informationen über Produktentwicklungen, das Design eines geplanten neuen Produktes oder Patente, die kurz vor der Eintragung stehen. Des Weiteren können Informationen zum Unternehmen, wie Organigramme oder Berechtigungen zur Vorbereitung eines CEO-Frauds oder Social Engineering genutzt werden.

Diese Betrugsversuche frühzeitig zu entdecken und zu verhindern, zählt zu unseren zentralen Aufgaben. Hier arbeitet die Commerzbank intensiv mit Behörden und Organisationen zusammen und ist bereits ein angesehener Partner unserer Mittelstandskunden. Die Erfolgsquote bei der Erkennung und Abwehr von solchen Betrugsversuchen ist sehr hoch. Dadurch konnten wir allein 2017 unrechtmäßige Auszahlungen von mehr als 120 Millionen Euro identifizieren und nahezu alle stoppen. Das heißt, in diesen Fällen hat die Commerzbank eine Zahlung als risikoreich identifiziert und Überweisungen an Betrüger rechtzeitig verhindert oder nach sofortiger Rückfrage beim Kunden die Überweisung eingefroren und zurückgeholt.

Wir als Bank spüren eine große Verantwortung im Umgang mit den Kundendaten. Wir genießen ein hohes Vertrauen in Punkto Beratung und Datensicherheit. Kunden sehen uns als Statthalter/Treuhänder in der komplexen digitalen Welt. Die rechtlichen Rahmenbedingungen und europäische Werte unterstützen uns dabei.

Großes Potenzial für Datenschutz „made in Europe“

Europa hat mit der Datenschutzgrundverordnung einen Standard gesetzt, der international neue Maßstäbe setzt. Um die strengen Schutzstandards durchzusetzen, arbeiten wir mit Methoden wie Anonymisierung, Pseudonymisierung und Mikro-Segmentierung. Das heißt, wenn die Daten in die Cloud wandern, sind sie einzelnen Personen nicht mehr zuzuordnen. Bei sogenannten „de-risked Data“ werden personenbezogene Daten, sogenannte Personally Identifiable Information (PII), vollständig entfernt, sodass niemand, weder innerhalb noch außerhalb der Bank, in der Lage ist, PII im Data Lake oder in der Cloud zu sehen. Und dabei bleibt der inhaltliche Wert der Daten weitgehend erhalten.

Datenschutz made in Europe hat großes Potenzial. Der vertrauensvolle und sichere Umgang mit Daten wird sich zum entscheidenden Wettbewerbsfaktor entwickeln. Diese Herausforderung nehmen wir an. Denn Datensicherheit ist der neue Rohstoff des 21. Jahrhunderts und Vertrauen die wichtigste Währung.

Augmented Reality

Mehr Durchblick beim Beschäftigtendatenschutz

Foto: Syda Productions/shutterstock.com

Tilman Liebchen, Team der Begleitforschung des Technologieprogramms „Smart Service Welt I“, gefördert vom Bundesministerium für Wirtschaft und Energie

„Zentral bei der Einführung adaptiver Assistenzsysteme ist eine menschengerechte Technikgestaltung, die nicht unzulässig in die Persönlichkeitsrechte von Arbeitnehmern eingreift.“

von Tilman Liebchen

Augmented Reality (AR) kann in der Industrie dazu beitragen, Arbeitsprozesse für die Mitarbeiter zu erleichtern und effizienter zu machen. Intelligente Datenbrillen steigern beispielsweise die Bewegungsfreiheit und verringern Unterbrechungen im Arbeitsablauf. Doch die Nutzung von digitalen Assistenten wie Datenbrillen oder Tablets wirft viele Fragen auf - nicht zuletzt, wie es sich mit dem Beschäftigtendatenschutz bei diesen neuen Technologien verhält. Ein vom Bundesministerium für Wirtschaft und Energie (BMWi) gefördertes Projekt namens „Glass@Service“ hat im Rahmen der Entwicklung einer intelligenten Datenbrille mit einem Datenschutzgutachten gezeigt, wie sich innovative Assistenzsysteme datenschutzkonform nutzen lassen.

AR schafft Freiheiten

Was sich hinter den Begriffen Augmented Reality oder „erweiterter Realität“ im Detail verbirgt, ist für viele Menschen nicht immer klar. Doch spätestens seit dem Erscheinen des Smartphone-Spiels „Pokémon Go“ hat AR einen großen Bekanntheitsgrad erreicht. Bei diesem und ähnlichen Spielen wird die per Kamera erfasste reale Umgebung auf dem Display mit zusätzlichen künstlichen Einblendungen ergänzt. So kann zum Beispiel während eines Spaziergangs durch das Brandenburger Tor in Berlin mit dem Smartphone auf Punktejagd gegangen werden.

Was bislang vor allem im Unterhaltungsbereich bekannt war, setzt jetzt seinen Siegeszug in der Wirtschaft fort. Denn mit Augmented Reality können auch Unternehmen ihre Produktionsprozesse optimieren, z.B. mit intelligenten Datenbrillen. Die im geförderten Projekt „Glass@Service“ entwickelten Brillen besitzen eine sogenannte Durchsichtoptik, sodass die Arbeitsumgebung direkt durch die Brille hindurch sichtbar ist und nicht als „abgefilmte“ Umgebung angezeigt wird. Die Realität wird dann direkt im Blickfeld des Brillenträgers um nützliche Informationen ergänzt. So ist es zum Beispiel möglich, bei Instandhaltungsarbeiten für Maschinen und Anlagen die Anleitungen oder Anweisungen direkt im Sichtfeld einzublenden und Servicetechniker Schritt für Schritt durch die nötigen Arbeiten zu führen. Die Brillen erweisen sich dabei vor allem in beengten Einsatzfeldern als nützlich, wie bei der Montage in Maschineninnenräumen: Die Hände der Monteure bleiben frei und der Blick muss nicht immer von der Anleitung zum Bauteil hin- und herwandern. Gesteuert werden die Brillen über Gesten oder Augenbewegungen.

Um die Beschäftigten bei ihren Tätigkeiten zu unterstützen, sind AR-Assistenzsysteme darauf angewiesen, permanent große Mengen an Daten zu erfassen und weiter zu verarbeiten. Das können etwa GPS-Signale zur Positionsermittlung sein, aber auch Kamerabilder, die Umgebung oder Handbewegungen erfassen.

Aus den gewonnenen Informationen können zum Beispiel Standortinformationen abgeleitet oder Markierungen für die richtige Platzierung von Ersatzteilen erzeugt werden. Allerdings können die Informationen auch mehr verraten: Etwa, wie lange ein Mitarbeiter für einen bestimmten Arbeitsschritt gebraucht hat, oder wie lange er an einem bestimmten Ort war.

Zweck der Datenerhebung ist entscheidend

Die Daten können dabei nicht nur Informationen zu den jeweiligen Brillenträgern enthalten, sondern auch von Kollegen in der näheren Umgebung, die ebenfalls von den Kameras aufgenommen werden. Die Mitarbeiter bemerken dabei meist nicht, dass oder wie sie erfasst werden und haben oft keinen Einfluss auf die über sie aufgezeichneten Informationen. Unternehmen sollten sich daher vor der Einführung solcher Technologien folgende Fragen stellen: Welche Informationen dürfen überhaupt erhoben und zu welchen Zwecken genutzt werden? Welche Mitbestimmungsrechte haben die Beschäftigten hierbei? Wie müssen personenbezogene Daten geschützt werden? Und in welcher Form müssen die Betroffenen der Nutzung ihrer Daten zustimmen?

Um die Rechtssicherheit beim Einsatz digitaler Arbeitsmittel zu überprüfen und zu verbessern, hat die Bundesanstalt für Arbeitsschutz und Arbeitsmedizin (BAuA) als Partner im Glass@Service-Projekt ein Gutachten zu den rechtlichen Datenschutz-Anforderungen bei adaptiven Assistenzsystemen erstellen lassen. Das Gutachten liefert wichtige Erkenntnisse zur rechtssicheren Gestaltung und Umsetzung dieser neuen Technologien:

Zentral bei der Einführung adaptiver Assistenzsysteme ist eine menschengerechte Technikgestaltung, die nicht unzulässig in die Persönlichkeitsrechte von Arbeitnehmern eingreift. Das oft beschriebene Szenario einer „gläsernen Fabrik“, in der alle möglichen Daten erhoben und für beliebige Anwendungen weiterverarbeitet werden, ist daher unrechtmäßig. Das Erheben und die Verarbeitung personenbezogener Daten müssen immer einem bestimmten Zweck im Interesse des Unternehmens dienen. Wichtig ist dabei auch, dass das Verarbeiten von Informationen zu einem anderen Zweck als ursprünglich bei der Datenerhebung vorgesehen nur sehr begrenzt möglich ist.

Eine Kollektivvereinbarung, die den Einsatz etwa von AR-Brillen im Unternehmen regelt, vereinfacht den Umgang mit dem Datenschutz für Firmen. Zwar hat die Datenschutzgrundverordnung (DSGVO) die individuellen Rechte der Mitarbeiter bezüglich ihrer Daten gestärkt, sodass sie Informations- und Auskunftsansprüche und das Recht auf die Übertragbarkeit ihrer Daten haben. Allerdings kann es sein, dass Geschäfts- oder Betriebsgeheimnisse diese Ansprüche begrenzen.

Darüber hinaus sind, wie bei allen technischen Entwicklungen, möglichst datenschutzfreundliche Voreinstellungen zu treffen, damit nicht mehr Informationen als nötig erhoben werden. Beispiele dafür sind die Anonymisierung und Pseudonymisierung von Daten. Dieser technische Datenschutz wurde ebenfalls durch die DSGVO gestärkt.

Die Chancen überwiegen

Auch wenn neue Technologien wie Augmented Reality gleichzeitig neue Datenschutzfragen aufwerfen, können diese Herausforderungen durch eine gute Vorbereitung gemeistert werden. Wichtig ist, dass sich durch Rechtssicherheit auch das Vertrauen der Mitarbeiter in die neuen Technologien stärken lässt. Eine offene Kommunikation über Chancen, Risiken und datenschutzrechtliche Absicherungen kann dazu beitragen, dass Mitarbeiter den Nutzen von AR-Technologien schneller wertschätzen und ihnen mit weniger Bedenken oder Misstrauen entgegentreten. Die Einführung innovativer und zukunftsorientierter Assistenzsysteme in der Industrie ist damit einfacher zu gestalten.

Vom Ende der Einwilligung

Illu: Victor Z/shutterstock.com

von Jörg Steinhaus

Im katholischen Rheinland werden zu St. Martin traditionell Weckmänner, ein süßes Figurengebäck, an Kinder verteilt. Groß war daher die Entrüstung, als die Stadt Kevelaer in diesem Herbst mangels scheinbar erforderlicher Einwilligung auf die Verteilung an Kinder und auch Senioren in Alterseinrichtungen verzichten wollte. Dabei steht dem Brauchtum als wichtigem gesellschaftlichen Interesse kein überwiegendes Risiko für die betroffenen Kinder und Senioren entgegen, so dass sich eine Datenverarbeitung für die Verteilung ohne weiteres auf Basis der europäischen Datenschutz-Grundverordnung (DSGVO) begründen ließe. Der Hype um die Einwilligung und das Unwissen der Stadt verhinderten dies jedoch.

Auch in der Arztpraxis erfährt man viel von den Spuren des Wahnsinns, den die Einwilligungspropheten herbeibeten. „Sie müssen dann hier unten noch einwilligen, sonst können wir Sie nicht behandeln“, heißt es gleich am Eingang - als würde das Gesundheitswesen durch den Datenschutz ausgehebelt. Eine kurze Anmerkung, dass eine Einwilligung aber freiwillig zu erteilen sei, wird mit erbostem Blick der Arzthelfer quittiert.

Zu wenig Information

Dabei hat die Einwilligung als solches nichts Böses an sich. Sie ist der höchste Ausdruck der Zustimmung der Person, deren Daten verarbeitet werden sollen, und spätestens seit dem Volkszählungsurteil von 1983 der heilige Gral des deutschen Datenschutzes. Die Beteiligung des Betroffenen soll ihn vor unerwarteter Verarbeitung und der Kombination ansonsten belangloser Daten schützen. Aber die Einwilligung basiert auf der Annahme vollständiger oder zumindest klar ausreichender und verständlicher Information für denjenigen, der sie erteilen soll. Und das ist heute deutlich öfter die Ausnahme als die Regel. Daten werden in einer digitalisierten Welt vielfältiger und weitergehender verarbeitet und umfassender analysiert als vor über 30 Jahren. Immer seltener gibt es eine kurzzeitige und auf nur einen Zweck ausgerichtete Verarbeitung ohne weitere Anforderungen und Hintergedanken und mit konsequenter und zeitnaher Datenlöschung.

Damit steigt aber auch die Schwierigkeit, der betroffenen Person diejenigen Informationen vorzulegen, die diese zwingend für eine wirksame Entscheidungsfindung benötigt. Sind es zu viele oder zu komplexe, wird möglicherweise nicht alles gelesen oder verstanden. Und lässt man Teile der Beschreibung weg, so fehlt hierfür nach diesem Konzept die Rechtsgrundlage für diese Datenverarbeitung.

Als letztes kommen die Hürden für die Freiwilligkeit der Erklärung hinzu, die gerade der EuGH in Bezug auf Cookies klargestellt hat. Ohne aktives Handeln keine Einwilligung. Vorangekreuzte Auswahlfelder spiegeln das nicht wider, da der Betroffene sie übersehen kann oder das oftmals vielleicht auch will.

Mehr Verantwortung übernehmen

Die richtige Konsequenz aus diesem Informationsungleichgewicht und dem Handlungszwang ist die klare Zuschreibung der Verantwortlichkeit an denjenigen, der die Daten verarbeiten will. Die Einwilligung ist zu oft billige Ausrede, um solche Verantwortung nicht wahrnehmen zu wollen, da der Betroffene

ja schließlich aus eigener Entscheidung zugestimmt habe. Dass dieser den Umfang der Verarbeitung weder umfassend überschauen noch verstehen kann, nimmt aber der verfassungshistorischen Betonung ihre Grundlage.

Damit bleibt die Herausforderung, datenschutzrechtlich korrekt zu handeln, dort, wo sie hingehört: beim Verantwortlichen. Er hat festzulegen, welche Daten zur Zweckerfüllung erforderlich sind, und darauf zu verzichten, weitere Daten zu erheben. Er hat die Daten vor Missbrauch zu schützen und eine Weitergabe an Dritte rechtlich abzusichern. Und er hat immer noch die Pflicht, dem Einzelnen gegenüber in allen Belangen transparent zu sein: in einer ersten Information, die einfach und verständlich sein muss, und dafür unter Umständen auf nebensächliche Details verzichten kann. Und später ebenso, wenn der Betroffene nachfragt, was genau mit bestimmten Daten gemacht wurde.

Forschung braucht Freiheit

Diese Herausforderungen finden sich auch in der Forschung und hier insbesondere im medizinischen Bereich. Wenn ein Patient an einer Studie teilnehmen will, muss er nach geltendem Recht in Deutschland sowohl in die Teilnahme an der Studie als auch in die Verarbeitung von in der Studie erhobenen Daten einwilligen. Die Aufsichtsbehörden für den Datenschutz haben jüngst ausführlich dargelegt, warum die Einwilligung in die Datenverarbeitung getrennt zu erfolgen habe, und welche spezifische Rolle diese Erklärung spielt. Das Interesse des Patienten an einer verständlichen Aufklärung blieb dabei allerdings unerwähnt.

Dabei sind Daten in der klinischen Forschung ohnehin so kodiert, dass kein Unternehmen mehr Schlüsse auf den dahinterstehenden Patienten ziehen kann. Allein die Mediziner in der durchführenden Klinik halten den Schlüssel in der Hand, um im Fall neuer Erkenntnisse oder bei behördlicher Anweisung auch die Patienten zu deren eigener Sicherheit erneut kontaktieren können.

Noch schwieriger wird es, wenn Daten aus einer Studie für weitere Forschungszwecke verwendet werden sollen. Eine Identifizierung ist dann eine nur sehr theoretische Möglichkeit, bremst aber die weitere Forschung aus, da deren Zwecke zum Zeitpunkt, an dem die Einwilligung eingeholt wurde, in der Regel nicht bekannt waren. Insbesondere innovative Ansätze, die schnell zu neuen Therapiemöglichkeiten führen sollen, können so nur mühsam weiterverfolgt werden.

Eine Lösung wäre hier möglicherweise die rechtliche Begründung der privaten Forschung über das Mittel des öffentlichen Interesses. Insbesondere bei teuren Forschungsvorhaben, etwa im Bereich der Onkologie, könnte hier das privatwirtschaftliche Geld zum Nutzen allgemeinen Therapiefortschritts verwendet werden. Dies bedarf unter Umständen einer Anpassung des Arzneimittelrechts, zumindest aber eines Umdenkens bei den Aufsichtsbehörden für den Datenschutz. Da das öffentliche Interesse eine eigene Rechtsgrundlage in der DSGVO darstellt, wäre die Einwilligung des Patienten an dieser Stelle obsolet.

Alles basiert auf besseren Informationen

Die Einwilligung hat somit an vielen Stellen ihre Berechtigung verloren. Handelt ein Unternehmen grundsätzlich datenschutzkonform, so kann es nahezu überall auf die Einwilligung verzichten und die Verarbeitung mit einer anderen Rechtsgrundlage legitimieren. Bei einfachen Vorgängen, wie dem Versand von Newslettern, hat sich ohnehin etabliert, die Abmeldung jederzeit unkompliziert per Mausklick durchzuführen. Kaum ein Nutzer wird dies als Widerruf einer informierten Einwilligung wahrnehmen, sondern als normale Handlung der Zusendungsbeendigung.

„Handelt ein Unternehmen grundsätzlich datenschutzkonform, so kann es nahezu überall auf die Einwilligung verzichten.“

Wichtig ist daher die Kompensation des Einwilligungsverzichts durch eindeutige Offenheit über die Art und den Zweck der Datenverarbeitung. Dies hatte der Gesetzgeber auch vorgesehen, als er Informationen in einfacher und verständlicher Sprache gefordert hat. In Kontinentaleuropa überwiegt das kodifizierte Recht. Wir sind daher weit weg von US-amerikanischen Verhältnissen, in denen jedes Wort einer möglichst umfassenden Erklärung über Wohl und Wehe eines Unternehmens im Fall eines Strafschadensersatzes entscheiden kann. Es zeugt daher von einer Schwerfälligkeit der deutschen Juristerei, die grundlegenden Datenverarbeitungen nicht in einfache Worte fassen zu können.

Schleichendes Ende der Einwilligung

An Stelle eines völligen Paradigmenwechsels erleben wir so ein schleichendes Ende der Einwilligung, bei dem das Aufbäumen eines veralteten Rechtsinstruments mehr Aufmerksamkeit generiert als ihm gebührt. Wir brauchen klare Regeln für die Verarbeitung personenbezogener Daten und müssen sehr wohl die Risiken für die betroffenen Personen erkennen und reduzieren. Niemand soll seine Krankenversicherung verlieren, weil er bestimmte genetische Informationen in sich trägt. Aber dass es so weit kommt, bedarf schon einer sehr abenteuerlichen Konstruktion von Zufällen und mehrerer klarer Verstöße gegen das geltende Datenschutzrecht. Doch bis zum Ende der Einwilligung werden weiterhin Patienten zu sinnfreien Erklärungen gezwungen und Kinder enttäuscht, deren Augen sonst beim Anblick eines Weckmanns gestrahlt hätten. Und dies auch, weil es der Politik in aller Breite nicht gelungen ist, der Gesellschaft den guten Hintergrund eines insgesamt vernünftigen Datenschutzrechts zu erklären.

Foto: Eva Speith

Jörg Steinhaus, Konzerndatenschutzbeauftragter, Merck KGaA

DSGVO

Benchmark und Wirtschaftsfaktor

von Ulrich Kelber

Die Europäische Datenschutzgrundverordnung (DSGVO) ist seit Mai 2018 verbindlich anzuwenden und hat für viele Diskussionen wegen der vermeintlichen Zunahme von Formularen und Vorgaben sowie angeblicher Behinderung von Optimierungsprozessen gesorgt. Auch aktuell wird sie wieder als Bürokratiemonster diffamiert, das die wirtschaftliche Entwicklung behindere. Ich antworte darauf schlicht mit: Das ist Unsinn!

Die DSGVO hat nach meiner festen Überzeugung unter anderem wesentlich dazu beigetragen, dass das Thema IT-Sicherheit endlich die Bedeutung bekommt, die es haben muss. Schauen wir uns doch mal die Fakten an. Cyberkriminalität nimmt rasant zu und schadet der deutschen Wirtschaft enorm. Datendiebstahl, Industriespionage und Sabotage durch Virenangriffe kosten die deutsche Wirtschaft jährlich rund 55 Milliarden Euro. Erst in den letzten Wochen sind wieder ganze Firmennetzwerke durch Ransomeware angegriffen und lahmgelegt worden. Den Unternehmen droht nicht nur ein Vertrauensverlust ihrer Kunden, sondern durch Datendiebstahl verschwinden auch Ideen, Patente und vertrauliche Dokumente.

Und das Bedrohungspotenzial nimmt eher zu als ab, wie sowohl das Bundesamt für Sicherheit in der Informationstechnik (BSI) als auch der Bitkom feststellen. Ich stimme deshalb der Forderung des Bitkom vollkommen zu, dass es unser Ziel sein muss, die Angriffsflächen zu reduzieren. Hersteller, Anwender, Infrastrukturbetreiber, Politik, Aufsichtsbehörden und Strafverfolgungsbehörden müssen gemeinsam darauf hinwirken, diese Angriffsfläche so klein wie möglich zu halten. Und dazu zählt neben den technischen Sicherungsmaßnahmen eben auch der Datenschutz, vom Anfang der Entwicklung bis zur Auslieferung und Nutzung.

Gerade für kleine und mittlere Unternehmen ist es wichtig, dass Datenschutz und IT- Sicherheit zur Chefsache gemacht wird. Selbst wenn sie keinen betrieblichen Datenschutzbeauftragten benennen müssen, sollte die Chefetage sich selbst als solcher verstehen. Das BSI gibt gute Hilfestellungen zum IT-Basisschutz, aber es muss auch auf alle Schnittstellen und vernetzten Geräte geachtet werden. Die Nutzung mobiler Endgeräte, gerade auch im Ausland, sind beliebte Einfallstore für Datenklau und Spionage. Genauso wie hier auf die Sicherheit der firmeneigenen Daten geachtet werden muss, gilt dies auch für die Kunden- und Nutzerdaten.

Die DSGVO soll mit ihren Datenschutzbestimmungen dazu beitragen, die geschäftlichen und privaten Nutzerdaten zu schützen und gefährlichen Angriffen vorzubeugen. Sie soll das Vertrauen in die zunehmend digitalisierte Wirtschaft stärken. Davon profitieren die Unternehmen mehr als manche Wirtschaftsverbandsvertreter oder auch Politiker wahrhaben wollen. Ich weiß, dass die DSGVO u.a. bei Informations- und Dokumentationspflichten übers Ziel hinausschießt. Dort wollen wir im Rahmen des Evaluierungsprozess im nächsten Jahr nachbessern. Im Vergleich zu Kommunen, Finanzämtern und IHKs sind die Formularanforderungen der Datenschutzbehörden aber schon heute geradezu spartanisch.

Wir sollten nicht aus dem Auge verlieren: Die DSGVO ist Benchmark für einen der größten Wirtschaftsräume und setzt darüber hinaus auch zunehmend den internationalen Standard. Wer hier gut aufgestellt ist, der profitiert nicht nur innerhalb der EU, sondern weltweit. Die DSGVO öffnet mit ihren einheitlichen Regeln neue Märkte. Die DSGVO sorgt außerdem für Unternehmen, die in mehreren EU-Ländern angesiedelt sind, für eine deutliche Entbürokratisierung, da mit dem One-Stop-Shop-Verfahren grundsätzlich nur noch eine Datenschutzaufsichtsbehörde in der EU zuständig ist.

Bei allem unüberhörbaren Murren aus Wirtschaftsverbänden über Einzelpunkte in der DSGVO bin ich überzeugt, dass die Wirtschaft in Deutschland und der EU von ihr profitiert. Zum einen, weil viele Unternehmen gezwungen waren und sind, ihre Datenverarbeitungsprozesse zu kontrollieren, zu überarbeiten und damit in aller Regel zu optimieren. Zum anderen, weil die DSGVO nicht nur für den Schutz personenbezogener Daten steht, sondern weil sie gleichzeitig präventives Handeln, Kontrolle der eigenen Systeme und damit auch das Schließen möglicher Löcher fördert.

Ich bin sicher, für die Unternehmen, in denen die Digitalisierung voranschreitet, ist der Datenschutz und die damit einhergehende IT-Sicherheit unter dem Strich ein Gewinn. Ohne das Vertrauen der Bürgerinnen und Bürger, also der Kundinnen und Kunden, in die Sicherheit von Daten und Prozessen wird die Digitalisierung nicht funktionieren.

Ulrich Kelber, Bundesbeauftragter für den Datenschutz und die Informationsfreiheit

Foto: Bundesregierung/Kugler

„Gerade für kleine und mittlere Unternehmen ist es wichtig, dass Datenschutz und IT-Sicherheit Chefsache sind.“

ADVERTORIAL

Achillesferse Berechtigungsmanagement

Sichere Infrastruktur im Internet of Things

von Felix ‚FX' Lindner

Die Erfahrung aus der IT-Sicherheitsberatung zeigt: Zur Achillesferse moderner Projekte wird oft das Berechtigungsmanagement. Wer darf was, wann und auf welche Art mit wem? Fehler an dieser Stelle haben weitreichende Konsequenzen. Fällt das System gar aus, ist dies fatal. Zunehmend zeigt sich, dass bestehende Technologien hier keine hinreichenden Lösungen bieten.

Mit wachem Blick in die Zukunft und dem geballten Wissen aus über einer Dekade IT-Sicherheitserfahrung wurde daher vor fünf Jahren die P3KI als Tochterunternehmen der Recurity Labs gegründet. Die Mission: Die Entwicklung des Berechtigungssystems der Zukunft. Das Ergebnis ist P3KI Core, eine Berechtigungslösung, welche komplett dezentral und trotz Extrembedingungen wie Ausfall der Kommunikationsverbindung oder Teilen der Infrastruktur die Reaktionsfähigkeit des Kunden sicherstellt.

Ermöglicht wird dies durch eine einfach zu integrierende Software. Die gebotene Sicherheit basiert auf der Kombination von kryptografischen Algorithmen und einer hochflexiblen und mathematisch beweisbaren Berechtigungssprache. Auf Hype-Technologien wie Blockchain und Distributed Ledgers wurde bewusst verzichtet. Das Besondere: Berechtigungen können ganz oder teilweise weitergegeben und jederzeit vollständig verifiziert werden, ohne dabei auf zentrale Infrastruktur angewiesen zu sein.

Inspiriert wurde die Lösung ursprünglich durch den ISO 20828 Standard der Automobilbranche. Dieser beschrieb bereits 2006 die Notwendigkeit einer verteilten Public Key Infrastruktur (PKI). Antworten auf wesentliche technische Fragen, die für eine sichere Umsetzung notwendig gewesen wären, blieb der Standard jedoch schuldig. Recurity Labs erkannte diese Lücke und adressierte sie durch eigene Forschungsmittel und ultimativ der Ausgründung der P3KI. Die von P3KI geschaffene Lösung P3KI Core beantwortet diese Fragen nun vollumfänglich, bietet weitreichendere Möglichkeiten und Garantien. Von besonderer Relevanz ist P3KIs neue Technologie dabei für Systeme, die auf Angriffe und Ausfall großer Teile der Infrastruktur agil reagieren müssen, um den Weiterbetrieb auch unter widrigsten Bedingungen zu garantieren.

Felix ‚FX' Lindner ist ein weltweit renommierter Whitehat Hacker, Sicherheitsforscher und Gründer der Recurity Labs und P3KI. Die Recurity Labs GmbH berät seit rund vierzehn Jahren internationale Kunden ganzheitlich zu allen Themen der IT-Sicherheit. Die P3KI GmbH entwickelt dezentrale, offline-fähige Rechtedelegationslösungen für das Internet of Things, Automotive- und Industrieanwendungen.

www.recurity-labs.com | www.p3ki.com

Recurity Labs

P3KI

„Die größte Herausforderung unserer Kunden ist die Gewährleistung von Sicherheit in Zeiten unaufhaltsam wachsender Vernetzung, Cloud-Lösungen und rasantem technologischem Fortschritt."

Felix ‚FX' Lindner

CONCORDIA:

Europas Cybersicherheit vernetzt sich

Hintergrund: Ivision 2u/shutterstock.com

von Prof. Dr. Gabi Dreo Rodosek

Die Informations- und Kommunikationstechnologie ist die Schlüsseltechnologie unserer digitalen Gesellschaft und die Cybersicherheit deren Fundament. Derzeit sind die Cybersicherheitskompetenzen in Europa fragmentiert. Um dieser Fragmentierung zu begegnen sowie die Vernetzung unterschiedlicher Akteure zu fördern, hatte die EU einen Call im Rahmen des EU-Förderprogramms für Forschung und Innovation „Horizont 2020“ hierzu ausgeschrieben.

Das Projekt CONCORDIA hat die Ausschreibung gewonnen. CONCORDIA hat eine Laufzeit von vier Jahren und wird von der EU mit 16 Mio. EUR finanziert. Zu dieser Summe kommen noch nationale Förderungen und Unternehmensmittel in Höhe von 7 Mio. EUR. Gestartet mit ursprünglich 42 Partnern, koordiniert das Forschungsinstitut CODE der Universität der Bundeswehr München dieses Projekt, das nach nur 10 Monaten Laufzeit mittlerweile 55 Projektpartner umfasst. Dazu zählen 28 Universitäten und Forschungseinrichtungen sowie 27 Unternehmen. Zu den universitären Partnern gehören renommierte Hochschulen und Forschungsinstitutionen wie die Universität Twente, die Universität Mailand, das Imperial College London, RISE aus Schweden, die Universität OsloMet und das Leibniz-Rechenzentrum. Bei den Unternehmenspartnern sind es Weltkonzerne wie Siemens, Infineon, Airbus Space and Defence, Lufthansa, Telefonica, Telekom Italia, Deutsche Telekom, Allianz, Atos, secunet, klein- und mittelständische Unternehmen wie Bitdefender sowie Organisationen wie die Caixa-Bank.

Ziel von CONCORDIA ist die Vernetzung von Cybersicherheitszentren in Europa, die Entwicklung von IT-Produkten und - Dienstleistungen gemeinsam mit Forschung und Industrie entlang der gesamten Wertschöpfungskette sowie die Etablierung von Plattformen für die europaweite Aus- und Weiterbildung von IT-Kompetenzen. Damit wird ein einzigartiges Ökosystem aufgebaut, in dem führende europäische Partner aus Forschung, Technologieentwicklung, Industrie und dem öffentlichen Sektor gemeinsam agieren.

Hauptsächlich, aber nicht ausschließlich, wird im Rahmen von CONCORDIA ...

- eine Roadmap entwickelt, um im Bereich der Cybersicherheit leistungsstarke Forschungsansätze zu identifizieren, experimentelle Validierung, Prototyp- und Lösungsentwicklung in einer agilen Weise durchzuführen und erfolgreiche, aber auch erfolglose potenzielle Produktentwicklungen schnell zu identifizieren.

- die Entwicklung von Cybersicherheitslösungen der nächsten Generation vorangetrieben, indem ein ganzheitlicher, datengetriebener End-to-End-Ansatz aus Datenerfassung, Datentransport und Datennutzung genutzt wird. Dabei stehen jederzeit die benutzerorientierte Netz-, Software-, System- und Anwendungssicherheit im Fokus.

- eine Infrastruktur virtueller Labore und Dienstleistungen (der „CONCORDIA Dienstkatalog“) zusammengetragen, um Forschung und Innovation zu unterstützen oder auch erst zu ermöglichen.

Prof. Dr. Gabi Dreo Rodosek,
Leitende Direktorin des Forschungsinstituts CODE,
Koordinatorin von CONCORDIA,
Universität der Bundeswehr München

„Der Aufbau einer digitalen Souveränität in Europa ist nur durch den Aufbau von digitalen Ökosystemen möglich.“

- an sektorspezifischen (Telekommunikations-, Finanz-, Verteidigungs-, Automotive- und Gesundheitssektor) und sektorübergreifenden (horizontale) Industriepiloten sowie dem Aufbau von Gründerzentren gearbeitet.

- eine Serie offener Ausschreibungen („Open Calls“) generiert, um Unternehmern und Einzelpersonen zu ermöglichen, ihre Ideen Realität werden zu lassen.

- ein europäisches Bildungsökosystem für Cybersicherheit aufgebaut. CONCORDIA erweitert daher traditionelle um neue virtuelle Kurse (MOOCs = Massive Open Online Courses und SPOCs = Small Private Online Courses) und eine Vielzahl von Outreach-Aktivitäten, einschließlich der Entwicklung von Kursen für Professionals und Cyber Ranges (virtuelle Trainingsumgebungen).

- Fachwissen für europäische Entscheidungsträger und die Industrie bereitgestellt.

- die Diversität im Berufsumfeld der Cybersicherheit aktiv durch die Initiative „Women in Cyber“ gefördert, um durch Netzwerke, Mentoring und Scholarship-Programme aufzubauen und zu nutzen.

Der Aufbau einer digitalen Souveränität in Europa ist nur durch den Aufbau von digitalen Ökosystemen, in denen unterschiedliche Stakeholder Kräfte und Ressourcen bündeln, um die Entwicklung von IT-Produkten und -Dienstleistungen entlang der gesamten Wertschöpfungskette zu unterstützen, möglich. CONCORDIA liefert dazu einen erheblichen Beitrag und ist die Blaupause für das European Cybersecurity Competence Network and Center.

ADVERTORIAL

Just Super/shutterstock.com

Autonomes Fahren

Datenschutz-Zertifikate schaffen Vertrauen

Joachim Mohs ist Partner bei PwC Deutschland im Bereich Cyber Security. Der Handelsblatt Journal Redaktion hat er erklärt, warum sich Unternehmen von den (datenschutzrechtlichen) Risiken des autonomen Fahrens nicht den Schlaf rauben lassen sollten.

Herr Mohs, wie hat sich die Bedeutung von Sicherheit und das Vertrauen in Daten beim autonomen Fahren in den letzten Jahren gewandelt?

Die Gefahren und Risiken beim autonomen Fahren rauben heute schon vielen Experten den Schlaf. Selbstfahrende Autos sind dabei erst der Gipfel verschiedener, sich bereits im Einsatz befindlicher Vorläufertechnologien wie autonome Entscheidungssysteme oder lernende Algorithmen. Bezüglich der Sicherheit unterscheiden sich die künftigen Risiken der autonomen Systeme nicht wesentlich von den Risiken der existierenden Vorläufertechnologien. Sie nehmen jedoch mit der steigenden Verbreitung dieser Technologien und ihrer wachsenden Leistungsfähigkeit und Vernetzung erheblich zu.

Wie können wir uns das konkret vorstellen?

Nehmen wir das Beispiel eines Windsurfers. Dieser hat ein vitales Interesse daran, von einem Surf-Spot zum anderen zu reisen – sozusagen stets auf der Suche nach der perfekten Welle. Optimalerweise gesteuert durch eine Wetter-App sucht sein Camper für ihn die passende Location und fährt ihn autonom über Nacht zum schönsten Strand.

Auch wenn vieles davon heute schon technisch möglich und umsetzbar ist, stellt das Szenario alle Hersteller vor große Herausforderungen: Woher bekomme ich zuverlässige Informationen? Wie können diese über sichere Kanäle übertragen werden? Und wem vertraue ich die Informationen an? Kurzgefasst: Das Qualitätsversprechen „Made in Germany“ muss auf digitalisierte Produkte übertragen werden, um das Vertrauen der Kunden zu rechtfertigen.

Wie können Unternehmen heute denn überhaupt noch einen korrekten Ablauf ihrer Prozesse und Produkte gewährleisten?

Heutzutage werden bei der Fahrzeugherstellung etwa vier Fünftel des Produktionsprozesses von Zulieferern abgedeckt. Die Digitalisierung wird diesen Effekt in fast allen Branchen deutlich verstärken. Spätestens nach einem Sicherheitsvorfall möchte ich als Autohersteller natürlich wissen: Wo stehe ich? Wie ist der Status Quo bei meinen Partnern und Zulieferern? Hier kann ein Sicherheits- oder Datenschutz-Zertifikat helfen, Vertrauen bezüglich des sicheren Umgangs mit sensiblen Daten bei den Geschäftspartnern in der Wertschöpfungskette zu gewährleisten.

In der Automobilindustrie können wir sowohl auf etablierte Zertifizierungsverfahren zurückgreifen als auch eine Reihe deutlich jüngerer Ansätze verfolgen, die spezielle Aspekte wie funktionale Sicherheit oder Managementsysteme adressieren. In unserer Arbeit nutzen wir risikoorientierte, auf Reifegradmodellen basierende Bewertungsstandards, die eine modulare Bewertung der Sicherheit und Qualität gemäß Sicherheitsniveau ermöglichen und dabei die gesamte Wertschöpfungskette abdecken.

So können Unternehmen ihre Geschäftspartner nach Risikoaspekten auswählen. Die Sicherheit der Daten und Funktionen bedarf eines anerkannten Qualitätsmaßstabs, vergleichbar mit dem „Spaltmaß“ im Karosseriebau. Und zwar nicht nur für einzelne Komponenten oder Funktionen – wie autonomes Fahren – sondern entlang der gesamten Wertschöpfungskette.

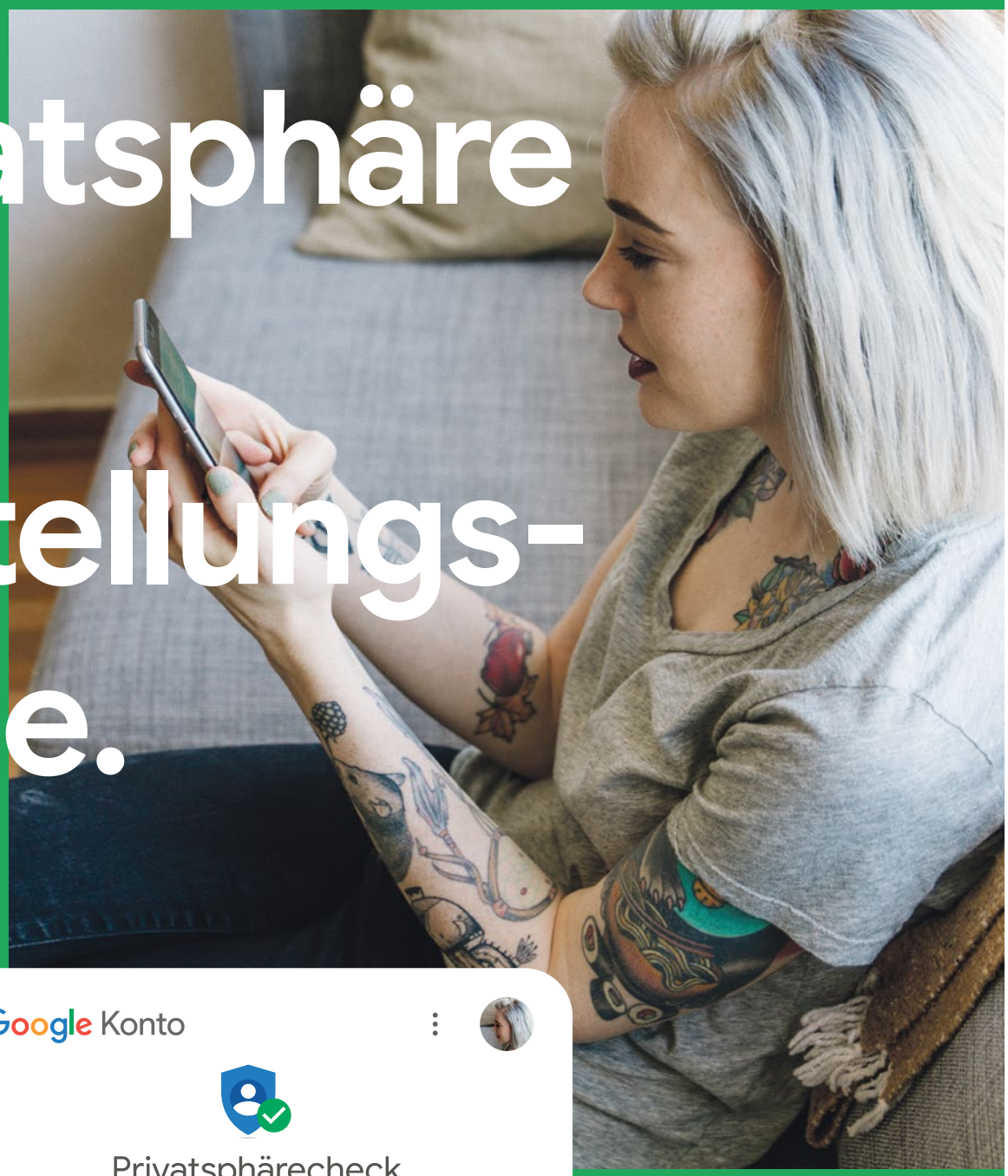
www.pwc.de/cybersecurity

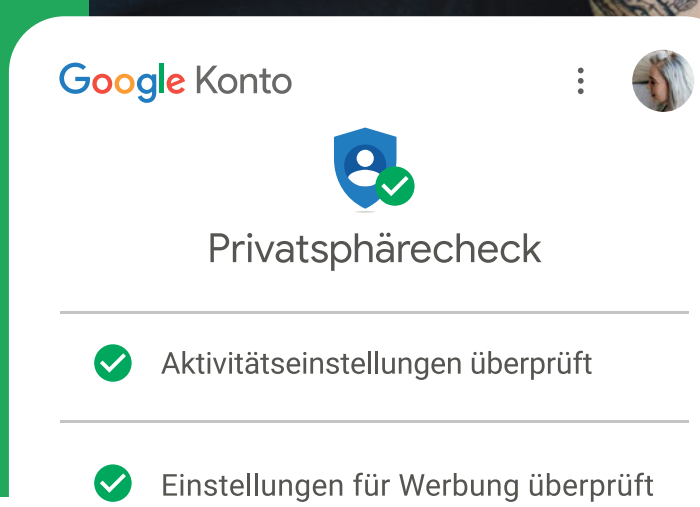
Foto: Roeder-Moldenhauer

Joachim Mohs

„Das Qualitätsversprechen ‚Made in Germany‘ muss auf digitalisierte Produkte übertragen werden, um das Vertrauen der Kunden zu rechtfertigen.“

Privatsphäre ist Einstellungs-sache.





Wählen Sie in wenigen Schritten wichtige Einstellungen:
g.co/privatsphaerecheck

Google

ADVERTORIAL

Digitaler Wandel der Autobranche

Cybersicherheit als Erfolgsfaktor

von Hans-Peter Fischer und Dr. Moritz Minzlaff

Cyberangriffe wie der Hack eines Jeeps im Jahr 2015 haben Cybersicherheit für Fahrzeuge nicht nur in den Fokus der Öffentlichkeit gebracht, sondern auch den Gesetzgeber aufmerksam gemacht. Dementsprechend wird die anstehende UN-Regulierung einen Paradigmenwechsel mit sich bringen: Eine Typzulassung wird nur noch mit nachgewiesenen Schutzmaßnahmen möglich sein. Spätestens damit steht Cybersicherheit auf der Agenda jedes Automobil-CEOs.

Der vom Weltforum für die Harmonisierung von Fahrzeugvorschriften der Vereinten Nationen (WP.29) entwickelte Regulierungsentwurf enthält zwei Kernforderungen für die Typzulassung:

- den Betrieb eines zertifizierten Cybersecurity-Managementsystems (CSMS) sowie
- die Anwendung des CSMS auf den Fahrzeugtyp.

Die EU plant, die Einhaltung dieser Vorgaben ab 2022 zu fordern. In Anbetracht der Entwicklungszeiten im Automobilbereich müssen sich OEMs und Zulieferer also bereits heute mit diesen Anforderungen auseinandersetzen.

Eine wesentliche Herausforderung bei der Umsetzung eines CSMS ist die Berücksichtigung der Automobilspezifika: Neben der hohen Komplexität in Produkt und Lieferkette sind dies vor allem funktionale Sicherheit, Umweltvorschriften und Diebstahlschutz. Parallel zum WP.29-Entwurf erarbeitet die Automobilindustrie bis 2020 die ISO/SAE 21434. Diese Norm stellt Cybersicherheits-Anforderungen an Organisation und Prozesse für den kompletten Fahrzeuglebenszyklus. Besondere Relevanz erhält der Standard, da im Kontext der UN-Regulierung konsequent auf die ISO/SAE 21434 verwiesen wird. Dies schafft eine industrieweite Grundlage einer gemeinsamen Terminologie und Definition von Maßnahmen, auf der Hersteller und Zulieferer ihre Schnittstellen, geteilten Verantwortlichkeiten und Prozesse aufbauen können.

Mit der UN-Regulierung wird Cybersicherheit also zur Voraussetzung für die Wettbewerbsfähigkeit von OEMs und Zulieferern. Ein Schlüssel für eine erfolgreiche Digitalisierung wird sein, diese Vorgaben zu erfüllen und - bezogen auf die Unternehmensstrategie und Produkt-Roadmap - dafür den Ansatz mit der höchsten Wirksamkeit zu finden. Dabei ist aufgrund der Vernetzung der Fahrzeuge mit anderen Fahrzeugen, der Infrastruktur, sowie intelligenten Geräten und Diensten das komplette an Komplexität rasant zunehmende Ökosystem moderner Fahrzeuge einzubeziehen.

Wie andere Branchen wird auch die Automobilindustrie auf einen Ressourcenmangel blicken: Fachkräfte, die sowohl Cybersicherheit als auch die speziellen Anforderungen der Automobilbranche verstehen, sind rar. Dabei ist es aufgrund der Typzulassungsrelevanz kritisch, bereits im ersten Anlauf alle Anforderungen sicher und möglichst effizient umzusetzen. An dieser Stelle bieten etablierte Beratungsunternehmen wie ESCRYPT mit reichhaltiger Erfahrung in Cybersicherheit in der Automobilindustrie und KPMG als Experte für Informationssicherheit und Assessments passende Lösungen an, um Hersteller und Zulieferer erfolgreich durch die Entwicklung konformer Sicherheitsansätze zu leiten.

www.escrypt.com
https://home.kpmg/de/de/home/themen/overview/cyber-security

Hans-Peter Fischer,
Partner Cyber Security,
KPMG AG

Dr. Moritz Minzlaff,
Senior Manager,
ESCRYPT GmbH

„Fachkräfte, die sowohl Cybersicherheit als auch die speziellen Anforderungen der Automobilbranche verstehen, sind rar.“

escrypt SECURITY. TRUST. SUCCESS. | KPMG

Tschüss, alte Daten.

Sie können einstellen, ob und wie lange Ihre Suchanfragen gespeichert werden:
g.co/privatsphaeretools

Google

ADVERTORIAL

Fachkräftemangel – KEINE Frage der Digitalisierung

Daniela Schlegel ist Inhaberin von konzoom.de. Innerhalb ihrer Community betreut sie vor allem Kunden und Projekte rund um die Themen IT-Security und Datenschutz. Mit dem Fokus auf sicherheitsrelevante Infrastrukturen und deren Nutzen für die Gesellschaft folgt konzoom.de dem Prinzip einer humanistischen und sozialen Vision von New Work. Im Gespräch mit der Handelsblatt Journal Redaktion erläutert sie vor diesem Hintergrund, warum Digitalisierung, Fachkräfte und Gesellschaftsthemen zusammengehören.

Frau Schlegel, wie kommt es dazu, dass Sie sich mit dem Thema Fachkräftemangel auseinandersetzen?

Mir ist in meiner beruflichen Praxis immer wieder aufgefallen, dass hier bewusst oder unbewusst einiges durcheinandergebracht und dementsprechend auch falsch angegangen wird: Ein Fachkräftemangel ist gegeben, wenn der Bedarf an ausgebildeten Fachkräften das aktuelle Angebot überschreitet. Dem entgegengestellt ist der Arbeitskräftemangel, der weder die notwendige berufliche Qualifikation noch die formal beruflich Qualifizierten einbezieht. In unserem digitalen Zeitalter muss man aber nicht bedingungslos die Frage nach Fach- und Arbeitskräften auslösen, sondern eher die Frage beantworten können, wie das Arbeitsumfeld und die Berufsbilder neu definiert und ausgestaltet sein müssen. In erster Linie müssen sich Unternehmen und vor allem die Behörden die Frage gefallen lassen, warum sie keine modernen Arbeitsplatzstrukturen und Arbeitszeitmodelle schaffen.

Das heißt, Ihrer Auffassung nach gibt es gar keinen Fachkräftemangel?

Nein und mit dieser Auffassung bin ich wirklich nicht allein. Auch laut Bundesinstitut für Berufsbildung (BIBB) und der Fachkräfteengpassanalyse von der Bundesagentur für Arbeit gibt es nicht per se einen Flächenbrand. Schwierigkeiten in der Stellenbesetzung bestehen nur für einzelne Berufe/Berufsfelder, bestimmte Qualifikationen oder sind regional verortet. Zudem werden ganze Altersgruppen überhaupt nicht berücksichtigt. Die Generationen zwischen 45-67 werden viel zu oft übergegangen und auf deren Erfahrungsschatz fast vollständig verzichtet. Arbeitgeber nutzen vielmehr noch viel zu selten digitale Prozesse, zeitgemäße Kommunikationstechnologien und Arbeitsplatzmodelle, um Stellen zu besetzen. Mitarbeiter ab 45 und moderne Technologien ist absolut kein Widerspruch. Ganz im Gegenteil, die Lernbereitschaft ist zum Teil sogar größer, um mit Kindern und Enkelkindern auf Augenhöhe zu bleiben.

Warum aber ist das Thema dann Ihrer Meinung nach so präsent?

Der Teufel steckt bekanntlich im Detail und man muss sich die Entwicklung genau anschauen. Es gibt gesellschaftsrelevante Berufsbilder, die sich allein durch eine geringe Wertschätzung und Vergütung zum Fachkräftemangel entwickelt haben. Gesundheits- und Pflegeberufe, Erziehungs- und Ausbilderberufe oder auch Berufe in der Bau- und Landwirtschaft sind gesellschaftskritisch. Die mediale Darstellung, dass die Digitalisierung der Grund für den Fachkräftemangel ist, soll über die jahrlange Abwertung durch Politik und Wirtschaft hinwegtäuschen. Beispielhaft ist zudem, dass ausgerechnet diese akuten Beispiele überhaupt nicht auf digitale Arbeitsplatzstrukturen angewiesen sein sollten.

Gehen wir also davon aus, dass der Fachkräftemangel so (noch) nicht existiert. Wie würden Sie ihm vorbeugen?

Unternehmen und Behörden müssen die Digitalisierung als Fundament nutzen und neuen Arbeitszeitmodellen gegenüber offen sein. Wenn der Arbeitsplatz historisch wirkt, dann sollte Homeoffice das Minimum sein. Erfahrungsgemäß wird die Anwesenheit von acht Stunden immer noch höher bewertet als die erbrachte Leistung oder erbrachten Erfolge. Auch müssen Arbeitgeber ihre Vorreiterrolle ernster nehmen. Viele Mitarbeiter müssen sonst den Spagat zwischen alter und neuer Arbeitswelt meistern, was nicht nur zu Unter- oder Überforderung führt, sondern schlichtweg unnötig ist. Arbeitgeber in Deutschland müssen deutlich flexibler werden, wollen Sie ihre Fachkräfte behalten und binden. Das ist unternehmerische Führung und keine Frage von analogen oder digitalen Prozessen.

Auch der behördliche Verwaltungsapparat muss insgesamt vereinfacht werden, damit Unternehmen und Start-Ups flexibler und damit schneller reagieren können. Schließlich müssen Banken die Zinspolitik endlich an den Markt weitergeben, um Gelder für Investitionen und Start-Ups fließen zu lassen.

Was wünschen Sie sich für die Zukunft?

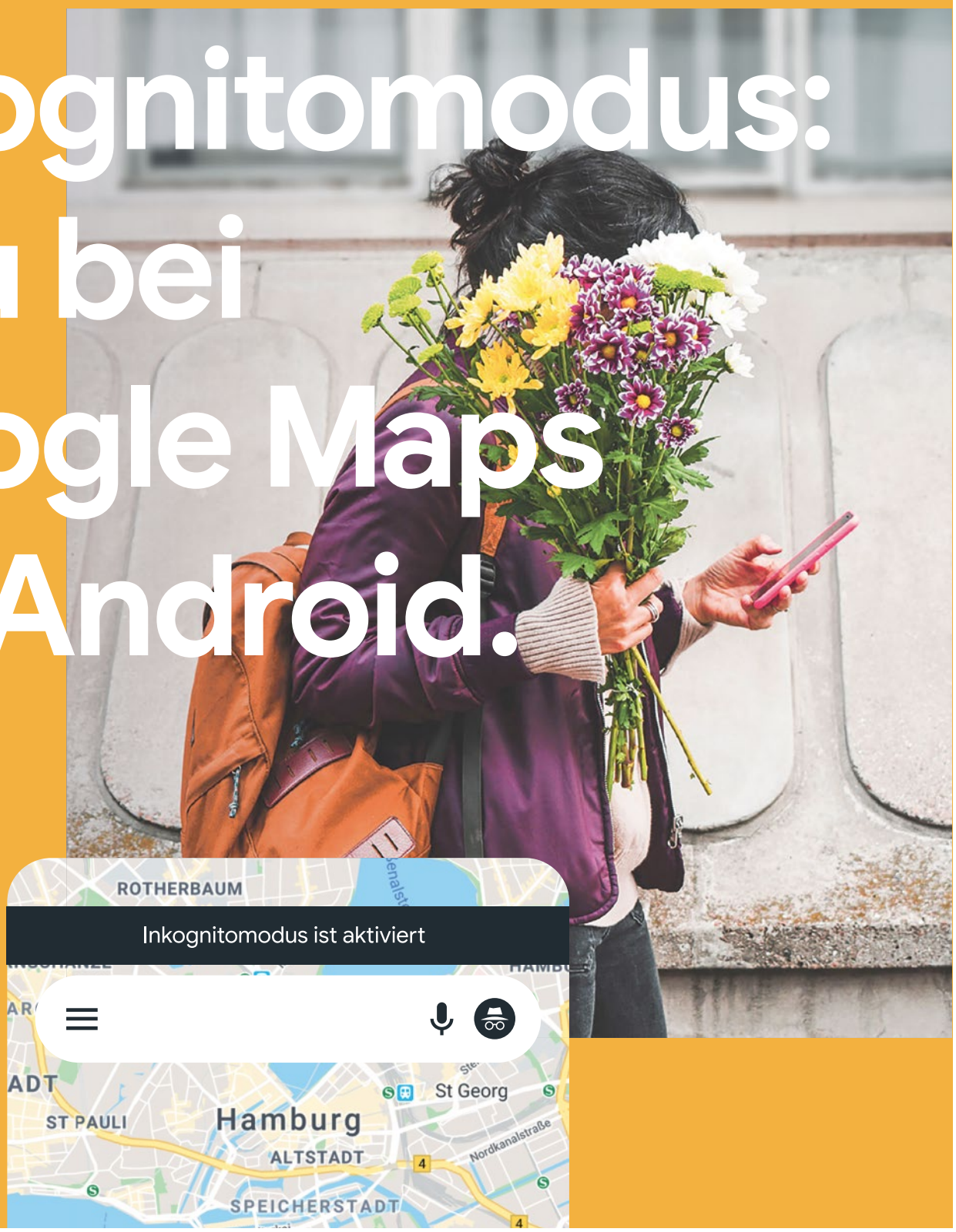
Ich wünsche mir bereits in der Gegenwart eine flexiblere und offenere Unternehmungskultur. Wieder mehr Zusammenarbeit an einem gemeinsamen, definierten Ziel. Und vor allem weg von Unternehmensführung via Excel. Prüfen Sie den Markt. Nutzen Sie digitale Methoden, um Ihre Mitarbeiter und sich selbst zu entlasten und weiterzuentwickeln. Schaffen Sie Raum für die eigentliche Wissensarbeit und für Kreativität. Mitarbeiter, die die Firma mitgestalten dürfen, binden sich und schaffen neue Potenziale. Fachkräfte eben! Speziell für die (sicherheitsrelevanten) Herausforderungen in der IT- und Digitalisierung sind motivierte Mitarbeiter der wesentliche und erste Garant für Sicherheit und Datenschutz.

www.konzoom.de


Daniela Schlegel

„Motivierte Mitarbeiter sind der wesentliche und erste Garant für Sicherheit und Datenschutz.“

Inkognitomodus: Neu bei Google Maps für Android.



Entdecken Sie weitere einfache Datenschutzeinstellungen bei Google:
g.co/privatsphaeretools

Google

Beauty is our business

phichak/shutterstock.com

Digitale Transformation mit hässlicher Software

von Prof. Dr. Sabine Radomski

Softwarequalität ist wie Schönheit. Stellen Sie sich vor: Sie fahren in einem autonomen Fahrzeug und ein Hacker übernimmt die Kontrolle, weil er die Immunschwäche der Software ausnutzen konnte. Viren, Würmer usw. befallen die IT Systeme. Eine Person mit Akne (einer Immunschwäche) sieht nicht gut aus. Leider ist die Immunschwäche der Software nicht so leicht sichtbar. Mit unserer Forschung wollen wir Softwarequalität sichtbar machen und Sicherheitsschwachstellen aufzeigen.

Wir müssen das Immunsystem der Software stärken, die Sicherheitsschwachstellen beseitigen. Um das zu erreichen, muss Qualität vom Nutzer wertgeschätzt werden. Software-Anwender müssen deshalb bei jeder Software auf Qualität achten. Aber das ist leichter gesagt als getan. Woran erkennt man sichere Software? Software-Qualität muss sichtbar werden: Wir brauchen einen TÜV für Software.

Ausgangssituation

Edsger W. Dijkstra sagte 1978 „Beauty is our Business, wenn wir uns klarmachen, dass der Kampf gegen Chaos, Durcheinander, und unbeherrschte Kompliziertheit eine der größten Herausforderungen der Informatik ist."

Täglich werden neue Sicherheitslücken in Sachen Software veröffentlicht: WannaCry, Stimmen- und Fotomanipulationen, Phishing-Attacken mit Office365, Nord VPN Server gehackt und Zugriff auf private Schlüssel. Die Liste lässt sich beliebig fortführen. Jeder hört und liest diese Schlagzeilen, aber nichts geschieht: Es wird weiter hauptsächlich kostenlose Software genutzt, einfache Passwörter verwendet, Sicherheitsupdates nicht eingespielt, unsichere Software an Kunden ausgeliefert etc.

Die fortschreitende Digitalisierung stellt hohe Anforderungen an die Qualität von Software. Aber technische Schulden werden im Projektablauf aufgenommen und nicht abgezahlt. Ein Teufelskreis, der, getrieben durch hohen Kostendruck, zu mangelhafter Software führt. Kunden sind an fehlerbehaftete Software gewöhnt und nicht mehr bereit, für Qualität tiefer in die Tasche zu greifen. Dieser Sparwahn öffnet dem Cybercrime Tür und Tor dank eines geschwächten Immunsystems der Software.

Im Jahr 2014 wurden laut HPI weltweit fast 6500 Sicherheitsschwachstellen in Software gemeldet. In 2017 waren es dann schon 15038 entdeckte Schwachstellen entsprechend CVSS (Common Vulnerability Scoring System). Für OpenSSL, eine Open Source Software zur Bereitstellung von verschlüsselten Netzwerkdiensten, wurden über 200 Sicherheitslücken gemeldet. Das ist positiv, denn jede gemeldete Sicherheitslücke kann behoben werden, ein schneller Release Wechsel bei OpenSSL zeigt das. Software von Microsoft, Apple, Google, Mozilla, Oracle, HP, Adobe etc. reiht sich mit kritischen Sicherheitslücken in die Statistik ein. Nicht berücksichtigt bleiben alle Sicherheitslücken, die existieren, aber nicht gemeldet werden.

KI als komplexe Software

Da Künstliche Intelligenz (KI) im Wesentlichen komplexe Software ist, treffen diese Aussagen auch auf KI zu: „KI könnte das schlimmste Ereignis der Menschheit werden", so warnte Stephen Hawking vor den potenziellen Gefahren der KI beim Web Summit 2017 in Lissabon. Denn besonders bei Systemen der Künstlichen Intelligenz sind die Folgen einer Manipulation nicht abzuschätzen. So gilt es nicht nur, die persönlichen Daten, sondern auch die KI vor Manipulation zu schützen. In der Digitalen Transformation werden „Dinge" intelligent, die Vernetzung von realer Welt und virtueller Welt lässt neue disruptive Geschäftsmodelle entstehen und fördert diese zugleich.

Dabei trägt KI bereits heute maßgeblich zur Wertschöpfung in vielen Branchen bei. Dieser Trend wird weiter anhalten und die bereits angesprochenen Risiken verstärken. Es ist nicht nur mit weiteren Cyberattacken zu rechnen, sondern einem Blackout der IT Systeme, der auf Grund der starken Abhängigkeit der Wirtschaft und Gesellschaft von funktionierenden IT Systemen einen Blackout des realen Lebens nach sich zieht.

Autonomes Fahren

Autonomes Fahren ist ein Beispiel für die Digitale Transformation. Teilautomatisiertes Fahren wie die Einparkhilfe oder den Tempomaten nutzen wir heute täglich. Aber bereits die Software der Klimaanlage kann mit einer Sicherheitslücke dazu führen, dass das gesamte Fahrzeug von außen gesteuert werden kann.[1]

Die Systeme des autonomen und automatisierten Fahrens sind sowohl von der Qualität der steuernden Software als auch von der Korrektheit der zu verarbeitenden Daten (Stauinformationen, Informationen über die Geschwindigkeit der Fahrzeuge, Wetter- und Routeninformationen) abhängig. Softwarefeh-

[1] https://www.wired.com/2015/07/hackers-remotely-kill-jeep-highway/.

ler und Manipulationen an den Daten oder der Software können zu Gefahrensituationen und zu Schäden führen. Deshalb ist insbesondere in diesen Systemen eine hohe Softwarequalität unbedingt notwendig. Für diese Schäden muss laut Produkthaftungsgesetz der Hersteller haften. Der Hersteller muss also im eigenen Interesse an einer hohen Qualität der Software interessiert sein.

Testen für die Digitale Transformation

Fassen wir noch einmal zusammen: KI wirkt heute zusammen mit Open Source Komponenten in einem IoT Netzwerk in Verbindung mit Big Data Informationen in einem Cloud Umfeld.

Vor diesem Hintergrund wird Software meist nur zu 30% getestet, uralte Software wird verwendet, die nicht mehr gepflegt wird, und Software ausgeliefert, bei der einfachste Entwicklungsregeln nicht berücksichtigt wurden.

Das führte uns zur Auffassung, dass der Software-Testprozess noch intensiver mittels Continuous Integration/Continuous Deployment (CI/DC) mit der Software-Entwicklung verknüpft werden muss, als es heute der Fall ist. Dazu wurde ein alt bekanntes Modell an die neuen Rahmenbedingungen angepasst. Das an der Hochschule für Telekommunikation Leipzig (HfTL) entwickelte V-Modell gibt der Testphase die notwendige Bedeutung und zeigt auch visuell, dass Testen 50% der Entwicklung umfasst. Alle V-Modelle zeigen einen linken produktiven und einen rechten destruktiven Entwicklungsbereich. Im rechten Bereich wird mit verschiedensten Methoden getestet, um Fehler so früh wie möglich zu erkennen, da durch eine zeitige Entdeckung Kosten gespart werden können.

Die ursprünglichen V-Modelle basieren auf einem Zeitverlauf von links nach rechts und nicht - wie in dem neuen V-Modell von oben nach unten. Das neue V-Modell ermöglicht so ein frühzeitiges Testen. Es integriert eine intensive anforderungsbezogene Überprüfung (kann diese Anforderung getestet werden?) mit einem in den Entwicklungsprozess integrierten Testen auf der Grundlage von CI/CD. Dabei wird auf eine hohe Automatisierung in jedem Prozessschritt geachtet. Testfälle werden automatisch ausgewählt und können durch weitere, neue Testfälle manuell ergänzt werden.

Ein derart getestetes System kann ein Gütesiegel/Sicherheitszertifikat erhalten, um die Qualität sichtbar zu machen. Nur so kann der Nutzer entscheiden, welche Software zum Einsatz kommen soll, und kann somit zur Verbesserung der Softwarequalität bewusst beitragen.

Haftung in der Digitalen Gesellschaft

Jeder Nutzer von Software kennt die AGBs, die vor Installation der Software bestätigt werden müssen. Es sind viele Seiten unverständlicher Nutzungsklauseln, die kaum jemand liest. Denn man hat keine Chance, der einen oder anderen Klausel zu widersprechen. Entweder, man stimmt zu oder verzichtet auf die Nutzung der Software. In einer Studie an der HfTL wurden 13 verschiedene Software-Produkte mit ihren Lizenzen untersucht und diese mit dem Produkthaftungsgesetz verglichen. Bei den Haftungsausschlüssen wurde in lediglich zwei der 13 Lizenzen darauf hingewiesen, dass der Hersteller in jedem Fall für grobe Fahrlässigkeit und Personenschäden haftet. Insbesondere wurde die Produkthaftung bei allen Open Source Lizenzen ausgeschlossen. Entsprechend der deutschen und europäischen Rechtsprechung ist ein solcher vollständiger Haftungsausschluss jedoch unwirksam, es gelten die gesetzlichen Haftungsvorschriften und die Entwickler-Community müsste für Personen- und Sachschäden haften.

Ebenso wurde bei elf der untersuchten Lizenzen versucht, entweder die Gewährleistung komplett auszuschließen, oder die dem Verbraucher zustehenden Gewährleistungsansprüche einzuschränken. Trotz AGB-Recht und Produkthaftungsgesetz ist es problematisch, dass die Hersteller nicht im Zugzwang stehen, ihre Lizenzbestimmungen vollständig an das vorliegende Recht anzupassen und somit Rechtsunsicherheiten zu vermeiden.

Fazit

Sind die Verbraucher wirklich durch die Gesetze vor Schäden durch Softwaremängel ausreichend geschützt? Oder werden diese Schäden wie Naturkatastrophen behandelt? Wann haben HP, Microsoft etc. je die Haftung für Datenverluste übernommen? Eine digitale Transformation mit unsicherer Software wird in einem realen Blackout enden.

Eine zusätzliche Kontrollinstitution/ein TÜV kann sowohl Sicherheitslücken aufdecken als auch mit einem Qualitätskennzeichen (BSI) für mehr Sicherheit in der IT sorgen. Wir haben dafür die neuesten Technologien kombiniert und weiterentwickelt, um ein Gütesiegel oder Qualitätskennzeichen zu definieren.

Wir alle haben es in der Hand - machen wir unsere Software schön: durch den Kauf von geprüfter, sicherer Software, mit einem Software TÜV, den Verzicht auf kostenlose Software.

Foto: Matthias Popp

Prof. Dr. Sabine Radomski (re.), Professorin im Fachbereich Nachrichtentechnik, Hochschule für Telekommunikation Leipzig

„Software-Qualität muss sichtbar und vom Nutzer geschätzt werden: Wir brauchen einen TÜV für Software.“

Sichere Authentifizierung

Identitätsschutz ist Grundrechtsschutz

Ein einfaches Passwort als Identitätsnachweis reicht in Zeiten zunehmender Digitalisierung nicht mehr aus. Anbieter von IT-Diensten müssen die Authentifizierung systematisieren und ihren Nutzerinnen und Nutzern wirksamere Lösungen zum Identitätsschutz anbieten.

Illu mit Material von : Irina Strelnikova/shutterstock.com | 300 librarians/shutterstock.com

von Barbara Thiel und Uwe Robra

Nutzerinnen und Nutzer von IT-Systemen und -Diensten haben ein großes Interesse daran, die eigenen Daten vor neugierigen Blicken unberechtigter Dritter zu schützen. Denn gerät die eigene Identität in falsche Hände, kann das schlimme Folgen haben – sowohl für die Nutzer selbst als auch für die Anbieter. Deshalb müssen verantwortungsbewusste Datenverarbeiter ein durchdachtes Konzept zur Authentifizierung anbieten. Dabei ist die Verunsicherung groß: Was ist nötig, um Informationen vor den zunehmenden Cyberangriffen mit potenziell großem Schaden zu schützen? Und wie lässt sich das Einfallstor für einen Identitätsdiebstahl wirksam schließen?

Benutzer erhalten heute je nach gewähltem Authentifizierungsverfahren einen oder mehrere Faktoren, um sich gegenüber dem System als zugriffsberechtigt ausweisen zu können. Zu diesen Faktoren zählen etwa ein persönliches Passwort, ein Token, eine PIN oder eine EC-Karte. Höherwertige Authentifizierungsmechanismen sind dabei klar gegenüber dem einfachen Zugriff über eine Zugangskennung mit Passwort zu bevorzugen.

Zugangskennung mit Kennwort oder PIN

Dieses einfache Verfahren stützt sich auf die ausschließliche Verwendung von Wissensfaktoren (also Faktoren, die nur der Nutzer kennt). Die Stärke eines Passwortes hängt dabei maßgeblich von seiner Länge und dem genutzten Zeichenvorrat ab. Allerdings beeinflusst die Länge eines Passworts seine Stärke wesentlich mehr als der Zeichenvorrat: Laut einer Veröffentlichung des US-amerikanischen National Institute of Standards and Technology von 2017 erzeugten viele der gängigen Empfehlungen (Groß- und Kleinschreibung, Sonderzeichen, häufiges Wechseln der Passwörter) nur wenig bis gar keine zusätzliche Sicherheit. Passwörter sollen nach der aktuellen Empfehlung mindestens 8 Zeichen lang sein, die Obergrenze sollte nicht unterhalb von 64 Zeichen liegen.

Aktuelle Verschlüsselungsverfahren sind technisch so weit fortgeschritten, dass sie in der Praxis – außer durch das Austesten aller möglichen Schlüssel, der sogenannten Brute-Force-Methode – meist nur durch einen Wörterbuchangriff geknackt werden. Das heißt, jedes Wort einer Wörterliste wird durch einen Algorithmus systematisch ausprobiert. Die Schwachstelle ist bei beiden Angriffen das vom Benutzer gewählte Passwort.

Bei Passwörtern für Benutzerkonten mit erweiterten Rechten, etwa für Administratoren, sollte man besonders großen Wert auf eine hohe Qualität legen, da das Schadenspotenzial eines Missbrauchs deutlich höher ist. Darüber hinaus ist es empfehlenswert, nicht personengebundene Administrationspasswörter zu notieren und in einem verschlossenen und ggf. zusätzlich versiegelten Umschlag in Tresoren oder Schließfächern zu verwahren. Bei sehr hohen Anforderungen an die Sicherheit sollten Nutzer die Aufteilung des Passworts erwägen, um einen berechtigten Zugang mit administrativen Rechten nur zwei Personen gemeinsam zu ermöglichen („Vier-Augen-Prinzip"); dann jedoch in Verbindung mit der noch zu betrachtenden Zwei-Faktor-Authentifizierung.

In der Praxis sind zunehmend so genannte Single-Sign-On-Lösungen (SSO) anzutreffen, bei denen sich der Benutzer zu Beginn seiner Tätigkeit einmalig am System oder einem SSO-Dienstleister anmeldet. Das System oder der Dienstleister handhabt dann selbstständig die weiteren Anmeldungen des Benutzers an einer Vielzahl von Anwendungen. Aufgrund des offensichtlichen Gefahrenpotenzials ist für solche Verfahren eine Zugriffskontrolle unzureichend, die ausschließlich auf der Angabe einer Nutzerkennung und eines Passwortes beruht. Hier muss eine Zwei- oder Mehr-Faktor-Authentifizierung die Identität eines berechtigten Nutzers sicherstellen.

Stand der Technik: Zwei-Faktor- und Multi-Faktor-Authentifizierung

In diesem Verfahren sind mindestens zwei unterschiedliche und vor allem unabhängige Komponenten (Faktoren) zur Authentifizierung nötig. Bei der Zwei-Faktor- (2FA) und Multi-Faktor-Authentifizierung (MFA) werden üblicherweise drei Kategorien von Faktoren unterschieden:

1. etwas, das nur der Nutzer kennt, z. B. Passwort, PIN oder TAN (Wissensfaktoren)

2. etwas, das nur im Besitz des Nutzers ist, z. B. Smartphone, Smartcard, Token oder andere Hardware-Schlüssel (Besitzfaktoren) und

3. ein biometrisches Merkmal, das einzig und allein dem Nutzer zugeordnet werden kann, und das untrennbar zu ihm gehört, z. B. der Scan des Fingerabdrucks oder der Netzhaut (biometrische Faktoren)

Im Alltag zum Einsatz kommt die 2FA etwa bei der Bankkarte am Geldautomaten: Erst die Kombination aus Karte und PIN ermöglicht die Transaktion. Bei der Auswahl von Faktoren für eine 2FA sollte man im Sinne der Sicherheit jeweils Faktoren aus zwei unterschiedlichen Kategorien kombinieren. Nur so lässt sich ein Missbrauch befriedigend einschränken.

So ist es bei der Wahl zweier Wissensfaktoren (wie z. B. PIN und TAN beim Onlinebanking) in der Vergangenheit mittels Social Engineering schon häufig zum Missbrauch gekommen.

Schwachstellen der Zwei-Faktor-Authentifizierung

Allerdings bietet auch die 2FA bei der Nutzung von Faktoren aus unterschiedlichen Kategorien keinen absoluten Schutz. Das gilt z. B., wenn beim Besitzfaktor eine technologische Schwachstelle zum Tragen kommt wie etwa der Magnetstreifen der EC-Karte. Kriminelle sind mittlerweile auch in der Lage, SIM-Karten zu klonen, um diese Authentifizierungsmethode zu überlisten. Bei einem sehr hohen kriminellen Interesse kann selbst ein Nachweiscode während eines Telefonats abgefangen werden, wenn ein Mobilfunknetz kompromittiert ist oder Täter auf die Portierung von Telefonnummern zurückgreifen, um Anrufe zu empfangen. Trotzdem bleibt hier der Aufwand zum Missbrauch immer noch höher als bei der Verwendung nur eines Faktors.

Um die größtmögliche Sicherheit bei der Authentifizierung sicherzustellen, ist neben einem Wissensfaktor ein weiterer nötig, der den physischen Besitz eines Gegenstandes (z. B. Smartphone, Smartcard, Transponder, Token oder andere Hardware-Schlüssel) oder eines biometrischen Merkmals nachweist. Das ist in diesem Bereich des Datenschutzes Stand der Technik.

Ansprüche an Authentifizierungsverfahren nach DSGVO

Die Datenschutz-Grundverordnung (DSGVO) verlangt vom Verantwortlichen vor Beginn eines Verarbeitungsprozesses eine Risikobewertung. Dafür sind typischerweise die Bedrohungsszenarien zu betrachten. Entscheidend für die Auswahl einer geeigneten Authentifizierung sind das Anwendungsszenario und die Analyse des darin enthaltenen Risikos.

Es ist also relevant, wozu das gewählte Verfahren dient:

- der Anmeldung an einem lokalen System (z.B. im LAN),
- der Nutzung externer Accounts (z.B. Mail oder Webseiten),
- der Zutritts- bzw. Zugriffskontrolle (z.B. Betreten von Räumen, Nutzung von Geldautomaten) oder
- dem Zugriff auf einzelne Dokumente, ZIP-Archive o.Ä.

Je nach Umgebung und Aufgabenstellung sind die Rahmenbedingungen für den Einsatz von Authentifizierungsverfahren recht unterschiedlich. Die Anforderungen an das Verfahren müssen deshalb an die jeweiligen Gegebenheiten angepasst werden. Bei Zugangskennungen ist es etwa wichtig, welche Schutzmaßnahmen gegen den Missbrauch eines Passwortes getroffen werden, besonders ob die Zahl der möglichen Fehleingaben wirkungsvoll beschränkt wird. Wird eine Kennung nach drei oder fünf Fehleingaben für einen längeren Zeitraum gesperrt oder gar ein zusätzliches Medium eingezogen, genügt ein kürzeres und weniger komplexes Passwort.

Wurde die Passwort-Strategie in einer Organisation an der Bedrohungslage und den möglichen Angriffsszenarien ausgerichtet, gibt es nur noch wenige Anlässe für einen Passwortwechsel. Dies ist dann nur noch bei der Erstkonfiguration nötig und wenn das Passwort ausgespäht oder weitergegeben wurde.

LfD Niedersachsen/Heike Göttert

Barbara Thiel, Die Landesbeauftragte für den Datenschutz (LfD) Niedersachsen

Art of Photo, Gehrden

Uwe Robra, Referatsleiter technisch-organisatorischer Datenschutz bei der LfD Niedersachsen

„Um die größtmögliche Sicherheit bei der Authentifizierung sicherzustellen, ist neben einem Wissensfaktor ein weiterer nötig, der den Besitz eines Gegenstandes oder eines biometrischen Merkmals nachweist.“

Die Landesbeauftragte für Datenschutz bietet Hilfestellung

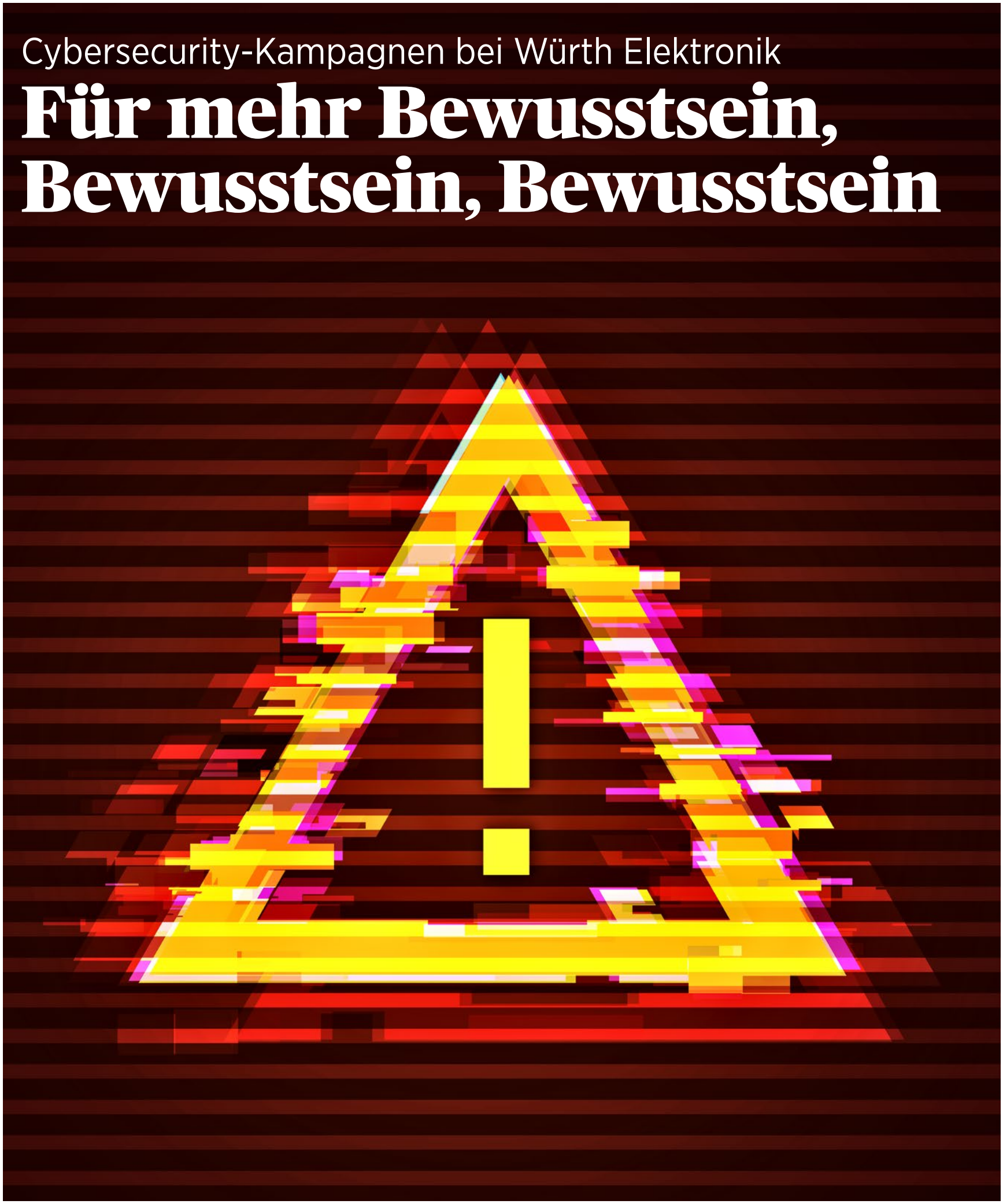
Wegen der grundlegenden Bedeutung des Schutzes vor unbefugtem Zugriff hat die LfD Niedersachsen in diesem Jahr eine aktuelle Handlungsempfehlung zur sicheren Authentifizierung veröffentlicht, die alle zentralen Anforderungen im Sinne der DSGVO beschreibt. Sie richtet sich an Nutzer, Verantwortliche und Dienstleister: **https://t1p.de/authentifizierung**

8 REGELN FÜR DEN EINSATZ VON ZUGANGSKENNUNGEN

1. Erkannte Gefahren sofort bannen
2. Passwort stets unbeobachtet eingeben
3. Vorab-Einstellungen (Default) sofort ändern
4. Für jeden spezifischen Zweck ein eigenes Passwort verwenden
5. Auch die Kennung (Nutzername) kann ein Geheimnis darstellen, wenn sie Wortfragmente beinhaltet, die auch in anderen Zusammenhängen bekannt sind (z.B. E-Mail-Adresse, Vor- und Zuname oder Organisationseinheit). Sie muss dann genauso wie das Passwort geheim gehalten werden.
6. Sichere Freigabe von gesperrten Zugangskennungen gewährleisten, das heißt, nur im Rahmen definierter Prozesse durch vertrauenswürdige Stellen
7. Passwortsammlungen nur in gesicherter Umgebung aufbewahren
8. Für Schicksalsschläge vorsorgen: Eine für den Notfall angelegte und sicher verwahrte Passwortliste und/oder die Aufnahme in das eigene Testament regeln bei Eintritt eines plötzlichen Todes- oder Pflegefalls das digitale Erbe.

Cybersecurity-Kampagnen bei Würth Elektronik

Für mehr Bewusstsein, Bewusstsein, Bewusstsein



SkillUp/shutterstock.com

Joachim Süpple, Head of IT der Würth Elektronik eiSos Gruppe

„Cybersicherheit ist ein bewegliches Ziel. Wer sich hier auf seinen Lorbeeren ausruht, hat bereits verloren.“

Viele sehen in Cybersecurity eine technische Aufgabe: IT-Systeme härten, Schwachstellen schließen, Angriffe erkennen und abwehren. Doch in der Kette der Sicherheitsmaßnahmen gibt es ein weiteres wichtiges Glied: Den Menschen. Und Menschen machen Fehler. Ein falscher Klick und der Angreifer hat Zugang zum Unternehmensnetz. Joachim Süpple, Head of IT der Würth Elektronik eiSos Gruppe, erläutert, wie sein Unternehmen bei Mitarbeitern und Mitarbeiterinnen Awareness für Cyberbedrohungen schafft.

Herr Süpple, Ihr Unternehmen hat eine differenzierte IT-Security-Strategie – fehlt den Mitarbeitern dafür das Bewusstsein?

IT-Lösungen, Hard- und Software, die uns vor Cyberangriffen schützen sollen, werden von unseren internen und externen Spezialisten nach bestem Wissen und Gewissen mit größter Sorgfalt eingerichtet. Angewandt werden die IT-Systeme jedoch von Kolleginnen und Kollegen überall in der Unternehmensorganisation. Folglich hängt die Sicherheit maßgeblich von jedem einzelnen Anwender ab. Wer seine IT-Security verbessern will, muss insbesondere für die Abwehr von Social-Engineering-Attacken immer an die ganze Systemkette denken – einschließlich der Schnittstellen zu allen Geschäftspartnern. Ein Schwachpunkt in dieser Kette reicht Angreifern bereits. Im täglichen „Kampf“ gegen die Angreifer brauchen wir die aktive Mithilfe aller Anwender. Als Verantwortliche dürfen wir das Thema IT-Security nicht in den IT-Teams abladen, sondern müssen alle Anwender aktiv einbinden und informieren. Awareness ist bei Würth Elektronik zentraler Bestandteil der IT-Security-Strategie.

Cybersicherheit hat ja wenig mit den Aufgaben der meisten Mitarbeiter zu tun. Wie kann es gelingen, das Bewusstsein für diese Themen zu wecken?

Das Gefahrenbewusstsein ist ein Schlüsselfaktor im Bereich der Cybersicherheit. Um Cybersecurity ins Bewusstsein zu bringen und dort zu halten, braucht es einen kontinuierlichen Prozess. Unsere diesjährige Kampagne „#weprotect“ zeigt das sehr gut. Wir haben zunächst definiert, welche Themenfelder wir aktuell und ganz konkret angehen wollen. Dieses Jahr machen wir plakativ und provokant auf vier Themen aufmerksam – und liefern dann fundierte Informationen und Anleitungen. Die Themen sind „Auf unternehmensfremde Personen achten“, „E-Mail-Sicherheit“, „Schutz von Unternehmensdaten“ und „Datenschutz/Schutz des eigenen Rechners“. Diese wurden dann jeweils zwei Monate lang intensiv mit Newslettern, Plakaten und Aufklebern immer wieder ins Bewusstsein gebracht. Aber ich warne: Diese Maßnahmen zu kopieren, wird nicht reichen. Awareness braucht individuell auf das Unternehmen und Mitarbeiter abgestimmte Strategien, kontinuierliche Maßnahmen, kritische Erfolgskontrolle und auch viel Engagement und beispielhaftes Vorleben bei Verantwortlichen und Managern.

Auf Fremde im Unternehmen zu achten, klingt nicht nach Cybersicherheit.

Könnte man meinen, aber für uns ist es ebenfalls ein Bestandteil der IT-Security-Strategie. Wenn jemand in öffentlich zugänglichen Bereichen eines Unternehmens – also etwa Kantine, Eingangsbereich, Parkplatz etc. – Dinge belauscht, kann ihm dies für einen Social-Engineering-Angriff mit einer Phishing-Mail die entscheidenden Informationen geben. Wir haben genau dieses Szenario bei der Auftaktveranstaltung spielerisch verdeutlicht, indem IT-Mitarbeiter, erkennbar an schwarzen Hüten, versuchten, möglichst viele Gespräche zu belauschen. Mitarbeitern und Mitarbeiterinnen sollte klar werden: Cybergefahren können auch analoge Einfallstore haben. Ein anderes Beispiel: Die Kampagne „Für Sie ist es Müll – für andere pures Gold“. Hier fordern wir zum sensiblen Umgang mit digitalen Datenträgern und Dokumenten auf – Papierlisten, USB-Sticks, Smartphones und vieles mehr. Sie alle können wertvolle Unternehmensdaten enthalten. Wer über Social Engineering unsere IT angreifen will, erhält so wertvolle Informationen zu Angriffspunkten.

Wie kommen Sie von diesem Bewusstmachen zu einem sachgemäßen Verhalten der Mitarbeiter? Informationen allein ändern Verhalten doch selten.

Das stimmt. Deshalb sind wir bereits am ersten Aktionstag ans Eingemachte gegangen. Da gab es Live-Hacking-Vorführungen und ein faszinierendes Interview mit einem Auftragshacker. Das Ausnutzen von Sicherheitsschwachstellen live zu erleben, beeindruckt und sensibilisiert Zuschauer nicht nur auf der rationalen Ebene. Die Vorführungen wurden gefilmt, um auch nicht anwesenden Kollegen und Kolleginnen Gelegenheit zum Gruseln zu geben. Viele im Team werden selbst zu Multiplikatoren, indem sie anderen das Video zeigen. Die Mitarbeiter müssen erleben, wie konkret die Gefahren sind und wie rasend schnell man als Einzelner und als Unternehmen zum Opfer wird. Dann folgten im Nachgang die Trainingseinheiten beispielsweise eine Präsenzschulung zum Social Engineering. Unser Ziel: Wir wollen ein Eigeninteresse, ja ein Grundbedürfnis an Datensicherheit wecken.

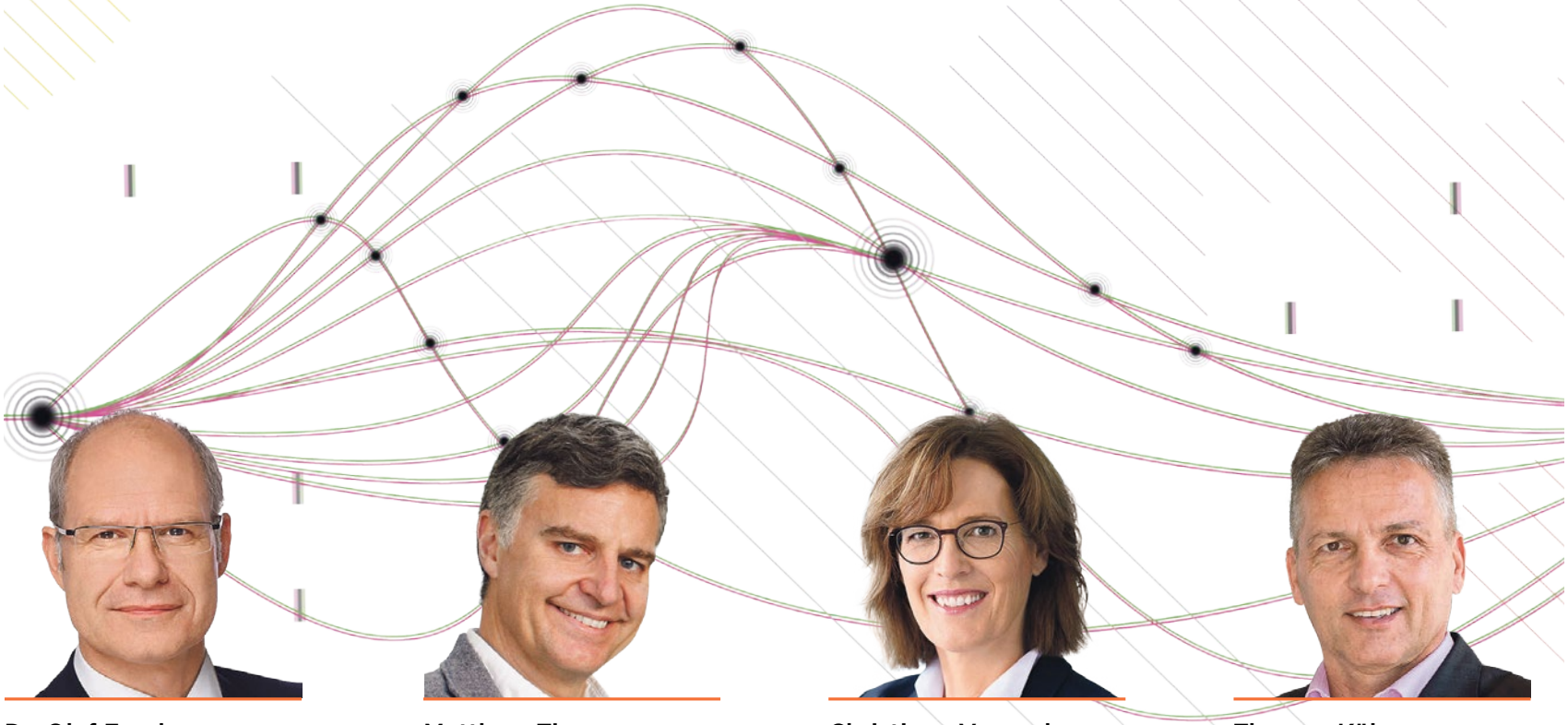
Wie bewerten Sie die Nachhaltigkeit des Awareness-Trainings?

Wir wollen dauerhaft Verhalten ändern, daher braucht es regelmäßige Auffrischung und Erfolgskontrolle. Um immer wieder an die Themen der Kampagne zu erinnern, haben wir vier Videos mit bekannten Kollegen als Darstellern gedreht. Und natürlich wird es weitere Aktionen und Trainings geben. Awareness-Training ist zentraler Teil unserer IT-Prozess-Optimierung und deshalb kontrollieren wir auch den Erfolg. Zunächst über die Auswertung von Teilnehmerzahlen und Klicks auf die Posts im Intranet. Zudem gibt es regelmäßige Phishing-Tests. Je geringer die Klickraten dann sind, desto erfolgreicher waren unsere Kampagnen. Aber wir wissen, dass unsere Arbeit im Bereich Awareness immer weitergehen muss, um es Angreifern so schwer wie irgend möglich zu machen. Cybersicherheit ist ein bewegliches Ziel – neue IT-Systeme werden eingeführt, Techniken und Strategien der Angreifer ändern sich, es kommen neue Standorte und Mitarbeiter hinzu. Wer sich hier auf seinen Lorbeeren ausruht, hat bereits verloren.

Handelsblatt Jahrestagung | 20. – 22. Januar 2020, München

Strategisches IT-Management

SCALING UP
Die nächste Welle intelligenter Digitalisierung



Dr. Olaf Frank
Head of Business Technology,
Munich Re

Matthew Timms
Chief Digital Officer,
E.ON

Christiane Vorspel
CIO, LBBW

Thomas Külpp
CIO Opel Automobile,
Opel Automobile GmbH

Jetzt anmelden: it-jahrestagung.de

Hauptpartner

Handelsblatt
Substanz entscheidet.