ManagerWISSEN

ANZEIGE

Ausgabe Mai 2020

Ad Special für die Gesamtausgabe manager magazin
www.manager-wissen.com

Cyber Security: Vertrauen durch Sicherheit für eine digitale Welt

Von Hans-Peter Fischer und Dr. Frank Damm

Dieses Special Manager WISSEN beschäftigt sich mit der besonderen Bedeutung des Vertrauens, das für eine erfolgreiche Digitalisierung erforderlich ist: Welche Bedeutung hat Cyber Security für das Vertrauen, wie kann Vertrauen erreicht werden und welche Herausforderungen begegnen uns dabei?

Unter dem Begriff Digitalisierung werden viele Entwicklungen zusammengefasst, die unseren Alltag und unser Berufsleben teilweise grundlegend verändern. Miniaturisierung macht einfache Gegenstände des Alltags zu kleinen Computern, die extrem große Mengen an Daten erzeugen; und die gestiegene Rechnerleistung ermöglicht es auch, diese systematisch auszuwerten. Robotics und KI ermöglichen es, immer mehr und komplexere Aufgaben zu automatisieren.

Viele Abläufe in der analogen Welt waren einfach, sichtbar und fanden in der physischen Gegenwart der beteiligten Personen statt, wie z. B. der Kauf von Büchern in der Buchhandlung im Tausch gegen Bargeld. Nun werden bei der Digitalisierung einzelne Schritte durch komplexe digitale Prozesse ersetzt, wie z. B. Online-Bestellungen oder kontaktloses Bezahlen. Beim Online-Kauf von Büchern sind Waren- und Geldströme nun nicht mehr sichtbar, einzelne Teile davon finden an mehreren und weit voneinander entfernten Orten statt (im Cyber Space) und sind für den Anwender im Detail nicht nachvollziehbar. Diese Problematik der geringeren Sichtbarkeit und Nachvollziehbarkeit bei höherer Kleinteiligkeit gilt umso mehr für Unternehmen, deren Datenströme und Schnittstellen, durch umfassende Integration von Kunden und Dienstleistern in die internen Abläufe, neue Komplexitäten und Abhängigkeiten schaffen, die für den Beteiligten nicht vollständig sichtbar und nachvollziehbar sind.

Bei diesen Abläufen entstehen neue Arten von Datenströmen und bisher unbekannte Mengen an Daten. Aber wenn selbst vermeintlich einfache Vorgänge, wie der Datenfluss beim Online-Bücherkauf, von den Anwendern nicht mehr nachvollzogen werden können – wie soll da eine gesellschaftsweite Akzeptanz der Digitalisierung geschaffen werden? Sollen alle diese neuen digitalen Prozesse erfolgreich in die verschiedenen Lebensbereiche integriert werden, so müssen die Nutzer trotz fehlender Nachvollziehbarkeit Vertrauen aufbauen. Doch was bedeutet Vertrauen, in welchem Zusammenhang steht Transparenz dazu – und wie erreicht man Vertrauen in der digitalen Welt?

Dies betrifft die meisten Lebensbereiche, und diese Entwicklung wird sich in den nächsten Jahren wahrscheinlich fortsetzen. Automatisierung am Arbeitsplatz, in der Produktion und in der Dienstleistung führt zu Arbeitserleichterungen und Beschleunigungen von Prozessen und gleichem Output bei weniger Ressourceneinsatz, was besonders in Zeiten des Fachkräftemangels ein entscheidendes Kriterium darstellt. Im Lebensbereich einer Privatperson werden z. B. die Finanzen online erledigt. In anderen Lebensbereichen wird die Mobilität digitalisiert wie z. B. beim autonomen Fahren.

Digitalisierung weckt Erwartungen an Funktionalität und Sicherheit

Digitalisierung ermöglicht und verspricht dem Benutzer neue Möglichkeiten, Verbesserungen und Vereinfachung. Sie wird dadurch von impliziten menschlichen Erwartungen begleitet. Diese betreffen

- die Funktionalität und Verfügbarkeit des Produktes an sich,
- den Schutz vor Nutzung und Beeinflussung durch Unbefugte,
- die Vertraulichkeit und Nutzung der neu entstehenden Daten.

Nimmt man das Beispiel eines autonomen Gabelstaplers in einem Logistiklager, wird natürlich die Funktionalität erwartet, dass dieser sich genauso gut wie ein analoger Gabelstapler im Lager bewegt, Paletten aus Lieferantenfahrzeugen holt und in Regale bringt. Darüber hinaus wird erwartet, dass Unbefugte den Gabelstapler nicht nutzen und beeinflussen können. Und es wird erwartet, dass die Daten, die hier neu entstehen, angemessen genutzt und vertraulich behandelt werden. Der Gabelstapler agiert eigenständig, erzeugt Daten und sendet diese an die Steuerzentrale des Lagers.

Digitalisierung kann nur dann erfolgreich sein, wenn sie ihr Versprechen einlöst und die drei oben genannten impliziten Erwartungen erfüllt, und zwar sowohl für die Anteile im analogen Raum als auch für die Anteile im Cyber Space. Daher müssen bei jedem Digitalisierungsvorhaben und bei jedem digitalen Produkt alle drei Erwartungshaltungen analog und im Cyber Space bedacht und bearbeitet werden.

Sicherheit wird eingebaut – Security by Design

In der analogen Welt werden bei Bedarf geeignete Sicherheitsmaßnahmen verwendet, wie z. B. Mauern, Stacheldrahtzäune, Videoüber-

Die Autoren

Hans-Peter Fischer *ist Partner im Bereich Cyber Security der KPMG AG Wirtschaftsprüfungsgesellschaft. Schwerpunkte seiner Tätigkeit sind Cyber Security in der Digitalisierung, Advanced Cyber Defense und die Entwicklung neuer Cyber-Security-Beratungsdienstleistungen für KPMG.*

Dr. Frank Damm *ist Senior Manager im Bereich Cyber Security bei KPMG mit langjähriger Erfahrung in Cyber Security in den Bereichen Finanzdienstleistungen, Automotive, Telekommunikation und Informationstechnologie.*
Internet: www.kpmg.de/
Telefon: 069 9587 0

Impressum
Verlag: Reif Verlag GmbH · Peter Reif · Alfred-Jost-Str.11
69124 Heidelberg · E-Mail: peter.reif@reifverlag.de

Redaktion: Christian Deutsch · Redaktionsbüro
Grabengasse 4 · 69117 Heidelberg
E-Mail: info@deutsch-werkstatt.de

Internet: www.manager-wissen.com
Layout: metropolmedia · 69245 Bammental
Druck: ColorDruck Solutions GmbH · 69181 Leimen

Vertrauensaufbau

Es gibt verschiedene vertrauensbildende Maßnahmen. Dazu gehören vor allem:

Direktes Nachvollziehen

- Der Nutzer ist unmittelbarer Teil einer Transaktion und sieht und kontrolliert alle Schritte selbst, zum Beispiel beim Tausch von Lebensmitteln gegen Bargeld im Supermarkt.
- Die Nutzer machen die praktische Erfahrung, dass nichts Kritisches passiert.

Sicherheitsmaßnahmen einsetzen wie z. B. Türschlösser

Indirektes oder transitives Nachvollziehen

- Prüfung der Sicherheit durch unabhängige Experten
- Information der Nutzer zur Sicherheit und zu Sicherheitsmaßnahmen durch Kommunikationsmaßnahmen.
- Nutzer verlassen sich auf Testberichte und Erfahrungen von anderen.
- Nutzer verlassen sich auf Freunde von Freunden oder noch weiter entfernten Personen, d. h. Aufbau eines Vertrauensnetzwerks.

Risikoabwälzung auf Dritte

- Versicherungen für den Schadenfall.

wachung und Vorhängeschlösser. In der digitalen Welt hingegen vollziehen sich zahlreiche wesentliche Schritte im Cyber Space – also anderswo, unsichtbar und automatisch. Es ist immer weniger erkennbar, ob Unbefugte dort zugreifen. Daher werden geeignete Sicherheitsmaßnahmen eingebaut, die unbefugte Zugriffe verhindern, z. B. eine Verschlüsselung der Daten und eine kryptographische Authentisierung einzelner Benutzer.

Der Nutzer muss vertrauen – Trust

Gleichzeitig können Unternehmen und Endbenutzer bei Produkten und Prozessschritten mit der Digitalisierung immer weniger sehen und überprüfen, ob ihre Erwartungen erfüllt werden, weil sie wesentliche Teile nicht nachvollziehen können. Sie haben dann nur die eine Möglichkeit: auf die Erfüllung der Erwartungen vertrauen, also der Sicherheit vertrauen.

In der analogen und in der digitalen Welt hängen Sicherheit und Vertrauen zusammen: Wenn die beteiligten Menschen zu wenig Vertrauen in die Sicherheit haben, steigt der Sicherheitsbedarf und zusätzliche Maßnahmen werden eingesetzt.

Cyber Security bedeutet Sicherheit im Cyber Space

Viele Teile der Produkte und der Prozessschritte in der digitalen Welt sind im Cyber Space, z. B. in kleinen und großen Computern, auf elektronischen Speichermedien, in Netzwerken und dem Internet. Dies sind solche Komponenten, deren Funktionsweise der Nutzer nicht nachvollziehen kann.

Ist die digitale Welt sicher, kann der Nutzer darauf vertrauen, dass die relevanten Erwartungen erfüllt werden. Die Cyber Security kümmert sich um die Sicherheit im Cyber Space und ist daher ein wesentlicher Erfolgsfaktor der digitalen Welt. Es ist eine logische Konsequenz zunehmender Digitalisierung, dass die Bedeutung und Sichtbarkeit von Cyber Security zunimmt.

Konkrete praktische Problemstellungen und Lösungsansätze

KPMG ist Wirtschaftsprüfer und damit ein wesentlicher Teil der vertrauensbildenden Maßnahmen in unserer Marktwirtschaft. KPMG unterliegt strengen Auflagen in Bezug auf Unabhängigkeit und Vertraulichkeit. Vertrauenswürdigkeit und Zuverlässigkeit sind zentrale Elemente unseres Handelns. Verbunden mit unserer fachlichen Expertise mit über 170 Cyber-Security-Experten in Deutschland und 3.000 Cyber-Security-Experten weltweit können wir die Sicherheit von digitalen Lösungen und die Wirksamkeit von digitalen Sicherheitsmaßnahmen bewerten. Damit können wir als „Trusted Advisor“ unseren Kunden die Zuversicht geben, sicher in die digitale Welt aufzubrechen und so unseren Beitrag zum Vertrauensnetzwerk beisteuern.

In den vier folgenden Artikeln wollen wir einige konkrete praktische Problemstellungen und Lösungsansätze zur Schaffung von Vertrauen durch Sicherheit näher betrachten. Dabei geht es um:

- Identitäts- und Zugriffsmanagement,
- sichere Fahrzeuge,
- Nervensysteme im Cyber Space
- und einfache Benutzbarkeit.

Identitäts- und Zugriffsmanagement

Der erste Artikel beschäftigt sich mit Identitäts- und Zugriffsmanagement. Cyber Security beginnt mit dem Zugangsschutz zu Daten und IT-Systemen. Es ist dabei von grundlegender Bedeutung, dass Zugriffsrechte auf den Personenkreis eingeschränkt sind, der diese Rechte für seine legitimen Tätigkeiten benötigt. Gleichzeitig müssen diese Benutzer bei veränderten Bedürfnissen schnell mit den entsprechenden neuen Zugriffsrechten ausgestattet werden, und die alten Zugriffsrechte müssen entzogen werden. Identity & Access-Management-Systeme (IAM) steuern hierfür zentral die Zugangsrechte in der gesamten Unternehmens-IT.

Sichere Fahrzeuge

Der zweite Artikel befasst sich mit den Herausforderungen von sicheren Fahrzeugen. Diese sind heutzutage „rollende IT-Systeme“. Im Fahrzeug gibt es dutzende Geräte mit einer IT-Funktionalität, die miteinander vernetzt sind. Das Fahrzeug ist mit dem Hersteller und mit der Außenwelt vernetzt, z. B. für Notrufe, Servicerufe und Updates der Fahrzeugsoftware. Sichere Fahrzeuge sorgen dafür, dass unbefugte Zugriffe in die Fahrzeug-IT nicht möglich sind und dass die im Fahrzeug entstehenden Daten vertraulich behandelt werden. Da es auch Safety-Anforderungen an die Sicherheit der Fahrzeuge im Cyber Space und des Cyber Space in den Fahrzeugen gibt, wird das nötige Vertrauen hier durch Standards und Zertifizierungen unterstützt.

Cyberabwehr als Nervensystem im Cyber Space

Das frühzeitige Erkennen von Angriffen auf die Systeme ist essenziell für Unternehmen, um Schaden abzuwenden. Dazu dienen Security Operations Center (SOC) oder auch Cyber Defence Center (CDC), welche als „Digitales Nervensystem“ Anomalien aufdecken und Angriffe schon frühzeitig verhindern können.

Einfache Benutzbarkeit von Sicherheitslösungen

Im abschließenden Artikel geht es um die Bedeutung der einfachen Benutzbarkeit (Usability) von Cyber Security u. a. am Beispiel der AusweisApp2 des Personalausweises.

Digitalisierung ist überall und verlegt Teile von Geschäftsabläufen und von Produkten in den Cyber Space. Quelle: KPMG in Deutschland, 2020

KI im IAM – intelligente Hilfe im Berechtigungsmanagement

Von Niels von der Hude

Identity Management ist ein wichtiger Baustein für die Informationssicherheit von Unternehmen. Die sichere Berechtigungsvergabe führt aber in den Fachabteilungen zu zusätzlichen Aufgaben. KI kann dabei helfen, die Verantwortlichen zu entlasten und Entscheidungen im Berechtigungsmanagement schneller und besser zu treffen.

Vom technischen Tool zum Unternehmensprozess

Das Verständnis eines „Berechtigungsmanagements" hat sich in den letzten Jahren sehr verändert: Die ursprüngliche Aufgabe bestand in der zentralen Administration von Zugangsrechten aller IT-Systeme. Heute unterstützt Identity & Access Management (IAM) die Abläufe der Unternehmen mit vielfältigen Diensten rund um die Berechtigungsvergabe. Dabei wurde die Verantwortung für die Vergabe von Zugriffsrechten von der IT-Administration in die Fachabteilungen verlagert. So entscheiden heute fachliche Vorgesetzte nicht nur in Antragsverfahren über die Berechtigungsvergabe. Sie müssen auch durch sogenannte Rezertifizierungen in ihrem Verantwortungsbereich prüfen und sicherstellen, dass Mitarbeiter nur die Rechte besitzen, die sie für ihre Tätigkeiten benötigen. IAM-Systeme wie GARANCY von Beta Systems bieten für diese Aufgaben browsergestützte Anwendungen, in denen den Verantwortlichen die Zugangsrechte zur Bestätigung bzw. Ablehnung benutzerfreundlich und verständlich präsentiert werden.

Vorgangsflut und Routine gefährden die Sorgfalt

Überprüfungsvorgänge und Antragsverfahren haben in der Praxis dabei einen Umfang erreicht, der im Arbeitsalltag der Mitarbeiter und speziell der Vorgesetzten einen merklichen Raum einnimmt. Erfahrungswerte bei größeren Unternehmen zeigen, dass 1.000 tägliche Berechtigungsprozesse in einem Unternehmen keine Seltenheit sind.

Die Menge dieser Vorgänge ist eine Herausforderung für die Unternehmen. Zum einen verringern diese Arbeiten die verfügbare Kapazität für fachliche Aufgaben. Andererseits besteht aber auch ein direkter Zusammenhang zwischen der Häufigkeit von Anträgen und einer nachlassenden Sorgfalt des Entscheiders: Auswertungen zeigen, dass Verantwortliche bei regelmäßigen Anfragen deutlich schneller und weniger kritisch entscheiden. Eine solche Bearbeitungsroutine verhindert aber die erforderliche kritische Genauigkeit in den Entscheidungen des Berechtigungsmanagements. IAM-Systeme von Beta Systems bieten daher schon seit einigen Jahren die Möglichkeit, Berechtigungen mit einer Kritikalität zu versehen: Durch die Anzeige des implizierten Risikos können Bearbeiter die Tragweite ihrer Entscheidung besser einschätzen.

Wie kann man erkennen, welche Entscheidungen die volle Aufmerksamkeit verlangen?

Um die Aufmerksamkeit der Entscheider besser zu steuern, wird eine Einschätzung benötigt, wie „relevant" die jeweilige Entscheidung tatsächlich ist. Diese Relevanz eines Berechtigungsvorgangs ist aber nicht nur von der Kritikalität abhängig. Beeinflusst wird die Relevanz auch vom Grad ihrer Ungewissheit. Zeigt die Historie vergleichbarer Vorgänge eine unklare Entscheidungstendenz, so ist eine erhöhte Sorgfalt des Entscheiders erforderlich.

Aber wie kann man „vergleichbare Vorgänge" erkennen? Die Vergleichbarkeit zeigt sich für den Menschen oftmals durch unbewusste Verknüpfung verschiedener Kriterien: Die Konstellation von Antragsteller und Entscheider wird mit den betroffenen Zugangsrechten und anderen Faktoren zu einer Aussage über die Vergleichbarkeit verbunden.

Über den Werdegang eines Mitarbeiters müssen seine Zugangsrechte kontinuierlich angepasst werden.

Hier bietet der Einsatz von KI-Systemen eine Chance, die Relevanz anstehender Berechtigungsentscheidungen mit höherer Präzision zu beurteilen. Durch das Erkennen und Auswerten vergangener vergleichbarer Vorgänge kann KI eine Einschätzung der Bestätigungswahrscheinlichkeit (des Konfidenzniveaus) ermitteln. Der (selbst-)lernende Charakter von KI-Systemen passt diese Einschätzung bei verändertem Entscheidungsverhalten im Nachlauf eigenständig an und wird mit jedem analysierten Entscheidungsverlauf präziser in seiner Expertise.

Niels von der Hude, Director Product Strategy IAM der Beta Systems Software AG

KI als Ersatz für menschliche Entscheidungen?

Diese Entscheidungswahrscheinlichkeit könnte in zukünftigen Generationen unserer IAM-Systeme dafür genutzt werden, um Vorgänge mit hoher Bestätigungswahrscheinlichkeit und geringer Kritikalität teilautomatisiert oder mit geringer(er) Häufigkeit durch menschliche Entscheider bestätigen zu lassen. Studien der KPMG zeigen ebenfalls derartige Optimierungsmöglichkeiten, die in einer besser gesteuerten Aufmerksamkeit und einem geringeren Zeiteinsatz der menschlichen Entscheider resultieren würden.

Beta Systems arbeitet zusätzlich daran, derartige KI-Konzepte auch in der Analyse von Berechtigungsdaten einzusetzen. So können nach ersten Versuchen gerade bei großen Datenmengen Abweichungen besser erkannt und dem menschlichen Entscheider vorverarbeitet zur weiteren Bewertung vorgelegt werden.

KI wird den Entscheidungsprozess im Identity Management nicht übernehmen. Durch den Einsatz von KI kann aber die wertvolle „Ressource Mensch" gezielter und effizienter eingesetzt werden. Eine größere Sicherheit in der Berechtigungsvergabe und eine höhere Akzeptanz von Identity Management Systemen kann so aus der Nutzung von KI in Zukunft entstehen.

Der Autor

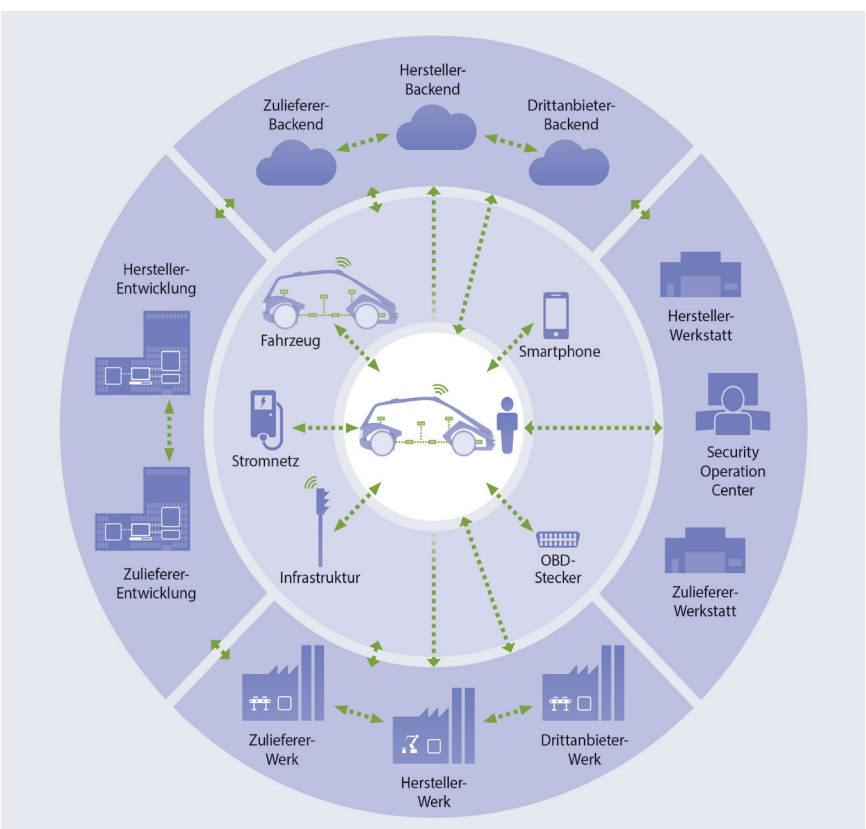
Niels von der Hude *ist Director Product Strategy IAM der Beta Systems Software AG. Als einer der maßgeblichen Experten des IAM-Marktes steuert er mit seinem Team die Produktausrichtung und -vermarktung des IAM-Portfolios. Die Beta Systems IAM Software AG aus Berlin ist der größte unabhängige europäische Anbieter von Identity- und Access-Management-Lösungen (IAM) für Unternehmen. Internet: www.betasystems-iam.com/de/ Telefon: 030 726 118 0*

Digitalisierung und UN-Regulierung: Cybersicherheit als kritischer Erfolgsfaktor in der Automobilbranche

Von Dr. Moritz Minzlaff und Jan Stölting

Durch zunehmende Digitalisierung und wachsende Zahl an veröffentlichten Hacks ist die Cybersicherheit von Fahrzeugen in den Fokus von Verbrauchern, Unternehmen und Regulatoren gelangt. In der Folge laufen weltweit Bestrebungen, Cybersicherheit zu regulieren und zu standardisieren, um Vertrauen und einen angemessenen Schutz zu erhalten. Die neuen Anforderungen stellen für die gesamte Branche einen Paradigmenwechsel dar: Die Typgenehmigung von Fahrzeugen wird künftig an die angemessene Implementierung eines Cyber Security-Managementsystems (CSMS) geknüpft sein. Damit wird die schnelle, risikoangepasste und konforme Umsetzung der Produktsicherheit zu einem zentralen Aspekt der Wettbewerbsfähigkeit von Herstellern und Zulieferern.

Die Anzahl und Reichweite möglicher Angriffsszenarien auf Fahrzeuge nimmt drastisch zu. Das Risiko nicht ausreichend geschützter Fahrzeuge für Hersteller, Besitzer und Verkehrsteilnehmer zeigt sich immer deutlicher. Ein wesentlicher Grund liegt in der wachsenden Angriffsfläche durch zunehmende Digitalisierung und Konnektivität der Fahrzeuge. Aufgrund der hohen Komplexität sowohl der Produkte als auch der Lieferkette im Automobilbereich müssen Cyberrisiken über den gesamten Lebenszyklus eines Fahrzeuges von Konzeption und Entwicklung bis zu Produktion und Betrieb sowie Cyber Security-Abhängigkeiten von Lieferanten und Dienstleistern betrachtet und fortlaufend behandelt werden.



Das komplexe Automobil-Ökosystem mit seinen vielen Beteiligten und Wechselwirkungen aus Security-Sicht.

Cybersicherheit im automobilen Ökosystem

Um das Vertrauen in die Cybersicherheit aufrechtzuerhalten, bedarf es einer genauen Analyse der Teilnehmer im automobilen Ökosystem und ihres jeweilig notwendigen Beitrags zu einem angemessenen Schutzlevel. Dieser Level muss durch technische und organisatorische Maßnahmen untermauert werden: Zum einen müssen in den Produkten selbst Vertrauensanker implementiert sein, bspw. Hardware Security Module oder Trusted Execution Environments; zum anderen kann über Audits und Zertifizierungen das Vertrauen in die Fähigkeiten der Zulieferer und Hersteller gestärkt werden.

Neue Vorgaben für Cybersicherheit von Fahrzeugen

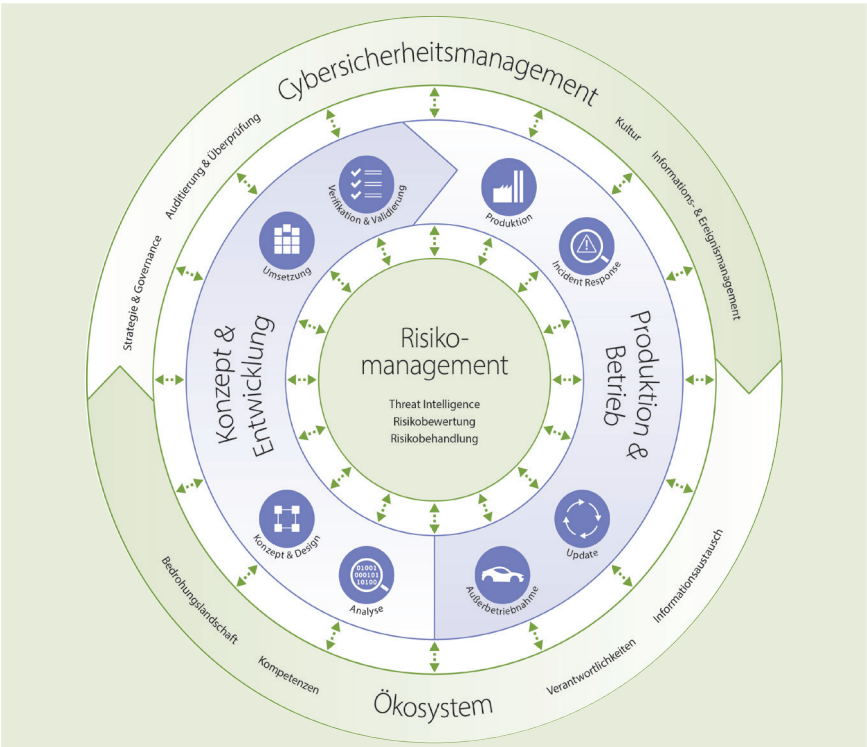
Weltweit laufen daher Bestrebungen, Cybersicherheit weiter zu regulieren, zu standardisieren und einen ganzheitlichen Ansatz im Umgang mit den entsprechenden Risiken zu fordern. So gibt es Gesetzesinitiativen in allen wesentlichen Märkten, von den USA über die EU bis hin zu China und Japan. In all diesen Regulierungen lassen sich drei wesentliche Trends erkennen:

- Eine stärkere Konkretisierung von Cybersicherheit auf Spezifika der Automobilindustrie,
- die Anforderung, die Sicherheit der Fahrzeuge im Feld aufrechtzuerhalten, sowie
- der zunehmend verpflichtende Charakter der Vorgaben und deren Überprüfung zum Zeitpunkt der Typgenehmigung.

Diese Trends manifestieren sich insbesondere in der aktuellen regulatorischen Initiative der UNECE WP.29 TF-CS/OTA und der kommenden Norm ISO/SAE 21434, die explizite Managementsysteme zum Schutz von Fahrzeugen definieren.

Im Spannungsfeld zwischen Zeitdruck und Ungewissheit

Die Automobilindustrie hat seit dem Jeep-Hack 2015 den Schutz von Fahrzeugen zwar verstärkt, mit der UN-Regulierung und dem neuen ISO/SAE-Standard jedoch wird Cybersicherheit über den unverbindlichen Status hinauswachsen und zur Voraussetzung für die Geschäfts- und Wettbewerbsfähigkeit von Herstellern und Zulieferern. Dabei bewegen sich die Unternehmen in einem Spannungsfeld zwischen dem Zeitdruck, die Anforderungen bis zur Typgenehmigung neuer Fahrzeugtypen ab 2022 umzusetzen, und der Ungewissheit, wie die finalen Vorgaben der Regulatoren für ein angemessenes CSMS im Detail aussehen werden. Die Norm ISO/SAE 21434 als wesentlicher Baustein und Orientierung für ein angemessenes Managementsystem zum Schutz von Fahrzeugen wird erst Ende 2020 in einer finalen Version vorliegen. Unternehmen



Ein CSMS umfasst klassische Domänen des Security-Managements (außen und innen) sowie Domänen mit Fokus auf den Produkten und ihren Anwendern (mittlerer Ring)

müssen aber spätestens jetzt ihre Maßnahmen zur ganzheitlichen Umsetzung eines CSMS starten, um den Nachweis der Anwendung im Rahmen der Typgenehmigung erbringen zu können. Das CSMS muss nicht nur implementiert, sondern gemäß dem Plan-Do-Check-Act (PDCA)-Zyklus eines Management-Systems auch operativ gelebt werden, zumal typische Entwicklungszyklen im Automobilbereich 3-5 Jahre betragen.

Zwar kann auf Erfahrungen mit Informationssicherheitsstandards wie der ISO 27000-Reihe zurückgegriffen werden, jedoch besteht die wesentliche Herausforderung bei der Ausgestaltung eines CSMS in der Berücksichtigung der Automobilspezifika. Zum einen sind Produkt und Lieferkette überaus komplex. Zum anderen unterliegt das Fahrzeug ganz spezifischen kritischen Aspekten wie etwa den Wechselwirkungen mit funktionaler Sicherheit, der Einhaltung von Umweltvorschriften und dem Diebstahlschutz.

Die Erfahrung aus anderen regulierten Branchen wie Energie, Pharma oder dem Finanzsektor zeigen zudem, dass es nicht nur gilt, die regulatorischen Anforderungen zu erfüllen, sondern diese sachgerecht zu interpretieren, um gemäß der eigenen Unternehmensstrategie einen optimalen, risikoorientierten Security-Ansatz mit der höchsten Wirksamkeit zu wählen. Der Ansatz sollte dazu führen, dass durchgängig für den Fahrzeugtyp, dessen externe Schnittstellen und dessen Subsysteme ein angemessenes Schutzniveau ermittelt, erreicht und erhalten werden kann.

Nachrüstung von Fahrzeugen

Ab 2024 soll die UN-Regulierung auch beim Neuverkauf von bereits vor 2022 zugelassenen Fahrzeugtypen greifen. Hersteller und Zulieferer müssen daher potenziell erneut in Komponenten und Systeme investieren und damit ihre Entwicklungsabteilung der Doppelbelastung aussetzen, sowohl die nächste Produktgeneration fristgerecht fertigzustellen als auch Legacy-Produkte bis 2024 ggf. nachzurüsten.

Daher ist es kritisch, die Balance zwischen tatsächlichem Sicherheitsgewinn und Wirtschaftlichkeit zu wahren. Eine technische Lückenanalyse der Fahrzeugarchitektur – vergleichbar mit einem internen Audit der Organisation auf Prozessebene – kann eine solide Entscheidungsgrundlage für diese Abwägungen schaffen.

Mit Erfahrung, Expertenwissen und eigenen Stärken zum Ziel

Umfangreiche Expertise aus der Managementsystem-Erfahrung, Compliance und Automotive Security muss zusammengeführt werden, um ein effektives CSMS aufzusetzen und die Typgenehmigungen zu meistern. Wie viele andere Branchen wird auch die Automobilindustrie auf einen Fachkräftemangel blicken: Experten sind rar, die sowohl Cybersicherheit als auch die speziellen Anforderungen der Automobilindustrie verstehen.

Gleichzeitig wachsen die Cyberrisiken aufgrund der Digitalisierung so rasant, dass das eigene Wissen der Unternehmen auf dem Gebiet der Cybersicherheit typischerweise nicht ausreicht, um alle Herausforderungen rechtzeitig und alleine zu bewältigen. Denn aufgrund der Typgenehmigungsrelevanz ist es dringend geboten, bereits im ersten Anlauf alle Anforderungen sicher und möglichst effizient umzusetzen. Bestandsaufnahmen schaffen hierfür eine Grundlage: Sie identifizieren vorhandene Bausteine, wie erprobte Prozesse im Bereich funktionaler Sicherheit oder bestehende Managementsysteme. Daraus lassen sich auf die individuelle Situation des Unternehmens passgenaue Umsetzungspläne ableiten.

Angesichts der komplexen Aufgabenstellung ist es ratsam, auf die Hilfestellung externer Cybersicherheitsexperten zurückzugreifen. Fahrzeughersteller und Zulieferer benötigen Security-Partner, die einerseits spezielle Erfahrung darin haben, Cybersicherheit in der Automobilindustrie von der Konzeption bis hin zur Serienreife zu führen und anschließend im Betrieb das gewünschte Sicherheitsniveau aufrechtzuerhalten, und andererseits große Fachkenntnis im Assessment und dem Ausrollen von Sicherheitsmanagementsystemen mitbringen. Eine derartige Symbiose komplementärer Expertise ermöglicht es, die – im Sinne eines holistischen Ansatzes – notwendigen Änderungen auf der Organisations- und Prozessebene so zu gestalten, dass Auswirkungen auf die Entwicklung und den wirtschaftlichen und effektiven Betrieb der Sicherheitslösungen berücksichtigt und optimiert sind. Erfahrung im Aufbau von Managementsystemen, Expertenwissen zu Automotive Security und eigene Stärken sind die wesentlichen Faktoren erfolgreicher Cybersicherheits-Programme.

Die Autoren

Dr. Moritz Minzlaff *ist Senior Manager bei der ESCRYPT GmbH. Er hat über zehn Jahre Erfahrung im Bereich Cyber Security und berät dazu Automobilunternehmen weltweit, von spezialisierten Zulieferern und Herstellern bis hin zu den Top 5 OEMs. Bei ESCRYPT trägt er die Gesamtverantwortung für die Beratungsdienstleistungen zu Cyber Security-Managementsystemen. Internet: www.escrypt.com/, Telefon: 0234 43870 200*

Jan Stölting *ist Senior Manager bei der KPMG AG Wirtschaftsprüfungsgesellschaft. Er hat über zehn Jahre Erfahrung in der Beratung im Bereich Cyber Security und insbesondere der Steuerung von großen Security-Transformationsprojekten und berät u.a. große OEMs und Zulieferer der Automobilbranche. Internet: www.kpmg.de/, Telefon: 069 9587 0*

Cyberabwehr – die letzte Verteidigungslinie gegen Hacker

Von Dr. Karl-Friedrich Thier

IT-Systeme gegen jeden Cyberangriff vollständig abzusichern ist heute nicht mehr möglich. Um das Vertrauen in digitale Technologien und Prozesse zu erhalten, wird es daher immer wichtiger, dass Unternehmen Angriffe auf ihre Systeme rechtzeitig erkennen und aktiv abwehren können. Wie eine schlagkräftige Cyberabwehr funktioniert, zeigen Beispiele aus der ITK-Branche.

Dr. Karl-Friedrich Thier ist Principal Consultant für Cyber Defense Management bei Telekom Security, der Security-Einheit von T-Systems und der Deutschen Telekom

19. Dezember 2019: Die Website der Stadt Frankfurt ist offline, Ämter werden geschlossen, Bibliotheken leihen keine Bücher mehr aus. Der Grund: Ein Mitarbeiter eines Bürgeramts hat einen E-Mail-Anhang mit der gefährlichen Malware Emotet geöffnet und seinen Rechner infiziert. Zum Glück schlägt die Antivirensoftware Alarm – und das IT-Team der Stadt reagiert schnell. Die Spezialisten fahren vorübergehend alle Systeme herunter und verhindern so Schlimmeres.

Emotet ist nur ein Beispiel für die immer ausgefeilteren Angriffsmethoden von Cyberkriminellen. Die Zahl der Cyberangriffe nimmt zudem stetig zu. So verzeichnete die Deutsche Telekom im Januar 2020 fast 18-mal so viele bösartige Zugriffe auf ihre Infrastruktur wie noch im Frühjahr 2017. Laut Digitalverband Bitkom[1] verursachten Hacker in der deutschen Wirtschaft einen Schaden von 100 Milliarden Euro pro Jahr. Entsprechend wählten die Teilnehmer einer Umfrage des Versicherungskonzerns Allianz Cybervorfälle zum größten Unternehmensrisiko für 2020[2].

Die Spur des Hackers

Fortgeschrittene und komplexe Cyberangriffe bestehen üblicherweise aus mehreren aufeinanderfolgenden Phasen, die von Experten als „Cyber Kill Chain" bezeichnet werden:

- Reconnaissance: Der Angreifer sammelt Informationen über sein Ziel.
- Attack Delivery: Der Hacker übermittelt Schadsoftware, etwa über bösartige Mails.
- Exploit & Install: Die Schadsoftware wird ausgeführt – etwa durch Klick auf einen Mailanhang – und installiert.
- Command & Control: Der Angreifer steuert die Schadsoftware über einen Server von außen.
- Local Compromize: Der Hacker erweitert seine Fähigkeiten im internen Netz, zum Beispiel indem er Zugangsdaten ausspäht oder weitere Schadsoftware installiert.
- Internal Reconnaissance: Dank seiner neuen Fähigkeiten kundschaftet der Gegner die interne IT aus.
- Lateral Movement: Nun kann der Eindringling weitere Systeme infizieren und kompromittieren.
- Actions & Exfiltration: Erst jetzt erreicht der Hacker sein eigentliches Ziel: Er spioniert zum Beispiel Geschäftsdaten aus oder zerstört kritische Systeme.

Einsatzzentrale gegen Eindringlinge

Die große Herausforderung für Unternehmen, Behörden und andere Organisationen: Sie müssen jedes ihrer Systeme und Netze zu jedem Zeitpunkt sorgfältig sichern. Ein Hacker braucht dagegen nur eine einzige temporäre Schwachstelle. Aus diesem Grund reichen vorbeugende Sicherheitsmaßnahmen wie Firewalls und Virenscanner schon lange nicht mehr aus. Sie können zum Beispiel durch eine Phishing-Mail leicht umgangen werden. Unternehmen müssen daher eine Cyberabwehr aufbauen, um Hackerangriffe frühzeitig zu erkennen und schnell und effizient abzuwehren.

Firewalls oder Virenscanner reichen nicht mehr aus.

Die IT- und Kommunikationsbranche betreibt seit vielen Jahren Security Operations Center (SOC) oder Cyber Defense Center (CDC), die diese Aufgabe wahrnehmen: Die Telekom Security zum Beispiel verfügt über eines der größten und modernsten Cyberabwehrzentren in Europa. Rund um die Uhr überwachen hier circa 200 Experten die Sicherheit der Systeme der Telekom und ihrer Kunden. Pro Tag analysiert das Zentrum etwa 2,5 Milliarden Hinweise auf mögliche Sicherheitsvorfälle. Ziel ist es, einen Angriff zu erkennen und abzuwehren, bevor ein nennenswerter Schaden entstanden ist. Die Detektion und Abwehr gliedern sich in drei Schritte: Datenbasis herstellen, Datenanalyse und Vorfallerkennung, Angreifer abwehren.

Schritt 1: Datenbasis herstellen

Eine effektive Cyberabwehr nutzt zwei unterschiedliche Datentypen: relevante Event-Daten aus den IT-Systemen und Sensoren des Unternehmens sowie Kontextinformation aus externen Quellen. Erstere stammen zum Beispiel aus Sicherheitssystemen wie Antiviren-Systemen oder Firewalls, aber auch aus den Protokolldaten von Applikationen und Server-Betriebssystemen. Hinzu kommen spezielle Sensoren, die zum Beispiel Auffälligkeiten im Datenverkehr des Firmennetzes erkennen können.

Ist ein bestimmtes Ereignis auf einen Security-Vorfall zurückzuführen? Um das zu klären, braucht es Kontextinformationen aus der sogenannten Threat Intelligence. Security-Dienstleister, Forschungseinrichtungen, Behörden oder andere Cyberabwehrzentren erheben und teilen diese Art von Daten, um ihre Gegner besser zu verstehen. Die Informationen beinhalten zum einen Erkenntnisse aus der Analyse vergangener Angriffe und der dabei eingesetzten Schadsoftware. Zum anderen behalten Experten stets einschlägige Internetforen und soziale Medien im Blick. Dort tauschen sich Hacker oft über neuentdeckte Schwachstellen und Angriffsmethoden aus. Entsprechende Chats lassen sich über Schlagwörter wie „Exploit" identifizieren.

Schritt 2: Datenanalyse und Vorfallerkennung

Die Datenbasis für die Angriffsdetektion ist meist extrem groß und heterogen. Eine Echtzeitanalyse ist daher nur möglich, wenn die Daten automatisiert verarbeitet und korreliert werden. Dafür kommen sogenannte Security Information and Event Management (SIEM) Systeme zum Einsatz. Anhand des typischen Ablaufs eines Angriffs (siehe Kasten) und der Threat-Intelligence-Informationen modellieren Sicherheitsexperten Angriffe, leiten Indizien für bestimmte Detektionsszenarien ab und übersetzen diese in Algorithmen für das SIEM-System.

Ein Cyberabwehrzentrum überwacht ständig die IT und Netze von Organisationen und wehrt Angriffe ab.

Ein Beispiel: Erreichen das Unternehmen vermehrt Mails mit unbekannten oder ausführbaren Dateianhängen und erfolgt zeitnah der Aufbau einer Kommunikation ins Internet, besteht eine hohe Wahrscheinlichkeit für einen digitalen Einbruch. Das Analysesystem gibt sofort einen Alarm aus.

Nicht bei jedem Alarm handelt es sich um einen kritischen Sicherheitsvorfall. Ein Team von Security-Analysten steht daher rund um die Uhr bereit, um die Alarme zu verifizieren und anhand ihrer Priorität zu bearbeiten. Ein Level-1-Analyst filtert zunächst Fehlalarme heraus und leitet bei bestätigten Vorfällen Sofortmaßnahmen ein. In unklaren Fällen übergibt er an Level-2- oder Level-3-Spezialisten. Diese führen weitere Analysen durch – in der Regel in enger Abstimmung mit dem IT-Betrieb.

Schritt 3: Angreifer abwehren

Ist der Angriff einmal erkannt, geht es darum, möglichst schnell und effektiv zu reagieren. Incident-Response-Experten stehen in dieser Phase der IT-Organisation zur Seite, um angemessene Maßnahmen zur Eindämmung und Beseitigung eines Angriffs einzuleiten und potenziell ausgefallene IT-Systeme wiederherzustellen. Bei besonders schwierigen oder kritischen Fällen hilft ein IT-Forensiker. Dieser digitale Detektiv versucht herauszufinden, wie ein Hacker vorgegangen ist, und sichert Beweise.

Eigenbetrieb oft zu teuer

Eine erfolgreiche Cyberabwehr benötigt also effektive Detektions- und Analysetools, ein rund um die Uhr verfügbares, qualifiziertes Expertenteam und den kontinuierlichen Informationsaustausch mit anderen Akteuren eines Security-Ökosystems. Daher ist für viele Unternehmen der Aufbau und Betrieb eines eigenen Cyberabwehrzentrum zu komplex und zu teuer. Als Alternative lassen sich einzelne Aufgaben – zum Beispiel die Level-1- und Level-2-Analyse – oder auch die gesamte Detektion und Unterstützung bei der Vorfallbehebung auslagern.

Für viele Unternehmen sind Aufbau und Betrieb eines eigenen Cyberabwehrzentrums zu komplex und zu teuer.

Telekom Security hilft Unternehmen dabei, eine für sie passende Cyber-Defense-Strategie zu entwickeln und umzusetzen. Die Telekom schöpft dazu wertvolles Wissen aus der Cyberabwehr für ihre eigene Infrastruktur und viele andere Kunden sowie aus den vielfältigen Kontakten zu Behörden und anderen Netzbetreibern. Jeder Kunde profitiert unmittelbar von diesem Netzwerk, das durch jedes neue Mitglied noch stärker wird.

Nachholbedarf im Mittelstand

Der Finanzsektor sowie viele große Unternehmen anderer Branchen haben bereits erfolgreich Cyberabwehrzentren installiert oder sind dabei, diese aufzubauen. Besondere Anforderungen gelten dabei für Betreiber kritischer Infrastrukturen wie Telekommunikation oder Energieversorgung, die auch ihre Anlagen vor Angriffen schützen müssen. Auch für den Automobilbereich gibt es bereits branchenspezifische Lösungen[3]. Anders bei kleinen oder mittleren Unternehmen: Trotz ausreichend verwertbarer Daten fehlt vielfach eine automatisierte Datenanalyse sowie ausreichend Personal zur Behandlung der Alarme.

Wir empfehlen Unternehmen jeder Größe und Branche eine angepasste Angriffsdetektion und -abwehr. Nur so können Unternehmen, Mitarbeiter und Kunden den Weg in die Digitalisierung sicher und vertrauensvoll beschreiten.

Quellen:
1 Bitkom, „Angriffsziel deutsche Wirtschaft: mehr als 100 Milliarden Euro Schaden pro Jahr", November 2019, https://www.bitkom.org/Presse/Presseinformation/Angriffsziel-deutsche-Wirtschaft-mehr-als-100-Milliarden-Euro-Schaden-pro-Jahr
2 Allianz, „Allianz Risk Barometer", Januar 2020
3 T-Systems, „Cyberabwehr für das vernetzte Fahrzeug", 2018, https://www.t-systems.com/de/de/whitepaper-download/cyberabwehr-fuer-das-vernetzte-fahrzeug-10560

Der Autor
Dr. Karl-Friedrich Thier *ist Principal Consultant für Cyber Defense Management bei Telekom Security, der Security-Einheit von T-Systems und der Deutschen Telekom. In dieser Funktion berät er Unternehmen aus allen Branchen beim Auf- und Ausbau ihrer Cyberabwehr-Fähigkeiten. Internet: www.t-systems.com/de/de/security, Telefon: 00800 33 09030*

Sicherheitslösungen müssen benutzbar sein

Von Prof. Dr. Andreas Heinemann

Die voranschreitende Digitalisierung lässt den Kreis potentieller Nutzer kontinuierlich wachsen. Damit müssen IT-Sicherheitslösungen auch bedienbar sein für Menschen ohne Affinität zur Technik. Hier sind interdisziplinäres Arbeiten und eine nutzerzentrierte Sichtweise auf die Cyber Security gefragt.

IT-Anwender setzen die ihnen zur Verfügung stehende Hard- und Software für die Erfüllung ihrer jeweiligen Aufgaben ein und verfolgen damit unterschiedlichste Ziele. So sind Computer ein Hilfsmittel der Kommunikation, der Interaktion und Koordination, sie dienen der Informationsbeschaffung und bilden die Basis für Geschäftsprozesse.

Aus Sicht eines Anwenders sind die Cyber Security und die damit verbundenen Ziele[1] wie Vertraulichkeit, Integrität oder Verfügbarkeit kein primäres Ziel ihres Handelns, sondern nachgelagert. Oft fühlen sich die Anwender durch die IT-Sicherheitsziele und die damit verbundenen Maßnahmen bevormundet und bei ihrer täglichen Arbeit behindert. Bereits 1999 haben Adams und Sasse[2] im Kontext von Passwort-Richtlinien gefordert, den Nutzer nicht als „Feind" zu betrachten, sondern als *first line of defense* eines Unternehmens.

Mit der weiter zunehmenden Digitalisierung aller Lebensbereiche ist es daher immens wichtig, den IT-Anwender ins Zentrum der Betrachtung zu stellen. Hier setzt das Forschungsfeld der „Benutzbaren Sicherheit" an. Anhand der eID-Funktion des Personalausweises soll skizziert werden, wie eine nutzerzentrierte Betrachtung das Vertrauen in und damit die Akzeptanz von IT-Sicherheitsfunktionen stärkt. Mit Handlungsempfehlungen schließt dieser Beitrag.

Forschungsfeld „Benutzbare Sicherheit"

Die Benutzbarkeit von IT-Systemen mit Sicherheitsfunktionen lässt sich verbessern, indem man den Nutzer in das Zentrum der Betrachtungen rückt und insbesondere seine Kenntnisse und Fähigkeiten zu verstehen sucht. Zurko und Simon haben hierfür den Begriff *User-Centered Security* geprägt und schlagen u.a. vor, Usability-Tests früh bei der Neu- oder Weiterentwicklung von IT-Systemen mit Sicherheitsfunktionen durchzuführen. Nur so können spätere potentielle Bedienfehler, die ein Cyber Security-Risiko bedeuten, frühzeitig durch die angedachten zukünftigen Nutzer erkannt werden.

Neben dem Anwender rücken in letzter Zeit auch Systemadministratoren und Softwareentwickler ins Zentrum des Interesses der Forschung, da z. B. Usability-Probleme bei der Administration von Firewalls oder der unsachgemäße Einsatz von Programmbibliotheken ein Sicherheitsrisiko für IT-Anwendungen und damit letztendlich für Unternehmen darstellen.

Die eID-Funktion des Personalausweises

Der deutsche Personalausweis bietet mit der eID-Funktion die Möglichkeit für seinen Besitzer, sich gegenüber einem sogenannten Diensteanbieter auszuweisen[3]. So ist es bspw. für einen Bürger möglich, online ein Führungszeugnis zu beantragen. Die Technik der eID-Funktion des Personalausweises ist im Vergleich zu anderen Verfahren sehr sicher gestaltet. So muss man einen Personalausweis besitzen und seine sogenannte eID-PIN kennen. Die eID-Funktion stellt also von jeher eine Zwei-Faktor-Authentisierung (bestehend aus Wissen und Besitz) dar.

Für die erfolgreiche Nutzung der eID-Funktion müssen jedoch eine Reihe von Voraussetzungen gegeben sein: Die eID-Funktion muss aktiviert sein, der Bürger muss seine eID-PIN gesetzt haben und kennen, auf dem Rechner muss eine spezielle Softwarekomponente (heute die AusweisApp2) eingerichtet sein und der Nutzer benötig einen Kartenleser[4], damit die Daten überhaupt ausgelesen werden können. Es handelt sich somit um ein recht komplexes Setting für den digitalen Identitätsnachweis über das Internet. Herausfordernd kommt hinzu, dass potentiell alle Bürger, also auch Personengruppen ohne tieferes Verständnis von Technik und Cyber Security, die eID-Funktion nutzen möchten.

Vor diesem Hintergrund und bekannter Usability-Schwächen der ersten AusweisApp hat das Bundesministerium des Innern (BMI) die Neuentwicklung der AusweisApp in Auftrag gegeben. In diesem Zuge sollte insbesondere die Benutzbarkeit verbessert werden. Es hat sich gezeigt, dass es zuträglich ist, frühzeitig den Anwender zu betrachten und entwicklungsbegleitend Usability-Tests durchzuführen. So fiel auf, dass Nutzer des macOS-Betriebssystems i. d. R. nicht damit vertraut sind, Gerätetreiber für Kartenleser eigenhändig zu installieren und bereits Probleme hatten, den Kartenleser in Betrieb zu nehmen, während Nutzer des Windows-Betriebssystems dies nicht als Herausforderung wahrnahmen. Weiter wurden in Anlehnung an die von Patrick et al. formulierten Richtlinien zur Steigerung des Vertrauens des Nutzers in ein technisches System nicht nur die AusweisApp2 selbst, sondern auch alle weiteren offiziellen Informationsquellen und Kanäle betrachtet und verbessert. So werden heute bspw. anhand von mehreren Erklärvideos dem Bürger die eID-Funktion nähergebracht und es wird auf einheitliche Sprache und einheitliches Design zwischen Webauftritt und AusweisApp2 geachtet.

Erwähnenswert ist an dieser Stelle aber auch, dass eine sicherheitstechnische Spezifikation sich unter Umständen auf die Gestaltung der Nutzerschnittstelle auswirken kann. So kennt die eID-Funktion eine fünfstellige Transport-PIN und eine sechsstellige eID-PIN. Diese unterschiedliche Länge der PINs macht es für den User-Interface Entwickler herausfordernd, den Nutzer auf Fehleingaben hinzuweisen. Dies zeigt, wie wichtig es ist, UI-Entwickler so frühzeitig wie möglich in Softwareentwicklungsprozesse einzubinden.

Zusammenfassung

Mit der weiter voranschreitenden Digitalisierung wird auch der Kreis der potentiellen Nutzer zunehmen und es wird sich auch der Anwendungskontext erweitern (mobile Nutzer, kleine Displays, Interaktion mittels Sprache, …). Für die korrekte Bedienung sicherheitskritischer Funktionen ist es daher wichtig, den Nutzer mit seinen Bedürfnissen, Kenntnissen und Fähigkeiten zu verstehen und dies im Gestaltungs- und Entwicklungsprozess zu berücksichtigen. Dies erfordert interdisziplinäre Teams (u.a. Usability-Experten, Designer, Cyber Security-Experten, Entwickler, Domänenexperten) und eine frühe Einbindung zukünftiger Nutzer.

Darüber hinaus sollten IT-Entscheider und Manager bei der Weiterentwicklung ihrer IT-Landschaft die zukünftigen Systeme nicht nur hinsichtlich der Erfüllung von Cyber Security-Anforderungen nach Stand der Technik, sondern auch hinsichtlich der Benutzbarkeit durch die Anwender auswählen. Eine gute Usability sollte ein wesentliches Qualitätsmerkmal von Sicherheitssoftware sein.

Der Autor
Prof. Dr. Andreas Heinemann *ist Professor für Computernetzwerke und IT-Sicherheit am Fachbereich Informatik der Hochschule Darmstadt. Internet: fbi.h-da.de/personen/andreas-heinemann, Telefon: 06151 163 84 82*

1 Die Cyber Security spricht hier genauer von Schutzzielen.
2 Die Quellenangaben sind in einer leicht erweiterten Online-Version dieses Beitrags zu finden unter https://manager-wissen.com/heinemann
3 Eine Übersicht der Diensteanbieter findet sich unter https://www.ausweisapp.bund.de/online-ausweisen/anbieter/ (abgerufen am 16.03.2020)
4 Mittlerweile ist es auch möglich, ein geeignetes Smartphone als Kartenleser zu verwenden.