secuview

Das secunet Kundenmagazin 2022

Globale Heraus-forderungen angehen

Christina Schlichting von Volkswagen über das konzernweite Informationssicherheits-Programm

Auf Herz und Nieren geprüft

Performance-Check im Netzwerk des Bundesinstituts für Arzneimittel und Medizinprodukte

From Zero to Hero

Wie aus „Zero Trust“ mehr als ein Buzzword wird

National

International

Titel

Wissenschaft

Technologien & Lösungen

Kurz notiert

Service

Liebe Leserinnen und Leser,

kaum hat sich die Pandemie abgeschwächt, müssen wir seit Februar dieses Jahres mit einer weiteren Krise globalen Ausmaßes leben. Der Russland-Ukraine-Krieg bringt in erster Linie viel menschliches Leid und führt darüber hinaus weltweit zu politischer und wirtschaftlicher Unsicherheit.

Als Cybersicherheitsunternehmen werden wir oft gefragt, welche Auswirkungen die Situation auf die Sicherheit digitaler Infrastrukturen in Staat, Wirtschaft und Gesellschaft hat. Die Frage hat zwei Aspekte. Der erste ist die konkrete Bedrohungslage, und diese wird vom Bundesamt für Sicherheit in der Informationstechnik (BSI) im aktuellen Kontext als „erhöht" eingestuft. Der zweite Aspekt ist die Wirksamkeit der Schutzmaßnahmen. Hier lohnt sich ein unaufgeregter Blick – denn in dieser Hinsicht hat sich gar nicht viel verändert. Die Schutzmechanismen, die gegen Cyberbedrohungen wirken und für digitale Souveränität sorgen, sind immer noch dieselben. Die veränderte Weltlage erzwingt keinen Strategiewechsel in der Cybersicherheit, stattdessen sollte der bisherige Weg noch konsequenter weitergegangen werden. Das tun wir gemeinsam mit unseren Kunden.

Das heißt allerdings nicht, dass wir nichts Neues zu erzählen hätten. Im Mai 2022 haben wir die bisher größte Akquisition unserer Firmengeschichte getätigt und den Cloud- und Kubernetes-Spezialisten SysEleven übernommen. Mit der Akquisition haben wir unser Cloud-Portfolio um einen weiteren Eckpfeiler erweitert und bieten nun ein umfassendes, maßgeschneidertes, sicheres Cloud-Angebot für Behörden, Verwaltungen und sicherheitsaffine Unternehmen. Für uns ist das eine zukunftsweisende Entwicklung, denn die Zukunft der IT liegt in der Cloud, und dasselbe gilt für die IT-Sicherheit.

Was uns noch in der Welt der Cybersicherheit umtreibt, zeigt ausschnittartig die vorliegende secuview. Wie immer kommen dabei auch unsere Kunden und Partner sowie externe Experten zu Wort. Zur letzten Kategorie gehört unser Titelbeitrag, über den ich mich besonders freue. Darin beschreibt Christina Schlichting, wie sie bei der Volkswagen AG ein konzernweites Informationssicherheitsprogramm steuert.

Ihnen wünsche ich viel Spaß bei der Lektüre. Bleiben Sie gesund!

Ihr Axel Deininger

Performance-Check im Netzwerk des Bundesinstituts für Arzneimittel und Medizinprodukte

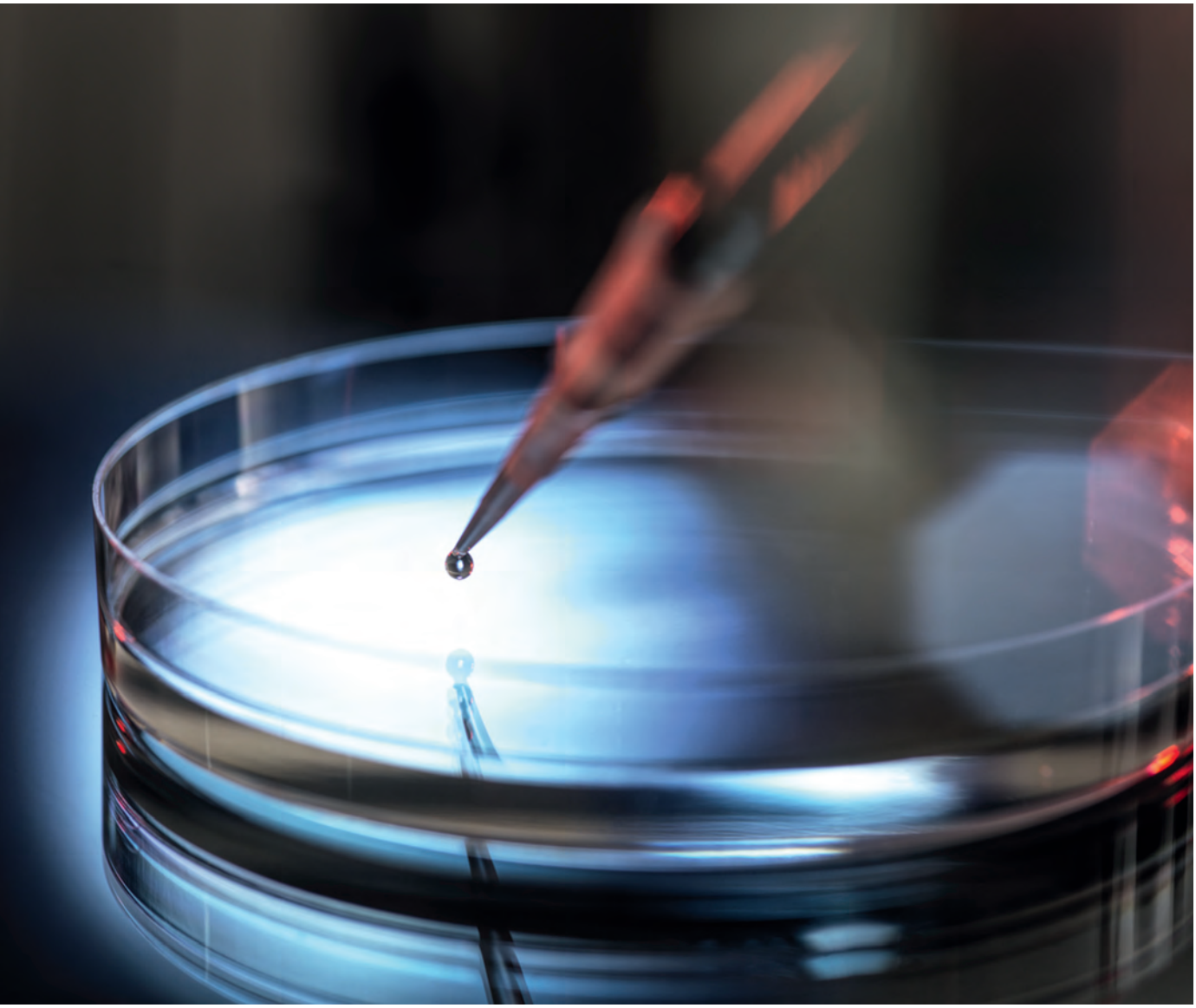
Auf Herz und Nieren geprüft

Das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) beschäftigt rund 1.350 Mitarbeiterinnen und Mitarbeiter – darunter Ärzt*innen, Apotheker*innen, Chemiker*innen, Biolog*innen, Informatiker*innen, Jurist*innen, Ingenieur*innen, technische Assistent*innen und Verwaltungsmitarbeiter*innen. Sie arbeiten an der Zulassung und der Verbesserung der Sicherheit von Arzneimitteln, der Risikoerfassung und -bewertung von Medizinprodukten sowie der Überwachung des Betäubungsmittel- und Grundstoffverkehrs. Darüber hinaus stellt die Behörde hochwertige Informationen für alle Bereiche des Gesundheitswesens zur Verfügung. Oberstes Ziel aller Maßnahmen ist die Erhöhung der Arzneimittel- und damit der Patientensicherheit.

Diesen Aufgaben kommen die Mitarbeiterinnen und Mitarbeiter des BfArM immer häufiger mobil bzw. aus dem Homeoffice nach. Die Behörde setzt hierzu ein mit SINA abgesichertes IT-Netzwerk ein. Dieses Netzwerk galt es im Herbst 2021 auf Herz und Nieren zu prüfen, da unerklärbare Performance-Schwankungen die Arbeit von außerhalb des Instituts erschwerten. Hierfür führte secunet gemeinsam mit dem Partner consistec einen sogenannten SINA Check-up durch.

Viele Bundesbehörden, die wie das BfArM mit sensiblen oder eingestuften Informationen arbeiten, nutzen die Sichere Inter-Netzwerk-Architektur SINA. Sie sorgt durch eine Vielzahl ineinandergreifender Sicherheitskomponenten zum Beispiel dafür, dass Dritte keine Daten mitlesen können, wenn Nutzer*innen sich mobil per Virtual Private Network (VPN) ins Behördennetz eingewählt haben. Mit der besonders abgesicherten SINA Workstation im Laptop-Format spielt es dabei keine Rolle, ob die Mitarbeitenden sich im Büro, zu Hause oder unterwegs aufhalten. Zudem sind SINA Netzwerke und Komponenten so konzipiert, dass sie trotz ihres hohen Sicherheitsniveaus einfach zu bedienen sind, auf zehntausende Nutzer*innen skalieren und eine hohe Performance zeigen.

Trotzdem beobachtete das BfArM in unregelmäßigen Abständen nicht erklärbare Leistungsabfälle bei der mobilen Arbeit bzw. bei der Arbeit aus dem Homeoffice. Dies äußerte sich für die Nutzer*innen unter anderem in Verbindungsabbrüchen von Outlook oder Schwierigkeiten bei Videokonferenzen. Das kann viele



Mit der Sicheren Inter-Netzwerk-Architektur SINA können Mitarbeiter*innen von Behörden oder Unternehmen sicher mit sensiblen oder gar eingestuften Informationen umgehen – innerhalb oder außerhalb des Büros. SINA Lösungen verbinden Sicherheit und Nutzerfreundlichkeit. Ein regelmäßiger SINA Check-up kann dabei helfen, die Performance des abgesicherten Netzwerks jederzeit aufrechtzuerhalten. Dabei prüfen secunet Berater*innen die SINA Umgebung hinsichtlich der Funktionsweise aller relevanten Komponenten. Fehlkonfigurationen und Inkompatibilitäten werden proaktiv erkannt und können behoben werden. Ein Abschlussbericht dokumentiert nicht nur den Ist-Zustand, sondern enthält auch die passenden Handlungsempfehlungen. So kann ein Optimierungsbedarf frühzeitig festgestellt werden, beispielsweise hinsichtlich Hardwareauslastung und Performance.

Ursachen haben. Auf Netzwerkebene sind insbesondere die Internetanbindung der Nutzer*innen, die Netze des Bundes und das eigentliche Behördennetzwerk des BfArM zu nennen. Hinzu kommen weitere Elemente wie Hardware-Ressourcen, Leistungsverluste durch Virtualisierung oder Dockingstations. Durch die Komplexität des Gesamtsetups war es zudem wahrscheinlich, dass je Vorfall eine oder mehrere der potentiellen Ursachen zusammenspielten.

Die Gründe für die Performance-Schwankungen konnten sich also tief im gesamten Setup verstecken. Wichtig war es daher, die Suche einzugrenzen. Analysedaten waren gefragt, damit die verschiedenen potentiellen Ursachen voneinander getrennt und damit auch untersucht werden konnten. Und hier kam der SINA Check-up ins Spiel, den secunet gemeinsam mit consistec durchführte.

Flugschreiber für das Netzwerk

Dafür nutzten die Expert*innen zusätzlich zur üblichen konzeptionell-heuristischen Analyse durch den SINA Berater das Tool caplon Network & Service Monitoring. In enger Zusammenarbeit zwischen dem Projektleiter auf Seiten des BfArM und

Das Bundesinstitut für Arzneimittel und Medizinprodukte (BfArM) in Bonn

der SINA Beratung sowie consistec wurde mit der caplon Appliance eine Messtechnik im Netz installiert, die es ermöglicht, den Netzwerkverkehr auch bei hohen Datenraten vollständig und verlustfrei zu erfassen. Die gewonnenen Rohdaten werden für eine permanente Indiziensicherung vorgehalten und bieten auch die Möglichkeit, in die Vergangenheit zu schauen. So können sporadisch auftretende Probleme analysiert werden oder die Daten für forensische Analysen genutzt werden. Somit stellt das Tool quasi eine Art Flugschreiber für das Netzwerk dar.

Alle Verbindungen zwischen den verschiedenen Systemen werden analysiert und visualisiert, sodass technische Probleme und Performance-Einbrüche frühzeitig erkannt werden können. Damit konnte das Team von secunet und consistec die gesamte mit SINA abgesicherte Infrastruktur unter die Lupe nehmen. Insgesamt wurden von caplon 57 Terabyte Daten in 85,5 Milliarden Paketen analysiert. Um Datenschutzrichtlinien umfassend zu erfüllen, wurde neben Non-Disclosure Agreements (NDAs) zusätzlich das caplon Modul privacy protection eingesetzt. Damit können Daten online pseudonymisiert werden, sodass keinerlei Rückschlüsse auf personenbezogene Daten oder kritische Infrastrukturdaten möglich sind.

Nach dem Untersuchungszeitraum von sechs Wochen erhielt das BfArM Ende November 2021 einen mehrseitigen Abschlussbericht, der dem Prüfbericht eines unabhängigen Instituts wie zum Beispiel dem TÜV ähnelt. In diesem Dokument fanden sich neben den Analyseergebnissen auch praktische Handlungsempfehlungen wieder, um das Netzwerk-Setup weiter zu optimieren.

„Das Projekt mit secunet und consistec hat uns bei der Performanceanalyse sehr geholfen“, so Jan Franzen, Leiter Informationstechnik beim BfArM. „Wir konnten das Problem eingrenzen und erhielten auch Gewissheit darüber, dass unsere SINA Installation einwandfrei funktionierte.“

Marcel Göhler, Teamleiter Key Account Management bei secunet, resümiert: „Der SINA Check-up ist eine gute Möglichkeit, um Kunden bei der Instandhaltung ihrer SINA Lösung zu unterstützen. Der Kunde erhält einen Nachweis über die Sicherheit und Performance des Systems, Fehler können so frühzeitig erkannt werden. Die caplon Appliance kann dazu eine sinnvolle Ergänzung darstellen, um das System noch einmal tiefgreifender zu analysieren. Die Zusammenarbeit mit consistec war sehr partnerschaftlich und erfolgreich – wir freuen uns auf weitere gemeinsame Projekte.“

Marcel Göhler
marcel.goehler@secunet.com

consistec Engineering & Consulting GmbH ist ein inhabergeführtes, mittelständisches Unternehmen mit über 20 Jahren Erfahrung im Bereich Netzwerk-Monitoring. Mit der Produktlinie caplon – made in Germany – überwacht consistec die Qualität, Verfügbarkeit und Performance von IT/OT-Infrastrukturen und geschäftskritischen Anwendungen.

Damit haben Unternehmen einen umfassenden Überblick über alle im Netzwerk ablaufenden Vorgänge und die volle Kontrolle über das Netzwerk unter Betriebs-, Planungs- und Sicherheitsaspekten.

Neue secunet easygates in Polen

Witamy w Polsce: Polnische Grenzpolizei baut automatisierte Grenzkontrolle weiter aus

Weniger Wartezeit, einfaches Handling und zufriedene Gesichter: Seit 2018 sind die secunet easygates in Polen im Einsatz und erleichtern dort die Grenzkontrollen. Nun wird die Partnerschaft mit Enigma, dem zuständigen Sicherheitsunternehmen, erweitert. In Kürze sind secunet easygates auch am Flughafen Gdańsk im Einsatz.

secunet easygates (hier am Flughafen Sofia, Bulgarien) sorgen bald auch am Flughafen Gdańsk für automatisierte Grenzkontrollen.

Insgesamt sichert secunet damit bereits sechs Flughäfen in Polen ab: Wrocław, Gdańsk, Kraków, Poznań, Warszawa-Modlin sowie den Chopin-Flughafen in Warszawa. Dabei sind inzwischen mehrere easygate Generationen im Einsatz – und dank der Modularität der Systeme funktionieren Komponenten der neuen Generation problemlos mit den Vorgängergenerationen. Eine Besonderheit der easygate Installationen in Polen ist die zentrale Steuerung sämtlicher Automated Border Control (ABC)-Systeme über Serversysteme am Standort Warszawa.

„Seit 2018 unterstützen wir gemeinsam mit secunet die polnische Grenzpolizei und entlasten die Beamten an den wichtigsten Flughäfen des Landes. Automatische Vorgänge bei der Grenzkontrolle erleichtern und beschleunigen die Prozesse auch für Passagiere und sorgen für ein unkompliziertes Reiseerlebnis. Wir freuen uns darauf, die Partnerschaft mit secunet auszubauen“, sagt Radosław Frydrych, Vice President des Management Board bei Enigma.

Doch wie funktioniert das secunet easygate eigentlich? Vereinfacht gesagt prüft es optisch und elektronisch die Authentizität von elektronischen Identitätsdokumenten wie Reisepass und Personalausweis. Dazu liest das System das Gesichtsbild vom Chip im elektronischen Identitätsdokument aus und vergleicht die biometrischen Daten mit dem tatsächlichen Erscheinungsbild des Reisenden, das mittels einer Gesichtsbildkamera erfasst wird.

Insgesamt werden an internationalen Flughäfen heute bereits mehr als 450 secunet easygates eingesetzt – neben Polen beispielsweise in Deutschland, Österreich, Tschechien, Ungarn, Litauen und Bulgarien. „Witamy w Polsce“ heißt übrigens „Willkommen in Polen“.

Michael Schwaiger
michael.schwaiger@secunet.com

EU-Verordnung zu Schengen-Visa

Das Papier-Visum bekommt digitale Hilfe

Seit dem 1. Mai 2022 gelten neue Regeln für Schengen-Visa. Die analogen Dokumente müssen nun durch ein digitales Siegel ergänzt werden und gelten nur noch in einem solchen „Kombipaket". Zu diesem Zweck wurde der secunet Digital Seal Signer entwickelt. Er bietet ein sicheres Reisemanagement und Behörden wie Botschaften den notwendigen Schutz vor Betrug. Bis November 2022 gibt es noch eine Übergangsfrist, dann wird das digitale Siegel Pflicht für alle Visa.

Bisher existieren Visa nur auf gedrucktem Papier oder im Reisepass. Doch das soll sich ändern. Denn nur die analoge Variante ist zu unsicher und zu anfällig für Betrug. Blanko-Papiere, auf die Behörden und Botschaften die individuellen Reisedaten aufdrucken, waren bei Betrügern begehrt und mussten daher aufwändig in Safes aufbewahrt werden. Deshalb hat die EU-Kommission am 30. April 2020 entschieden: Wir brauchen ein digitales Siegel als Ergänzung zur analogen Version. Seit Mai 2022 gilt das für alle Visa.

Schutz vor Betrugsmaschen

Die passende Lösung dazu ist der secunet Digital Seal Signer. Informationen wie das Datum, die genehmigte Aufenthaltsdauer und die Reisepassnummer werden durch einen 2D-Barcode digitalisiert und durch die jeweilige Behörde signiert. Diesen Barcode generiert ein sicherer Webservice und schon kann der Druck auf das Visum erfolgen. So entsteht eine zusätzliche technische Absicherung zur Druckversion. Als erste Partner setzen bereits Estland und Island auf den Digital Seal Signer.

Andreas Hellrung
andreas.hellrung@secunet.com

Erfahrungswerte bei Volkswagen

IT-Sicherheitsstrategien vor globalen Herausforderungen – gegensteuern, aber wie?

Von Christina Schlichting, Head of Group Information Security Programs & Projects (GISP), Volkswagen AG

Die gesamte Wirtschaftswelt befindet sich im digitalen Umbruch. Davon ist keine Branche ausgenommen. Der Volkswagen-Konzern treibt Modernisierung und Digitalisierung mit Hochdruck voran, in seinen Produkten und dem gesamten Ökosystem. Als Konzern-Informationssicherheit konzentrieren wir uns mit unseren Aufgaben und Verantwortungen im Wesentlichen auf die Unternehmens-IT mit vielen Schnittstellen auch zu Software, die im Fahrzeug verbaut wird, oder auf die Kundenschnittstelle, die beispielsweise im Handel eine wichtige Rolle spielt.

Mit unseren zwölf Marken, 120 Fertigungsstätten, mehr als 670.000 Mitarbeiter*innen im Konzern, 153 Ländern, in denen unsere Fahrzeuge angeboten werden, und der Fahrzeugproduktion gehören weitere Geschäftsfelder wie Großdieselmotoren, Dampf- und Gasturbinen, Kompressoren, Batteriefertigung, Finanzen, Ökostrom u. v. m. dazu – das zeigt die hohe Komplexität, in der wir uns mit der Informationssicherheit bewegen.

Historie

Großprojekte und Programme in der IT sind bei uns an der Tagesordnung. So hat der Volkswagen Konzern bereits 2011 ein konzernübergreifendes Informationssicherheitsprogramm aufgesetzt.

Das Programm beinhaltete zwölf sehr komplexe Projekte und Themen, die sich im Wesentlichen mit der konzernübergreifenden Erhöhung des Informationssicherheitsniveaus, einheitlichen Prozessen, Standards und technischen Lösungen befasste. Als 2019 dieses Programm abgeschlossen wurde, bescheinigte PwC:

„Die großen IT-Sicherheitsinitiativen bilden die Grundlage zur Erhöhung des Informationssicherheitslevels im gesamten Konzern, die Vereinheitlichung von Standards und Tools sowie für den Einsatz zentraler Lösungen in den Marken und Gesellschaften." (PwC-Audit ITSP2)

Und das sollte sich auch fortsetzen, allerdings unter leicht angepassten Vorzeichen und Rahmenbedingungen:

- Kürzere, schnellere Intervalle – auf Basis jährlich neu definierter Schwerpunkte
- Weiterhin marken- und regionenübergreifend
- Noch mehr Synergien zwischen den Marken
- Leichte Adaptierbarkeit, damit ein gut orchestrierter Rollout ermöglicht wird

IT-Sicherheitsinitiativen und -projekte im Volkswagen-Konzern

Vorgehensweise

Das konzernübergreifende Gremium der Informationssicherheit bestehend aus den CISOs (Chief Information Security Officer) der Marken analysiert jährlich gemeinsam das Bedrohungsradar des Information Security Forum (ISF) und leitet entsprechende Risiken ab. Aus diesen Risiken werden Maßnahmen definiert, die dann priorisiert in das Group Information Security Programm (GISP) einfließen.

Das Programm umfasst jährlich andere Schwerpunkte. Die Projekte werden durch verschiedene Markenvertreter und einen Promotor besetzt, der als Mitglied des CISO Gremiums für das Programm das gesamte Gremium vertritt und nicht nur die Interessen seiner Marke im Auge hat.

Gesteuert werden die Projekte über ein querschnittlich organisiertes Global Program Management (GPM) mit Reporting, Finanzen, Kommunikation, Qualitätssicherung und Risikomanagement.

Seit Beginn 2022 kam ein weiteres Querschnittsthema hinzu: der Rollout der Arbeitsergebnisse in den Marken und Standorten. Die in den ersten zwei Jahren entwickelten Arbeitsergebnisse werden jetzt systematisch und priorisiert in die Linienfunktionen der Marken integriert. Dabei werden die Marken durch dezidierte Rollout-Manager, einen engen Austausch zwischen den Projektleitern zu Best-Practice-Ansätzen und mit buchbaren Rollout-Paketen bei der Umsetzung unterstützt.

Zu den aktuellen Projekten im GISP gehören die Themen Cloud Security, Identity & Access Management, PKI Enhancement, Shopfloor Security, Cross Functional Monitoring, Endpoint Security, Secure Software Development und Governance.

Erfolgsfaktoren

Rückblickend sind die PwC-Empfehlungen auch gleichzeitig Erfolgsfaktoren für die Umsetzung des Programms. Die weiter oben genannten Empfehlungen wie schnellere Intervalle und Adaptierbarkeit sind wesentliche Aspekte.

Aber auch die markenübergreifende Besetzung in den Projektverantwortungen und die aktive Rolle des Promotors tragen zur hohen Akzeptanz des Programms bei.

Für die Programmsteuerung sind es die folgenden Faktoren:

- Regelmäßige Projektleitermeetings
- Regelmäßige Retrospektiven
- Feedback & Maßnahmen umsetzen
- Regelmäßige Prüfung der Abhängigkeiten zwischen den Projekten
- Risiken aktiv managen
- New Work (Covid19): Neue Methoden ausprobieren!

„Das konzernübergreifende Gremium der Informationssicherheit analysiert jährlich gemeinsam das Bedrohungsradar des ISF und leitet entsprechende Risiken ab. Aus diesen Risiken werden Maßnahmen definiert, die dann priorisiert in das Group Information Security Programm einfließen."

Aus früheren Programmen haben wir natürlich auch gelernt. Diese Aspekte sind ebenfalls wichtige Erfolgsfaktoren:

- Keine Überregulierung
- Geringe Administration
- Professionelles Programmmanagement
- Hohe Selbstorganisation in den Teams
- Rollout nicht sich selbst überlassen

Die Zusammenarbeit zwischen den Konzernmarken auf Management- und Mitarbeiterebene wurde verstärkt und die aktive Kommunikation des Programms mit Best Practices und Erfahrungswerten trägt dazu bei, dass sich aus der Konzern-Informationssicherheit eine globale Community entwickelt.

Christina Schlichting

Twitter @xiexingna

Nach dem Studium der Sinologie, Politischen Wissenschaften und Germanistik startete Christina Schlichting ihr Arbeitsleben Ende 1990 mit einem internationalen Traineeprogramm bei der Volkswagen AG in Wolfsburg. 1993 erfolgte ein Wechsel zur Audi AG nach Ingolstadt in verschiedenen Positionen, unter anderem als Sales Managerin für die VR China, in der sie auch den Aufbau und die Leitung des Audi Beijing Office inne hatte.

2003 erfolgte dann ein Wechsel in den Bereich Informationstechnologie und Organisation. In diesem Bereich übernahm sie dann nach abermaligem Wechsel zur Volkswagen AG 2005 verschiedene Leitungsfunktionen im Bereich IT Personal, Entwicklung von Dienstleistungssystemen und IT Governance. Seit September 2019 ist Christina Schlichting unter anderem für den Aufbau und die Umsetzung eines konzernweiten Informationssicherheitsprogramms verantwortlich.

Industrie 4.0

„Am E4TC kann echte Innovation stattfinden“

Die digitale Transformation der Industrie lebt von agiler Erarbeitung und Umsetzungserfahrung. Hier setzt das European 4.0 Transformation Center (E4TC) an, das im Jahr 2015 als Kooperationsplattform auf dem RWTH Aachen Campus gegründet wurde. Seinen Mitgliedern aus Industrie, Forschung und IT, zu denen auch secunet gehört, bietet das E4TC die Möglichkeit, ganzheitliche Prozessszenarien oder Lösungsarchitekturen weiterzuentwickeln und zu teilen. secuview sprach mit Prof. Dr. Thomas Gartzen, Geschäftsführer des E4TC.

Wie ist der Stand der digitalen Transformation der Industrie heute?

Prof. Dr. Thomas Gartzen: Spätestens seit den Herausforderungen, die die Corona-Pandemie für die Industrie mit sich gebracht hat, ist einem Großteil der Unternehmen sehr deutlich klar geworden, dass sie nur durch Digitalisierung und Vernetzung ihrer Arbeitswelten die notwendige Resilienz für solche dynamisch-instabilen Situationen aufbauen können. Insofern hat sich insbesondere in den letzten beiden Jahren unheimlich viel bewegt in der Industrie und wir sehen heute nahezu überall digitale Transformationsprogramme auf den strategischen Agenden der Unternehmen – ob Mittelständler oder Konzerne. Selbstverständlich sind die Reifegrade einzelner Unternehmen und Industrien ganz unterschiedlich. Wichtig ist diesbezüglich, dass der Status quo im Unternehmen transparent ist, denn nur mit einem unverstellten Blick auf die eigenen Prozesse und Applikationslandschaften und ohne unrealistische Erwartungen kann eine digitale Transformation gelingen.

Welches sind die größten Hindernisse, die bei Digitalisierungsprojekten auftauchen können?
Aus meiner Sicht gibt es zwei verschiedene Arten von Hindernissen. Zum einen sind da die klassischen technologischen Hürden, die durch die Vernachlässigung einer langfristigen strategischen Planung entstehen. Allzu oft wird in der Industrie in voneinander abgekapselten Use Cases und Proof of Concepts gedacht. Ohne eine übergeordnete Digitalisierungsstrategie und dazugehörige IT-Architektur, die als Nordstern alle Digitalisierungsaktivitäten auf ein gemeinsames Ziel ausrichtet, ist das spätere Skalieren der initialen Lösungen oft nicht möglich. Dies führt dazu, dass das eigentliche Potential durchgängiger Informationsflüsse, nämlich das Schließen von Regelkreisen im und über das Unternehmen hinweg, nicht ausgeschöpft werden kann.

Zum anderen sind auch organisatorische Hindernisse zu überwinden. Digitalisierungsprojekte sollten nicht nur Top-down angeordnet werden, sondern immer auch die Anwender*innen in den Entwicklungsprozess mit einbeziehen und sie zu aktiven Akteur*innen der Transformation machen. So wird einerseits implizites Wissen sinnvoll genutzt, andererseits werden eingebundene Mitarbeitende die Projekte auch viel besser akzeptieren. Denn viele Menschen in Unternehmen begegnen Digitalisierungsprojekten mit großen Vorbehalten, da dadurch Prozessroutinen aufgehoben sowie neue Abläufe und Standards eingeführt werden, die zuerst gelernt und sich angeeignet werden müssen. Je partizipativer dieser Gestaltungsprozess ist, desto steiler ist die Lernkurve bei deren Einführung und desto minimaler sind die Vorbehalte gegenüber digital vernetzen Arbeitsprozessen.

Gleichzeitig ist es wichtig, Erfolge stets bewusst zu reflektieren und Digitalisierung als einen kontinuierlichen Prozess anzusehen. Eine agile Arbeitsweise in Sprints, in der in kurzen Zyklen Veränderungen eingesteuert, verprobt und evaluiert werden können, hat sich dabei bewährt.

Welchen Stellenwert hat Ihrer Erfahrung nach das Thema Datensicherheit bei der digitalen Transformation hin zur Industrie 4.0?
In der Transformation zur Industrie 4.0 ist Datensicherheit eines der zentralen Handlungsfelder. Ziel der Digitalisierung und Vernetzung unserer Produktions- und Arbeitswelten ist es, neben den Arbeitsprozessen auf der Maschinen- und Anlagenebene insbesondere die planerischen und regelnden Abläufe zu automatisieren. Das heißt: Mitarbeitende durch digitale Hilfsmittel bestmöglich bei ihren Aufgaben und Entscheidungen zu unterstützen. Dies setzt voraus, dass unternehmensspezifisches, meist implizites Know-how digital abgebildet wird, um es etwa für KI-Anwendungen nutzbar zu machen. Auf diese Art und Weise können IT-Applikationen beispielsweise Maschinenführer*innen dabei helfen, Produktionsanlagen nachhaltiger zu steuern, indem Qualitätsverluste und ein zu hoher Energieverbrauch in Echtzeit datenbasiert prognostiziert und somit

Die Partner des **European 4.0 Transformation Centers (E4TC)** sind Forschungsinstitutionen sowie langjährige Mitglieder des RWTH Aachen Campus, welche sich als Technologieanbieter bzw. Industrieunternehmen der digitalen Transformation in ihrem jeweiligen Bereich engagieren. Sie bilden im E4TC eine exklusive Kooperationsplattform für eine kontinuierliche und langfristige wissenschaftliche Zusammenarbeit.

In Versuchsumgebungen können Expert*innen Produktionsanlagen in Testszenarien aufbauen und verbessern. Mit seiner Demonstrationsfabrik steht das E4TC Industrieunternehmen bei deren digitaler Transformation mit Rat und Tat zur Seite – so zum Beispiel beim Thema Industrial Internet of Things (IIoT).

secunet ist seit Frühjahr 2022 Mitglied des E4TC und bringt vor allem seine Expertise im Bereich der industriellen IT-Sicherheit ein. Ein erstes Projekt gemeinsam mit Liebherr IT und Hewlett Packard Enterprise (HPE) ist bereits gestartet.

In der Demonstrationsfabrik des E4TC können Industrieunternehmen technologische Lösungen in einem größeren und anwendungsbezogenen Kontext darstellen.

verhindert werden. Jedoch ist das dafür notwendige Wissen über den Produktionsprozess, welches expliziert und digital abgebildet werden muss, für ein Unternehmen wettbewerbsrelevant und unbedingt schützenswert. Die entsprechenden IT/OT-Infrastrukturen müssen also zuverlässig vor Angriffen geschützt werden, die sowohl über das Internet als auch vor Ort erfolgen können. Es wird deutlich, dass die Lösungen der Industrie 4.0 ihren Nutzen nur entfalten können, wenn eine umfassende Datensicherheit gewährleistet ist.

Wie wurde das E4TC ins Leben gerufen und welche Ziele verfolgt es?

Das E4TC ist eine Kollaborationsplattform auf dem RWTH Aachen Campus und bringt seit 2015 Industrieunternehmen, Technologieanbieter und Wissenschaft zusammen, um gemeinschaftlich neue Lösungen zur digitalen Transformation der produzierenden Industrie zu erarbeiten. Der Betrachtungsbereich, den unser Ökosystem dabei einnimmt, ist bewusst sehr breit gewählt. Denn unserer Überzeugung nach muss in einer Industrie 4.0 die digitalisierte Vernetzung schon in den Entwicklungsprozessen eines Unternehmens berücksichtigt werden. Von dort erstreckt sie sich über die Produktion bis in die Kundenprozesse, bei denen beispielsweise Daten über die Nutzung eines Produkts gesammelt werden. Insbesondere in der aktuellen Forschung zur Realisierung einer Circular Economy wird sehr schnell deutlich, dass eine echte Kreislaufwirtschaft ohne solch eine digitale Datendurchgängigkeit nicht realisierbar ist.

Im E4TC werden solche Ansätze zur Erprobung und Validierung beispielsweise in der Demonstrationsfabrik konkret umgesetzt. Das dient gleichzeitig der anschaulichen und erfahrbaren Weitervermittlung dieser Lösungen. Somit steht die Mitglieder-Community des E4TC auch Industrieunternehmen außerhalb unseres Ökosystems bei Fragen rund um die digitale Transformation mit Rat und Tat zur Seite.

Wie läuft die Zusammenarbeit im Rahmen des E4TC konkret ab?

Unsere Zusammenarbeit verfolgt immer das Ziel, in Form von konkreten Projekten neue digitale Technologien zusammenzuführen oder zu erweitern, um sie auf industrielle Applikationsfelder anzuwenden und ihren Nutzen nachzuweisen.

Nachdem eine gemeinsame Aufgaben- und Zielstellung definiert worden ist, wird ein agiles Projektteam mit Expert*innen unserer Mitgliedsunternehmen sowie Kolleg*innen des Centers und der universitären Institute gebildet. Dieses heterogen zusammengesetzte Team erarbeitet dann in kurzzyklischen Sprints während eines Zeitraums von drei bis sechs Monaten eine konkrete Lösung in Form eines Minimal Viable Products (MVP). Wir gehen dabei ganz gezielt über

„Nach dem Motto ‚Zeigen ist besser als behaupten' wird im E4TC Kompetenz glaubhaft demonstriert."

die reine theoretische Konzeption hinaus und haben immer zum Ziel, keine PowerPoint-Präsentation, sondern eine funktionsfähige digital-physische Lösung zu entwickeln. Hierbei kommt uns selbstverständlich die einmalige Infrastruktur des RWTH Aachen Campus mit seiner Demonstrations- und Anlauffabrik sowie diversen Reallaboren zugute.

Wie profitieren die Mitglieder von Technologien und Erkenntnissen, die im Rahmen des E4TC entwickelt werden?

Die Vernetzungs- und Kollaborationsmöglichkeiten in dem Ökosystem des RWTH Aachen Campus, das aus Spitzenforschungsinstituten und über 400 innovativen Unternehmen besteht, sind aus meiner Sicht in Europa einzigartig.

Im E4TC steht, wie bereits erwähnt, die konkrete Umsetzung und stetige Weiterentwicklung funktionsfähiger digital-physischer Lösungen im Vordergrund. Da dies immer im Verbund mit anderen Mitgliedern geschieht, kommen die Unternehmen unmittelbar mit neuen Technologien und Ansätzen in Berührung und können gleichzeitig die eigene Expertise in einem realen Ökosystem demonstrieren.

Durch regelmäßig stattfindende Führungen, Workshops und Events der einzelnen Mitglieder sehen nicht nur Vertreter*innen der Mitgliedsunternehmen, sondern auch viele Entscheider*innen aus der Industrie diese Lösungen. Frei nach dem Motto „Zeigen ist besser als behaupten" wird so Kompetenz glaubhaft demonstriert. Die Darstellung des eigenen technologischen Lösungsbestandteils in einem größeren und anwendungsbezogenen Kontext wie etwa in der Demonstrationsfabrik hilft dabei ungemein, den Technologienutzen erfahrbar zu vermitteln. Anhand klar definierter, praxisrelevanter und oft sogar aus der direkten Industriepraxis unserer Mitglieder abgeleiteten Aufgabenstellungen kann am E4TC echte Innovation stattfinden. Mit unseren Mitgliedern arbeiten wir dabei stets an der Umsetzung des technologisch Möglichen. Von der Ideengenerierung über iterative Verprobung und Weiterentwicklung bis hin zum Anstoß der Re-Industrialisierung decken wir alle Phasen ab. Dabei unterstützen wir mit langjähriger Expertise sowie einem starken Netzwerk aus Praxis und Wissenschaft.

Prof. Dr. Thomas Gartzen

Prof. Dr. Thomas Gartzen verfügt über mehr als zehn Jahre praktische Erfahrung in der digitalen Transformation sowie der Realisierung von Industrie 4.0-Projekten entlang der gesamten Wertschöpfungskette produzierender Unternehmen. Thomas Gartzen studierte an der RWTH Aachen Maschinenbau und war nach seiner Promotion 2012 als Geschäftsführer der DFA Demonstrationsfabrik Aachen GmbH tätig, einer Referenzfabrik für Industrie 4.0 auf dem RWTH Aachen Campus. Seit 2016 ist er in geschäftsführender Funktion für die European 4.0 Transformation Center GmbH verantwortlich. Thomas Gartzen ist zudem seit 2021 Inhaber der Professur für Fertigungssysteme an der Technischen Hochschule Köln.

Studie von secunet und techconsult

IoT-Projekte in Unternehmen: Externe Expertise häufig unerlässlich

Welchen Stellenwert hat das Internet of Things (IoT) für deutsche Unternehmen? Welche Hürden beeinträchtigen die Umsetzung und welche Arten von Sicherheitsvorfällen gab es in Zusammenhang mit IoT-Systemen? Um diese und weitere Fragen zu beantworten, hat das Research- und Analystenhaus techconsult im Auftrag der secunet Security Networks AG mehr als 150 Unternehmen im Rahmen der Studie „IoT – aber sicher. Sichere Infrastrukturen in einer vernetzten Welt“ befragt.

Jan Ludwig Tiedemann

jan.tiedemann@secunet.com

Die Ergebnisse zeigen, dass das Bewusstsein für die Chancen von IoT in deutschen Unternehmen wächst, gleichzeitig gibt es noch Nachholbedarf in der Praxis. Obwohl die Technologie für knapp die Hälfte der Firmen eine hohe oder sehr hohe Relevanz hat, geben lediglich 13% der Befragten an, IoT bereits breitflächig umgesetzt zu haben. Das ist auch darauf zurückzuführen, dass sich nur rund ein Viertel überhaupt dazu in der Lage sieht, die IoT-Projekte vollständig in eigener Regie zu realisieren. Mehr als 60% der Unternehmen setzen deshalb auf externe Partner, um fachliche, technische und rechtliche Ebenen von Beginn an angemessen berücksichtigen zu können.

Gleichzeitig weist die Studie auf einen erheblichen Mangel an Sicherheitsvorkehrungen hin. 44% der Unternehmen haben demnach keine speziellen Maßnahmen zur IoT-Absicherung getroffen. „Viele Firmen glauben, dass nur die großen Konzerne im Visier von Cyberkriminellen stehen“, so Jan Ludwig Tiedemann, Senior Solution Architect bei secunet. „Das ist ein hartnäckiger Irrglaube: Rund 30% der Unternehmen mit weniger als 1.000 Mitarbeitern waren laut unserer Erhebung bereits von Angriffen betroffen. Cybersicherheit geht eben alle an.“

Chancen von IoT-Systemen

Vernetzte Geräte, Maschinen oder Anlagen im IoT halten für Firmen aus unterschiedlichen Branchen zahlreiche Chancen bereit. Die befragten Unternehmen versprechen sich jedoch vor allem erhöhte Produktqualität (45%), Prozessoptimierungen (44%), Verbesserungen von bestehenden Produkten und Services (42%), geringere (Produktions-)Kosten (38%) sowie erhöhte Kundenzufriedenheit (36%).

Wie setzen Sie Ihre IoT-Projekte um, beziehungsweise planen Sie diese umzusetzen?

Basis: 151 Unternehmen

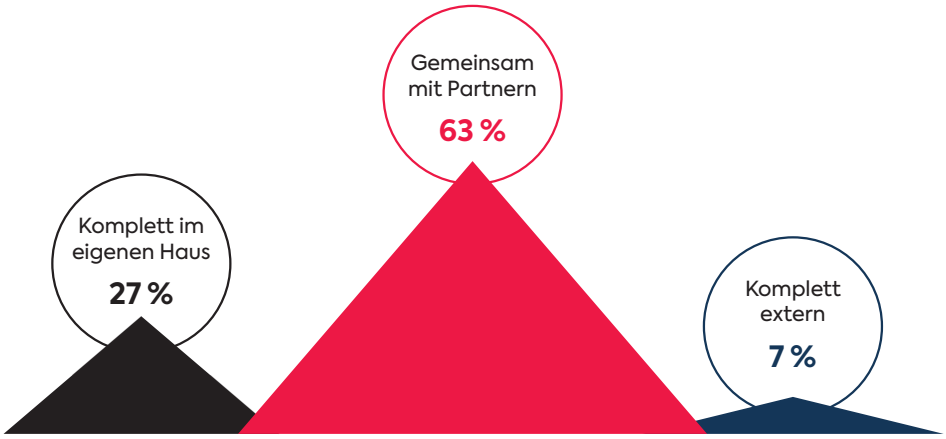


Abbildung 1: secunet/techconsult Studie „IoT – aber sicher. Sichere Infrastrukturen in einer vernetzten Welt“.

Hürden bei der sicheren Umsetzung

Datenschutz- (43 %) und Sicherheitsbedenken (36 %), fehlendes Know-how (38 %) und Einbindung in die vorhandene IT-Infrastruktur (36 %) sehen die Firmen als größte Hürden bei der Umsetzung von IoT-Projekten an. Die Kompatibilität mit der vorhandenen Infrastruktur wiederum ist für die Hälfte der befragten Unternehmen die größte Herausforderung bei der Implementierung von IoT-Security. 46 % gaben außerdem an, dafür nicht über ausreichend Fachwissen zu verfügen und 38 % fehlt schlichtweg das nötige Fachpersonal.

Häufigste Sicherheitsvorfälle

Knapp 70 % der Unternehmen, die von Cyberangriffen betroffen waren, wurden einmal oder sogar mehrfach über vorhandene (Alt-)Geräte infiziert. 44 % der befragten Unternehmen waren in den letzten zwei Jahren einmal von einer solchen Attacke betroffen, die Dunkelziffer dürfte noch höher ausfallen. Bei einem Viertel der Unternehmen wurden diese Schwachstellen sogar mehrfach ausgenutzt. Ebenfalls knapp 70 % berichten von gezielter Sabotage oder von Industriespionage. Rund die Hälfte gab an, von der Kompromittierung der IoT-Geräte oder deren Missbrauch für kriminelle Zwecke betroffen gewesen zu sein.

Ansprüche an IoT-Security-Dienstleister

Damit Firmen ihre IoT-Systeme ausreichend vor Cyberkriminellen schützen können, sind sie in der Regel auf die Expertise eines Security-Partners angewiesen. Von diesem wünschen sie sich vor allem hohes technologisches Know-how (50 %), Verständnis für Prozesse (45 %), Branchenkompetenz (41 %), Innovationskraft (40 %) sowie Sicherheitszertifikate (36 %).

Alle Ergebnisse der Studie finden sich unter dem folgenden Link:
https://www.secunet.com/iot-aber-sicher

Wo sehen Sie die größten Herausforderungen bei der Implementierung von IoT-Security?

Basis: 151 Unternehmen

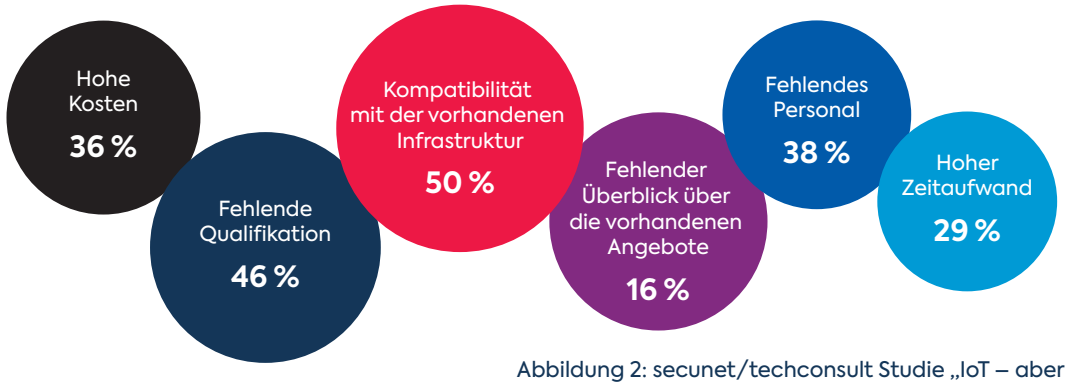


Abbildung 2: secunet/techconsult Studie „IoT – aber sicher. Sichere Infrastrukturen in einer vernetzten Welt“.

Wie aus „Zero Trust“ mehr als ein Buzzword wird

From Zero to Hero

Ein Kommentar von Dr. Kai Martius, Chief Technology Officer der secunet Security Networks AG

Zero Trust und Zero Trust Architectures (ZTA) sollen das neue Allheilmittel für die IT-Sicherheit sein. Sind sie das wirklich – oder eher fauler Zauber? Zunächst einmal ist der Begriff für mich etwas irreführend. Ich möchte nicht in einem Wolkenkratzer leben, den ein Zero-Trust-Architekt gebaut hat. Auf der anderen Seite möchte ich mich als Ingenieur nicht zu sehr über die – und das ist ernst gemeint – oft sehr kreativen Marketing-Leute beschweren, die derartige Begriffe verbreiten. Nähern wir uns dem Thema also wohlwollend und schauen wir uns an, was Zero Trust bedeuten kann und was es bedeuten sollte.

Wenn es in erster Linie darum geht, den inflationären Gebrauch des Wortes „Trust“ auf Null zu reduzieren, bin ich absolut einverstanden. Wenn es darüber hinaus bedeutet, das Konzept der Vertrauenswürdigkeit zu hinterfragen, dann: ja, bitte! Wir müssen tatsächlich Gründe dafür finden, unseren IT-Systemen zu vertrauen.

Wenn ich mir ZTA-bezogene Konzepte wie „datenzentrierte Sicherheit“ ansehe, stelle ich mir vor, ich säße ich in einer supersicheren Kommandozentrale ganz oben in meinem ZTA-Wolkenkratzer. Ich hoffe, dass alles darunter sicher genug ist, dass der Wolkenkratzer nicht einstürzt. Weil ich aber nicht

darauf vertraue – Zero Trust –, schaue ich manchmal in ein beliebiges Stockwerk weiter unten. Wenn ich dann eine Menge Leute herumlaufen sehe, die bröckelnden Putz reparieren und Löcher in der Wand zuspachteln, habe ich wahrscheinlich einen „Patch Day" erwischt. Das ist zunächst einmal nichts Schlechtes: Natürlich müssen wir Schwachstellen flicken und heutzutage sind wir sehr gut darin, Löcher in der Wand im Handumdrehen zu schließen. Ein mulmiges Gefühl stellt sich allerdings ein, wenn jeden Tag jemand klingelt und ein Loch repariert, von dem man bisher nichts ahnte.

Aber lassen Sie uns ein bisschen positiver sein: Wenn gute ZT-Architekt*innen den Wolkenkratzer gebaut haben, fühle ich mich in meiner Kommandozentrale im obersten Stockwerk viel wohler. Denn sie haben daran gedacht, alle Stockwerke mit starken Stützpfeilern auszustatten. Wenn etwas zusammenbricht, gibt es eine zweite Verteidigungslinie. In der Sicherheitstechnik ist es gängige Praxis, dass man Systeme auf der Grundlage des Konzepts „Defense-in-Depth" baut. Wann immer es möglich ist, sollte man von diesem Prinzip Gebrauch machen, schließlich kann man mit einer einzigen Säule kaum genügend Vertrauenswürdigkeit (da ist sie wieder!) herstellen. Ob die Gesamtarchitektur dann unter dem Namen ZTA läuft oder morgen schon wieder anders heißt, ist zweitrangig, denn das Prinzip stimmt. Auch Zwei-Faktor-Authentisierung (2FA) ist ein sehr gutes Konzept. Die Verwendung von virtuellen Maschinen als zweite Trennschicht um Container-Workloads herum ist ebenfalls sehr hilfreich, falls jemand Ihren Dienst angreift.

Eine weitere Variante des ZT ist eine verteilte oder geschichtete Anordnung von Kontrollpunkten. Da es in meinem Hochhaus viele verschiedene Hausbewohner mit vielen verschiedenen Vorstellungen von „Vertrauen" gibt, wäre ein einzelner Wachmann im Erdgeschoss mit der Kontrolle überfordert. Natürlich wäre es genauso wenig ratsam, den Zugang nur von meinem Kontrollzentrum im obersten Stock zu kontrollieren. Denn was passiert dann, wenn jemand den zweiten Stock wegsprengt?

Eine grobe Zugangskontrolle am Gebäudeeingang könnte darin bestehen, eine Basisidentität zu überprüfen. Eine Kontrolle sämtlicher Pakete und Lieferungen im Erdgeschoss ist allerdings kaum möglich, da heute überall Verschlüsselung eingesetzt wird. Hier sind wir wieder beim Thema Vertrauenswürdigkeit: Wenn ein Paket von einem vertrauenswürdigen Lieferdienst kommt, kann es durchaus in den zweiten Stock geschickt werden. Letztlich sollte man das Paket sowieso nur öffnen, wenn man weiß, wer es geschickt hat. Ein guter mehrschichtiger Ansatz könnte also folgendermaßen aussehen: Rechteverwaltung auf der Anwendungsdatenschicht, Transportverschlüsselung und Client-Zertifikatsvalidierung mit TLS und eine eher grobkörnige Zugangskontrolle auf der Netzwerkschicht mit VPNs.

Es wäre wenig ratsam, den Zugang nur von meinem Kontrollzentrum im obersten Stock zu kontrollieren. Denn was passiert dann, wenn jemand den zweiten Stock wegsprengt?

Manchmal muss man auch Pakete von Absendern annehmen, die man nicht kennt. Dann wäre es gut, einen Bunkerraum zu haben, der stark genug ist, um unseren Wolkenkratzer nicht zum Einsturz zu bringen, wenn etwas explodiert. Heute gibt es solche Bausteine auf der Basis virtueller Maschinen für isolierte Umgebungen.

Wenn wir also nicht mehr auf den einzelnen, übermenschlich vertrauenswürdigen Wächter im Erdgeschoss setzen, wie sage ich dann all den Kontrollpunkten (auch „Policy Enforcement Points“ genannt), was wir hereinlassen dürfen und was nicht? Sicherlich ist der mehrschichtige Ansatz komplizierter zu verwalten als eine einzelne Perimeter-Firewall. Wenn ZTA-Produkte dabei helfen, die verschiedenen Ebenen im Griff zu behalten, ist das wirklich eine Verbesserung!

Übrigens: Die Vielzahl von Vertrauensbeziehungen, mit denen wir es in den heutigen Architekturen und Betreibermodellen zu tun haben, wurde bereits in den 1990er Jahren in den Konzepten der multilateralen Sicherheit gut erforscht. Die Idee dahinter war, bei null Vertrauen anzufangen – und dann Vertrauensbeziehungen zwischen allen beteiligten Parteien aufzubauen, bis ein Teilnehmer bereit war, Daten mit anderen zu teilen, natürlich nur im Rahmen ausgehandelter Schutzmechanismen.

Auch im menschlichen Alltag tun wir das ständig: Vertrauen aufbauen, bis eine Beziehung vertrauenswürdig genug ist, um Daten zu teilen. Es beginnt sozusagen mit Zero Trust, aber endet mit Vertrauenswürdigkeit.

Ganz ohne Vertrauenswürdigkeit kommen wir also nicht aus. Die Frage ist: Wie stellt man sie her? Wir müssen uns einen riesigen Technologie-Stack vorstellen, der über viele Länder verteilt letztendlich von Menschen und Unternehmen aufgebaut und betrieben wird – hoffentlich auf sichere Weise. Wenn Sie sich diesen vernetzten Technologie-Stack vor Augen führen, können Sie sich vorstellen, welche Ausmaße unser bildlicher Wolkenkratzer hat.

Zum Glück ist eine Menge Arbeit im Gange, um die Situation in diesem Hochhaus systematisch zu verbessern. Eingebaut werden zum Beispiel neue felsenfeste Ziegel („Rust“, eine sicherere Programmiersprache) oder magische Türen (gut erforschte Kryptographie). Viele undurchsichtige Wände werden durch Glasbausteine (Open Source) ersetzt, die viel mehr Transparenz bieten und erkennen lassen, wie stabil eine Wand wirklich ist. Und wir beginnen, die Gesetze der Physik zu verstehen und die Statik des Gebäudes zu berechnen (mathematische Korrektheitsnachweise, automatisierte Testmethoden für Software). Nichts daran ist wirklich neu, aber durch die Vielzahl ineinandergreifender Ansätze und Technologien wird IT-Sicherheit immer praktikabler.

Gleichzeitig wird das Thema immer dringlicher. So wie neue Maschinen und neues Wissen es uns erst im 20. Jahrhundert ermöglicht haben, Wolkenkratzer zu bauen, sind wir heute in der Lage, wirklich sichere IT-Infrastrukturen umzusetzen.

Als wir vor vielen Jahren angefangen haben, unseren heutigen „Weltcomputer“ zu bauen – haben wir das so getan, wie wir im Mittelalter einen Wolkenkratzer gebaut hätten? Möglicherweise. Aber mit den technologischen Bausteinen und dem Wissen, das wir seit einiger Zeit haben, können wir ihn renovieren. Wir sollten unser Vertrauenslevel ständig überprüfen, messen und in Frage stellen. Wenn Zero Trust uns dazu bringt, so zu arbeiten, hat sich das Konzept schon gelohnt.

P.S.: Trotzdem werde ich mein supersicheres Kontrollzentrum im obersten Stockwerk wohl bald aufgeben und vermieten. Ich bin mir sicher, dass sich jemand finden wird, der die Aussicht genießt und sich dort immer noch wohlfühlt. Aber wir haben begonnen, einen neuen Bunker auf einem soliden Fundament zu bauen. Er besteht komplett aus stabilen Glasbausteinen. Wer kommt mit? Die Aussicht ist zwar nicht so toll wie oben auf dem Wolkenkratzer, aber man fühlt sich viel sicherer!

Dr. Kai Martius

IT und Cybersicherheit im Automotive-Umfeld

„Komplexe automobile Architekturen erfordern kompromisslose Hardware- und Software-Sicherheit“

Herr Mühleck, Sie waren in Ihrer Karriere sowohl CIO der Volkswagen AG und der DaimlerChrysler AG als auch CIO des Bundesministeriums für Verteidigung und haben somit sowohl die Perspektive der Privatunternehmen als auch des Staats eingenommen. Welche Entwicklungen bei der IT-Sicherheit haben Sie in dieser Zeit wahrgenommen und auch teilweise mit angestoßen?

Klaus Hardy Mühleck: Mit Einzug des Internets in alle Bereiche des Lebens hat die IT-Sicherheit eine gewaltige Entwicklung genommen. So haben wir in der Automobilindustrie bereits in den Neunzigerjahren begonnen, Sicherheitsmechanismen in den Kommunikationsbeziehungen zu implementieren, zum Beispiel bei Video-Konferenzsystemen und IT-Zugriffen in den Fabriken. Ich kann mich auch noch gut an die digitale Ausgestaltung der ersten sicheren Wegfahrsperre unserer Fahrzeuge erinnern und den Übergang von der Disc-geprägten Wartungssoftware hin zur netzwerkbasierten Dialog-Wartung. Das war vor über 15 Jahren. Danach ging es Schlag auf Schlag: intelligente Firewalls, Intrusion-Detection, Trust-Center und PKI bis in die Gegenwart zu SOC mit semantischer KI-Unterstützung in einer Security Information and Event Management (SIEM) Welt.

Auch die staatlichen Institutionen mussten früh ihre digitalen Welten mit Systemen für VS-NFD oder GEHEIM und NATO SECRET absichern oder beispielsweise dynamische PKI-Schlüssel für den Einsatz von militärischen Großgeräten verwenden. Polizeibehörden, Botschaften, Dienste und Ministerien wie das Finanzministerium mit ELSTER nutzen moderne Technologien zur Absicherung und auch zur Fahndung. Erst vor kurzem wurde eine sechsstellige Anzahl hochsicherer Kommunikations-Router in Deutschland ausgerollt (wie zum Beispiel der secunet konnektor, Anm. d. Red.), die alle Arztpraxen mit der Telematikinfrastruktur des Gesundheitsweisens vernetzen. Hochsicherheit ist in all diesen Bereichen

Klaus Hardy Mühleck

Nach dem Studium der Elektrotechnik, Prozessautomatisierung und Datenverarbeitung begann Klaus Hardy Mühleck seine berufliche Laufbahn bei der Siemens AG. Danach arbeitete er 14 Jahre im Daimler-Konzern, zuletzt als CIO-Automotive und Mitglied des Daimler-Direktoriums. Mit dem Wechsel in den Volkswagen-Konzern übernahm er die Verantwortung als CIO für die Markengruppe AUDI und danach als CIO für den gesamten VW-Konzern. Mitte 2016 wurde Mühleck nach Berlin gebeten, als CIO zum Aufbau der Cyber- und IT-Organisationen des Bundesministeriums der Verteidigung.

unvermeidlich. Und Firmen wie secunet haben diese hochsicheren IT-Strukturen ermöglicht.

Inwieweit sehen Sie im Automobilbereich einen Wandel von monolithisch denkenden Automobilkonzernen hin zu einem Austausch innerhalb der Branche unter Einbindung von Akteuren aus anderen Bereichen wie Politik oder Infrastruktur?
Traditionell hat sich die Automobilbranche in Deutschland mit der Entwicklung und Produktion von hochwertigen und innovativen Fahrzeugen beschäftigt. Der Austausch über verschiedene Kompetenzen sowie auf Fahrzeugmessen hat schon immer stattgefunden, vor allem in den klassischen Disziplinen, aber auch partiell in der IT. Sehr großen Anteil haben daran Zulieferpartner und Engineering-Dienstleister. Sie haben den Technologietransfer ermöglicht.

Doch der große Wandel kommt mit den digitalen Ecosystemen im und um das Fahrzeug: Die Anbindung Cloud-basierter Online-Dienste, Services im Elektrofahrzeug zum Lademanagement mit Ladestopps entlang der Route, Parkleitsysteme bis hin zum (teil)autonomen Fahren sowie Notfallhilfen sind heute fast schon Standard.

Der Wandel, ein Fahrzeug als Teil verschiedener Ecosysteme der automobilen Umwelt zu sehen, ist voll im Gange. Tesla ist hier sicher ein Wegbereiter oder sogar Disruptor. Die deutsche Automobilbranche tut sich immer noch schwer mit diesem digitalen Einfluss der umgebenden Cloud-Welt. Aber sie holt auf und wappnet sich für die Zukunft.

Doch auch unsere Politik ist gefragt. Denn wir benötigen die notwendige Infrastruktur zu 6G, um diesen Wandel in Deutschland schnell und innovativ voranzubringen. Hier sehe ich noch sehr großen Handlungsbedarf. So sind Finnland und die asiatischen Länder wesentlich schneller unterwegs. Das liegt auch an datenschutzrechtlichen Bestimmungen in Deutschland. Die politischen und rechtlichen Hürden in Deutschland sollten zeitgemäß angepasst und die Datenhaltung so intelligent aufgebaut werden, dass sie kein Hemmschuh bleibt und gleichzeitig die personenbezogenen Daten schützt.

Stichwort Vernetzung – von Telematik im Fahrzeug über Fahrzeuge, die mit anderen Geräten kommunizieren, bis hin zum autonomen Fahren: Wo sehen Sie für die Automobilbranche die größte Herausforderung, um die Kommunikation zwischen so vielen Playern zu realisieren?
Die Vernetzung in Fahrzeugen lässt sich heute nicht mehr wegdenken. Bereits Ende der Neunzigerjahre haben wir unsere US-LKWs bei Freightliner an Logistik-Netzwerke angebunden, um „Route-Planning“ zu ermöglichen und über tausende Kilometer hinweg die Fahrrouten zu optimieren. Die LKWs hatten bereits Laptops, die sicher kommunizieren konnten. Dies war damals noch sehr mühsam, heute ist die Technik sehr viel weiter vorangeschritten.

Telematik-Dienste gibt es schon lange, aber erst Tesla hat diese mit Mut auf ein Niveau gebracht, an dem sich alle messen müssen. Das Auslesen von Fahrzeugdaten und das Flashing liefen bisher über die Werkstätten, kontrolliert vom Wartungstechniker. Heute geht Flashing auch über die Online-Telematik-Schnittstelle und ohne Werkstattaufenthalt. All diese Zugriffe müssen sicher sein und es darf nicht zu unkontrollierten Eingriffen kommen. Dies wird vor allem dann ein wesentlicher Faktor sein, wenn die Car2Car Kommunikation und die Anbindung an 5G-Netze das autonome Fahren ermöglichen sollen.

„Ganzheitliche Sicherheitsarchitekturen über alle Layer der Fahrzeug- und Umfeld-Komponenten werden maßgeblich über den Erfolg künftiger Fahrzeuggenerationen entscheiden."

Die große Herausforderung für die Automobilbranche besteht in der Ablage und Auswertung sowie Vernetzung von Sensordaten aus dem Fahrzeug und aus der erfassten Umwelt. Diese Datenmengen müssen mit hoher Rechnerleistung über KI ausgewertet und dem Automobil zur Fahrzeugsteuerung bereitgestellt werden. Die Aktoren steuern darüber dann das Fahrzeug.

All dies bedarf hoher softwaretechnischer Kompetenz und semantischer KI der nächsten Generation, sogenanntes 6G. Diese neue Dimension der virtuellen Systemintegration im Digital Twin des Automobils muss durch die Automobilindustrie erst noch ganzheitlich erschlossen und mit vielen Partnern gemeinsam abgestimmt werden.

Welche Rolle spielt die IT-Sicherheit dabei?
Vernetzung und Datenablage bedingen in solch komplexen automobilen Architekturen eine kompromisslose Hardware- und Software-Sicherheit. Dies beginnt im Fahrzeug auf Binary-Unit-System (BUS)-Ebene mit allen gängigen Protokollen und vernetzten Electronic Control Units, umfasst die Ad-hoc-Netze in der Car2Car-Kommunikation bis hin zur Vielzahl an Services in der Cloud. Schon heute spielen zum Beispiel die Wegfahrsperre sowie verfügbare Remote-Access-Funktionen mit Keyless-Go in der Fahrzeugsicherheit eine zentrale Rolle.

Alle Schnittstellen und die Kommunikation zwischen den Systemen erfordern Sicherheitstechnik. Dies beginnt im Fahrzeug mit BUS-Systemen und „Embedded Sicherheitskomponenten" in den bereits heute verfügbaren Netzwerken wie CAN, LIN, FLEXRAY, geht über die Car2X-Kommunikation in mobilen Ad-hoc-Netzwerken (MANets) mit Sicherheitsverfahren wie Secure Dynamic Source Routing (SDSR) bis hin zur Datenhaltung und KI in der Cloud.

Die Automobilentwicklung der Zukunft schließt erfolgsbedingt ganzheitliche Sicherheitsarchitekturen über alle Layer der Fahrzeug- und Umfeld-Komponenten ein. Dies wird maßgeblich über den Erfolg künftiger Fahrzeuggenerationen entscheiden.

Die hochfrequenten automobilen Produktionsprozesse sind stark anfällig für Störungen bei Zulieferern. Wie werden sich die Lieferketten zukünftig ändern und wie kann der OEM sicherstellen, dass er der kompletten Lieferkette vertrauen kann?
Das ist eine interessante Frage! Die Wertschöpfungsketten der OEMs sind heute extrem durchgetaktet und global ausgerichtet. Die Optimierungen stammen aus der „LEAN-Production-Zeit", mit all den zugehörigen Verfahren von „Just in Time", KABAN und „Just in Sequence". Hinzu kam die Auslagerung von vielen Produktionsschritten und Komponenten in Länder mit günstigen Kostenstrukturen.

Das Zusammenspiel der gesamten Zulieferkette vom First-Tier-Supplier bis zum Fifth-Tier-Supplier ist immens heterogen und schwierig zu steuern. Die OEMs versuchen, diese Ketten zu übersehen und über Planungsnetze zu steuern. Komplexe Modelle der vorausschauenden Planung sind bereits heute im Einsatz.

Trotzdem können Ereignisse wie Corona-Lockdowns oder ein Krieg nicht vorhergesehen und vorhergeplant werden. Diese Ereignisse haben allerdings gravierende Auswirkungen auf die Lieferfähigkeit der Netzwerke. Etwa 70 bis 75 Prozent aller Teile im Fahrzeug sind Zulieferteile. Diese hohe Anzahl bringt immer Abhängigkeiten mit sich. Ein ständiger Kostendruck im Fahrzeugbau hat über Outsourcing zu solchen Strukturen geführt.

Eine Möglichkeit der Korrektur ist, dass die OEMs und ihre First-Tier-Supplier wieder mehr Eigenfertigung in stabilen Ländern durchführen, wie zum Beispiel Mitteleuropa, USA, Kanada, Japan oder Südkorea. Dies führt aber sofort zu Kostensteigerungen und die Verbraucher sind nicht bereit, das Doppelte zu bezahlen.

Irgendwo in der Mitte wird sich der zukünftige Weg des Produktions- und Lieferverbundes im OEM-Netzwerk einschwingen. Stabile Lieferketten bedingen stabile Partner in stabilen Ländern sowie das Überdenken der globalen Lieferketten-Philosophie. Mehr Eigenanteil der OEMs in relevanten Bereichen der Karosserie, des Antriebs, der Elektronik und der Software reduziert Abhängigkeiten. Hinzu sind Partner zu wählen, die in einem stabilen Umfeld produzieren.

Dies alles gilt es zu überdenken und die Klimakrise wird uns zusätzlich zwingen, die Lieferketten wieder näher an die OEMs heranzurücken, mit allen Vorteilen und Nachteilen einer überschaubaren Globalisierung und Lokalisierung.

Sichere IT (nicht nur) für KRITIS

Von kritischen Infrastrukturen lernen

Unsichere Zeiten machen deutlich, in welch starken Abhängigkeiten wir leben und wie sehr wir im Alltag auf diese Fundamente bauen. Besonders bei kritischen Infrastrukturen (KRITIS) wie beispielsweise Energieversorgern oder Krankenhäusern treffen uns Einschränkungen oder Ausfälle hart. Deshalb unterliegt deren IT-Sicherheit gesetzlichen Regelungen. Von den Sicherheitstechnologien, die für KRITIS konzipiert wurden, können auch andere Unternehmen lernen, die mit sensiblen Daten umgehen. Und auch eine Cloud-Lösung kann ein Baustein einer Sicherheitsstrategie sein.

Im Hinblick auf die IT-Sicherheit sehen sich KRITIS-Betreiber mit einer Bedrohungslage konfrontiert, die sich rapide wandelt. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) stellte allein im letzten Lagebericht zur IT-Sicherheit in Deutschland rund 144 Millionen neue Schadprogramm-Varianten fest – ein Zuwachs von 22 Prozent gegenüber dem Vorjahr. Besonders Attacken mit Ransomware – Schadsoftware, die Daten verschlüsselt oder droht, diese zu leaken, um Gelder zu erpressen – haben stark zugenommen. Die Folgen eines solchen Angriffs können verheerend sein: 2021 konnte ein Universitätsklinikum nach einem erfolgreichen Angriff beispielsweise für 13 Tage keine Notfallpatient*innen mehr aufnehmen.

Um unter diesen Umständen zu bestehen, sollten Unternehmen und Betreiber Cybersicherheit nicht

DIE SICHERE CLOUD

Für öffentliche Institutionen und stark regulierte privatwirtschaftliche Unternehmen wie Energieversorger oder Gesundheitsdienstleister kam Cloud Computing bisher kaum in Frage. Um das zu ändern, hat secunet ein Cloud-Portfolio aufgebaut, das digitale Souveränität in die Cloud bringt. Einer der Eckpfeiler ist das Cloud-Betriebssystem SecuStack, das secunet und Cloud&Heat auf Basis von Open-Source-Software entwickelt haben. Mit SecuStack werden Daten durchgängig mit den gleichen Sicherheitsbausteinen verschlüsselt, die secunet seit vielen Jahren im Hochsicherheitsbereich einsetzt. Die kryptographischen Mechanismen sind transparent integriert und somit prüfbar. Die Hoheit über Daten und Anwendungen verbleibt jederzeit bei den Anwender*innen. Mit der Übernahme des Cloud- und Kubernetes-Spezialisten SysEleven (siehe folgende Doppelseite) hat secunet in diesem Jahr sein Cloud-Portfolio um einen weiteren Eckpfeiler erweitert. Nun bietet secunet ein umfassendes, maßgeschneidertes Cloud-Angebot für Behörden, Verwaltungen und sicherheitsaffine Unternehmen.

nur als einmalige Investition verstehen, erklärt Dr. Marius Feldmann, COO der Cloud&Heat Technologies GmbH und CEO der secustack GmbH: „IT-Sicherheit ist ja nicht einfach ein Zustand, den man erreicht. Das ist ein dauerhafter Prozess, zu dem ein dauerhafter Kompetenzaufbau gehört – und die entsprechenden Akteure, die vor Ort genau selbiges tun wollen." Das ist nicht nur im Schadensfall von Vorteil, es trägt ebenso zur Prävention künftiger Cyberattacken bei.

Das IT-Sicherheitsgesetz 2.0 als Chance

Im Mai 2023 tritt das neue IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) in Kraft, mit dem für KRITIS-Unternehmen schärfere Vorgaben gelten. Auch wird der Kreis der betroffenen Unternehmen deutlich erweitert – und zwar vor allem um die sogenannten „Unternehmen im besonderen öffentlichen Interesse" (UBI). Auch der Katalog der Mindestanforderungen wird umfangreicher. Wie aber sehen wirklich sichere IT-Infrastrukturen aus?

Auch viele Kliniken gehören zu den kritischen Infrastrukturen.

Das IT-SiG 2.0 macht dazu eine Reihe konkreter Vorgaben. Zum Beispiel dürfen sämtliche sicherheitsrelevanten Netz- und Systemkomponenten nur von vertrauenswürdigen Herstellern stammen. Auch müssen Unternehmen Systeme zur Angriffserkennung im Einsatz haben, durch die Angriffe im Idealfall gar nicht erst die Unternehmen erreichen, weil sie bereits frühzeitig erkannt und gestoppt werden.

Bei der Ausgestaltung der Sicherheitsmaßnahmen stehen aber immer die konkreten Anforderungen der jeweiligen Organisation im Vordergrund. Zunächst braucht es daher engagierte Akteure und auch Kompetenzen vor Ort oder die richtigen Partner an der Seite, um festzustellen, welche Anforderungen die Systeme erfüllen müssen. In einer umfassenden Analyse sollten nicht nur mögliche Risiken dokumentiert werden, sondern auch, wie das System von Anwender*innen genutzt wird und welche langfristigen Interessen berücksichtigt werden müssen. Vor allem bei strukturellen Entscheidungen zahlt es sich daher aus, langfristig zu denken. Auch wenn immer wieder einzelne Schwachstellen gezielt geschlossen werden können, zeigen die letzten Jahrzehnte, dass IT-Sicherheit nicht als jeweils akutes Problem, sondern als beständige Herausforderung gesehen werden sollte.

Zu den wichtigsten Säulen für sichere IT-Infrastrukturen zählen die Konstruktion und die Standards des Systems an sich. Dabei geht es um die Frage, ob Hersteller schon während der Entwicklung an Sicherheit und den Schutz vor äußeren Einflüssen gedacht haben. Systeme, die „secure by design" oder „secure by default" entwickelt wurden, zeichnen sich unter anderem durch eine sichere Konfiguration ab dem

Zeitpunkt der Installation aus. Das stattet Systeme mit einer grundlegenden Resilienz gegenüber Zugriffen von außen aus und hilft dabei, menschliche Fehlentscheidungen und daraus entstehende Sicherheitslücken bereits im Vorfeld zu verhindern.

Im Allgemeinen ist die Resilienz gegenüber menschlichen Fehlern ein entscheidendes Merkmal einer sicheren IT. Deshalb gilt es auch hier, Lösungen zu finden, die diesen Faktor berücksichtigen, denn er stellt im laufenden Betrieb ein Risiko für Phishing oder Social-Engineering-Angriffe dar, das minimiert werden sollte. Ein hoher Grad an Automatisierung, eine Standardisierung, wo möglich, und eine sichere Cloud-Infrastruktur können dabei helfen, das Potenzial für menschliche Fehler zu reduzieren, erklärt Dr. Kai Martius, CTO von secunet und CEO der secustack GmbH: „Es ist sehr wichtig, mögliche Fehlentscheidungen im Vorfeld zu verhindern und Systeme auch in dieser Hinsicht möglichst sicher zu konstruieren. Ich glaube, dabei hat die kritische Industrie in ihrem angestammten Feld sehr viel Erfahrung. Doch diese Möglichkeiten wurden noch längst nicht in allen IT-Systemen umgesetzt. Hier können Cloud-Technologien durch ein hohes Maß an Automatisierung weiterhelfen."

Entscheidend ist die Partnerwahl

Selten sind alle Kompetenzen vorhanden, um die benötigten IT-Infrastrukturen selbst aufzusetzen oder zu verwalten. Es kommt also darauf an, die richtigen Partner zu wählen – und dabei unnötige Abhängigkeiten zu vermeiden: Die Einführung einer neuen Cloud-Infrastruktur zum Beispiel erfordert eine zeit- und kostenintensive Integrationsarbeit mit den bestehenden Systemen. Das macht einen nachträglichen Wechsel zu einem anderen Anbieter manchmal nur schwer möglich, selbst wenn diese andere Lösung besser zu den eigenen Anforderungen passt. Genau diese Vendor Lock-in Szenarien gilt es zu vermeiden. Hier sollten also mittel- und langfristige Interessen vor kurzfristigen Kostenvorteilen im Mittelpunkt stehen.

Zuletzt geht es in puncto Sicherheit aber auch immer um Vertrauen. Wird sich der Sicherheitspartner mit Priorität um alle Herausforderungen kümmern, die auftreten könnten? IT-Sicherheit als Prozess zu verstehen, bedeutet auch, aus Angriffen zu lernen und so potentielle Risiken weiter zu minimieren. Dieses Verständnis sollte der Partner teilen.

Dr. Kai Martius
kai.martius@secunet.com

Dr. Marius Feldmann (links) und Dr. Kai Martius

SECUNET LÖSUNGEN FÜR KRITIS UND UBI

Die für ein transparentes IT-Sicherheitsmonitoring und eine frühzeitige Angriffserkennung entwickelte Lösung **secunet monitor** erstellt ein Lagebild, um potenzielle Sicherheitsvorfälle schnell sichten, bewerten, eindämmen oder direkt unterbinden zu können. Zusätzlich erleichtert die Lösung die Bewertung durch das Management und die zuständigen Behörden. So werden Unternehmen in die Lage versetzt, viel zielgerichteter kurz-, mittel- und langfristige Strategien und Maßnahmen zu entwickeln und umzusetzen.

Mit der Sicheren Inter-Netzwerk Architektur **SINA** können Unternehmen sämtliche Sicherheitsvorgaben abdecken, die das BSI für die Arbeit mit sensiblen Daten und Unterlagen vorsieht. Mitarbeiter können mit SINA auf ihren Endgeräten unabhängig von ihrem Standort auf sensible Daten zugreifen, wobei die Lösung selbst die Anforderungen für Verschlusssachen in Behörden erfüllt. Dabei kann SINA aufgrund der großen Vielfalt an verfügbaren Komponenten auf sehr unterschiedliche Sicherheitsanforderungen zugeschnitten werden – auch auf diejenigen von KRITIS und UBI.

Zudem bietet secunet umfangreiche **Beratungs-, Penetrations- und Forensik**-Dienstleistungen an. Mehr Informationen: https://www.secunet.com/versorger

Sicheres Cloud Computing

secunet übernimmt SysEleven und baut Cloud-Portfolio aus

Im Mai 2022 erwarb secunet 100 Prozent der Anteile an der SysEleven GmbH. Mit der Akquisition baut secunet das Lösungsangebot in den Bereichen Cloud und Cloud Security deutlich aus.

SysEleven ist ein unabhängiger deutscher Anbieter von Cloud-Infrastruktur, Cloud Services, Managed Services und Managed Kubernetes. Das Unternehmen verfügt über eine eigene, Open-Source-basierte Cloud-Infrastruktur mit ISO27001 zertifizierten Rechenzentrumsstandorten in Deutschland (Infrastructure-as-a-Service) und stellt mit MetaKube eine Plattform für die effiziente Verwaltung und Optimierung von Rechen-, Speicher- und Netzwerkressourcen auf Basis von Kubernetes bereit (Managed Kubernetes).

„Mit der Übernahme von SysEleven beschleunigen wir unsere Aktivitäten im stark wachsenden Markt für sichere Cloud-Infrastruktur. Wir stärken unsere technologische Position und gewinnen ein Team hochqualifizierter Experten mit ausgewiesenen Fähigkeiten in der Projektumsetzung und bei Managed Services sowie großer Expertise in OpenStack und Kubernetes“, kommentiert Axel Deininger, Vorstandsvorsitzender von secunet. „Nachdem wir bereits mit SecuStack ein Open-Source-basiertes Cloud-Betriebssystem für Kunden entwickelt haben, die ihre Cloud ‚on premise’ betreiben, können wir nun auch eine Lösung ‚as a Service’ anbieten und gemeinsam weiterentwickeln. Unsere Kunden, die in der Regel mit sicherheitskritischen Anwendungen und vertraulichen Informationen arbeiten, profitieren in doppelter Hinsicht: einerseits von der Flexibilität in Bezug auf Verfügbarkeit, Kosten und Leistung, andererseits von der hohen Qualität und der Sicherheitsexpertise, für die secunet seit über 25 Jahren steht.“

Die SysEleven GmbH wurde im Jahr 2007 gegründet und beschäftigt über 100 Mitarbeiterinnen und Mitarbeiter. Die Gesellschaft mit Sitz in Berlin betreut über 175 Kunden im DACH-Markt und verfolgt einen langfristigen Partnerschaftsansatz mit Fokus auf Kunden, die Wert auf Sicherheit und Unabhängigkeit von Hyperscalern legen. Das Unternehmen, das Mitglied der europäischen Initiative zum Aufbau einer leistungs- und wettbewerbsfähigen, sicheren und vertrauenswürdigen Dateninfrastruktur (GAIA-X) ist, wird auch nach der Übernahme durch secunet von den bisherigen Geschäftsführern Marc Korthaus, Jens Ihlenfeld und Andreas Hermann operativ geleitet. „Wir gießen digitale Souveränität in praktikable Produkte und werden die energische Weiterentwicklung unserer Cloud-Lösungen nun mit noch höherem Tempo angehen und um weitere Sicherheitsaspekte ergänzen“, sagt Marc Korthaus über die Vorteile der neuen Konstellation.

Abhörsichere Sprachkommunikation

SINA Communicator H mit iF Design Award ausgezeichnet

Für Telefonate auf dem hohen Sicherheitslevel GEHEIM müssen viele technologische Hürden überwunden werden. Daher hatten die Produktentwickler von secunet zunächst vor allem Technologie im Kopf, als sie die Aufgabe angingen, ein hochsicheres Gerät für Sprachkommunikation zu entwickeln. Wie lassen sich die vielen Besonderheiten und Vorgaben der Kommunikation im GEHEIM-Umfeld ins Zeitalter der IP-Telefonie übertragen? All-IP-Technologie auf höchstem Sicherheitsniveau – klar. Moderne NATO-Protokolle – selbstverständlich. Abhörsicher und abstrahlgeschützt – selbstredend. Aber die Entwickler von secunet mögen Herausforderungen. Und daher fragten sie sich bald, ob es genügt, nur die technischen Aspekte abzudecken.

Wir alle nutzen im Alltag Smartphones, die zusätzlich zum Telefonieren eine Vielzahl anderer Funktionen bieten und dabei auch noch ziemlich gut aussehen. Sollen Mitarbeitende in Ministerien und bei den Streitkräften etwa auf all dies verzichten, wenn sie abhörsicher kommunizieren? „Nicht mit uns“, sagten sich die secunet Entwickler und schufen ein Produkt, das nicht nur State-of-the-art-Sicherheit bietet – zum Beispiel ist es das erste nationale Gerät, das Post-Quanten-Kryptographie-fähig ist –, sondern auch ausgezeichnete Nutzbarkeit und hervorragendes Design.

Mit seinem großen Touch-Display hat der SINA Communicator H mehr Ähnlichkeit mit einem Tablet als mit einem Telefon. Sein Bedienkonzept ist so einfach und intuitiv, dass jeder, der ein Smartphone besitzt, mühelos die vielfältigen Funktionen aufrufen und zwischen unterschiedlichen Geheimhaltungsstufen wechseln kann.

Das sieht auch die iF Jury so und verlieh im Mai 2022 dem SINA Communicator H den renommierten iF Design Award. Der Preis zeichnet nicht nur das tolle Design, sondern auch die Usability aus. So wurde der SINA Communicator H zum weltweit einzigen preisgekrönten Gerät für GEHEIM-Kommunikation.

Etwas unerwartet machte der SINA Communicator H im September 2022 auch in der breiten Öffentlichkeit Furore: Zunächst twitterte Bundeskanzler Olaf Scholz ein Foto von sich am Schreibtisch, auf dem eine rote Version des Geräts steht. Dafür wiederum interessierte sich Deutschlands reichweitenstärkste Tageszeitung, die BILD, und brachte das Foto auf die Titelseite. „Wenn beim Kanzler das rote Telefon klingelt“, war daneben zu lesen. Außerdem spürte die BILD einen „Hauch von James Bond im Kanzleramt“. Wer möchte da widersprechen?

Sichere und vertrauenswürdige Patientenversorgung

secunet beteiligt sich an dem Projekt SEMECO

Mehr Flexibilität, schnellere Zulassungsprozesse und kürzere Innovationszyklen – das strebt das Projekt Secure Medical Microsystems and Communications (SEMECO) an. Innovationen in der Medizintechnik sollen so schneller denen nutzen, für die sie gedacht sind: den Patient*innen. Gefördert wird SEMECO innerhalb der „Zukunftscluster-Initiative“ (Clusters4Future) des Bundesministeriums für Bildung und Forschung. Mit Know-how in der Entwicklung von Hochsicherheitslösungen sowie der langjährigen Erfahrung im regulatorischen Umfeld beteiligt sich secunet an zwei Querschnittsprojekten.

Um die Patientenversorgung weltweit sicherer und vertrauenswürdiger zu gestalten, zielt SEMECO auf ein Ökosystem sowie verlässliche Partner, die gemeinsam die Medizintechnik- und Mikroelektronikindustrie revolutionieren möchten. Dabei sind IT-Sicherheit und Datenschutz Grundvoraussetzung für die Etablierung einer vertrauenswürdigen Systemarchitektur und der angestrebten Technologieplattform. Denn der Schutz netzwerkfähiger Medizintechnik, medizinischer Software sowie Patientendaten vor digitalen Angriffen ist essenziell für das Gelingen moderner Lösungen in der Medizin.

„Als führendes deutsches IT-Sicherheitsunternehmen kann secunet dabei einen entscheidenden Beitrag liefern, der nachhaltig den Schutz von Patient*innen, medizinischen Daten und von Medizintechnik erlaubt“, sagt Dr. Tobias Urban, Business Development Manager eHealth bei secunet. Konkret beteiligt sich das Projektteam an der Entwicklung von sicheren und vertrauenswürdigen Systemarchitekturen sowie einer KI-assistierten Regulatorik für Medizin und Cybersecurity. Dabei liegt der Fokus zum einen auf der digitalen Absicherung der medizinischen Geräte und Software und zum anderen auf der Entwicklung dieser entlang geltender und gegebenenfalls noch zu definierender Industriestandards.

Durch den ganzheitlichen Ansatz des Clusters bietet sich für secunet und alle anderen Projektpartner die Möglichkeit, Lösungen zu erforschen, die einfach zu Produkten weiterentwickelt werden können und so schnell und effizient die medizinische Versorgung verbessern können – sicher und vertrauenswürdig.

Das Projekt ist noch in der Anfangsphase – stay tuned für Updates und erste Ergebnisse!

Dr. Tobias Urban

VIT unterstützt Projekte zwischen Wissenschaft und Industrie

Innovation und Forschung in Wirtschaft und Gesellschaft integrieren – das ist Ziel des Vereins für Innovation und Transfer an der Technischen Universität Ilmenau (VIT w. V.). Seit 2019 finanziert der wirtschaftliche Verein Projekte zwischen Wissenschaftler*innen der Universität und der Industrie. Vergangene Woche hat Thüringens Innenminister Georg Maier (rechts im Bild) feierlich die Gründungsurkunde an Prof. Gunther Notni (links im Bild) der TU Ilmenau übergeben. secunet unterstützt Forschungsaufträge des VIT w. V. vor allem im Fachgebiet Telematik/Rechnernetze im Kompetenzfeld Netz- und IT-Sicherheit.

Strategien gegen den Fachkräftemangel

secunet bildet wieder aus

Die neuen Auszubildenden mit den Ausbilder*innen Irene Wolff (rechts) und Olaf Stottrop (2.v.l.)

secunet hat den Ausbildungsbetrieb am Standort Essen im Sommer wieder aufgenommen. Ab 1. August 2022 begrüßte das Team zwei angehende Kaufleute für Büromanagement und zwei Auszubildende Fachinformatiker*innen mit dem Schwerpunkt Systemintegration. Als Unternehmen strebt secunet eine mittel- und langfristige Zusammenarbeit mit Fachkräften an, die seine Werte und seine Vision teilen.

Der Ablauf der Ausbildung ist in einen praktischen und einen theoretischen, schulischen Teil aufgeteilt. Die Auszubildenden sind im Wechsel am secunet Standort und in der jeweiligen Berufsschule. Den jungen Kolleg*innen steht jeweils ein/e Ausbilder*in zur Seite, der oder die sie über die drei Jahre der Ausbildung begleitet. Diese kann nach Rücksprache auch auf zweieinhalb Jahre verkürzt werden.

Zusätzlich zum Ausbildungsbetrieb startet ab 1. Oktober 2022 das Trainee@secunet Programm. Im Bereich Cybersecurity werden gleich drei Nachwuchstalente gesucht: in Consulting, Sales und Software Development. In zwei Jahren durchlaufen die Trainees insgesamt vier Stationen und lernen dabei nicht nur die Divisionen und Bereiche, sondern auch die verschiedenen secunet Standorte kennen.

Termine – Oktober bis Dezember 2022

25. bis 27. Oktober 2022
it-sa | Nürnberg

25. bis 27. Oktober 2022
NATO Edge | Mons, Belgien

2. November 2022
Protekt | Leipzig

3. November 2022
SPS Nürnberg | Nürnberg

3. November 2022
Digitaler Polizeitag | Online

8. bis 9. November 2022
HB Konferenz Health – The Digital Future | Düsseldorf

15. bis 17. November
International Face Performance Conference | Digital

15. bis 17. November 2022
SpaceTechExpo | Bremen

14. bis 17. November 2022
MEDICA | Düsseldorf

16. November 2022
Entscheiderfabrik: Ergebnis-Präsentation 45. Deutscher Krankenhaustag | Düsseldorf

30. November bis 1. Dezember 2022
Berliner Sicherheitskonferenz | Berlin

Haben Sie hierzu Fragen oder möchten Sie sich anmelden? Schicken Sie uns gern eine E-Mail an events@secunet.com.

Impressum

Herausgeber
secunet Security Networks AG
Kurfürstenstraße 58, 45138 Essen
www.secunet.com

Leitung Redaktion, Konzeption und Gestaltung (V.i.S.d.P.)
Marc Pedack, marc.pedack@secunet.com

Design und Satz
sam waikiki GbR, www.samwaikiki.de

Der Inhalt gibt nicht in jedem Fall die Meinung des Herausgebers wieder.

Bildnachweis
Titel, S. 10, 11: Volkswagen AG
S. 2 (unten), 5, 8, 18, 21, 29: Getty Images
S. 2, 24: kbarzycki / Adobe Stock
S. 3, 7, 14, 16, 17, 20, 26, 28 (Mitte und unten), 29 (unten), 30 (unten): secunet
S. 6: Schoening / Alamy Stock Photo
S. 12: Scharfsinn/Alamy Stock Photo
S. 15: Rheinisch-Westfälische Technische Hochschule Aachen
S. 22: Klaus Hardy Mühleck
S. 25: senivpetro / freepik
S. 28 (oben): iF International Forum Design GmbH
S. 30 (oben): Technische Universität Ilmenau

klimaneutral gedruckt
www.klima-druck.de
ID-Nr. 22125467
bvdm.

FSC
www.fsc.org
MIX
Papier aus verantwortungsvollen Quellen
FSC® C006990

Was tun Sie bei einem Hackerangriff?

Entspannt bleiben – denn mit secunet sind Daten und Infrastruktur premiumsicher.

Wo Daten und IT-Infrastrukturen vor Cyberangriffen geschützt werden müssen, steht secunet bereit. Als IT-Sicherheitspartner der Bundesrepublik Deutschland bieten wir Behörden und Unternehmen Expertenberatung und premiumsichere Lösungen zum Schutz von Kommunikation und Daten.

secunet.com protecting digital infrastructures

secunet