secuview

Das secunet Kundenmagazin 1•2021

„Das fortschrittlichste Einreise-/Ausreisesystem der Welt“

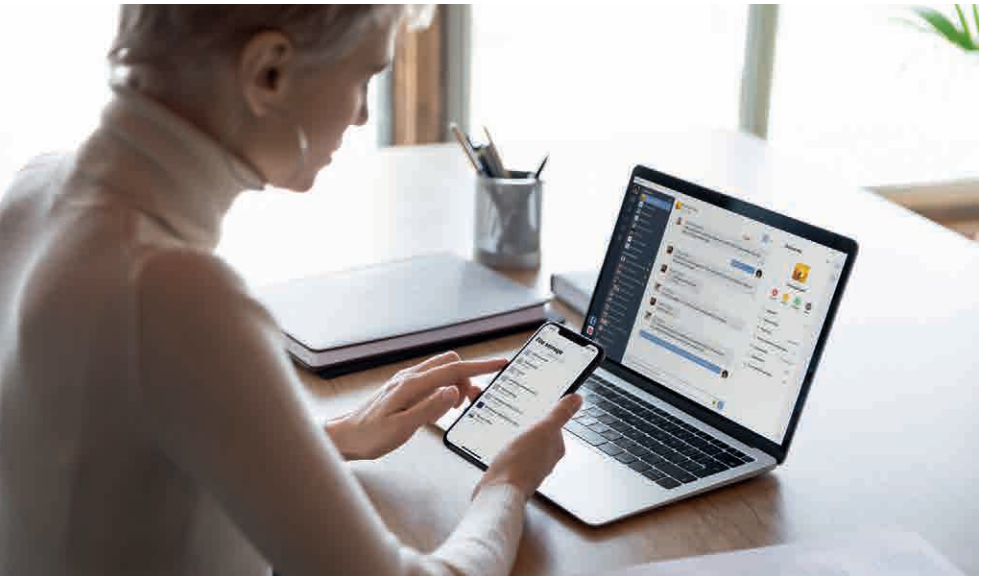
Matthias Oel von der Europäischen Kommission über das kommende Entry-/Exit-System der EU

Transformation statt Revolution

Digitalisierung und „New Work“ beim Bundesamt für Migration und Flüchtlinge

Gesundes Sicherheitsniveau

Web-Isolation beim Klinikum Fürth



National

International: Titelthema EES

International

Technologien & Lösungen

In eigener Sache

Kurz notiert

Service

Liebe Leserinnen und Leser,

Ende letzten Jahres habe ich an dieser Stelle noch die Hoffnung geäußert, dass uns das Jahr 2021 eine Rückkehr in die Normalität bescheren wird. Diese Rückkehr verläuft nun langsamer als erhofft, die Pandemie ist noch nicht überstanden, und doch fühlt sich das Leben in vielen Bereichen schon wieder etwas normaler an. Das liegt einerseits daran, dass einige Einschränkungen bereits aufgehoben wurden. Andererseits wird wohl auch so manche bleibende Neuerung, wie etwa ein hoher Homeoffice-Anteil, mittlerweile von vielen als normal wahrgenommen.

Eines ist klar: Der tiefgreifende Wandel der Arbeitswelt, den viele Beobachter*innen schon zu Beginn der Pandemie prognostiziert haben, findet tatsächlich statt. Das zeigen zahlreiche Kundenprojekte von secunet, in denen es um sichere Infrastrukturen für mobiles Arbeiten geht. In der vorliegenden secuview beschreiben wir, wie das Bundesamt für Migration und Flüchtlinge mit SINA Technologie Schritt für Schritt in die neue mobile Arbeitswelt eingetreten ist.

Eine Akquisition, die secunet in diesem Jahr vorgenommen hat, passt ebenfalls zum „neuen Normal“. Das Unternehmen stashcat aus Hannover sorgt dafür, dass auch Organisationen mit hohem Sicherheitsbedarf, wie zum Beispiel die Polizei, eine Messenger-App nebst fortgeschrittenen Kollaborationsfunktionen nutzen können. Die Geschichte dieses spannenden Unternehmens und Produkts können Interessierte ab Seite 24 nachlesen. Ich freue mich auf den weiteren gemeinsamen Weg mit stashcat.

Auch unser Titelthema hat mit der Normalisierung zu tun, wenn auch etwas indirekter: Die EU-Staaten bereiten sich aktuell auf das europäische Einreise-/Ausreisesystem (EES) vor, mit dem ab Mitte 2022 die Schengen-Außengrenzen noch besser abgesichert werden sollen. Dabei geht es auch darum, wie durch moderne Grenzkontrolltechnologie lange Schlangen an den Grenzübergängen verhindert werden, die als Folge der neuen biometrischen Registrierung von Drittstaatsangehörigen entstehen können. Überfüllte Flughäfen sind ein Szenario, das zu Pandemiezeiten unwirklich erscheint – aber die Grenzbehörden stellen sich auf wieder steigende Passagierzahlen ein, wenn die Beschränkungen nach und nach fallen.

Matthias Oel, Direktor für Schengen, Grenzen und Innovation in der Generaldirektion Migration und Inneres der EU-Kommission, erläutert im Interview ab Seite 8 seine Sicht auf das EES. Und er erzählt, dass auch bei diesem Projekt pandemiebedingte Hürden überwunden werden mussten.

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

Ihr Axel Deininger

Digitalisierung und „New Work“ beim Bundesamt für Migration und Flüchtlinge

Transformation statt Revolution

So wie die meisten Behörden und Unternehmen stand auch das Bundesamt für Migration und Flüchtlinge (BAMF) im Jahr 2020 bedingt durch die Corona-Pandemie vor der Herausforderung, Büroarbeitsplätze ins Homeoffice zu verlagern. Noch dazu musste dies auf einem sehr hohen Sicherheitslevel geschehen. Anders als andere war das BAMF vorbereitet, denn es nutzte zu dem Zeitpunkt bereits eine SINA Lösung, die sicheres mobiles Arbeiten ermöglicht. Seitdem treibt die Behörde den Wandel zu einer neuen Arbeitswelt voran – gut dosiert und Schritt für Schritt.

Ursprünglich ging es bei der Implementierung einer mobilen, sicheren IT-Infrastruktur im BAMF gar nicht um das Thema Homeoffice. Vielmehr entstand der Bedarf im Jahr 2015 im Zusammenhang mit der Flüchtlingskrise. Während dieses Jahres registrierte das BAMF rund 890.000 Schutzsuchende, die nach Deutschland eingereist waren. Das Personal wurde massiv aufgestockt. Die BAMF-Mitarbeiter*innen, die in den Erstaufnahmestellen an den EU-Außengrenzen Dienst taten, benötigten eine IT-Infrastruktur, mit der sie sensible Informationen wie personenbezogene Daten sicher verarbeiten und übermitteln konnten.

Das Bundesamt für Migration und Flüchtlinge (BAMF) ist eine Bundesbehörde im Geschäftsbereich des Bundesministeriums des Innern (BMI). Als Kompetenzzentrum für Migration und Integration in Deutschland ist das Bundesamt nicht nur zuständig für die Durchführung von Asylverfahren und den Flüchtlingsschutz, sondern auch Motor der bundesweiten Förderung der Integration. Zur Bandbreite der Aufgaben gehört auch die Migrationsforschung. Mit seinen dezentralen Standorten, darunter Außenstellen, Ankunftszentren sowie Entscheidungszentren, steht es in direktem Kontakt mit allen Akteuren des Flüchtlingsschutzes und der Integrationsarbeit.

Zu diesem Zweck installierte secunet eine SINA Lösung mit 1.500 SINA Workstations – und das innerhalb weniger Wochen, denn in der damaligen Situation war Zeit ein besonders knappes Gut. „Ein großer Besprechungsraum des BAMF wurde kurzerhand zum Installationsbüro umfunktioniert", erinnert sich Norbert Müller, Divisionsleiter Öffentliche Auftraggeber bei secunet. „Wir mussten sehr pragmatisch vorgehen, damit wir das knappe Timing halten konnten." Die SINA Workstations waren in Kofferlösungen integriert, die die wichtigsten Instrumente zur Registrierung der Flüchtlinge enthielten wie zum Beispiel Fingerabdruckscanner und Dokumentenleser. Die erfassten Daten konnten dann direkt bearbeitet und sicher übermittelt werden.

Wachstum bringt IT-Herausforderungen mit sich

Die gestiegene Arbeitsbelastung aufgrund der Flüchtlingskrise war bald auch in administrativen und zentralen Bereichen des BAMF deutlich bemerkbar. Daher musste die Behörde zahlreiche Maßnahmen ergreifen, um die neuen Anforderungen zu erfüllen und dem Arbeitsvolumen gerecht zu werden. Dazu gehörten zum Beispiel ein weiterer Personalaufwuchs und die Verbesserung von Arbeitsabläufen.

Für das Jahr 2018 bewilligte der Gesetzgeber dem BAMF rund 7.800 Stellen, für das Jahr 2019 rund 8.100. Es werden somit dauerhaft über 8.000 Mitarbeiter*innen im BAMF tätig sein. Im Vergleich zum Personalstand vor 2014 bedeutet dies nahezu eine Vervierfachung.

Zudem ändern sich die Erwartungen der Mitarbeitenden: Attraktiven Arbeitsbedingungen kommen in der heutigen Arbeitswelt eine immer größere Bedeutung zu. Das BAMF ist als obere Bundesbehörde dazu verpflichtet, die Familienfreundlichkeit sowie die Vereinbarkeit von Familie und Beruf zu verbessern. Bei all diesen Entwicklungen kommt der IT des Bundesamts eine Schlüsselrolle zu.

Dabei besteht die zusätzliche Herausforderung, dass ein sehr hohes Sicherheitsniveau gefragt ist: Auf den Rechnern der Mitarbeiter*innen befinden sich teilweise hoheitliche Daten, zum Beispiel besonders schützenswerte Informationen zu politisch verfolgten Asylsuchenden.

Im BAMF erkannte man schnell, dass SINA diese Punkte erfüllt, Homeoffice und mobiles Arbeiten ermöglicht und dies von den Beschäftigten sehr geschätzt wird.

Gleiche Lösung, neuer Zweck

Unter anderem aus diesen Gründen entschied sich die Behörde, als im Jahr 2019 die Wartungsverträge ausliefen, bei SINA zu bleiben und ein Refresh mit Erweiterungen durchzuführen. Dabei wurde die Installation auf den neuesten Stand gebracht, veraltete Komponenten wurden ersetzt.

Im Frühjahr 2020 stand dann plötzlich die Coronakrise vor den Toren. Während viele Behörden und Unternehmen unter großem Zeitdruck ihre ersten Erfahrungen mit mobilen Arbeitsplätzen sammeln mussten, gehörte das BAMF zu den Organisationen, die schon einen Schritt weiter waren. Die SINA Lösung war bereits erfolgreich im Einsatz. Nun lag es nahe, sie zu erweitern.

Laut Kausik Munsi, Chief Technology Officer (CTO) des BAMF, gab es vier Gründe, warum die Behörde damals erneut auf SINA setzte: „Erstens mussten wir einen Partner finden, der sehr zuverlässig liefern konnte, da ging es auch um Vertrauen. Zweitens war uns natürlich auch die Technologie wichtig und SINA war sowohl hochsicher, wie durch die BSI-Zulassung bestätigt wurde, als auch – das ist der dritte Punkt – sehr einfach zu bedienen. Viertens hatten wir einen flexiblen Rahmenvertrag, mit dem wir SINA abrufen konnten."

Der Aspekt der Lieferfähigkeit war mitten in der Pandemie nicht trivial, denn bei IT-Bauteilen gab es auf dem Weltmarkt Engpässe. Doch schon während der Flüchtlingskrise hatte secunet unter Beweis gestellt, in kritischen Zeiten ein verlässlicher Partner zu sein. Auch diesmal konnte schnell und in hohen Stückzahlen geliefert werden. Das BAMF beschaffte in mehreren Wellen jeweils mehrere tausend SINA Workstations. Inzwischen sind bereits nahezu alle Arbeitsplätze beim BAMF mit SINA Workstations ausgestattet. Während viele Organisationen durch die Revolution der Arbeitswelt, die die Pandemie schlagartig erzwungen hat, überrumpelt wurden, gestaltete das BAMF den Wandel in vielen kleineren Schritten.

„Wir mussten einen Partner finden, der sehr zuverlässig liefern konnte, da ging es auch um Vertrauen."

Kausik Munsi, CTO des BAMF

Daher erfolgt auch der Rollout kontinuierlich. Drei Parteien arbeiten dabei zusammen: Das BAMF, dessen IT-Dienstleister ITZ Bund und secunet. Berater von secunet sind fortwährend vor Ort, um die Implementierung voranzubringen und Betriebsunterstützung zu leisten. „Die enge und partnerschaftliche Zusammenarbeit wissen wir sehr zu schätzen", so Norbert Müller von secunet. „Sie hat großen Anteil am Projekterfolg."

Blick in die Zukunft

„Der Trend zur mobilen Arbeit bleibt ganz klar weiter bestehen", so Munsi. „Außerdem gibt es beim BAMF eine Besonderheit: Wir haben eine sehr große Entwicklungsmannschaft, die zum Teil im Ausland sitzt und zum Teil zwischen verschiedenen Standorten unterwegs ist. Auch deswegen werden wir SINA weiterhin brauchen."

Die Zusammenarbeit zwischen dem BAMF und secunet hat auch über SINA hinaus Früchte getragen. So setzt die Behörde mittlerweile den secunet Session Border Controller (SBC) ein, um die Telefonie abzusichern und eine Audio- und Video-Trennung nach BSI-Vorgaben umzusetzen. Weitere IT-Zukunftsthemen sind derzeit in Diskussion. Kausik Munsi: „Unsere Mitarbeiterinnen und Mitarbeiter möchten unseren Kunden und Partnern die optimale Dienstleistung anbieten. Mit unserer IT möchten wir sie so unterstützen, dass sie dies erreichen können und darüber hinaus auch gern zur Arbeit kommen. Deswegen wollen wir eine medienbruchfreie Kommunikation ermöglichen und eine optimale, vernetzte Arbeitsumgebung schaffen."

Christian Eisenried
christian.eisenried@secunet.com

Mit einer **SINA Lösung** können Mitarbeiter*innen von Behörden oder Unternehmen sicher mit sensiblen oder gar eingestuften Informationen umgehen. Dabei ist es unerheblich, ob sie sich im Büro, zu Hause oder unterwegs aufhalten. Durch eine Vielzahl ineinandergreifender Sicherheitskomponenten sorgt SINA dafür, dass Dritte keine Daten mitlesen können, wenn Nutzer*innen sich per Virtual Private Network (VPN) ins Behördennetz einwählen. Die SINA Workstation fungiert im SINA Netzwerk als Client, der Sicherheit mit Bedienbarkeit vereint und in verschiedenen Desktop-, Laptop- und mobilen Formaten verfügbar ist. Selbst wenn eine **SINA Workstation** verlorengeht, bleiben die Daten dank Zwei-Faktor-Authentisierung und Festplattenverschlüsselung geschützt. SINA Komponenten sind für verschiedene Einsatzzwecke verfügbar und in ihren unterschiedlichen Varianten vom Bundesamt für Sicherheit in der Informationstechnik (BSI) für verschiedene Geheimhaltungsstufen freigegeben.

Mehr Informationen: www.secunet.com/sina

Themenspecial:
EU Einreise-/Ausreisesystem

Der Schengen-Raum umfasst 26 Staaten mit mehr als

1.800

GRENZKONTROLLSTELLEN

an Land-, Luft- und Seegrenzen

Quelle: eu-LISA Conference Report 2015

48° 35' N
7° 45' O

In Straßburg erfolgt das Betriebsmanagement des zentralen Entry-/Exit-Systems durch die eu-LISA.

Quelle: eu-LISA, EES-Leaflet

2019 reisten über 115 Millionen Drittstaatsangehörige in die Europäische Union ein, bis 2025 wird die Zahl voraussichtlich um

+53%

auf 176 Millionen steigen.*

* Aufgrund des COVID-bedingten Passagierrückgangs in 2020/2021 variieren die Prognosen in diesem Punkt derzeit sehr stark. Dennoch ist mit einem starken Anstieg ab 2025 zu rechnen.

Quelle: Frontex; Technical Guide for Border Checks on EES related equipment (05/2021)

Durch den Brexit wird die britische Bevölkerung, also

+66,65 Millionen

Menschen, bei Reisen in die Staaten des Schengen-Raums nun als Third Country Nationals angesehen.

Quelle: Embassy of Belgium in the United Kingdom

Die neue europäische Identitätsdatenbank, das Common Identity Repository (CIR), wird

300 MIO. EINTRÄGE

beinhalten. Hier fließen auch die Daten des Einreise-/Ausreisesystems mit ein.

Quelle: www.biometricupdate.com

89

SEKUNDEN

Abfertigungszeit für Third-Country-Nationals am Grenzkontrollschalter vor und nach Einführung des des Einreise-/Ausreisesystems

34

Quelle: Pilotbericht Smart Borders, Bundesverwaltungsamt

Im Interview: Matthias Oel

„Das fortschrittlichste Einreise-/Ausreisesystem der Welt“

Das europäische Einreise-/Ausreisesystem (EES) wurde von der EU-Kommission als Teil ihrer Smart Borders Agenda initiiert. Heute überwacht und koordiniert die Kommission die europaweite Einführung des EES aus einer rechtlichen Perspektive. secuview sprach mit Matthias Oel, Direktor für Schengen, Grenzen und Innovation bei der Generaldirektion (DG) Migration und Inneres der Europäischen Kommission.

Könnten Sie bitte kurz die Rolle der DG Migration und Inneres im Hinblick auf das EES beschreiben?

Matthias Oel: Die Europäische Kommission ist für die Überwachung der korrekten und fristgerechten Anwendung des EU-Rechts zuständig. Im Rahmen der Vorbereitungen für den Rollout des Einreise-/Ausreisesystems konzentrierten sich die Hauptaufgaben der Kommission auf allgemeine Koordinierung und Steuerung. In den vergangenen drei Jahren bedeutete dies vor allem die Ausarbeitung rechtlicher Vorgaben, die festlegen, wie das System auf technischer Ebene umgesetzt werden soll. Zu diesem Zweck haben wir einen Ausschuss ins Leben gerufen, in dem unsere technischen Experten, die EU-Länder und eu-LISA vertreten sind. eu-LISA ist die Europäische Agentur für das Betriebsmanagement von IT-Großsystemen im Raum der Freiheit, der Sicherheit und des Rechts; sie ist für die Entwicklung des Systems zuständig. Wir konzentrieren uns derzeit hauptsächlich auf die Überwachung der Vorbereitungen für die rechtzeitige Einführung des Einreise-/Ausreisesystems in den EU-Ländern. Mit diesen stehen wir in sehr engem Kontakt und halten technische Meetings und Besichtigungen ab.

Wie geht es mit der Einführung des EES voran?

Die Entwicklung des Einreise-/Ausreisesystems schreitet sehr gut voran. Gemeinsam mit eu-LISA und den EU-Ländern bereiten wir uns auf die Einführung des Systems vor und arbeiten daran, potenzielle Probleme im Vorfeld zu lösen. Nach derzeitiger Planung werden wir in der ersten Hälfte des Jahres 2022 über das fortschrittlichste Einreise-/Ausreisesystem der Welt verfügen. Das System wird mit anderen IT-Großsystemen der EU zusammenarbeiten und dazu beitragen, die Migration zu steuern und die Sicherheit zu erhöhen. Es wird Bona-fide-Reisenden das Überschreiten der

EU-Grenzen erleichtern und beschleunigen sowie gleichzeitig „Overstayer" – Personen, die nach Ablauf ihres genehmigten Aufenthalts im Schengen-Raum bleiben – und Fälle von Dokumenten- und Identitätsbetrug effizienter identifizieren.

Das Einreise-/Ausreisesystem soll das manuelle Abstempeln der Pässe ersetzen und ist ein erster wichtiger Schritt zu einem automatisierten und reibungsloseren Grenzübertritt. Dank des EES sollten mehr Reisende in der Lage sein, automatisierte Grenzkontrollen und Selbstbedienungssysteme zu nutzen. Dies ist schneller, als an einem Grenzkontrollschalter anzustehen, und bequemer für die Reisenden. Für die Zukunft würden wir uns zudem wünschen, dass zurückkehrende Reisende eine mobile App für ihre Grenzkontrolle nutzen können.

Wir treten jetzt in die letzte Vorbereitungsphase ein. Die erforderliche Rechtsgrundlage ist vorhanden und eu-LISA entwickelt nun das System. Parallel dazu laufen die Vorbereitungen für den Test der Verbindung der Mitgliedsstaaten mit dem System. Dies ist eine kritische Phase und wir sind zuversichtlich, dass sich die sorgfältige Vorbereitung auszahlen wird.

Was waren die größten Herausforderungen?
Herausforderungen für die Vorarbeiten ergaben sich durch die Covid-19-Pandemie. Zum Beispiel haben die Zugangsbeschränkungen Arbeiten in Räumlichkeiten beeinträchtigt, in denen Hardware untergebracht werden soll. Zudem sind die Teams, die an dem Projekt arbeiten, multinational, und die Anreise zu Meetings wurde stark erschwert. Wir haben gemeinsam mit den EU-Ländern und eu-LISA hart daran gearbeitet, potenzielle negative Auswirkungen der Pandemie auf die Einführung des Einreise-/Ausreisesystems in Grenzen zu halten. Nun kann ich mit Zuversicht sagen, dass es uns bis jetzt gelungen ist, diese Herausforderungen ohne nennenswerte Auswirkungen auf das Projekt zu bewältigen.

Da wir uns dem geplanten Datum für die Inbetriebnahme nähern, konzentrieren wir uns jetzt auf die Unterstützung der EU-Länder bei der Vorbereitung auf den Betrieb des Systems. Die EU-Länder, die assoziierten Schengen-Staaten, eu-LISA und die Kommission fahren gewissermaßen wie Schiffe in einem Konvoi. Das letzte Schiff, das den Hafen erreicht, wird darüber entscheiden, wann das Einreise-/Ausreisesystem in Betrieb genommen werden kann. Deshalb müssen wir dafür sorgen, dass die Vorbereitungen bei allen Beteiligten in ähnlichem Tempo voranschreiten und dass jedes EU-Land rechtzeitig bereit ist. Die Kommission stellt den Mitgliedstaaten zudem erhebliche Mittel zur Verfügung, um die Einführung des Einreise-/Ausreisesystems auf nationaler Ebene zu unterstützen.

Das Einreise-/Ausreisesystem soll in der ersten Hälfte des nächsten Jahres in Betrieb genommen werden, rechtzeitig vor Ablauf einer allgemeinen Frist Ende 2023, wenn die EU-Informationssysteme für das Sicherheits-, Grenz- und Migrationsmanagement interoperabel werden und auf intelligente und zielgerichtete Weise zusammenarbeiten sollen.

Die Covid-19-Pandemie hat generell ein neues Licht auf das Potenzial der modernen Technologie geworfen. Dies gilt auch für das Grenzmanagement. Das Einreise-/Ausreisesystem wird dazu beitragen, den Grenzübertritt zu beschleunigen, da die Reisenden Selbstbedienungssysteme oder eGates an den Grenzen nutzen können, anstatt für das manuelle Abstempeln ihrer Pässe anstehen zu müssen.

„Das Einreise-/Ausreisesystem wird dazu beitragen, den Grenzübertritt zu beschleunigen, da die Reisenden Selbstbedienungssysteme oder eGates an den Grenzen nutzen können, anstatt für das manuelle Abstempeln ihrer Pässe anstehen zu müssen."

Wie geht es nach der Einführung des EES weiter?
Unsere Arbeit ist natürlich nicht mit der Inbetriebnahme des Einreise-/Ausreisesystems beendet. Im Gegenteil, das EES ist nur ein Teil unserer Bemühungen, ein hochmodernes Außengrenzmanagementsystem einzurichten und sicherzustellen, dass die Informationssysteme intelligent und zielgerichtet zusammenarbeiten.

Wir aktualisieren derzeit das Schengener Informationssystem (SIS), das am weitesten verbreitete und größte Informationsaustauschsystem für Sicherheits- und Grenzmanagement in Europa. Das aktualisierte SIS wird vor dem Einreise-/Ausreisesystem in Betrieb sein.

Matthias Oel

Matthias Oel ist Direktor Schengen, Grenzen und Innovation in der Generaldirektion (DG) Migration und Inneres der Europäischen Kommission.

Bevor er diese Position im Mai 2017 übernahm, war er seit Januar 2016 Direktor für Migrations- und Sicherheitsfonds in derselben Generaldirektion, Referatsleiter für Asyl (ab April 2012) und Sonderberater im Kabinett des Präsidenten des Europäischen Rats Herman Van Rompuy (ab Januar 2010).

Matthias Oel begann seine berufliche Laufbahn im deutschen Bundeswirtschaftsministerium und kam 1995 erstmals zur Europäischen Kommission als abgeordneter nationaler Sachverständiger im Kabinett von Kommissarin Dr. Monika Wulf-Mathies (Regionalpolitik). 1997 wechselte er in die Ständige Vertretung der Bundesrepublik Deutschland bei der EU, wo er während der deutschen EU-Ratspräsidentschaft 1999 als Referent für Industrie- und Regionalpolitik tätig war. Danach wurde er Beamter der Kommission und arbeitete als Koordinator des Parlaments und des Rats sowie als Assistent des Generaldirektors für Personal und Verwaltung. Von 2004 bis 2006 war er Mitglied des Kabinetts von Vizepräsident Günter Verheugen, wo er hauptsächlich für das Dossier Industriepolitik zuständig war.

Im Jahr 2006 wurde er nach Berlin abgeordnet, wo er als Leiter der Task Force „EU-Ratspräsidentschaft 2007" und anschließend als Direktor für EU-Angelegenheiten im Bundesministerium des Innern arbeitete, bis er in das Kabinett von Präsident Van Rompuy eintrat.

„Das EES ist nur ein Teil unserer Bemühungen, ein hochmodernes Außengrenzmanagementsystem einzurichten und sicherzustellen, dass die Informationssysteme intelligent und zielgerichtet zusammenarbeiten."

Auch das Visa-Informationssystem, die Datenbank, die den Schengen-Staaten den Austausch von Visadaten ermöglicht, wird modernisiert. Seine Infrastruktur verbindet die Konsulate in Nicht-EU-Ländern und alle Außengrenzübergänge der Schengen-Staaten. In Zukunft möchten wir den gesamten Visum-Antragsprozess digitalisieren.

Kurz nach dem SIS und dem Einreise-/Ausreisesystem wird das Europäische Reiseinformations- und -genehmigungssystem (ETIAS) in Betrieb genommen. ETIAS wird dazu beitragen, Sicherheitsrisiken, irreguläre Migration oder hohe epidemische Risiken zu erkennen, die von Personen ausgehen, die von der Visumpflicht ausgenommen sind und in den Schengen-Raum einreisen. Das System wird den Reisenden frühzeitig anzeigen, ob sie in die Schengen-Mitgliedstaaten einreisen dürfen. So wird legales Reisen über die Schengen-Grenzen hinweg einfacher. Sobald ETIAS in Betrieb ist, müssen sich Nicht-EU-Bürger, die in den Schengen-Raum reisen und von der Visumpflicht befreit sind, registrieren lassen und vor der Reise eine Genehmigung einholen. In den allermeisten Fällen (voraussichtlich in über 95 Prozent der Fälle) wird dies automatisch genehmigt. Das Verfahren wird einfach, schnell und erschwinglich sein: Die ETIAS-Genehmigung wird einmalig sieben Euro kosten und ist drei Jahre lang und für mehrere Einreisen gültig.

Darüber hinaus müssen wir mit Blick auf die Zukunft technologische Innovationen, die den Reiseverkehr und die Grenzverwaltung künftig prägen werden, sowohl kennen als auch vorantreiben. In den letzten Jahren hat die Kommission Forschungsarbeiten finanziert, die der Entwicklung von Systemen und Technologien für heute – zum Beispiel des Einreise-/Ausreisesystems – und für die Zukunft dienten. Die heutige Forschung untersucht und bereitet die Systeme der nächsten Jahrzehnte vor. Dies ist nicht nur wichtig, um europäische technologische Fähigkeiten zu ermöglichen, sondern auch um zu verstehen, wie sich technologische Entwicklungen im Hinblick auf die Grundrechte von EU-Bürgern und Nicht-EU-Bürgern verhalten, sowie um sicherzustellen, dass unsere Systeme aktuell, sicher und mit den Werten der EU vereinbar sind.

Alle IT-Großsysteme der EU sind keine eigenständigen Projekte, sondern bilden ein interoperables Ganzes. Die Interoperabilität wird es diesen EU-IT-Systemen ermöglichen, sich gegenseitig zu ergänzen und die Nutzung von Informationen in vielen Bereichen wie Grenzen, Visumverfahren, Sicherheit, Migrationsmanagement und Strafverfolgung zu verbessern, wobei die Grundrechte und die Datenschutzvorschriften in vollem Umfang eingehalten werden.

Installation von secunet easygates am Flughafen Sofia, Bulgarien

Einführung biometrischer Grenzkontrollen im Schengenraum

Wer ist fit fürs EES?

Das europäische Einreise-/Ausreisesystem (Entry-/Exit-System, EES) beschäftigt Grenzkontrollbehörden und Technologieanbieter schon seit Jahren. Zwischenzeitlich hat sich bei diesem Thema in Europa einiges getan: Auch wenn einige Länder noch mitten in der Vorbereitung ihrer EES-Ausschreibungen stecken, sind die technologischen Weichen in den allermeisten Staaten gestellt. secuview gibt einen Überblick, worum es eigentlich geht, und zeigt Praxisbeispiele aus Ländern, in denen secunet aktuell EES-Projekte umsetzt.

EES kurz erklärt

Mit der Einführung des Entry-/Exit-Systems sollen die Schengen-Außengrenzen in Zukunft einheitlich abgesichert werden. Das EES-Projekt der EU-Kommission zielt darauf ab, die Grenzverwaltung zu modernisieren, die Sicherheit des Schengen-Raums zu erhöhen und durch die Automatisierung von Prozessen die Grenzkontrolle effizienter zu gestalten, um die stetig steigende Zahl an Grenzübertritten bewältigen zu können.

Das EES dient der elektronischen Erfassung der Ein- und Ausreisen von Drittstaatsangehörigen sowie der automatischen Berechnung der Aufenthaltsdauer im Schengen-Raum. Reisende aus Drittstaaten müssen sich daher voraussichtlich ab Mitte 2022 bei der Einreise in eines der Länder des Schengen-Raums an Land-, See- und Luftgrenzen mit vier Fingerabdrücken und Gesichtsbild registrieren lassen. Die heutige Praxis des manuellen Abstempelns der Reisedokumente wird durch einen Eintrag im EES ersetzt. Mit dem System sollen insbesondere sogenannte „Overstayer", die ihre Aufenthaltserlaubnis überziehen, einfacher entdeckt werden. Reisende ohne Ausweisdokumente sollen bei Kontrollen innerhalb des Schengen-Raums unter anderem mit Hilfe biometrischer Merkmale eindeutiger identifiziert werden können.

Die Kehrseite der Medaille ist, dass der gesamte Passagierprozess durch die umfassendere Prüfung und die Aufnahme der biometrischen Merkmale an der Grenze deutlich länger dauern wird. Zwar hat die Pandemie den Reisesektor stark getroffen, doch die Grenzbehörden müssen sich auf steigende Passagierzahlen einstellen, wenn sich die Situation wieder normalisiert. Es ist also sehr wahrscheinlich, dass es dann zu noch längeren Warteschlangen vor den Grenzkontrollschaltern kommen könnte. Das gilt es zu vermeiden – neben den Passagieren haben sowohl Flughäfen als auch Grenzpolizeien ein großes Interesse daran, dieses Szenario möglichst zu verhindern.

Daher laufen in nahezu allen europäischen Staaten derzeit zum einen Projekte, die die Umsetzung der Anforderungen des EES sicherstellen sollen, wie zum Beispiel die Installation von Gesichtsbildkameras und die Integration von EES-Prozessen. Gleichzeitig entscheiden sich aber viele Staaten für eine grundsätzliche Modernisierung ihrer Grenzkontrollinfrastrukturen. Denn durch eine Automatisierung und/oder Prozessoptimierung an den entscheidenden Stellen können sowohl der zusätzliche Zeitbedarf bei der Personenkontrolle als auch die kontinuierlich steigenden Passagierzahlen abgefedert werden.

Technologie, die dies leisten kann, bietet secunet im Rahmen seines Produktportfolios secunet border gears. Es besteht aus eGates, Selbstbedienungskiosken, Kamerasystemen sowie Grenzkontroll-Applikationen, mit denen sich im EES-Kontext die notwendigen Prozessoptimierungen umsetzen lassen.

EES in der Praxis

secunet unterstützt aktuell etliche Staaten dabei, die Anforderungen des EES umzusetzen – mehr dazu auf der nächsten Seite.

Grenzkontrollbeamtin am Flughafen Burgas, Bulgarien

SCHWEIZ

RUNDUMERNEUERUNG AM FLUGHAFEN ZÜRICH

Die Kantonspolizei Zürich hat secunet damit beauftragt, die Grenzkontrollinfrastruktur am Flughafen Zürich zu erneuern und weiterzuentwickeln. Der Auftrag umfasst zum einen, die Grenzkontrolle an die EES-Anforderungen anzupassen, um die gesetzlichen Anforderungen zu erfüllen. Zum anderen soll durch die Installation von Automatisierungstechnologien einer Verlangsamung der Passagierströme entgegengewirkt werden, welche durch zusätzlich notwendige Erfassungen und Prüfungen von Drittstaatenangehörigen verursacht wird.

In dem früheren Projekt „Greko NG“ hatte secunet im Auftrag der Kantonspolizei Zürich bereits die rund 100 stationären Arbeitsplätze von Grund auf erneuert und mit einer Grenzkontrollapplikation ausgestattet. Diese Anwendung fasst für die Beamten alle Prüfergebenisse aus unterschiedlichen Systemen auf einem Bildschirm übersichtlich zusammen. Dadurch wird der Prüfprozess deutlich vereinfacht und beschleunigt.

TSCHECHIEN

EES MITTEN IN DER UMSETZUNG

Die tschechische Grenzpolizei hatte im Februar VÍTKOVICE IT SOLUTIONS und secunet mit dem ersten und umfangreichsten Teil ihrer Implementierung des EES beauftragt. Komponenten aus dem secunet border gears Produktportfolio werden dazu beitragen, dass die Grenzkontrollen an tschechischen internationalen Flughäfen schnell, einfach und sicher bleiben – auch nach der Einführung des EES. Dies ist hier von besonderer Bedeutung, da Reisende aus Großbritannien zum Beispiel am Flughafen Prag einen größeren Teil der Reisenden ausmachen und seit dem Brexit auch als Drittstaatsangehörige behandelt werden müssen. secunet liefert konkret:

- secunet easykioske für die Vorregistrierung durch Drittstaatsangehörige
- secunet easytower zur Erfassung hochwertiger Gesichtsbildaufnahmen an den Grenzkontrollschaltern
- eine Software für die Prozessvisualisierung und Überwachung der Datenerfassung und -verifizierung sowie der im Hintergrund ablaufenden Prüfvorgänge
- die zentrale Serverkomponente, secunet easyserver, die die verschiedenen Grenzkontrollkomponenten verbindet und direkt mit dem zentralen EES der EU kommunizieren wird

Vítkovice als Generalunternehmer stellt Wartung und Support sowie Hardware-Peripheriegeräte für die manuelle Grenzkontrolle bereit. Der Rollout sämtlicher Komponenten ist für Ende 2021 geplant.

BULGARIEN

„BOARDING COMPLETED“: FLUGHÄFEN SIND EES-READY

In Kooperation mit dem bulgarischen Generalunternehmer SSARM hat secunet an den internationalen Flughäfen in Sofia, Varna und Burgas eine sichere Komplettlösung für EES-konforme Grenzkontrollen realisiert. Damit hat Bulgarien, als eines der ersten EU-Länder, seine Luftgrenzen mit secunet border gears auf das EU-weite Einreise-/Ausreisesystem EES vorbereitet und ist lange vor dessen Start betriebsbereit.

Zur Gesamtlösung gehören eGates (secunet easygate), Selbstbedienungskioske (secunet easykiosk) sowie Kamerasysteme (secunet easytower) und Fingerabdruckleser für die stationären Schalter. Alle Passagiergruppen, also EU-Bürger wie Drittstaatenangehörige, profitieren somit von komfortableren, automatisierten Prozessen an der Grenzkontrolle. Das Projekt wurde komplett während der Corona-Pandemie realisiert und die Installation – trotz aller Herausforderungen – zeitgerecht umgesetzt.

Lesen Sie dazu auch das Interview mit Nikolay Dimchev, Managing Director bei SSARM, auf der nächsten Seite.

Flughafen Varna, Bulgarien

Im Interview: Nikolay Dimchev

Neue EES-Technologien an den bulgarischen Flughäfen

SSARM ist der größte IT-Systemintegrator in Bulgarien und hatte nach einer Ausschreibung des bulgarischen Innenministeriums im vergangenen Jahr den Großauftrag erhalten, die bulgarischen internationalen Flughäfen mit EES-konformen Grenzkontrolllösungen auszustatten. Inzwischen hat SSARM eine sichere Komplettlösung an den Flughäfen Sofia, Varna und Burgas in Kooperation mit secunet vollständig installiert.

Nikolay Dimchev, Geschäftsführer von SSARM, spricht über das Projekt, seine interessantesten Erkenntnisse und den Mehrwert für Passagiere, Grenzkontrolle und Flughäfen.

Was genau haben Sie an den Flughäfen in Varna, Burgas und Sofia installiert und warum?

Nikolay Dimchev: Der Anlass für die Implementierung neuer Grenzkontrollsysteme steht in engem Zusammenhang mit der Entscheidung der EU, das Entry-/Exit-System ab 2022 im gesamten Schengenraum einzuführen. Durch die Aufnahme von Gesichtsbild und Fingerabdrücken wissen die Staaten in Zukunft besser, welche Drittstaatenangehörigen in die EU einreisen und stellen sicher, dass der einzelne Passagier seine Aufenthaltsdauer nicht überschreitet. Das dient unserer aller Sicherheit.

Durch die Integration dieser zusätzlichen Prozessschritte in der ersten Grenzkontrolllinie droht aber in einer unveränderten Infrastruktur der Kollaps, weil die Abfertigung im Schnitt 40 bis 45 Sekunden länger dauert – pro Passagier! Von daher ist eine

Prozessautomatisierung an allen möglichen Stellen, also auch an den Grenzkontrollschaltern, unumgänglich. Das Innenministerium hat sich daher für die umfassende technologische Modernisierung der Grenzkontrolle entschieden und uns mit der Umsetzung beauftragt. Wir haben dann – zusammen mit unserem Projektpartner secunet – eGates, Selbstbedienungskioske sowie Kamerasysteme und Fingerabdruckleser für die stationären Schalter an den drei passagierstärksten Flughäfen implementiert. Die Technologien erfüllen ganz unterschiedliche Funktionen und sind mitunter für unterschiedliche Passagiergruppen bestimmt – alle Technologien im Zusammenspiel werden den Grenzkontrollprozess spürbar beschleunigen und die zuständigen Beamten stark entlasten.

Warum haben Sie sich für den deutschen Partner secunet entschieden? Sie sind eigentlich ausschließlich im nationalen Markt unterwegs und zudem selbst ein gut aufgestellter IT-Systemintegrator.

Wir arbeiten mit secunet schon länger im Bereich der Hochsicherheitstechnologien zusammen und konnten uns in früheren Projekten davon überzeugen, dass die Qualität der Produkte nicht nur stimmt, sondern dass sie die Anforderungen unserer Kunden umfassend erfüllen. Daher haben wir für das EES-Projekt auch Kontakt zu secunet aufgenommen, denn wir sind zwar ein hervorragend aufgestellter Systemintegrator, der sich im bulgarischen Markt bestens auskennt, verfügen in diesem Bereich aber nicht über ein eigenes Produktportfolio.

Die EES-Lösungen von secunet haben uns dann auch überzeugt: Sie liefern Biometrieaufnahmen in bester, EES-konformer Qualität und sind höchst überwindungs- und fälschungssicher ausgelegt. Dies ist insbesondere für unbeaufsichtigte Systeme, bei denen der Beamte nicht unmittelbar danebensteht und jeden Passagier überwacht, extrem wichtig. Und nicht zuletzt haben alle Produkte ein äußerst ansprechendes, modernes Design – ein nicht zu unterschätzender Punkt, der für viele Flughäfen heute enorm wichtig ist.

Die Modernisierung der Grenzkontrollinfrastruktur war sicherlich eine größere Investition. Welche Vorteile bringt sie für Passagiere, Flughäfen und die Grenzkontrolle?

Die Vorteile sind schnell auf den Punkt gebracht: Passagiere – woher auch immer sie kommen – haben an den bulgarischen Flughäfen Sofia, Varna und Burgas nun Zugang zu Automatisierungstechnologien. Wenn man so will, haben sie mindestens einen Teil ihres Grenzübergangs selbst in der Hand. Dank der intuitiven Benutzerführung werden die Daten zügig aufgenommen und anschließend sicher und datenschutzkonform verarbeitet. Die hohe Qualität der aufgenommenen Daten ist natürlich insbesondere für die Grenzpolizei wichtig. Die Beamten werden durch die Technologien zudem optimal unterstützt und nicht noch zusätzlich belastet. Und die Flughäfen profitieren davon, dass es trotz umfangreicherer Grenzkontrollprozesse, die eigentlich mehr Zeit beanspruchen, eben keine deutlich längeren Warteschlangen und verpassten Anschlussflüge gibt.

Was sind Ihre wichtigsten Erkenntnisse aus diesem EES-Projekt?

Eigentlich waren wir im EES-Projekt mit denselben Herausforderungen konfrontiert wie in nahezu jedem komplexen IT-Projekt: Wenn Dinge konkreter als eine Beschreibung auf dem Papier werden, ergeben sich von Kundenseite nicht selten neue oder veränderte Anforderungen, die im laufenden Projekt kurzfristig umzusetzen sind. Das ist völlig normal und damit können wir gut umgehen.

Nikolay Dimchev

Nikolay Dimchev ist Ingenieur für Telekommunikation und hat einen MBA der Cotrugli Business School.

Seine zwanzigjährige Erfahrung in der IT erwarb er als Solution Consultant und Sales & Business Development Manager in Unternehmen wie Atos, Symantec und DXC. Im Jahr 2017 wechselte er zu SSARM als Head of Sales. Im Januar 2021 übernahm Nikolay Dimchev die Position des Managing Director.

Sein ausgeprägter technischer Hintergrund in Kombination mit seiner Erfahrung als Teamleiter erleichtert es ihm, das Tagesgeschäft des Unternehmens zu leiten, das Team zu entwickeln und die komplexesten und strategischsten Projekte des Unternehmens zu betreuen.

Bei den EES-Installationen haben wir beispielsweise die modernsten, sichersten Produkte verbaut und mussten feststellen, dass es damit alleine nicht getan ist. Es geht in Grenzkontrollprojekten eben doch um mehr, als „nur" Technologien zu installieren. Die Produkte sollen Passagierprozesse optimal steuern und sich perfekt in die jeweilige Umgebung einfügen und diese ist nun mal an jedem Flughafen, an jeder Landgrenze eine andere. Dies war eine wichtige Erkenntnis für uns. Konkret haben wir auch diesmal Funktionserweiterungen im laufenden Projekt integriert, die zunächst nicht geplant waren. Die Installation von Glaswänden zwischen stationärer und automatisierter Grenzkontrolle oder der Bau von speziellen Halterungen für die Fingerabdruckscanner, die sonst nicht perfekt für die Passagiere positioniert gewesen wären, sind Beispiele hierfür. Wir konnten zusammen mit secunet alle neuen Kundenanforderungen glücklicherweise schnell und bedarfsgerecht anbieten, in die Projektumsetzung integrieren und haben dennoch pünktlich abgeliefert.

Eine andere wichtige Erkenntnis ist also sicherlich keine ganz neue: Man muss bis zum Schluss flexibel reagieren und sich den Blick für die Details bewahren, wenn man passgenaue und ein Stück weit auch optisch ansprechende Installationen anstrebt.

Was möchten Sie besonders hervorheben?

Die EES-Installation war unser erstes Projekt im Bereich der Grenzkontrolle, unsere Premiere sozusagen. Wir sind stolz und erleichtert, dass wir den Auftrag zur vollsten Zufriedenheit des bulgarischen Innenministeriums erfüllt haben. Es war ein enormer Vorteil, die Leute von secunet an Bord zu haben, die sehr routiniert und erfahren sind. In Zeiten dieser Pandemie haben wir gemeinsam viel gelernt und uns gegenseitig gezwungenermaßen „remote" unterstützt. Anders wäre es nicht möglich gewesen, die Installation – trotz aller Herausforderungen – zeitgerecht umzusetzen. Durch dieses perfekte Zusammenspiel ist es uns gelungen, das erklärte Ziel des Kunden zu erreichen: Bulgarien ist als eines der ersten Länder in der EU an den drei internationalen Flughäfen mit einer EES-fähigen Gesamtlösung ausgestattet, lange vor dem voraussichtlichen Start des EU Entry-/Exit-Systems im Mai 2022. Darauf sind wir stolz.

SSARM wurde vor zehn Jahren gegründet und ist der sich am schnellsten entwickelnde IT-Systemintegrator in Bulgarien. Das Unternehmen ist spezialisiert auf die Lieferung, Installation und Integration von IT- und Kommunikationstechnologie – Hardware und Software – sowie auf Lösungen für die Sicherheit, den Schutz und die Speicherung von Daten. Zudem ist SSARM in den Bereichen staatliche Sicherheit und automatisierte Grenzkontrolllösungen aktiv. In den letzten vier Jahren hat das Unternehmen komplexe Projekte für die bulgarische Staatsverwaltung, den Finanzsektor und die Wirtschaft umgesetzt. SSARM baut seine Expertise für innovative Lösungen kontinuierlich aus, etwa im Bereich Grenzkontrolle, bei drohnenbasierten Lösungen und auf anderen Gebieten.

Biometrie-Qualität für das europäische Einreise-/Ausreisesystem

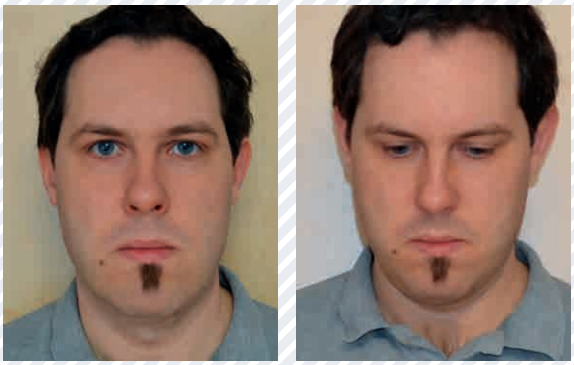
Das EES ist nur so gut wie seine Daten

Im EES-Register wird künftig zu jedem Reisenden aus Drittstaaten ein EES-Dossier abgelegt, das Daten zur Identität des Reisenden, zum Reisedokument sowie zu Datum und Ort der Einreise oder Ausreise enthält. Dazu kommen als biometrische Informationen ein Gesichtsbild und vier Fingerabdrücke. Diese Daten ermöglichen eine automatisierte Identifikation von Reisenden. Der Abgleich mit dem EES dient unter anderem dem Zweck, festzustellen, ob jemand bereits unter einer anderen Identität eingereist ist.

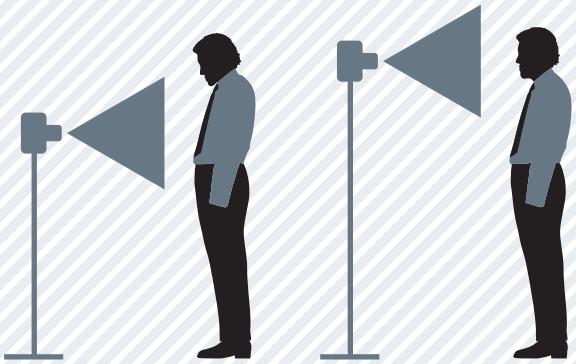
Bei der automatisierten Identifikation sind grundsätzlich zwei Arten von Fehlern möglich: Im Fall einer **Falschpositividentifikation** entscheidet der Algorithmus anhand eines Gesichtsbildes und/oder der Fingerabdrücke einer Person, dass deren biometrische Daten bereits in der Datenbank vorhanden sind, obwohl dies nicht der Fall ist. Bei der **Falschnegatividentifikation** entscheidet der Algorithmus, dass die biometrischen Daten einer Person nicht in der Datenbank vorhanden sind, obwohl dies der Fall ist.

Geringe Fehlertoleranz

Im Durchführungsbeschluss der EU zur Einführung des EES ist festgelegt, dass die Falschpositividentifikationsrate unter 0,1 Prozent liegen muss, also in weniger als 0,1 Prozent der Grenzübertritte jemand fälschlicherweise als eine andere Person identifiziert wird. Die Falschnegatividentifikationsrate muss unter 1 Prozent bleiben: In weniger als 1 Prozent der Fälle darf das System jemanden fälschlicherweise nicht seinem gespeicherten Dossier zuordnen. Die EU-Kommission erwartet, dass das EES-Register nach dem Jahr 2025 eine Größenordnung von 100 Millionen Dossiers umfassen wird. In diesen muss dann bei jedem Grenzübertritt eine effiziente und korrekte Suche und Identifizierung stattfinden.



Zwei Varianten eines Gesichtsbildes. Im linken Beispiel erfüllt das Bild die Anforderungen an eine Frontalaufnahme gemäß ISO/IEC 19794-5 (die Person schaut direkt in die Kamera und hat einen neutralen Gesichtsausdruck). Im rechten Beispiel verletzt die Aufnahme die Anforderung, dass die Person direkt in die Kamera schauen muss.



Zwei Varianten zur Erfassung von Gesichtsbildern. Variante 1 (links) mit höhenfixierter, horizontal ausgerichteter Kamera eignet sich nicht, um Frontalaufnahmen zu erfassen. Variante 2 (rechts) mit einem höhenverstellbaren Aufnahmemechanismus ermöglicht die frontale Erfassung von neutralen Gesichtern von Personen unterschiedlicher Größe.

Jeder Schengen-Staat ist selbst für die Umsetzung und die Erreichung der Qualitätsziele verantwortlich. Im Bereich der Gesichtserkennung gibt es in Deutschland schon wertvolle Erfahrungen aus dem EasyPASS-Grenzkontrollsystem der Bundespolizei. In diesem System, das von secunet gemeinsam mit der Bundesdruckerei ausgerollt wurde, erfolgt ein Live-Vergleich eines Gesichtsbildes mit gespeicherten Aufnahmen vom Reisedokument.

Beim EES gelten besondere Qualitätsanforderungen an das Livebild, das an der Grenze erfasst wird. Gemäß dem Standard für Gesichtsfrontalaufnahmen ISO/IEC 19794-5 muss das Bild gleichmäßig ausgeleuchtet sein, die Person muss gerade in die Kamera schauen und einen neutralen Gesichtsausdruck haben. Sinnvoll ist es, eine höhenverstellbare Kamera zu nutzen, um eine frontale, nicht gekippte Kopfhaltung der Reisenden sicherzustellen. Die Verwendung einer automatischen Höhenverstellung gegenüber einer manuellen kann zudem den Prozess der Gesichtsbilderfassung beschleunigen. Insgesamt steigt durch diese Maßnahmen die Qualität der Bilder, wodurch die Fehlerraten bei der Identifikation sinken und die Vorgaben der EU zur Fehlertoleranz erfüllt werden können.

Algorithmus erkennt Qualität von Fingerabdrücken

Auch für die Fingerabdruck-Scans gelten Mindestanforderungen: Sie müssen zum Beispiel eine Auflösung von 500 oder 1000 ppi aufweisen und werden mit dem NFIQ 2.0-Algorithmus des US-amerikanischen Normeninstituts NIST hinsichtlich ihrer Qualität bewertet.

NFIQ gibt einen Qualitätsscore zurück, als Maß dafür, wie viele Details in einem Fingerabdruck zum Zweck der Zuordnung verwertbar sind. Seit 2017 liegt der Algorithmus in der weiterentwickelten Version NFIQ 2.0 vor. Diese Version ist für das EES maßgeblich und wurde für diesen Einsatzzweck noch einmal speziell angepasst. Im Auftrag des BSI und in Zusammenarbeit mit dem NIST waren Experten von secunet an dieser Optimierung beteiligt. Zudem entwickelte

secunet easytower am
Flughafen Varna, Bulgarien

secunet ein modulares Software-Framework, mit dessen Hilfe NFIQ 2.0 mit Verfahren des maschinellen Lernens für den Einsatz in der smarten Grenzkontrolle weiter trainiert und verbessert werden kann.

Wenn das EES voraussichtlich Mitte 2022 den operativen Betrieb aufnimmt, sollte an den Schengen-Außengrenzen die optimale Infrastruktur vorhanden sein, um biometrische Daten in der geforderten Qualität zu erfassen. Nur so lässt sich sicherstellen, dass die Anforderungen erreicht werden und das EES seinen Zweck erfüllt.

Benjamin Tams
benjamin.tams@secunet.com

QUALITÄT UND TEMPO FÜR DIE BIOMETRISCHE ERFASSUNG AN DER STATIONÄREN GRENZKONTROLLE

Der **secunet easytower** sorgt bei der stationären Grenzkontrolle für eine schnelle und hochwertige Gesichtsbildaufnahme. Dabei garantiert er höchste biometrische Datenqualität gemäß der EES-Verordnung. Mithilfe einer Höhenanpassung der Kamera sowie einer zusätzlichen diffusen Beleuchtung wird die Aufnahmequalität des frontalen Gesichtsbilds nach ISO 19794-5:2011 sichergestellt. Somit sind sämtliche EES-Qualitätsanforderungen erfüllt.

Dank einer intuitiven Benutzerführung ist der easytower sowohl für Reisende als auch Grenzbeamte einfach zu benutzen. Ein eingebauter Feedback-Bildschirm zeigt die „Live"-Aufnahmen der Gesichtsbildkamera an. Der Reisende blickt in einen digitalen Spiegel mit zusätzlicher Benutzerführung, die – mehrsprachig verfügbar – den Reisenden ideal unterstützt. Je nach Bedarf wird ein vollautomatischer oder ein manueller Erfassungsmodus ausgewählt. Durch den intuitiven Erfassungsprozess garantiert der easytower eine geringe Aufnahmezeit und beschleunigt damit den Grenzkontrollprozess. Die integrierte Beleuchtung gewährleistet hierbei qualitativ hochwertige, gut ausgeleuchtete Aufnahmen und stellt auch bei ungünstigen Lichtverhältnissen eine homogene Belichtung des Gesichts sicher.

Kooperation zwischen Streitkräften

Multinationale Zusammenarbeit – dank oder trotz Cybersicherheit?

Von Marcel Taubert, Head of Division Defence & Space, secunet Security Networks AG

Zum Auftrag der Bundeswehr gehört es, die „europäische Integration, transatlantische Partnerschaft und multinationale Zusammenarbeit zu stärken" – so steht es in der Konzeption der Bundeswehr (KdB).[1] Die multinationale Ausrichtung gründet sich auf politischen Willen, bietet aber auch militärische Vorteile wie etwa ein verbessertes Gesamtlagebild, koordinierte Einsätze und Übungen sowie eine schnellere Entscheidungsfindung über Organisationsgrenzen hinweg. Doch was bedeutet multinationale Zusammenarbeit in der Praxis? Wo liegen die Herausforderungen und welche Rolle spielt die Cybersicherheit?

Hier besteht ein Gefälle entlang der strategischen, operativen und taktischen Ebene. Auf der strategischen Seite des Spektrums, gekennzeichnet durch einen hohen Abstraktionsgrad und eine begrenzte Anzahl handelnder und entscheidender Personen, kann multinationale Zusammenarbeit mit den bestehenden Ansätzen meist gut umgesetzt werden. Ein Beispiel ist das Multinationale Kommando Operative Führung in Ulm, das im Auftrag von UN, NATO oder EU die Führung von weltweiten Krisenmanagementeinsätzen übernimmt. Hier findet die Verzahnung auf einer Ebene statt, auf der konkrete strategische und militärpolitische Vorgaben in Planungen und Befehle für die ausführenden Streitkräfte umgesetzt werden. Reibungspunkte, die auf dieser hohen Ebene entstehen, sind überschaubar. Hinzu kommen technisch ausgereifte, hochsichere IT-Lösungen.

Bewegt man sich weiter auf das operativ-taktische Ende des Spektrums zu, werden die Herausforderungen größer. Nicht nur die IT spielt dabei eine Rolle. Auch kulturelle Aspekte fallen stärker ins Gewicht, etwa unterschiedliche Führungsstile der beteiligten Streitkräfte. Außerdem gelten unterschiedliche gesetzliche Rahmenbedingungen und Vorschriften, die zu Schwierigkeiten führen können. Die häufigen Personalwechsel, die für militärische Organisationen typisch sind, erschweren einen gemeinsamen Erfahrungsaufbau.

[1] Konzeption der Bundeswehr, 20. Juli 2018, S.19. https://www.bmvg.de/de/aktuelles/konzeption-der-bundeswehr-26384

Vielzahl von Sicherheitsdomänen

Auf technischer Ebene müssen die konkreten Sicherheitsanforderungen aller beteiligten Länder berücksichtigt und auf einen kleinsten gemeinsamen Nenner gebracht werden. Dabei hapert es weniger an technologischen Konzepten, sondern eher an fehlenden Interoperabilitätsstandards und gemeinsamen Architekturansätzen. Eine Hürde stellen die vielen unterschiedlichen Sicherheitsdomänen dar, die sich über nationale Einstufungen der beteiligten Länder, über gemeinsame NATO-, EU- oder missionsspezifische Anforderungen aufspannen. Die Interoperabilität von Hochsicherheits-Infrastrukturen wird durch diese Vielfalt enorm erschwert – und das, obwohl sich die Anforderungen für die Sicherheitsdomänen manchmal nur marginal unterscheiden. Aus technischer Sicht wäre eine Vereinheitlichung an dieser Stelle sicher begrüßenswert.

Eine Grundvoraussetzung, um gemeinsame Standards und Architekturen zu erreichen, ist der politische und militärische Wille – und der ist vorhanden. Als Beispiel für eine starke Verzahnung auf operativ-taktischer Ebene sei das I. Deutsch-Niederländische Corps erwähnt, bei dem unter anderem deutsche Offiziere niederländische Soldaten führen und umgekehrt. Darüber hinaus arbeiten zehn weitere Nationen im Rahmen dieses Corps zusammen. Dass eine enge Zusammenarbeit bereits bei der gemeinsamen Weiterentwicklung und Beschaffung geschehen kann, zeigt die multinationale Programmplanung Tactical Edge Network (TEN).

Marcel Taubert

Zu „Need to know“ kommt „Share to win“

Im multinationalen Kontext hat sich immer wieder gezeigt, dass der Austausch militärischer Informationen zwischen Partnern entscheidend sein kann. Beim Umgang mit sensiblen Informationen ist das „Need to know“-Prinzip (Kenntnis nur, wenn nötig) daher durch „Need to share“ (die Notwendigkeit, Informationen zu teilen) und sogar „Duty to share“ (die Pflicht, Informationen zu teilen) ergänzt worden. Die technischen Mittel dafür sind mittlerweile ausgereift: SINA Workflow, ein Kollaborationstool und digitales Verwaltungssystem für Verschlusssachen bis hin zu GEHEIM und entsprechende internationale Einstufungen, sorgt dafür, dass sensible Informationen ausschließlich in die richtigen Hände gelangen – und jederzeit nachvollziehbar bleibt, wer Kenntnis davon hat. „Share to win“ lautet das neue Stichwort, wobei „Need to know“ weiterhin jederzeit gewahrt bleibt.

Bei der täglichen Arbeit mit unterschiedlich eingestuften Informationen wünschen sich viele Angehörige in multinationalen Dienststellen das, was auf nationaler Ebene schon lange Realität ist: einen hochsicheren Datenaustausch über verschiedene Sicherheitsdomänen und -level hinweg – und zwar auf einem System ohne „Drehstuhlschnittstellen“, also ohne dass Nutzer*innen physisch zwischen mehreren Arbeitsplätzen wechseln müssen. Eine weitere Forderung sind synchrone und asynchrone Kommunikations- und Kollaborationstools inklusive einem Echtzeitaustausch per Video – mit steigenden Anforderungen an die Mobilität. Die Infrastruktur muss hochskalierbar sein und ausfallsicher (georedundant) aufgebaut werden. Zunehmend wichtig werden die Faktoren Resilienz und Flexibilität, noch dazu sollte die Lösung unter den Gesichtspunkten digitaler Souveränität „made in Europe“ sein.

Interoperabilität herstellen

Alle diese Anforderungen lassen sich heute technisch realisieren – mit Lösungen, die sich auf nationaler Ebene bereits viele Jahre lang bewährt haben. Ein Hindernis ist die oft noch fehlende multinationale Interoperabilität. Dafür müssen Standards vielfach erst noch aufgebaut und implementiert werden. Wo dies in Ansätzen bereits gelang, mussten oft sehr lange Entwicklungsphasen aufgrund unterschiedlicher Prämissen an die Kryptographie (Algorithmen) in Kauf genommen werden. Um diesem Problem entgegenzuwirken, sollten Interoperabilitätsstandards technisch minimal gehalten werden.

Generell gilt: Zulassungsanforderungen müssen hinreichend hoch angesetzt werden, um sich auf Informationen verlassen zu können und deren Missbrauch auszuschließen. Werden die Zulassungsanforderungen jedoch zu hoch geschraubt, leiden mitunter die Benutzbarkeit und der Wert einer Lösung im konkreten Einsatz. Die Einsatz- und Betriebsbedingungen müssen daher bei den Sicherheitsanforderungen mitbedacht werden, um eine Balance zwischen Usability und Security zu finden.

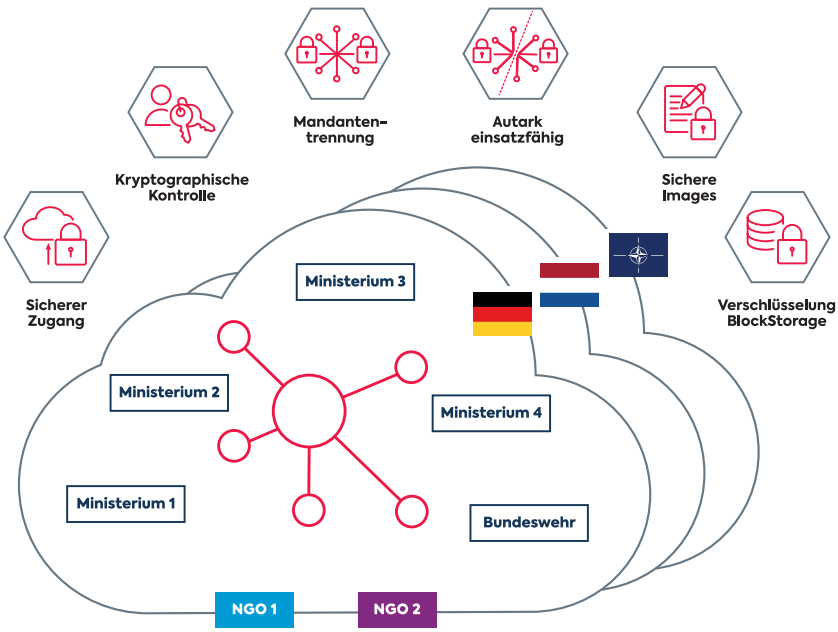
Marktverfügbare Lösungen

Als technische Grundlage für hochsichere multinationale Infrastrukturen kommen marktverfügbare Lösungen in Frage, die am Frontend multisessionfähige Clients bieten, welche sich über alle Domänen- und Sicherheitslevel hinweg nutzen lassen. Die Sichere Inter-Netzwerk Architektur SINA kann dies leisten. Am Backend könnten mittel- bis langfristig statt einer Trennung auf Hardware-Ebene hochsichere Private-Cloud-Systeme zum Einsatz kommen, die eine strikte Mandantentrennung mit kontrollierten Domänenübergängen ermöglichen.

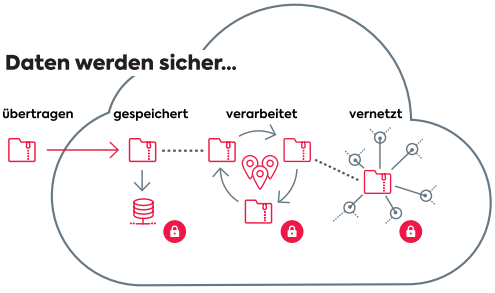
Hochsichere Cloud-Infrastrukturen könnten auch dazu genutzt werden, um im Rahmen eines Whole-of-Government-Cloud-Approachs die interdisziplinäre Zusammenarbeit verschiedener Ministerien, Staaten sowie mitunter auch NGOs zu fördern, die bei aktuellen Konflikten und Einsätzen immer häufiger gefragt ist. Für solche Einsatzszenarien muss eine Cloud besonderen Anforderungen genügen – etwa an die Mandantentrennung, an den Schutz der sensiblen Daten sowie an den sicheren Umgang mit eigenen kryptografischen Schlüsseln. Proprietäre Cloud-Stacks, sofern sie diese Vorgaben erfüllen, können nicht auf einfache Weise beschafft und souverän betrieben werden. Zudem ist die Sicherheit solcher Lösungen nicht evaluierbar. Diese Lücke schließt secunet mit seinem hochsicheren, Open-Source-basierten Cloud-Betriebssystem SecuStack.

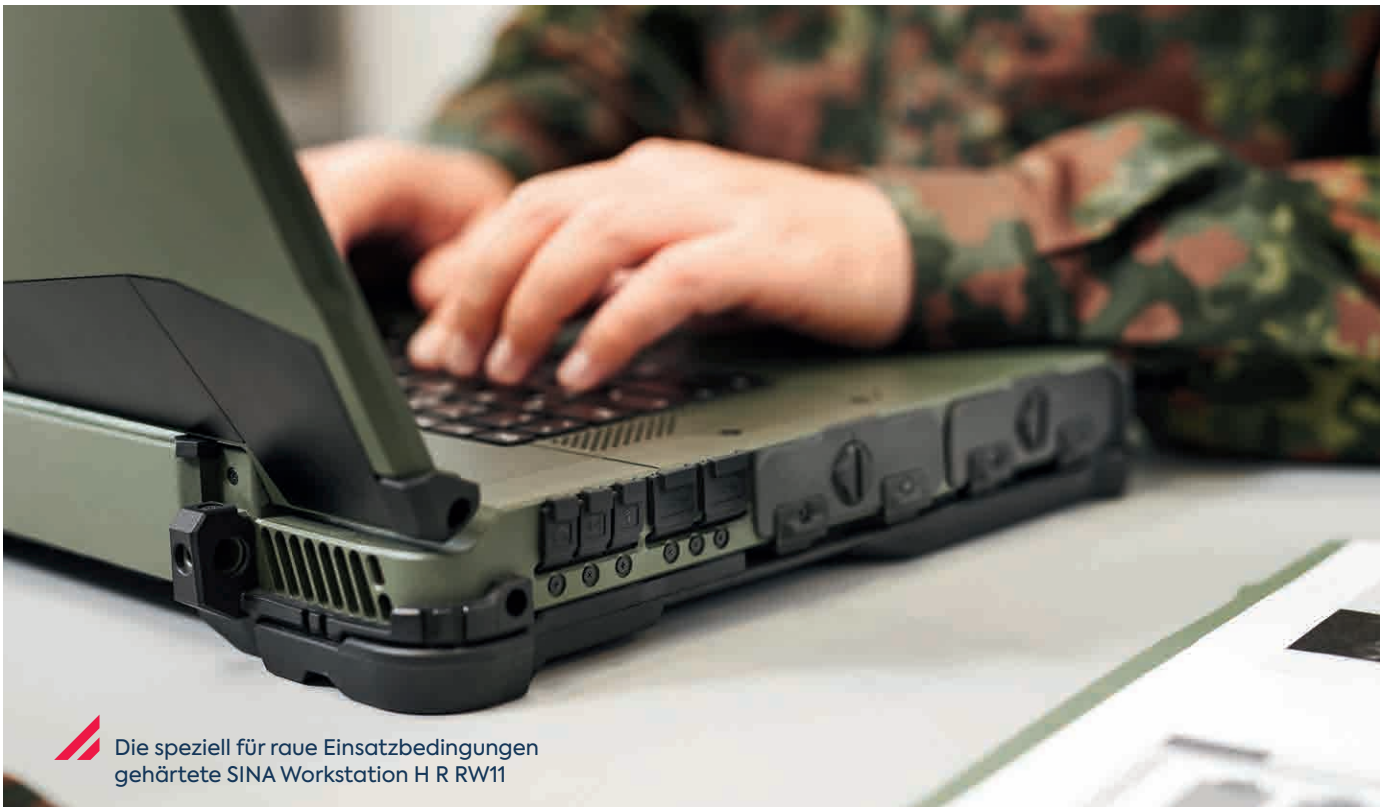
„Share to win“ funktioniert, auch wenn noch viele Herausforderungen bei der multinationalen Zusammenarbeit bestehen. Aktuelle Technologien zeigen bereits auf, was künftig möglich sein wird. Cybersicherheitsaspekte behindern eine weitere Verzahnung also nicht, sondern weisen ihr den Weg.

Marcel Taubert
marcel.taubert@secunet.com



Beim Whole-of-Government-Cloud-Ansatz muss die Cloud besonderen Anforderungen genügen.





Die speziell für raue Einsatzbedingungen gehärtete SINA Workstation H R RW11

SINA Technologie für schnelle Eingreiftruppe der NATO

Die Very High Readiness Joint Task Force (VJTF) der NATO, auch als „NATO-Speerspitze“ bekannt, ist ein schnell verlegbarer Eingreifverband und Teil der NATO Response Force. Sie ist multinational aufgestellt, unter starker Beteiligung der Bundeswehr. Die VJTF befähigt die NATO, noch schneller und flexibler auf sicherheitspolitische Entwicklungen zu reagieren.

Die Bundeswehr hat secunet mit der Lieferung einer größeren Anzahl von SINA Komponenten beauftragt, die für die IT-Infrastruktur der VJTF bestimmt sind. Mit ihnen lassen sich eingestufte Daten übermitteln, bearbeiten und speichern. Die Auftragssumme beläuft sich auf einen zweistelligen Millionen-Euro-Betrag, ausgeliefert wird bis Ende 2021.

Der Auftrag umfasst mehrere hundert Exemplare der leistungsstarken SINA Workstation H R, die auf einem gehärteten Notebook basiert und für den mobilen Einsatz unter besonders rauen Betriebsbedingungen ausgelegt ist. Die zugrundeliegende Hardwareplattform ist insbesondere gegen Schock, Vibration, Staub und Feuchtigkeit geschützt und kann auch bei extremen Temperaturen betrieben werden. Darüber hinaus liefert secunet eine größere Anzahl Exemplare der hochsicheren Netzwerkkomponente SINA L3 Box H.

secunet übernimmt stashcat

Messages, die ganz sicher rüberkommen

Nicht aus dem Silicon Valley, sondern aus dem beschaulichen Hannover kommt stashcat, der Messenger, der Slack, Teams und Co. Konkurrenz macht. Seit die beiden Gründer Christopher Bick und Felix Ferchland die Anwendung 2016 auf den Markt gebracht haben, erfreut sie sich zunehmender Beliebtheit: Aktuell zählt der Messenger über 1,3 Millionen aktive Nutzer*innen in Unternehmen, Behörden und Schulen, im Gesundheitswesen, bei der Polizei und der Bundeswehr – überall dort, wo der sichere Umgang mit vertraulichen Daten von besonderer Bedeutung ist. Mit der jüngst erfolgten Übernahme durch secunet bieten sich spannende Perspektiven.

Am Anfang steht die Idee eines sozialen Netzwerks, das sämtliche Kommunikation im Schulalltag von Lehrern und Schülern innerhalb einer Schule digital abbildet. Die beiden Hannoveraner Christopher Bick und Felix Ferchland gründen ihr erstes Unternehmen und versuchen, auf dem Bildungsmarkt Fuß zu fassen. Schnell wird klar: Neben E-Mails läuft ein Großteil der täglichen Kommunikation in Elterngruppen und Klassen über Messenger wie WhatsApp. Für den Schulalltag selbst scheiden diese Lösungen aber aus, weil sie nicht die Ansprüche an Datenschutz und Sicherheit erfüllen. Ein Problem, für das nicht einfach auf vorhandene Alternativen zurückgegriffen werden kann – und das auch ganz andere Branchen und Einrichtungen betrifft.

Die Idee für einen High-Secure-Messenger made & hosted in Germany ist geboren, 2015 starten die beiden jungen Gründer die Arbeit mit ihrer stashcat GmbH. Das Ziel: einfache Bedienbarkeit und höchste Sicherheitsstandards in einem Messenger zu kombinieren und damit eine Alternative zu Lösungen mit unklarem Datenschutz zu schaffen – die Nachfrage ist riesig. Bereits nach zwei Jahren gewinnt das Unternehmen wichtige Großkunden wie die Bundeswehr und die Polizei, auch auf dem Bildungsmarkt kann sich der Ableger schul.cloud erfolgreich positionieren und wird heute in über 7.500 Schulen deutschlandweit verwendet. Die Corona-Pandemie rückt die Digitalisierung für Unternehmen und Behörden dann nochmals in den Fokus und macht die Notwendigkeit zeitlich wie räumlich unabhängiger Kommunikation besonders deutlich.

Die beiden stashcat-Gründer Christopher Bick (links) und Felix Ferchland

Niedersachsens Innenminister Boris Pistorius (links) präsentiert den neuen Polizeimessenger „NIMes – Niedersachsen Messenger“

Gerade kleine und mittlere Unternehmen und Behörden sind darauf angewiesen, einfach, schnell und sicher ihre Arbeitsabläufe zu digitalisieren. Dazu Christopher Bick: „Spätestens der zweite Lockdown hat nochmals das Bewusstsein für die enorme Wichtigkeit der Digitalisierung geweckt. Abhängigkeiten vom Silicon Valley sind vielen Anwender*innen nicht zumutbar. Auch deshalb sind wir mit stashcat bereits in einigen Branchen Marktführer.“

Die Stärken von stashcat

Das Kernprodukt ist ein DSGVO-konformer High-Secure-Messenger, der sich dank integrierter Dateiablage, umfangreichen Kalenderfunktionen und einem Umfragemodul als zugängliches Kollaborationstool für Teams in unterschiedlichsten Organisationen bewährt hat. Optional sind auch Videotelefonie und -konferenzen möglich. Dabei kombiniert die Lösung die Funktionalitäten von bekannten Messengern und Cloud-Anwendungen wie WhatsApp oder Dropbox, gehostet wird datenschutzkonform im deutschen Rechenzentrum. stashcat bietet weitere wichtige Funktionen, wie beispielsweise eine von Handynummern unabhängige Kontaktdatenbank mit LDAP-Schnittstelle und Georeferenzierung. Unterstützt werden alle mobilen und stationären Endgeräte, die Nutzung ist via App oder Browser möglich.

Die Technik dahinter

Beim Versenden von Nachrichten wird eine Verschlüsselung auf dem Endgerät des Nutzers vorgenommen. Alle relevanten Daten werden somit auf dem Weg zum und vom Server verschlüsselt übertragen und auf den Servern ebenfalls verschlüsselt abgespeichert. Die übertragenen Daten werden durch aktuelle SSL/TLS-Verschlüsselungsverfahren gesichert. Die Server von stashcat befinden sich ausschließlich in Deutschland, durch den Betrieb von redundanten Server-Systemen und regelmäßigen, automatischen Backups wird einem Datenverlust durch Hardware-Ausfall vorgebeugt. Nutzerbezogene Daten werden direkt im hauseigenen Hochsicherheits-Datenzentrum gespeichert – wobei man sich ohnehin auf das Nötigste beschränkt und dank der Unabhängigkeit von Telefon- und Mobilnummer keinen Zugriff auf die persönlichen Kontakte der Nutzer*innen benötigt.

stashcat goes secunet – eine Partnerschaft mit Perspektive

„Messenger-Apps sind aus unserem Alltag nicht mehr wegzudenken. Im Gegensatz zu anderen Messengern stehen bei stashcat Sicherheit und Datenschutz klar im Vordergrund – das passt hervorragend zu den Ansprüchen von secunet und denen unserer Kunden“, erklärte Axel Deininger, Vorstandsvorsitzender von secunet. „Mit der Übernahme durch secunet schaffen wir ein zusätzliches Angebot zur sicheren und flexiblen Kommunikation und Kollaboration in Unternehmen, der Verwaltung und Sicherheitsbehörden wie zum Beispiel der Polizei.“

„Wir freuen uns, dass wir mit secunet einen starken Partner gefunden haben, der gemeinsam mit uns die erfolgreiche Geschichte von stashcat fortschreiben möchte,“ kommentierte stashcat-CEO Christopher Bick.

Mit der Übernahme begann für beide Seiten ein spannender Prozess. Für die unmittelbare Zukunft wird sich derzeit auf Vertriebsebene ausgetauscht, denkbar scheinen aber viele Möglichkeiten der Zusammenarbeit. Aljona Wehrhahn-Aklender, die als Produktmanagerin bei secunet das Thema „SINA Collaboration“ verantwortet, hält zum Beispiel eine Einbindung von stashcat als Anwendung auf den VS-Arbeitsplatz der SINA Workstations für eine spannende Möglichkeit zur Integration eines organisationsinternen Messengers in VS-Netzen. Alle Vorteile von stashcat könnten für die interne VS-Kommunikation eingesetzt werden und würden so den Funktionsumfang der SINA Workstations sinnvoll erweitern. Mit Blick in die Zukunft sind stashcat und secunet auch bezüglich der organisationsübergreifenden Kommunikation in intensivem Austausch. Christopher Bick blickt gespannt in die Zukunft: „Beide Unternehmen stehen für Innovationskraft und eine hohe Produktdynamik. Der gemeinsame Anspruch an die Sicherheit der angebotenen Soft- und Hardware sowie die Erfahrung und Expertisen beider Unternehmen werden zu weiteren, innovativen Lösungen führen“.

Christopher Bick
c.bick@stashcat.com

Das Klinikum Fürth

Web-Isolation im Krankenhaus

Gesundes Sicherheitsniveau

In kaum einer Branche kommen derzeit mehr Herausforderungen zusammen als im Gesundheitswesen – selbst ohne die Schwierigkeiten, die die aktuelle Pandemie verursacht. Schon lange bestehender Fachkräftemangel trifft auf dynamischen technologischen Fortschritt und Vernetzung, Konsolidierung von Standorten, Zusammenarbeit verschiedenster Fachgruppen unter Zeitdruck sowie natürlich Patientinnen und Patienten, die zu Recht einen respektvollen Umgang fordern – auch mit ihren sensiblen Daten. Wie lässt sich Cybersicherheit gewährleisten, ohne den täglichen Betrieb zu belasten? Das Klinikum Fürth hat gute Erfahrungen mit secunet safe surfer gemacht.

Ein ungehinderter Fluss von Informationen ist eine der wichtigsten Voraussetzungen für erfolgreiche Diagnose und Therapie: Patientenakten müssen zugänglich sein, Ärztinnen und Ärzte müssen auf aktuellste Studienergebnisse zugreifen können, der Austausch zwischen Fachgruppen im Krankenhaus und mit externen Spezialisten muss reibungslos verlaufen. Krankenhäuser sind daher immer mehr auf ihre digitale Infrastruktur angewiesen. Gleichzeitig sehen sie sich den gleichen Angriffsszenarien ausgesetzt wie alle vernetzten Unternehmen. Schadsoftware wie beispielsweise Ransomware und andere Zwischenfälle wie Phishing-Attacken betreffen immer wieder auch Einrichtungen im Gesundheitswesen und richten Schaden an, der nicht nur finanzieller Natur ist.

Cyberattacken in Krankenhäusern gefährden Menschenleben

Der letzte große Angriff auf ein Krankenhaus wurde im September 2020 bekannt: Das Düsseldorfer Uniklinikum wurde vom Verschlüsselungstrojaner

„Schon in der einmonatigen Teststellung überzeugte die unkomplizierte Nutzung des safe surfer."

Alexander Zetlmeisl, Leiter der IT am Klinikum Fürth

DoppelPaymer infiziert. Dieser verschlüsselte 30 Server des Uniklinikums und legte damit weite Teile von Forschung und Patientenversorgung lahm. Dem Erpresserschreiben zufolge war der Angriff zwar auf die Heinrich-Heine-Universität gerichtet gewesen – das änderte jedoch nichts daran, dass durch die Funktionsausfälle im Klinikum auch Patient*innen in Mitleidenschaft gezogen wurden, zum Teil mussten sie in weiter entfernte Häuser gebracht werden.

Bereits im März 2020 war die Uniklinik im tschechischen Brünn ebenfalls von einem Erpressungstrojaner befallen worden. Hier wurde mitten in der ersten Corona-Welle eines der größten SARS-CoV-2-Labore des Landes lahmgelegt, und auch hier mussten Patient*innen in weiter entfernte Kliniken verlegt werden.

Sicherheit durch Trennung von Arbeitsplatz und Internetzugang

Das Einfallstor für Schadsoftware und Phishing ist häufig der Internetzugang am Arbeitsplatz – trotz gängiger Sicherheitsmaßnahmen wie Virenscannern, Firewalls oder Content-Filtern. Den Internetzugang vollständig zu unterbinden ist allerdings in einer so heterogenen und informationsabhängigen Organisation wie einem Krankenhaus auch keine Option. Gefragt ist vielmehr eine Lösung, die den Nutzer*innen einen komfortablen Zugriff auf Ressourcen im Netz gestattet und gleichzeitig das Eindringen von Schadsoftware effektiv unterbindet.

secunet safe surfer fungiert als Web-Isolationslösung und Datenschleuse für sichere Internetnutzung. Die Lösung wurde auf der Basis der BSI-Sicherheitsarchitekturen Remote-Controlled Browser System (ReCoBS) und Browser-in-the-Box entwickelt. Dabei findet jede Browsersession in einer abgeschotteten Umgebung innerhalb eines speziell gehärteten Linux-Systems statt, das wiederum in einem separierten Netzsegment läuft. Diese entfernt stattfindende Browsersession wird vom Arbeitsplatz lediglich per Videostream ferngesteuert – nur Bild- und Tondaten werden übertragen. Durch diese sehr grundlegende Trennung werden sogar hardwarenahe Angriffe abgewehrt – neben allen gängigen Gefahren wie infektiösen Webseiten. Dennoch gestattet safe surfer das Anlegen von persönlichen Favoriten und den Upload und Download von Dateien wie ein nativer Browser. Mit der Zusatzfunktion safe reader lassen sich zudem infizierte E-Mail-Anhänge wirksam abblocken. Öffnet der Nutzer oder die Nutzerin einen kompromittierten Anhang mit safe reader, kann die Malware keinen Schadcode nachladen, da keine direkte Verbindung zum Internet besteht.

Erfolgreiche Einführung im Klinikum Fürth

Entscheidend für den Einsatz im Gesundheitswesen ist die Nutzerfreundlichkeit. Der safe surfer wurde so entwickelt, dass er wie ein herkömmlicher Browser mit allen Komfortfunktionen genutzt werden kann. Somit ist die Akzeptanz bei den Nutzer*innen gut und IT-Abteilungen werden nicht mit aufwändigen Schulungsmaßnahmen belastet.

Das bestätigen auch die Erfahrungen aus dem Klinikum Fürth, das den safe surfer 2020 hausweit eingeführt hat.

Anstoß für die Einführung des safe surfer gaben Berichte in der Fachpresse über Cyberangriffe auf große Kliniken sowie ein direkter Angriff (Emotet) auf das Klinikum im Dezember 2019. Im Februar 2020 nahm das Klinikum Kontakt mit secunet auf, ein erstes Webinar für ausgewählte Mitarbeiter*innen aus der IT-Abteilung fand statt. Kurz danach wurde das Einführungsprojekt gestartet.

Ausweitung auf Wunsch der Mitarbeiterinnen und Mitarbeiter

In diesem bestätigte sich die erhoffte Akzeptanz der Lösung: „Schon in der einmonatigen Teststellung überzeugte die unkomplizierte Nutzung des safe surfer, so dass wir die Zahl der Lizenzen im Einführungsprojekt auf Mitarbeiterwunsch hin deutlich erhöht

Über das Klinikum Fürth

Das Klinikum Fürth – ein Klinikum der Schwerpunktversorgung und universitäres Lehrkrankenhaus der Universität Erlangen-Nürnberg mit 13 Fachabteilungen sowie Instituten und Zentren – ist ein in der Region fest verwurzeltes, wirtschaftlich erfolgreiches Klinikum der Versorgungsstufe 2 mit 771 Betten sowie 36 Betten in der Geriatrischen Rehabilitation. Mehr als 2.500 engagierte Mitarbeiterinnen und Mitarbeiter versorgen jährlich 42.000 stationäre sowie 58.000 ambulante Patient*innen auf höchstem medizinischen und technischen Niveau. Dazu gehört insbesondere auch die minimal-invasive, roboterassistierte Chirurgie. Mit der umfangreichen baulichen Erweiterung und Erneuerung hat zudem im Rahmen eines der größten Krankenhausprojekte Bayerns der moderne, zukunftsweisende Umbau des Krankenhausstandortes Fürth bereits begonnen.

haben und damit nun alle Bereiche des Hauses mit einem sicheren Internetzugang versorgen“, so Alexander Zetlmeisl, Leiter der IT am Klinikum Fürth.

Pandemiebedingt verlief die Einführung von Frühjahr bis Sommer 2020 etwas langsamer als unter Normalbedingungen, seit Juli ist safe surfer nun aber im Produktivbetrieb. Eine flexible Erweiterung wird auch zukünftig möglich bleiben, denn safe surfer ist skalierbar im laufenden Betrieb, mit einem transparenten Lizenzmodell.

Akzeptanz auch auf den Stationen

Auch in den patientennahen Bereichen werde der safe surfer daher genutzt und habe nicht zu einem merklichen Anstieg der Supportanfragen an die IT geführt, berichtet das Klinikum Fürth. „Die Nutzung des Browsers funktioniert nahezu wie gewohnt. Ich kann beispielsweise Links in die Browserleiste kopieren, online Dateneingaben vornehmen oder entsprechende Daten sicher downloaden. Gerade in dynamischen Zeiten, wie in der aktuellen Pandemie, ist ein schneller, unkomplizierter und sicherer Datenaustausch mit anderen Kliniken – zum Beispiel auf Online-Portalen zu freien Behandlungskapazitäten – unerlässlich und für die tägliche Arbeit essentiell“, so Dr. Manfred Wagner, Medizinischer Direktor und Pandemiebeauftragter am Klinikum Fürth.

Und auch sonst schont safe surfer die Ressourcen in der IT-Abteilung: Durch einen Managementserver lässt er sich für alle Abteilungen zentral verwalten. Zahlreiche standardisierte Schnittstellen helfen bei Integration und Automatisierung.

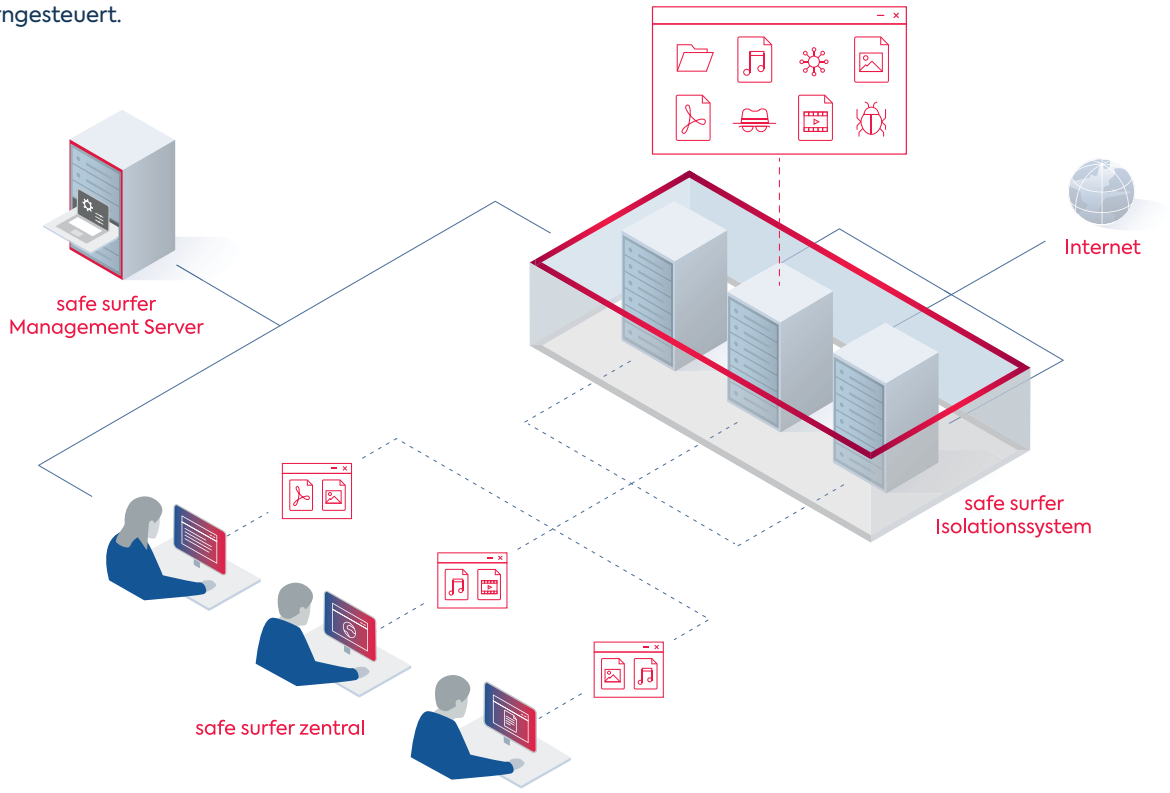
Nicht nur bekannte Angriffsvektoren werden abgewehrt

Das Klinikum Fürth ist zuversichtlich, mit dem safe surfer die optimale Lösung gefunden zu haben, um unbekannte Quellen isoliert zu halten. „Das Bundesamt für Sicherheit in der Informationstechnik (BSI) spricht sich dafür aus, den Zugriff auf das Internet über ein Remote-Controlled Browser System (ReCoBs) abzusichern. Dieser Empfehlung sind wir mit dem Einsatz von secunet safe surfer gerne gefolgt, um auch in dieser Hinsicht den Anforderungen aus dem IT-Sicherheitsgesetz an ein KRITIS-Haus zu entsprechen“, so Herbert Motzel, Leiter der Stabsstelle IT-Sicherheitssysteme am Klinikum Fürth.

Markus Ohnmacht
markus.ohnmacht@secunet.com

Interessierte Einrichtungen können kurzfristig einen Zugang zur Cloud-Testumgebung für secunet safe surfer erhalten und sich ein eigenes Bild von der Web-Isolationslösung machen.

Mit secunet safe surfer findet jede Browsersession in einer abgeschotteten Umgebung statt und wird vom Arbeitsplatz lediglich per Videostream ferngesteuert.



Informationstechnologie ist aus dem Arbeitsalltag in Kliniken kaum mehr wegzudenken.

Digitalisierung im Krankenhaus

Eine sichere Diagnose

Die elektronische Patientenakte ist nur das jüngste Symptom eines tiefgreifenden progressiven Digitalisierungsprozesses, der das gesamte Gesundheitswesen und damit auch die Krankenhäuser umtreibt. Dabei gilt: Der digitale Fortschritt braucht IT-Sicherheit, wenn er mehr Vorteile als Risiken bringen soll. secunet unterstützt mit langjähriger Erfahrung und umfassender Kompetenz.

Die Digitalisierung in der Medizin ist kein Selbstzweck: Pandemische Großlagen, demografischer Wandel, akuter Fachkräftemangel, herausfordernde Krankheitsbilder und optimierte Behandlungsmöglichkeiten verlangen eine Leistungsfähigkeit von Kliniken rund um die Uhr. Verwaltungs- und Versorgungsprozesse funktionieren nur, wenn der Zugriff auf medizinische Informationen und Anwendungen reibungslos abläuft. „Die Diagnose ist klar, und auch die Therapie: Nur eine moderne digitale Infrastruktur und die Vernetzung zahlreicher Datenquellen und medizinischer Gerätschaften bringt Entlastung und verbesserte Behandlungsoptionen in Krankenhäusern“, sagt Torsten Redlich, Leiter Abteilung Geschäftsentwicklung und stellvertretender Divisionsleiter eHealth bei secunet. „Gleichzeitig bedeutet der steigende Digitalisierungsgrad auch mehr Verletzlichkeit – neue Angriffsvektoren für Cyberattacken oder eine fehlende Beherrschbarkeit komplexer IT.“

Um Einrichtungen im Gesundheitsweisen möglichst umfangreich vor diesen Gefährdungen zu schützen, haben Bund und Länder im Krankenhauszukunftsgesetz (KHZG) zur Förderung der Digitalisierung in Kliniken festgelegt, dass mindestens 15 Prozent der bereitgestellten Mittel eines jeden Fördervorhabens in die IT-Sicherheit fließen müssen. Das ist für Krankenhäuser eine wichtige Grundlage, Datenschutz und Datensicherheit in den Projekten umfassend und von Beginn an zu berücksichtigen.

B3S legt Sicherheitsanforderungen fest

Um ein einheitlich hohes Schutzniveau der betriebskritischen IT herzustellen, werden IT-Sicherheitsmaßnahmen für Krankenhäuser an einem branchenspezifischen Standard (B3S für Krankenhäuser) ausgerichtet, der auch Nicht-KRITIS-Einrichtungen zur Orientierung dienen soll. Für KRITIS-Häuser ist er verpflichtend. „Um den B3S-Anforderungen Rechnung zu tragen, ist es wichtig, nicht nur einzelne Aspekte der Infrastruktur oder punktuell Lösungen in den Blick zu nehmen", so Redlich. „Es bedarf einer ganzheitlichen Sicherheitsarchitektur. Zudem sollten IT-Sicherheitslösungen direkt bei Anwender*innen eine hohe Nutzerfreundlichkeit aufweisen, damit der Arbeitsalltag in den Kliniken nicht beeinträchtigt wird."

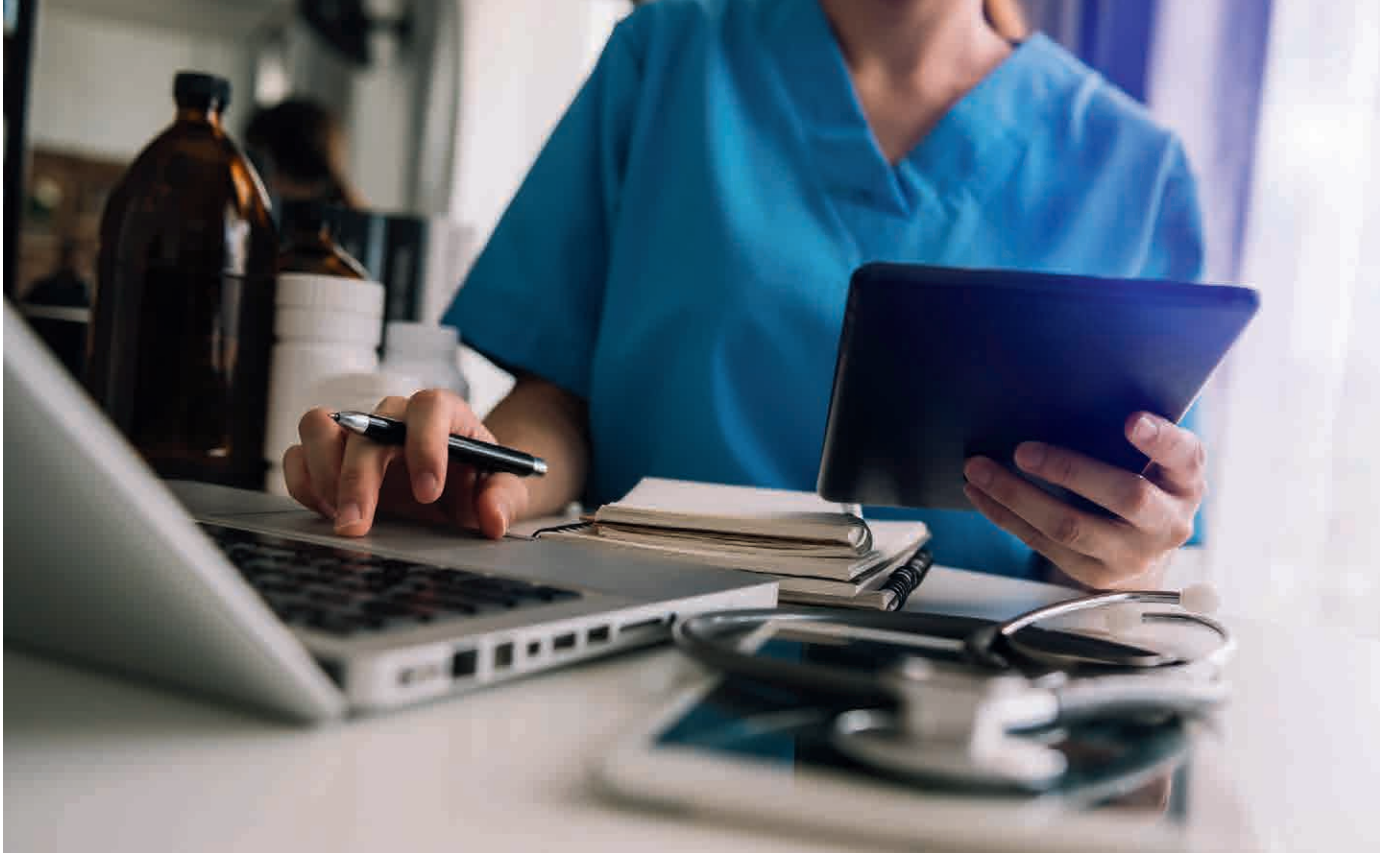
Eine solche nutzerfreundliche Lösung ist secunet safe surfer. Damit können Krankenhäuser die alltägliche Internetnutzung an sensiblen Arbeitsplätzen sicher gestalten: Bedrohungen von extern wie kompromittierende Websites, Phishing-Links, versteckte (verschlüsselte) Kommunikation zur Fremdsteuerung oder Datenabfluss werden unschädlich gemacht. Wie das in der Praxis aussieht, können Interessierte im Artikel „Gesundes Sicherheitsniveau" ab Seite 26 nachlesen.

Cloud am Horizont

Die nächste Phase der digitalen Transformation ist bereits abzusehen: „Der Trend in der Datenverarbeitung im Gesundheitswesen geht mehr und mehr in Richtung hyperkonvergenter Infrastrukturen, der Verschmelzung lokaler und zentraler Datenverarbeitung und der damit verbundenen übergreifenden Prozessroutinen", erklärt Redlich. „Die virtualisierten zentralisierten IT-Dienste werden aufgrund von Compliance-Vorgaben häufig noch „on premise" betrieben, bewegen sich aber stark in Richtung Auslagerung in die Cloud."

Daher werden aktuell weitere Konzepte erprobt, etwa zu Trusted Cloud Infrastructures, Edge-Plattformen und verteiltem Federated Machine Learning. Ziel ist es, sämtliche Wirkungskreise medizinscher Versorgung, wie zum Beispiel medizinische Netzwerke, Medizintechnik, Auswerteanalytik oder Medizinrobotik, sicher anzubinden – auch in ausgelagerten Computing- und Storage-Umgebungen (Cloud). Hier gilt es zunächst, wegweisende Sicherheitsfragen im Einklang mit der deutschen Gesetzgebung zu klären und die verfügbaren Sicherheitstechnologien als Basis für zahlreiche neue Anwendungen zu implementieren. secunet berät Krankenhäuser, Medizintechnikhersteller und Anbieter medizinischer Softwarelösungen dabei und realisiert sichere, vertrauenswürdige Infrastrukturen.

Torsten Redlich
torsten.redlich@secunet.com



Sicherer Zugriff auf die elektronische Patientenakte

Seit Anfang 2021 steht in Deutschland gesetzlich Versicherten die elektronische Patientenakte (ePA) zur Verfügung. Arztpraxen, Apotheken und Krankenhäuser können über die Telematikinfrastruktur (TI) darauf zugreifen. Dazu brauchen sie einen Konnektor mit Software-Upgrade für die Produkttypversion 4 (PTV4). Im Mai erhielt der secunet konnektor als erster im Markt die Zulassung dafür.

Bereits im Januar 2021 startete secunet gemeinsam mit dem Partner eHealth Experts eine Testphase mit dem Upgrade für die ePA. In ausgewählten Praxen und Krankenhäusern konnte die Funktionsfähigkeit und Sicherheit des Konnektors gemäß den Vorgaben der gematik, der Betreibergesellschaft der TI, erfolgreich nachgewiesen werden.

„Obwohl secunet gemeinsam mit dem Partner eHealth Experts erst spät in den Konnektormarkt eingestiegen ist, freuen wir uns natürlich umso mehr, dass wir als erster die Zulassung zum ePA-Upgrade erhalten haben. Für uns ist das auch die Bestätigung der Qualität unserer Arbeit“, erläutert Markus Linnemann, Leiter der Division eHealth bei secunet.

Ziel der ePA ist eine umfassende Vernetzung des deutschen Gesundheitswesens, sowohl zwischen verschiedenen Fachärzt*innen oder Apotheken als auch zwischen Arztpraxen, Apotheken und Patient*innen. Viele bisher analog oder in Papierform ablaufende Arbeitsschritte können durch die ePA digitalisiert und damit vereinfacht werden. Weitere Vorteile: Medizinische Informationen liegen transparent vor und erleichtern zukünftig viele Abläufe. Davon profitieren Patient*innen ebenso wie Ärzt*innen, Apotheker*innen, Therapeut*innen und anderes medizinisches Fachpersonal. Die Einrichtung und Nutzung einer ePA ist für Patient*innen freiwillig.

Cybersecurity für das vernetzte Fahrzeug

„Die gesamte Automotive-Branche ist gefragt“

Fahrzeuge werden stetig intelligenter und autonomer. Hersteller statten sie mit immer mehr Subsystemen aus, die von Sensoren mit Informationen gefüttert werden. So sollen die Automobile in bestimmten Verkehrssituationen eigenständiger reagieren können. Zugleich setzen die Autobauer auf ausgefeilte Software. Ziel ist es, das Fahrerlebnis sicherer und komfortabler zu gestalten, aber vor allem die zunehmend wichtiger werdende Kommunikation zwischen Fahrzeugen untereinander und mit der Verkehrsinfrastruktur zu ermöglichen. Der Bereich Automotive wird sich zu einem hochvernetzten System mit entsprechend vielen Schnittstellen entwickeln. Das wiederum potenziert die mögliche Angriffsfläche. Nur mit einheitlichen Security-Standards und strategischen Systemdesigns anstelle von Einzellösungen kann umfassende Sicherheit im Verkehr zukünftig gewährleistet werden.

Vom Parkassistenten bis hin zum autonomen Fahren – die software- und hardwarebasierte Technik von Fahrzeugen wird von Tag zu Tag vielfältiger und komplexer. Fahrassistenzsysteme, die auf das Internet, optische Kameras und Radargeräte zurückgreifen, gehören mittlerweile schon zum Standardrepertoire – und es ist nur eine Frage der Zeit, bis vollautonome Fahrzeuge öffentliche Straßen befahren. Hierfür müssen nicht nur ausgeklügelte Algorithmen herhalten, sondern auch immer mehr Informationen von außen miteinbezogen werden. Der Nachteil: Je vernetzter und intelligenter eine Verkehrsinfrastruktur wird, desto schwerwiegender können sich potenzielle Manipulationen dieses Systems auswirken. Das gilt nicht nur für einzelne Fahrer*innen, die darauf vertrauen müssen, dass die vom Auto verarbeiteten Informationen richtig sind. Denkbar wäre sogar der Kollaps einer gesamten Infrastruktur als Folge einer gezielten Beeinflussung.

Fahrzeuge werden Teil eines potenziell angreifbaren Systems

„Für eine umfassende IT-Sicherheit in der Verkehrsinfrastruktur reicht es nicht aus, die Fahrzeuge allein sicher zu machen. Denn je autonomer Autos werden, desto stärker sind sie von externen Informationen abhängig“, erklärt Jochen Schönweiß, Account Manager bei secunet, zuständig für Industriekunden der Region Südostdeutschland und Österreich. Die Informationen werden etwa von Verkehrsleitsystemen beziehungsweise den sogenannten Road Side Units, die unter anderem Daten über den Straßenzustand, Unfälle und mögliche Gefahren verarbeiten, übermittelt. Mit dieser Technik wird die Optimierung der Verkehrssicherheit und des Verkehrsflusses sowie die Reduzierung von Autoemissionen, beispielsweise durch eine verkürzte Fahrzeit, angestrebt.

Ein Auto jedoch, das hohen IT-Sicherheitsstandards gerecht wird, aber auf die Funktionen eines potenziell manipulierbaren Umfelds angewiesen ist, bleibt weiterhin gefährdet.

„Cybersecurity im Bereich Automotive kann nicht allein mithilfe von Einzellösungen gewährleistet werden – schon gar nicht im Falle einer hochvernetzten wie intelligenten Verkehrsinfrastruktur", betont Schönweiß. „Hersteller und Zulieferer sollten daher die gesamte technische Kette, angefangen bei der Hardware über Steuergeräte und interne wie externe Kommunikationsschnittstellen bis hin zum Backend, berücksichtigen und eine Gesamtlösung in Form eines umfassenden wie sicheren Systemdesigns anstreben."

Das Automobil – ein spezieller Kandidat für die IT-Sicherheit

Aber bereits die IT-Sicherheit eines Fahrzeugs zu garantieren, ist alles andere als trivial. Eine grundsätzliche Schwierigkeit besteht darin, dass die Hardware eines Autos typischerweise über dessen gesamten Lebenszyklus hinweg, also 20 Jahre und mehr, dieselbe bleibt. Das wäre in der schnelllebigen Unterhaltungselektronik, aber auch in anderen IT-Bereichen nicht denkbar, hier wird sie in regelmäßigen Abständen vollständig ersetzt. Im Gegensatz dazu ist die Hardware eines ansonsten noch fahrtüchtigen Autos irgendwann so alt, dass sie nicht mehr die Voraussetzungen erfüllt, um notwendige Softwareaktualisierungen zu integrieren. Hier steht die Autoindustrie vor einer großen Herausforderung.

Hinzu kommt: Gängige IT-Einzellösungen wie Public-Key-Infrastrukturen (PKI) oder Hardware-Sicherheitsmodule (HSM) verhindern zwar, dass Daten verändert oder gelesen werden können. Doch nützt dies wenig, wenn der Zugriff auf die Einzellösungen selbst nicht geschützt ist. „Im ungünstigsten Fall helfen HSM und PKI nach einem Angriff weiterhin perfekt beim Verschlüsseln und Signieren – aber dem Angreifer, der in das System eingedrungen ist", so Schönweiß. Auch kann etwa über einen Sicherheitschip die Dateninte-grität sichergestellt werden. Jedoch wird diese Maßnahme wirkungslos, wenn eine zweite, für die Analyse des Ergebnisses zuständige Software manipulierbar ist. Der beste Schutz der wichtigsten Schnittstellen ist unnütz, wenn sich über das Infotainmentsystem des Autos eine Schwachstelle und damit ein potenzielles Einfallstor auftut.

Der Zukunft einen Schritt voraus

Diese Beispiele zeigen: IT-Sicherheit für das vernetzte Fahrzeug muss ganzheitlich angegangen werden. Aber auch Flexibilität ist ein wichtiges Stichwort:

Jochen Schönweiß
jochen.schoenweiss@secunet.com

Harry Knechtel
harry.knechtel@secunet.com

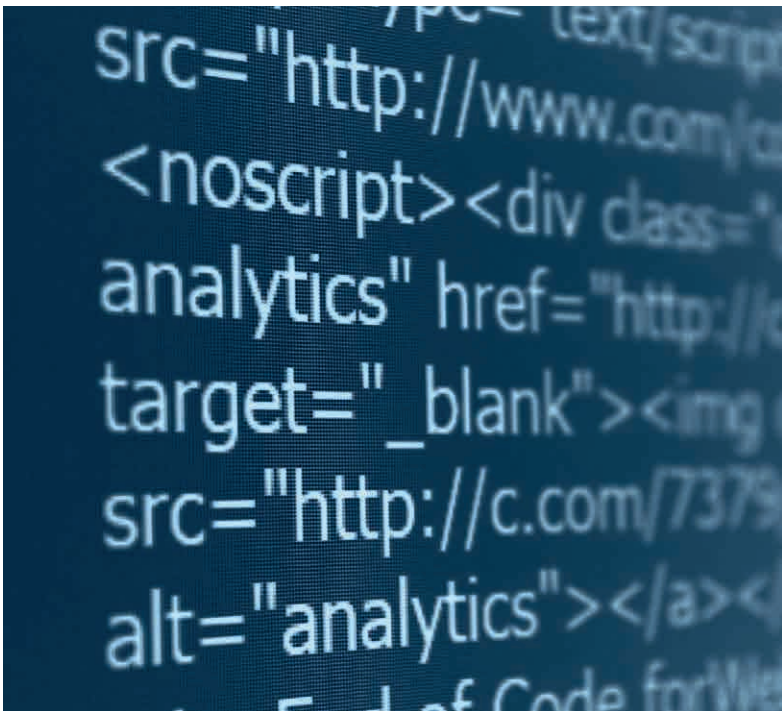
Anforderungen und Technologien ändern sich, darauf sollten Automotive-Unternehmen vorbereitet sein. Aus diesem Grund sind die Lösungen von secunet zum Beispiel nicht auf einen bestimmten HSM-Hersteller festgelegt. Über eine hauseigene Hardware Abstraction Layer gelingt sogar der gleichzeitige Betrieb von HSMs unterschiedlicher Hersteller. Auch die Cloud-HSM-Lösung von AWS wird unterstützt. Zudem ist ein Microservice Deployment möglich, so kann secunet seine PKI in Form von Docker-Containern zur Verfügung stellen. Darüber hinaus entwickelt secunet Prototypen, deren Anforderungen noch gar nicht vom Markt abgedeckt sind, oder implementiert bereits heute quantencomputerresistente Algorithmen.

Branchenweite Standards sind gefragt

„PKIs und HSMs können wichtige Elemente für ein einheitliches Systemdesign darstellen, sofern sie mit anderen Sicherheitskomponenten innerhalb einer stimmigen Gesamtarchitektur effektiv zusammenwirken“, sagt Harry Knechtel, Entwicklungsleiter der Division Industry von secunet, und ergänzt: „An dieser Stelle ist jedoch die gesamte Branche gefragt, die sich auf Rahmenbedingungen, besser noch auf konkrete Standards für die Sicherheitsanforderungen bei bestimmten Produkten einigen sollte.“ Ein gutes Beispiel für die Vereinheitlichung einer Car-2-Infrastructure-Communication ist die Norm ISO 15118, ein internationaler Standard für die Kommunikation zwischen Elektrofahrzeug und Ladeinfrastruktur, an deren Entwicklung secunet beteiligt war. Sie ermöglicht es, das Laden für die Nutzer*innen schneller und einfacher zu gestalten – das Motto lautet „Plug & Charge“ – und schützt zugleich dazugehörige Daten, etwa Informationen über Ladestromverträge, durch digitale Zertifikate.

Entwicklungen wie diese verdeutlichen, welche Chancen einheitliche IT-Sicherheitsstandards für die Branche bieten. Denn über den wichtigen Security-Aspekt hinaus ermöglichen diese mehr Kompatibilität und damit die nachgefragte Flexibilität von IT-Lösungen mithilfe von Modularisierungen. „Alles in allem“, resümiert Knechtel, „würden umfassende Regelungen auch die Wirtschaftlichkeit von Cybersecurity in der Verkehrsinfrastruktur erhöhen – und damit nicht zuletzt auch die IT-Sicherheit als solche.“

Zum Thema lesen Sie auch das Titelinterview der Fachzeitschrift ATZelektronik, Ausgabe 6/2021:



Live-Hacking als Security-Awareness-Maßnahme

Digitales Bauchgefühl entwickeln

„Wer von Ihnen nutzt bei seinem Handy den Fingerabdruckleser?“, fragt der IT-Sicherheitsexperte von secunet. Rund die Hälfte der rund 90 anwesenden Teilnehmer*innen zeigen auf und erfahren gleich darauf, wie leicht ein Fingerabdruck nachgeahmt werden kann. Die beiden secunet-Experten auf dem Podium formen kurzerhand mit Knete ein Positiv ihrer vorher erfassten eigenen Fingerabdrücke und demonstrieren, dass sich damit das Handy entsperren lässt. Es ist an diesem Vormittag nur eines von vielen Beispielen, die zeigen, mit welchen Tricks Cyberkriminelle vermeintliche Hürden schnell überwinden können. Das sogenannte Live-Hacking ist der Auftakt einer Awareness-Kampagne, mit der die Mitarbeiter*innen eines Unternehmens in den folgenden Monaten mittels Trainings, Plakaten, Flyern und mehr auf das Thema IT-Sicherheit und den eigenen Umgang damit aufmerksam gemacht werden.

In Unternehmen und Behörden schreitet die Digitalisierung voran. Um die Technik, die alltäglich zum Einsatz kommt, sicher zur Verfügung stellen zu können, ergreifen IT-Verantwortliche viele technische Maßnahmen. Doch ebenso wichtig ist es, dass sich Mitarbeiter*innen Fragen wie diese stellen: Wie sicher sind meine gewählten Passwörter? Wie leichtfertig gehe ich mit E-Mail-Anhängen um?

Gut gewappnet gegen digitale Bedrohungen ist, wer ein „digitales Bauchgefühl“ entwickelt. „Etwa 70 Prozent aller IT-Angriffe werden von den Nutzer*innen eingeleitet“, so Falk Gaentzsch, Senior Berater bei secunet. Oft werden zum Beispiel Sicherheitshinweise oder Fehlermeldungen ignoriert. „Wir sind darauf konditioniert, schnell Häkchen zu setzen und weiter zu klicken. Aber genaues Hinsehen ist wichtig: Kommt mir etwas komisch vor, hilft ein Anruf in der IT-Abteilung“, so Gaentzsch. Sensibilisierte Mitarbeitende sind die größte Hürde für E-Mail-basierte Angriffe auf IT-Systeme.

Live E-Mails abgreifen

In Live-Veranstaltungen demonstrieren Sicherheitsexperten, wie einfach Hacking geworden ist: Sie zeigen zum Beispiel, wie mit per E-Mail-Anhang eingeschleuster Schadsoftware die Festplatte ausgelesen wird. Die Beute: Passwörter, E-Mails oder geheime Quartalsberichte. Baukästen für Schadsoftware sind im Internet ganz einfach käuflich zu erwerben, wie ein Ausflug auf die entsprechenden Webseiten beweist. Ebenso warnen die Experten vor einem sorglosen Umgang mit WLAN unterwegs. „Das Handy verbindet sich mit dem stärksten Signal. Dieses Wissen nutzen auch Betrüger*innen, die ein öffentliches WLAN aufspannen und Daten abgreifen“, so Gaentzsch. Live führen die secunet-Experten vor, dass nur wenig Technik nötig ist, um ein WLAN-Signal auf dem Handy des Kollegen und auf den Handys der Zuhörerinnen und Zuhörer erscheinen zu lassen.

Lange Passwörter verwenden

Wie gute Passwörter dabei helfen können, den Zugang zu Daten zu erschweren, zeigt das Passwortraten. Dabei sollen die Teilnehmer eines Live-Hackings die tatsächlich gewählten Passwörter von Computernutzerinnen und -nutzern eines anonymisierten Unternehmens herausfinden – und werden meist fündig: Über ein Viertel der Passwörter lassen sich mit etwas Kreativität erraten. Dazu gehören zum Beispiel der Firmenname oder die Begriffe „geheim“, „Sommer“ oder „Passwort“. „Wir empfehlen ein

Passwort mit mindestens zwölf bis 14 Zeichen“, so Falk Gaentzsch. Merken lässt es sich zum Beispiel, wenn man die Anfangsbuchstaben und Zahlen von einem persönlichen Merksatz wählt. Sämtliche Passwörter können zusätzlich sicher in einem Passworttresor verwaltet werden.

Gegenmaßnahmen entwickeln

Bei Live-Hackings wird zwar in vielen verschiedenen Facetten gezeigt, mit welchen Methoden Angreifer*innen es schaffen, Computersysteme zu manipulieren oder Informationen abzugreifen. Der wesentliche Schwerpunkt liegt jedoch immer auf den konkreten Gegenmaßnahmen, die jede Benutzer*in persönlich treffen kann. Schließlich sollen die Teilnehmer*innen nicht demotiviert, sondern sensibilisiert werden.

Verschiedene Themenschwerpunkte

Kein Live-Hacking gleicht dem anderen. Das liegt zum einen am interaktiven Format, in dem das Publikum mit eingebunden wird und die Experten individuell auf die Fragen der Teilnehmer*innen eingehen. Zum anderen gibt es eine schier unendliche Anzahl an verschiedenen Themenfeldern, die präsentiert werden können. Diese erstrecken sich von Spezialthemen wie „Hacking von SCADA-Systemen, die in der Industrie zum Einsatz kommen“ oder „Sicherheit von Active Directory“ über alltägliche Themen wie „E-Mail-Sicherheit“ oder „Sicherheit von USB-Geräten“ bis hin zu speziellen Veranstaltungen, bei denen sich alles um das Thema „Social Engineering“ dreht.

Am Ende ist jedoch bei allen Themen wichtig, dass sie mit einem gewissen Augenzwinkern präsentiert werden. Auch wenn man das aus anderen Bereichen der IT-Sicherheit nicht gewohnt ist, darf hier auch geschmunzelt und gelacht werden – auch so baut man ein digitales Bauchgefühl auf.

awareness@secunet.com

Deutschlandstipendium

Perspektiven für junge Talente

Um Student*innen der Informatik und verwandter Fächer zu fördern, beteiligt sich secunet an den sogenannten „Deutschlandstipendien“. Was das ist und worum es dem Unternehmen dabei geht, erläutert Svenja Reinhardt, Leiterin des Bereichs Human Resources von secunet, im Interview.

Frau Reinhardt, wie will secunet beim Thema Personalgewinnung wettbewerbsfähig und zukunftssicher bleiben?

Svenja Reinhardt: Unsere Mitarbeitenden sind das wichtigste Kapital unseres Unternehmens. Doch wie in anderen Branchen auch wird es immer schwieriger, kompetente Fachkräfte zu finden. Daher ist es für uns umso wichtiger, bereits früh in Kontakt mit Studierenden zu treten, um verstärkt Aufmerksamkeit für IT-Sicherheit zu schaffen. Viele Informatikstudent*innen sind sich gar nicht bewusst, welche spannenden Perspektiven dieser Spezialbereich der IT bietet.

secunet arbeitet in der Forschung und auch beim Recruiting bereits seit Langem eng mit verschiedenen Universitäten zusammen. Darüber hinaus

beteiligen wir uns am Deutschlandstipendium des Bundesministeriums für Bildung und Forschung. Damit wollen wir dem Thema IT-Sicherheit an den Universitäten ein Gesicht verleihen, Talente fördern und sie für secunet begeistern. Wir haben dieses Jahr insgesamt acht Stipendienplätze vergeben. Die Unterstützung beginnt mit dem kommenden Wintersemester.

Wie kann man sich den Auswahlprozess für das Stipendium vorstellen? Gibt es bestimmte Kriterien?
Die Deutschlandstipendien zielen auf Studierende in den ersten Semestern eines Bachelorstudiengangs ab. Die Student*innen werden auf Basis verschiedener, bewusst breit gefasster Entscheidungsfaktoren wie Leistung, sozialem Engagement oder sozialem Hintergrund von den Hochschulen vorgeschlagen und schließlich von uns kontaktiert. Uns ist es außerdem sehr wichtig, Frauen für das Thema IT-Sicherheit zu gewinnen. Die IT-Sicherheitsbranche ist immer noch recht männerdominiert. Aus diesem Grund haben wir uns bewusst dafür entschieden, an der Ruhr-Universität Bochum drei Studentinnen für die Stipendienplätze auszuwählen.

Wie sieht die Unterstützung der Studierenden konkret aus?
Durch die Mittel der Bundesregierung und secunet können allen ausgewählten Studierenden 300 Euro pro Monat für eine Mindestdauer von zwölf Monaten, sprich zwei Semestern, zugesichert werden. Die Stipendiendauer gilt jedoch nicht einheitlich, sondern ist von der jeweiligen Hochschule abhängig. Teilweise ist eine jährliche Bewerbung für das Stipendium notwendig, während andere Hochschulen ein vollständig studienbegleitendes Programm anbieten.

Der wichtigste Aspekt für uns ist, dass wir an einer langfristigen Zusammenarbeit mit den jungen Talenten interessiert sind. Das gilt auch unabhängig vom Deutschlandstipendium. Wir unterhalten deutschlandweit zwölf Standorte und sind auch in der Nähe unserer verschiedenen Partner-Universitäten vertreten. So haben die Studierenden vor Ort die Möglichkeit, durch Praktika, als Werkstudent*innen sowie begleitend zur Bachelor- oder Masterarbeit secunet als Arbeitgeber kennenzulernen.

Svenja Reinhardt
svenja.reinhardt@secunet.com

Muss die IT-Sicherheitsbranche in Deutschland generell mehr tun, um ihr Themenfeld für Absolvent*innen attraktiver zu machen?
In den letzten Jahren ist in dieser Hinsicht schon einiges passiert: secunet zum Beispiel unterstützt eine Stiftungsprofessur am Institut für Internet-Sicherheit an der Westfälischen Hochschule in Gelsenkirchen. Ein Engagement lohnt sich, und zwar nicht nur für die Unternehmen selbst: Letzten Endes geht es um die digitale Souveränität Deutschlands und Europas beim Zukunftsthema IT-Sicherheit.

Vor zehn Jahren rief das Bundesministerium für Bildung und Forschung das Deutschlandstipendium ins Leben. Bund und private Förderer investieren damit in die Zukunft talentierter Studienanfänger*innen. Dies soll dazu dienen, Talente zu motivieren und sie auf ihrem Weg zu begleiten. So übernehmen Staat und Gesellschaft gleichermaßen Verantwortung für die Zukunft Deutschlands.

Sicherheit für die Industrie 4.0

secunet und Tech Data schließen Distributionsvertrag

secunet und Tech Data, einer der weltweit führenden IT-Distributoren, haben eine Kooperation geschlossen. Im Mittelpunkt steht die Lösung secunet edge, die eine sichere Digitalisierung, Vernetzung und Automatisierung im Industrial Internet of Things (IIoT) und im Edge Computing ermöglicht. Damit können Unternehmen das enorme Potenzial der Industrie 4.0 nutzen und zugleich die Sicherheitsrisiken minimieren.

Mit dem Vertrag baut Tech Data sein umfangreiches Portfolio von IT-Security-Lösungen im Bereich „Advanced Solutions" weiter aus und ergänzt es um IIoT-Security. Systemintegratoren und Vertriebspartner von Tech Data können ihren Kund*innen nun auf der Basis von secunet edge maßgeschneiderte IIoT-Lösungen bieten und so die digitale Transformation in Industrie und kritischen Infrastrukturen vorantreiben.

„Im Industrieumfeld setzen wir künftig vermehrt auf den indirekten Vertrieb", sagt Axel Deininger, Vorstandsvorsitzender von secunet. „Mit Tech Data haben wir dafür einen starken Partner gewonnen. Die Vertriebsexpertise und hervorragende Marktposition von Tech Data ergänzen die technologische Kompetenz von secunet im Bereich Industrie 4.0 in idealer Weise."

Ralf Stadler, Director der Business Unit Security, Mobility & IoT der Tech Data DACH, zu dem neuen Vertrag: „Ich freue mich sehr über den Vertragsabschluss mit secunet, mit dem wir nun noch konkreter unseren Vertriebspartnern im industriellen Bereich Sicherheitslösungen anbieten können. secunet hat in vielen Projekten bewiesen, dass sie widerstandsfähige, sichere digitale Infrastrukturen auf- und umsetzen können. Eine perfekte Ergänzung in meinen Augen auch für unsere Datech-Solutions-Partner, die viele Kund*innen im Industrie-4.0-Segment adressieren."

secunet spendet an Aktion Deutschland Hilft

Die Flutkatastrophe im Westen Deutschlands und in weiteren europäischen Ländern hat viele Menschenleben gekostet und Existenzen zerstört. Die Bewohner*innen der betroffenen Regionen und Orte werden noch lange mit den Auswirkungen der Ereignisse im Juli 2021 zu kämpfen haben.

Um die Hochwasseropfer zu unterstützen, hat secunet 50.000 Euro an die Aktion Deutschland Hilft gespendet. Dieses Bündnis deutscher Hilfsorganisationen leistet koordiniert Hilfe in Katastrophengebieten.

Wer sich über das Bündnis informieren oder ebenfalls spenden möchte, kann dies auf der folgenden Website tun:

www.aktion-deutschland-hilft.de/de/

Termine – Oktober bis Dezember 2021

Aufgrund der Corona-Pandemie ist verstärkt mit Änderungen zu rechnen.

12. bis 14. Oktober 2021
it-sa | Nürnberg

19. bis 22. Oktober 2021
Milipol | Paris, Frankreich

26. Oktober 2021
inova | Ilmenau

3. November 2021
Off-the-Record (Handelsblatt Health Circle) | digital

3. November 2021
Polizeitag Kiel | Kiel

15. bis 18. November 2021
Medica & Compamed | Düsseldorf

22. bis 24. November 2021
IKT Sicherheitskonferenz | Linz, Österreich

24. bis 25. November 2021
Handelsblatt Konferenz Health – The Digital Future | digital

24. bis 25. November 2021
Berliner Sicherheitskonferenz | Berlin

7. Dezember 2021
Azure Developer Community Day | München

13. bis 15. Dezember 2021
Zukunftskongress Staat & Verwaltung | Berlin

15. Dezember 2021
Polizeitag Düsseldorf | Düsseldorf

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: Europäische Kommission
S. 2, 4, 29, 31, 33: Adobe Stock
S. 3, 11, 12, 14, 18, 19, 21, 22, 23, 28, 37: secunet
S. 16: SSARM
S. 24, 25: stashcat
S. 26: Klinikum Fürth
S. 34: Bildschön/secunet
S. 35: alamy

klimaneutral gedruckt
www.klima-druck.de
ID-Nr. 21108075
bvdm.

FSC www.fsc.org
RECYCLED
Papier aus Recyclingmaterial
FSC® C006990

Damit sensible Daten nicht ungewollt auf Weltreise gehen.

Mit SINA sind Laptops und Tablets premiumsicher.

Wo sensible Daten und Kommunikation vor Cyberattacken geschützt werden müssen, steht secunet bereit. Als IT-Sicherheitspartner der Bundesrepublik Deutschland bieten wir mit dem SINA Mobil-Portfolio premiumsichere Clients bis zur Geheimhaltungsstufe GEHEIM.

secunet.com protecting digital infrastructures

secunet