secuview
Das secunet Kundenmagazin
1|2019

AXEL DEININGER NEUER SECUNET CEO

Kein Mangel an Zukunfts-themen

Sicherheit für die Industrie 4.0

Wie sich Maschinen im IoT-Umfeld vernetzen, absichern und überwachen lassen

Wandel an Europas Außengrenzen

Wie sich europäische Staaten auf das Einreise-/Ausreisesystem der EU vorbereiten

Vertrauen zwischen Maschinen: Wie die ifm-Unternehmensgruppe ihre Industrie-4.0-Komponenten mit digitalen Identitäten versieht

National

International

In eigener Sache

Technologien & Lösungen

Kurz notiert

Service

Interview mit Bernd Kowalski vom Bundesamt für Sicherheit in der Informationstechnik (BSI) zu den Biometrie-Vorgaben des neuen europäischen Einreise-/Ausreisesystems EES

Editorial

Liebe Leserinnen und Leser,

ab heute begrüßt Sie an dieser Stelle ein neues Gesicht. Zum 1. Juni 2019 habe ich den Vorsitz des Vorstands der secunet Security Networks AG von Dr. Rainer Baumgart übernommen, der nach 18 Jahren in dieser Position in den Ruhestand gegangen ist. Nun freue ich mich auf die großen und kleinen Aufgaben, die vor mir liegen. Als eine der kleineren gehört auch das Editorial der secuview dazu. Die Möglichkeit, regelmäßig einige Worte an Sie zu richten, werde ich gern wahrnehmen!

In den vergangenen Monaten hatte ich die Gelegenheit, mich intensiv mit einigen grundsätzlichen Fragen in Bezug auf secunet auseinanderzusetzen. Wie ist der Status quo, wo wollen wir hin, wie kommen wir dorthin? Antworten auf diese Fragen geben mein Vorgänger und ich in einem gemeinsamen Interview in dieser Ausgabe der secuview.

Nur so viel vorweg: Bei der IT-Sicherheit handelt es sich um einen außergewöhnlich dynamischen Markt, der ständig neue Kundenbedürfnisse generiert. Darauf wollen und werden wir uns bei secunet einstellen, indem wir uns stärker international orientieren und auch – mehr als bisher – den Industriesektor fokussieren.

Wie spannend die Veränderungsprozesse in der Industrie sind, die durch die Digitalisierung angestoßen wurden, zeigen zwei weitere Artikel in dieser Ausgabe: Das Unternehmen ifm stellt Komponenten für die Industrieautomation her, und diese Geräte werden mit vertrauenswürdigen digitalen Identitäten ausgestattet, damit sie in industriellen Infrastrukturen zweifelsfrei zugeordnet werden können. Zudem stellen wir dar, wie Maschinen im Umfeld der Industrie 4.0 sicher vernetzt werden können und mit Edge-Computing-Funktionen ihr volles Potenzial ausspielen.

Auch in unseren Kernmärkten tut sich einiges. Die Europäische Union führt im Jahr 2022 das Einreise-/Ausreisesystem EES ein, das die Schengen-Außengrenzen wirksamer absichern wird. Daneben wird das System aber auch erheblichen Mehraufwand bei der Grenzkontrolle verursachen. Viele Staaten führen daher automatische Grenzkontrolllösungen ein, die diesen Mehraufwand abfedern. In einem zwölfseitigen Themenspecial beleuchten wir den aktuellen Stand, mögliche Lösungen sowie bestehende Herausforderungen.

Nun wünsche ich Ihnen viel Spaß beim Lesen und eine schöne Herbstzeit!

Ihr Axel Deininger

Das Gas-und-Dampfturbinen-Heizkraftwerk Niehl 3 der RheinEnergie hat eine elektrische Leistung von 450 Megawatt und 265 Megawatt Fernwärme.
(c) RheinEnergie AG

SCHUTZ KRITISCHER INFRASTRUKTUREN

Sicherer als das IT-Sicherheitsgesetz vorschreibt

Die RheinEnergie AG versorgt rund 2,5 Millionen Menschen sowie Industrie, Handel und Gewerbe mit Energie, Trinkwasser, Erdgas und Wärme. Damit gehört das Unternehmen zu den kritischen Infrastrukturen, für die in Deutschland seit dem Jahr 2015 besondere Anforderungen an die IT-Sicherheit bestehen. Um diese abzudecken, hat sich die RheinEnergie entschieden, ein Informationssicherheits-Managementsystem (ISMS) einzuführen. Das System kommt unternehmensweit zum Einsatz und geht damit über die gesetzlichen Bestimmungen hinaus. Wir sprachen mit Patrick Porsch, der bei der RheinEnergie für die Etablierung des ISMS verantwortlich war.

Herr Porsch, Energie- und Wasserversorger wie RheinEnergie müssen sich mit einer ständig wachsenden Anzahl von Gesetzen und Regularien auseinandersetzen. Dazu gehören etwa das IT-Sicherheitsgesetz, branchenspezifische Sicherheitsstandards wie der B3S für virtuelle Kraftwerke oder die Sicherheitskataloge der Bundesnetzagentur. Jüngstes Beispiel ist der IT-Sicherheitskatalog für Energieanlagen, der im Dezember 2018 veröffentlicht wurde. Wie schafft es Ihre Organisation, mit dieser Flut umzugehen?

Stimmt, für ein Unternehmen wie die RheinEnergie, das in mehreren Sparten betroffen ist, ist der Umgang mit den vielen verschiedenen Anforderungen nicht einfach. Mit dem Betrieb des Strom- und Gasnetzes, der Wasserversorgung, dem virtuellen Kraftwerk für Sekundärregelleistung und den Kraftwerken sind wir von vier verschiedenen B3S bzw. Sicherheitskatalogen betroffen. Noch dazu enthalten diese Kataloge Anforderungen, die sich teilweise widersprechen.

Daher ist es für uns besonders wichtig, dass das Rahmenwerk des Informationssicherheits-Managementsystems (ISMS), welches wir in den letzten Jahren eingeführt haben, unternehmensweit einheitlich aufgebaut ist und nur sehr wenige bereichsspezifische Regelungen existieren. Eine Voraussetzung dafür war und ist die gute Zusammenarbeit der verschiedenen Hauptabteilungen, die sich alle auf das zentrale Rahmenwerk verständigen konnten.

Zudem ist der wertvolle Input von secunet im Rahmen des ISMS-Projekts zu nennen. secunet hat seine Kontakte zum Gesetzgeber eingebracht. So war es möglich, die gesetzlichen Anforderungen richtig zu interpretieren und umzusetzen.

Außerdem ist die Kommunikation innerhalb der für uns relevanten Branchen wichtig: Mit den anderen Energie- und Wasserversorgern tauschen wir uns regelmäßig über die Auswirkungen der gesetzlichen Änderungen und den Umgang damit aus, zum Beispiel im Verband kommunaler Unternehmen (VKU), im Bundesverband der Energie- und Wasserwirtschaft (BDEW) oder im Deutschen Verein des Gas- und Wasserfaches (DVGW).

Was gab seinerzeit den Anstoß zur Entwicklung des ISMS? Und wie gingen Sie bei dessen Aufbau vor?

Die Basis für den Beschluss, ein ISMS aufzusetzen, bildete das IT-Sicherheitsgesetz, das im Jahr 2015 in Kraft getreten ist. Wir sind jedoch über die gesetzlichen Anforderungen hinausgegangen: Obwohl lediglich einzelne Hauptabteilungen der RheinEnergie vom gesetzlich geforderten Geltungsbereich betroffen waren, haben wir uns dafür entschieden, das ISMS unternehmensweit auszurollen.

Security-Vorfälle kommen immer häufiger vor. Die Informationssicherheit wird damit für Unternehmen immer wichtiger. Daher wollten wir nicht nur die Informationssicherheit für die kritischen Infrastrukturen in unserem Unternehmen verbessern, sondern kontinuierlich das Sicherheitsniveau der gesamten RheinEnergie AG anheben.

Kurzfristig wirkt sich dies natürlich erstmal als Kostenfaktor aus. Mittel- und langfristig senken wir meines Erachtens durch IT-Sicherheitsmaßnahmen die Kosten, weil beispielsweise weniger Informationssicherheitsvorfälle auftreten, diese zudem früher erkannt und schneller behandelt werden können.

Dabei ist hervorzuheben, dass der Aufbau eines ISMS nach dem Top-Down-Ansatz erfolgen sollte: Es gilt, zunächst den Vorstand von dem Thema zu überzeugen und als Unterstützer ins Boot zu holen, dann sollte im nächsten Schritt die Einbindung der Abteilungen erfolgen. So sind wir auch beim Aufbau des ISMS vorgegangen. Zunächst haben wir ein unternehmensweites Rahmen- und Regelwerk definiert, um anschließend die Prozesse in den einzelnen Hauptabteilungen zu etablieren.

Welche Herausforderungen ergaben sich bei der Umsetzung?

Wegen der vielen verschiedenen Sektoren war eine Vielzahl von Anforderungen zu berücksichtigen, die alle unter einen Hut gebracht werden mussten. Wir hatten bereits mehrere Managementsysteme im Einsatz, etwa ein Qualitätsmanagementsystem oder ein Energiemanagementsystem. Informationssicherheit war in diesem Zusammenhang aber ein neuer Aspekt. Daher mussten viele Organisationseinheiten abgeholt und eingebunden werden. Insbesondere die Sensibilisierung der Mitarbeiter und Führungskräfte für das Thema Informationssicherheit war dabei sehr wichtig.

Insgesamt verlief die Umsetzung reibungslos, was unter anderem auf das fachliche Know-how der secunet-Mitarbeiter und die Art und Weise, wie sie ihr Wissen in das ISMS-Projekt eingebracht haben, zurückzuführen ist.

ZUM UNTERNEHMEN

Die RheinEnergie AG ist ein in Köln und der rheinischen Region verankerter, bundesweit aktiver Energiedienstleister, der neben Trinkwasser und Energie zahlreiche Energiedienstleistungen anbietet. Durch die Kooperation mit Unternehmen aus der Region hat sich die RheinEnergie sicher im deutschen Energiemarkt positioniert. Seiner Heimat bleibt das Unternehmen dabei eng verbunden und fördert mit seinen Lösungen die Wirtschaftskraft in Köln und dem Umland.

Hauptverwaltung der RheinEnergie AG am Parkgürtel in Köln
(c) RheinEnergie AG

Patrick Porsch
Informationssicherheitsbeauftragter der RheinEnergie AG
(bis Mai 2019)

IM INTERVIEW

Patrick Porsch war von Juni 2016 bis Mai 2019 bei der RheinEnergie AG als Informationssicherheitsbeauftragter tätig. In dieser Funktion war er für die Informationssicherheit der RheinEnergie verantwortlich. Er stellte sicher, dass die gesetzlichen Anforderungen an die Informationssicherheit eingehalten wurden und das Informationssicherheitsniveau kontinuierlich verbessert und überprüft wurde. Insbesondere kümmerte er sich um den Aufbau, die Steuerung und die Etablierung des Informationssicherheits-Managementsystems (ISMS). Zusätzlich war er mit der Ausgestaltung des IT-Notfallmanagements beschäftigt, um die Fortführung der IT-Services bei Unterbrechungen des IT-Betriebs gewährleisten zu können.

Vor dem Einsatz als Informationssicherheitsbeauftragter arbeitete Patrick Porsch als Softwareentwickler und Scrum Master für die RheinEnergie und begleitete in dieser Funktion mehrere agile Projekte. In dieser Zeit beschäftigte er sich bereits mit der Informationssicherheit der selbstentwickelten Anwendungen.

Welche Vorteile hat die Umsetzung eines ISMS für RheinEnergie?

Zunächst einmal hilft uns das ISMS, Sicherheitsrisiken frühzeitig zu erkennen und zu senken. So entsteht ein definiertes und transparentes Sicherheitsniveau. Informationen im Geltungsbereich des ISMS werden vor Bedrohungen im täglichen Betrieb stets angemessen geschützt.

Ein weiterer wichtiger Aspekt ist, dass wir mit dem ISMS eine Sicherheitskultur etablieren konnten, die von allen Mitarbeitern mitgetragen wird, insbesondere vor dem Hintergrund der Versorgungssicherheit für unsere Kunden.

Zudem ist durch das ISMS die Konformität zu allen relevanten Rechtsvorschriften gewährleistet. Last but not least unterstützt das ISMS unsere Unternehmensstrategie: Es ist uns wichtig, dass Gesellschafter, Kunden, Partner und Mitarbeiter die RheinEnergie als verantwortungsbewussten und vertrauenswürdigen Energieversorger wahrnehmen. Dazu leistet auch Informationssicherheit einen wertvollen Beitrag.

Wie hat das Risikomanagement – in Form des ISMS – Einfluss auf den täglichen IT-Sicherheitsbetrieb genommen? Welche Änderungen hat es gegeben? Sind positive Effekte sichtbar? Sind an manchen Stellen neue Herausforderungen entstanden?

Viele bereits vorhandene Prozesse haben wir hinsichtlich der Informationssicherheit optimiert, zum Beispiel die Berechtigungsvergabe oder das Change Management. Informationssicherheit betrifft letztendlich jeden Prozess und jedes IT-System in den kritischen Infrastrukturen. Dies wird auch von den Mitarbeitern immer mehr als integraler Bestandteil ihres Aufgabengebiets wahrgenommen.

Anfangs stellten Risikoanalysen und daraus abgeleitete Maßnahmen einen zusätzlichen Aufwand dar. Dieser blieb von den Mitarbeitern nicht unbemerkt, da er in der Regel zusätzlich zu den bisherigen Aufgaben anfiel. Wir haben daher die Vorteile klar kommuniziert und den Mehrwert für die einzelnen Mitarbeiter hervorgehoben. Ein Beispiel: Wenn Mitarbeiter ihre Prozesse detaillierter dokumentieren, ergibt sich ein klarer Vorteil, falls Kollegen für längere Zeit ausfallen. Denn dann ist man unabhängig von deren „Kopfmonopol“ und kann die Prozesse weiterhin umsetzen. Dies führte dann auch zu einer gesteigerten Akzeptanz bei den Mitarbeitern.

Positive Effekte ergaben sich auch dadurch, dass beim Einkauf von Dienstleistungen und Produkten die Informationssicherheit stärker in den Fokus gerückt ist und sich die Anforderungen an die Dienstleister und Lieferanten in dieser Hinsicht verändert haben. Auch dadurch konnten wir eine Verbesserung der Informationssicherheit bei RheinEnergie feststellen.

Welche Auswirkungen hat das ISMS auf die IT-Infrastruktur?

Natürlich hat das ISMS auch zu technischen Veränderungen geführt: Wir haben sowohl präventive als auch detektive Sicherheitsmaßnahmen realisiert. IT-Sicherheit ist ein Prozess, der nie abgeschlossen ist, und daher wollen wir uns in dieser Hinsicht kontinuierlich weiter verbessern und fortlaufend an der Sicherheit der IT-Infrastruktur arbeiten.

BAYERISCHE STEUERVERWALTUNG

Sensible Daten analysieren – im Mobile Office

Wo Finanz- und Steuerdaten mobil bearbeitet werden, ist maximale Absicherung gefragt. Wie dies ohne große Einbußen bei Effizienz und Benutzerkomfort gelingen kann, ist eine Frage, die sich der Bayerischen Steuerverwaltung im Jahr 2018 stellte. Ausgangspunkt war der Aufbau einer Analyseeinheit mit der Aufgabe, zu statistischen Zwecken sowie für Geschäftsprüfung und Controlling sensible Daten auszuwerten. Da klar war, dass viele Mitarbeiter der neuen Einheit von unterwegs aus arbeiten würden, sollte die neue IT-Infrastruktur dies ermöglichen – und gleichzeitig sehr hohen Sicherheitsanforderungen genügen.

Bei der Suche nach einer Lösung rückten die Clientsysteme schnell in den Mittelpunkt der Überlegungen. „Clientsysteme sind die Augen, Ohren und Finger einer Verwaltung, und damit ihr erweitertes Gehirn“ – dies war eine der Prämissen für das Projekt. Die zentrale Stellung der Clients macht sie besonders sicherheitsrelevant. Anders gesagt: Sobald ein Client kompromittiert ist, laufen viele Sicherungsmechanismen ins Leere.

Dies führte den IT-Betrieb der Bayerischen Steuerverwaltung schließlich zu einer SINA Infrastruktur: Die Sichere Inter-Netzwerk Architektur SINA kann eine maximale Absicherung bis hin zum Endgerät garantieren. Dabei kommt mit der SINA Workstation ein Client zum Einsatz, der verschiedene Sicherheitsdomänen auf einer Maschine abbilden kann, die gegeneinander abgeschottet sind.

Und wie sieht die Lösung heute konkret aus? Über eine Datendiode werden die Daten aus dem Rechenzentrum in den abgesicherten Bereich übergeben. Es bestehen zwei Zonen: eine normalsichere und eine hochsichere Zone. In der normalsicheren Zone haben die Mitarbeiter über LTE, WLAN oder LAN Zugriff auf ihre normale Büroumgebung. In der hochsicheren Zone können sie auf die dort in Datenbanken und sonstigen Dateisystemen abgelegten sensiblen Daten zugreifen. Die hochsichere Zone stellt dabei ein zusätzliches VPN im VPN dar.

Somit genügt die Lösung den beiden Anforderungen Mobilität und Sicherheit und lässt sich zudem auf einfache Weise verwenden: Nutzer der SINA Workstation benötigen keinerlei gesondertes IT-Wissen.

Christian Eisenried
christian.eisenried@secunet.com

Haupteingang des Dienstgebäudes des Bayerischen Landesamts für Steuern in München
(c) Bayerisches Landesamt für Steuern

THEMENSCHWERPUNKT: EINREISE-/AUSREISESYSTEM DER EU

Wandel an Europas Außengrenzen

Ab dem Jahr 2022 wird das Einreise-/Ausreisesystem (Entry-/Exit-System, EES) der Europäischen Union die Außengrenzen des Schengen-Raums absichern – und die Grenzkontrollprozesse dort erheblich verändern. Denn mit Einführung des EES müssen sich sämtliche Angehörigen von Drittstaaten, die in ein Land des Schengen-Raums einreisen wollen, an der Grenze mit vier Fingerabdrücken und Gesichtsbild registrieren lassen. Dieser Prozess löst das bisherige Stempelverfahren bei Reisepässen ab. Die biometrischen Daten werden zusammen mit weiteren Informationen zur Identität der Reisenden in einer zentralen Datenbank, die von der EU-Agentur eu-LISA betrieben wird, gespeichert. So wird es künftig einfacher zu überprüfen, wer sich innerhalb des Schengen-Raums aufhält und wer Aufenthaltsfristen überschreitet. Dies dient dem Schutz vor illegaler Einreise, Dokumenten- und Identitätsbetrug sowie organisierter Kriminalität und Terrorismus.

Für die Grenzkontrollbehörden der Schengen-Staaten ergeben sich durch die Einführung des EES einige Herausforderungen. Die Registrierung der Drittstaatsangehörigen an sämtlichen Land-, See- und Luft-Außengrenzen des Schengen-Raums bedeutet einen hohen Mehraufwand, sodass mit erhöhten Abfertigungszeiten und damit langen Schlangen an den Grenzen zu rechnen ist. Eine Lösung für dieses Problem besteht in der Automatisierung einzelner Elemente des Grenzkontrollprozesses. Während viele Länder diesen Weg an ihren internationalen Flughäfen bereits gehen – zum Beispiel durch den Einsatz von eGates –, bestehen gerade für Landgrenzen noch offene Fragen. Die folgenden Seiten beleuchten den Stand der Dinge aus unterschiedlichen Perspektiven.

ZAHLEN UND FAKTEN ZU DEN SCHENGEN-AUSSENGRENZEN

Zu Lande, zu Wasser und in der Luft

Die Schengen-Außengrenzen in Zahlen

644
Grenzüber-gangsstellen an Flughäfen

7.721 km
Landgrenze

42.673 km
Seegrenze

26
Staaten

Quelle: EU-Kommission

Regulärer, legaler Grenzverkehr pro Jahr

306.904.064
Grenzübertritte Gesamt

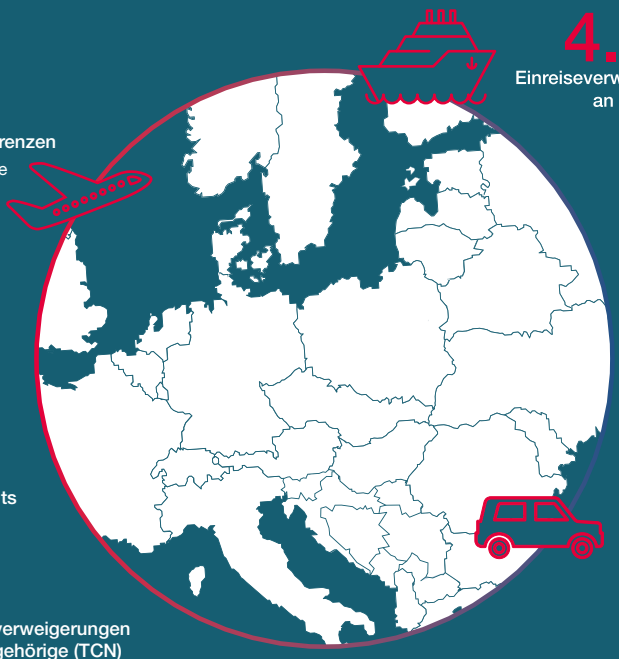
176.736.561
via Luftgrenzen

112.468.517
via Landgrenzen

17.698.986
via Seegrenzen

Quelle: Projekt SMILE – SMart mobILity at the European land borders, Zahlen aus 2017

Risiken und Herausforderungen



54.780
Einreiseverweigerungen an Luftgrenzen
z. B. aufgrund gefälschter Dokumente

6.667
Drittstaatenangehörige mit gefälschten Reisedokumenten bei der Einreise in den Schengenraum

361.636
erkannte Fälle illegalen Aufenthalts

504.590
Einreise- oder Aufenthaltsverweigerungen in Bezug auf Drittstaatsangehörige (TCN)
(Quelle: SIS Statistik)

4.481
Einreiseverweigerungen an Seegrenzen

150.114
erkannte illegale Grenzübertritte an EU-Außengrenzen

2.258
erkannte heimliche Grenzübertritte
z. B. Personen, die sich in Zügen, LKWs und anderen Fahrzeugen verstecken

131.641
Einreiseverweigerungen an Landgrenzen

Quelle: Frontex Risk Analysis (soweit nicht anders vermerkt)
Zahlen aus 2018

EES-VORBEREITUNGEN AN DEN LUFTGRENZEN

Mittlerweile Mainstream: Automatisierte Grenzkontrolle

Heute sind bereits mehr als 300 secunet easygates an großen internationalen Flughäfen im Einsatz, etwa in Deutschland, Österreich, Tschechien und Island. Die neuesten Installationen fanden in Litauen, Polen und Ungarn statt. Automatisierte Grenzkontrollsysteme können helfen, erhöhte Aufwände und Wartezeiten infolge der Einführung des europäischen Einreise-/Ausreisesystems EES zu vermindern.

Automatisierte Grenzkontrollsysteme wie das secunet easygate ermöglichen es in Verbindung mit elektronischen Identitätsdokumenten, die Grenzkontrolle in weiten Teilen durch automatisierte Prozesse zu beschleunigen. Die Mehrheit der Passagiere, die früher am Grenzkontrollschalter in der Warteschlange standen, kann somit heute den Grenzübertritt in Eigenregie vornehmen.

Der automatisierte Prozess ist denkbar einfach und weltweit inzwischen weit verbreitet. Daher sind die Passagiere zunehmend gut damit vertraut: Das secunet easygate überprüft optisch wie elektronisch die Authentizität des vorgelegten elektronischen Identitätsdokuments. Zudem liest das System das Gesichtsbild des Reisenden vom Chip im elektronischen Identitätsdokument aus und vergleicht die biometrischen Daten mit dessen Livebild. Dies alles geschieht innerhalb weniger Sekunden. Reisende nutzten die secunet easygates bereits rund 75 Millionen Mal. Die letzten neu installierten Systeme stehen an den internationalen Flughäfen Vilnius (VNO), Liszt Ferenc in Budapest (BUD), Debrecen (DEB), Chopin in Warschau (WAW) sowie Warschau-Modlin (WMI).

Von der Automatisierung profitieren sämtliche beteiligten Parteien: Grenzpolizeien werden entlastet, denn die Beamten überwachen den Prozess an nachgelagerten Monitoring-Arbeitsplätzen und können sich dabei auf diejenigen Reisenden konzentrieren, bei denen weitere Überprüfungen notwendig sind. Flughäfen profitieren von einem höheren Passagierdurchsatz. Die Reisenden schließlich freuen sich über kürzere Wartezeiten und die Möglichkeit, den Prozess selbst in die Hand zu nehmen.

secunet easygates am internationalen Flughafen in Vilnius, Litauen

› Wir sind sehr froh, mit einem flexiblen und erfahrenen Anbieter zusammenzuarbeiten, mit dessen Know-how wir eine Lösung implementieren können, die unseren Erwartungen entspricht. Dabei ist es uns wichtig, auch auf Best Practices anderer Flughäfen zurückgreifen zu können. ‹

Lina Laurynaitytė, Technology Project Manager,
Lithuanian Airports (LTOU)

Die europäischen Staaten stehen zurzeit zunehmend unter Druck, ihre Grenzkontrollprozesse zu optimieren: Bei weiterhin steigenden Passagierzahlen und unveränderter Infrastruktur würde die Einführung des EES, die ab 2022 europaweit geplant ist, für großen Mehraufwand sorgen. Denn dann wird es vorgeschrieben sein, deutlich umfassendere Prüfungen und die Erfassung von biometrischen Merkmalen bei der Einreise von Passagieren von außerhalb des Schengen-Raumes, sogenannten Drittstaatsangehörigen (Third Country Nationals, TCN), vorzunehmen. Längere Warteschlangen an den Grenzen sind demnach zu befürchten. Dieser Mehraufwand kann durch eine Automatisierung und Prozessoptimierung an den entscheidenden Stellen abgefedert werden: Alle Passagiere, die nicht zwingend am Grenzkontrollschalter überprüft werden müssen, werden direkt zu den automatisierten Systemen geleitet.

Automatisierte Grenzkontrollsysteme sind nicht nur als Einzelkomponenten, sondern auch als Elemente umfassenderer Lösungen verfügbar. So besteht das Produktportfolio secunet border gears aus einer Reihe von interoperablen Komponenten, die zusammengenommen eine verzahnte, modulare Grenzkontrollinfrastruktur ergeben. Sie decken bereits jetzt die Anforderungen des EES ab und lassen sich einzeln – oder als Gesamtlösung – in bereits bestehende Infrastrukturen integrieren. So kommt in vielen europäischen Projekten mit automatisierten Grenzkontroll-Lösungen neben den secunet easygates auch die zentrale Serverinfrastruktur secunet easyserver zum Einsatz. Diese sorgt zum Beispiel für einen zuverlässigen, schnellen und sicheren Zugriff auf Polizei-Hintergrundsysteme, Public-Key-Infrastrukturen (PKI) und Masterlisten.

Die Grenzkontrollprodukte des secunet border gears Portfolios sind erfolgreich seit vielen Jahren unter Berücksichtigung der jeweils landes- und kundentypischen Anforderungen im Einsatz: Bei jeder neuen Implementierung fließt implizit auch das Know-how aus der Zusammenarbeit mit anderen Flughäfen und Sicherheitsbehörden ein.

Georg Hasse
georg.hasse@secunet.com

10 JAHRE SECUNET EASYGATE: SICHERHEIT UND BENUTZERKOMFORT BEI DER GRENZKONTROLLE

Der Grundstein für das secunet easygate wurde im Jahr 2009 mit dem Start des EasyPASS-Pilotprojektes am Flughafen Frankfurt am Main gelegt. Als Generalauftragnehmer des Bundesamts für Sicherheit in der Informationstechnik (BSI) war secunet für dessen Planung, Umsetzung, Auswertung und für die Integration des Gesamtsystems verantwortlich. secunet lieferte die Softwareplattform secunet biomiddle, die das EasyPASS-System einzigartig flexibel macht, und unterstützte bei den Tests und der Entwicklung dieser neuen Grenzkontrolltechnologie.

Seit 2010 gehört EasyPASS fest zur Grenzkontrollstrategie der Bundespolizei. In enger Zusammenarbeit mit der Bundespolizei weiterentwickelt, zeichnet sich die aktuelle Generation der eGates unter anderem durch ihre einzigartige Überwindungssicherheit und eine optimierte intuitive Benutzerführung aus, die einen schnellen Passagierdurchlauf ermöglicht. In den Sommermonaten 2019 konnte EasyPASS einen Nutzerrekord von mehr als zwei Millionen Passagieren pro Monat verzeichnen, die mittels der automatisierten Grenzkontrollsysteme an deutschen Flughäfen die Grenze passiert haben.

„Automatisierung ist einer der Schlüsselfaktoren“

Im Interview: Petr Malovec, Leiter des National Border Situation Centre, Tschechische Grenzpolizei

COL. Mgr. Petr Malovec Ph.D. ist seit 2001 im Bereich der Grenzkontrolle tätig. In 2008 begann er mit umfangreichen Aktivitäten zur Bereitstellung biometrischer Daten und der zugehörigen PKI-Infrastruktur für die Grenzkontrollverfahren, die mit der erfolgreichen Implementierung von automatisierten Grenzkontrollsystemen (ABC-Systemen) am Václav-Havel-Flughafen in Prag endeten.

Als Leiter des National Border Situation Center ist er verantwortlich für den erfolgreichen Einsatz aller IKT-Technologien und -Systeme im Bereich Grenzschutz mit einer Vielzahl von Anwendungsfällen – von stationären über mobile bis hin zu ABC-Kontrollen.

Petr Malovec
Tschechische Grenzpolizei

Herr Malovec, welche Auswirkungen hat die Einführung des europäischen Einreise-/Ausreisesystems (EU Entry-/Exit-System, EES) auf die Grenzkontrolle?
Es ist offensichtlich, dass wir die Funktionalität der stationären Grenzkontrolllösung, die wir aktuell nutzen, erweitern müssen, um die EES-Verordnung in vollem Umfang zu erfüllen. Neben der Funktionalität stellt jedoch der Gesamtdurchsatz bei der Grenzkontrolle eine der größten Herausforderungen dar, auf die wir uns konzentrieren sollten. Das gilt insbesondere für den Václav-Havel-Flughafen in Prag, in dem sich die Situation ganz anders darstellt als bei kleineren Flughäfen, die einen niedrigeren Durchsatz an Reisenden und Drittstaatsangehörigen (Third Country Nationals, TCN) verzeichnen.

Welche Maßnahmen ergreift die tschechische Grenzpolizei in Vorbereitung auf die Einführung des EES?
Aktuell haben wir eine umfassende Projektstudie durchgeführt. Dazu gehört auch eine detaillierte Konzeptionsphase, in der wir geeignete Maßnahmen festlegen. Alle Ergebnisse der Studie werden regelmäßig von den Beteiligten am Prager Flughafen und an anderen Flughäfen diskutiert, um beispielsweise Umgestaltungsmaßnahmen an bestehenden Grenzkontrollstandorten ins Auge zu fassen.

Wir sind überzeugt, dass Automatisierung einer der Schlüsselfaktoren ist, die den gesamten Prozess unterstützen können. Im Hinblick auf die biometrische Erfassung, die vom EES gefordert wird, zeigt die Studie den Bedarf an einer effizienten Lösung zur automatisierten Erfassung von Gesichtsbildern, die allen relevanten Standards und Durchführungsbestimmungen entsprechen. Zwar steht eine solche Lösung ganz oben auf unserem Wunschzettel, aber sie ist nicht leicht zu finden.

Welche Erfahrungen haben Sie mit der Nutzung von eGates oder ABC-Gates (automatisierten Grenzkontrollschleusen) durch Drittstaatsangehörige gemacht?
Kürzlich haben wir in Prag das ABC-System EasyGO testweise für Staatsbürger aus Südkorea eröffnet. Dabei handelt es sich um eine temporäre Maßnahme bei der Ankunft eines täglichen Flugs aus Seoul, der im Durchschnitt 90 % Reisende aus Drittstaaten befördert. Bis jetzt zeigt der Test, dass sich der Einsatz von ABC-Gates in diesem Zusammenhang vorteilhaft auswirkt. So planen wir die Verwendung von ABC-Gates für das EES-Anwendungsszenario „Ausreise“, also beim Verlassen des Landes.

Welche Herausforderungen birgt der mögliche Brexit für den Grenzkontrollprozess am Václav-Havel-Flughafen in Prag?
Im günstigsten Fall werden Reisende aus Großbritannien nach dem Brexit als Freizügigkeitsberechtigte (Freedom Of Movement Travellers, FOM) gelten. Dann sind sie berechtigt, die für Reisende aus der EU, aus dem Europäischen Wirtschaftsraum und aus der Schweiz vorgesehenen Grenzkontrollverfahren zu nutzen. Andernfalls würden wir einen Anstieg von Reisenden aus Drittstaaten um ca. 25 % verzeichnen. Da wir jedoch alle möglichen unterstützenden Maßnahmen ergreifen möchten, planen wir, die Anzahl der Grenzkontrollschalter und eGates in beiden Grenzkontrollbereichen des Prager Flughafens zu erhöhen. Wir gehen davon aus, dass eine maximale Automatisierung des Grenzkontrollprozesses hier helfen kann.

Werden neben automatisierten Systemen an Flughäfen auch mobile Systeme in Tschechien eine Rolle spielen?
In dieser Hinsicht stellt sich die Situation in der Tschechischen Republik deutlich einfacher dar als bei den Luftgrenzen, da sich unsere Landgrenzen nicht mit Schengen-Außengrenzen überschneiden. Allerdings werden kleine Flughäfen auf der sprichwörtlichen grünen Wiese oder auch provisorische Flughäfen mobile Lösungen benötigen. Die tschechische Grenzpolizei nutzt bereits eine mobile Lösung, mit der sich Reisedokumente jeder Art, einschließlich Visummarken, kontrollieren lassen. Wir erwarten, dass diese Lösung künftig um sämtliche EES-relevanten Funktionen erweitert wird, insbesondere zu Zwecken der Dokumentenprüfung.

EES-IMPLEMENTIERUNG AN LANDGRENZEN

Vielfalt der Szenarien

An den Luftgrenzen dieser Welt – also an den Terminals internationaler Flughäfen – sieht es überall ähnlich aus, egal ob es sich um Flughäfen in Asien, Europa oder Nordamerika handelt. Auch die Maßnahmen, mit denen sich die Grenzkontrollbehörden auf die Einführung des europäischen Einreise-/Ausreisesystems EES an den Luftgrenzen vorbereiten, ähneln sich. Ganz anders im Fall der Landgrenzen: Hier bestehen erhebliche Unterschiede, und es sind auch noch etliche Fragen in Bezug auf die EES-Einführung zu klären.

Wer schon einmal in die USA eingereist ist, weiß, dass es zu Wartezeiten kommen kann, weil an der Grenze biometrische Daten erfasst werden. Mit der Einführung des EES in Europa wird dies künftig auch hier der Fall sein. Dies betrifft Reisende aus Drittstaaten (Drittstaatsangehörige oder Third Country Nationals, TCN), die in den Schengen-Raum einreisen oder ihn verlassen.

An Flughäfen werden dabei Selbstbedienungsterminals für die Vorregistrierung von Drittstaatsangehörigen sowie eGates für die automatisierte Abfertigung von Freizügigkeitsberechtigten eine entscheidende Rolle zur Gewährleistung eines effizienten Grenzkontrollprozesses spielen. Solche Technologien lassen sich hier vergleichsweise einfach einsetzen, weil das Anwendungsszenario fast immer dasselbe ist: Passagiere überqueren zu Fuß die Grenze innerhalb des Flughafens, nachdem sie sich am stationären Schalter oder auch an automatisierten Grenzkontrollsystemen der Dokumenten- und Personenprüfung unterzogen haben.

Individuelle Landgrenzen

Bei Landgrenzen jedoch besteht eine Reihe von Herausforderungen. So gleicht keine Landgrenze der anderen: An großen Grenzübergängen finden sich mitunter diverse Gebäude, umgeben von Parkplätzen, Straßen und Zugstrecken. Kleine Grenzübergänge dagegen weisen mitunter fast gar keine Infrastruktur auf. Zudem gibt es an der Landgrenze nicht nur Fußgänger – vergleichbar mit den Passagieren im Flughafen –, sondern der Grenzübertritt erfolgt per PKW, LKW, Bus, Zug oder auch per Fahrrad. Nicht nur Personen, sondern auch Fahrzeuge werden kontrolliert.

Wie bei allen anderen Grenzkontrollszenarien ist auch an Landgrenzen durch die vorgeschriebene Aufnahme der biometrischen Merkmale von Reisenden zukünftig mit längeren Wartezeiten zu rechnen. Der Aufwand für die Aufnahme und Prüfung der Personendaten am Grenzkontrollschalter erhöht sich. Es besteht die Gefahr, dass die Grenzkontrollbeamten ihre eigentlichen hoheitlichen und sicherheitsrelevanten Aufgaben nicht mehr erfüllen können.

Hinzu kommt, dass das Platzangebot an Grenzübergängen oft sehr limitiert ist. Es mangelt sowohl an externer Infrastruktur für zusätzliche Parkplätze als auch an Raum für neue Abfertigungssysteme zur Beschleunigung des Grenzkontrollprozesses.

Die EES-Verordnung verlangt, dass die Kontrolltiefe an jedem Grenzkontrollpunkt, also an jedem Ort, zu jeder Zeit und in jeder Lage gleichbleibend umfassend gewährleistet sein muss. Dies gilt unabhängig davon, ob es sich um eine Luft-, See-, oder Landgrenze handelt, und auch unabhängig von der dazugehörigen Infrastruktur, dem Grenzkontrollprozess sowie der Fortbewegungsart der Reisenden. Auch die Qualität der biometrischen Erfassung und Verifikation muss unter allen Umständen gleich gut sichergestellt werden.

Für Staaten mit Landgrenzen ist dies die größte Herausforderung: Wie können biometrische Daten effektiv erfasst werden, wenn man Personen in Fahrzeugen oder in Bussen kontrollieren muss? Wie lassen sich Landgrenzen EES-konform gestalten, ohne dass die Länge der Warteschlangen ins Unendliche wächst? Und wie lässt sich an Landgrenzen angesichts all der Herausforderungen und Widrigkeiten eine konstant hohe Kontrollqualität durchsetzen?

Mehrstufige Prozesse

Um die EES-Anforderungen zu erfüllen, ist auch an Landgrenzen ein mehrstufiger Prozess notwendig, der eine Vorregistrierung von Drittstaatsangehörigen einbezieht. Untersuchungen von secunet haben ergeben, dass viele Sicherheitsbehörden hierfür sowohl Selbstbedienungskioske als auch mobile Systeme – Kofferlösungen und Handheld-Geräte – in Betracht ziehen. Dabei liegt der Fokus auf ersterem: Fußgänger, Autofahrer, Busreisende, Lastwagenfahrer können ihre Daten selbstständig an einem Selbstbedienungskiosk erfassen, bevor sie sich zur Kontrolle an den stationären Schaltern begeben oder – je nach Szenario – direkt zur Schranke vorfahren.

So wird zum einen die stationäre Kontrolle entlastet, Grenzpolizisten können sich auf ihre eigentlichen Aufgaben konzentrieren. Zum anderen umfasst die Vorregistrierung am Selbstbedienungskiosk die Aufnahme der biometrischen Daten und garantiert also auch eine hohe und gleichbleibende Datenqualität. Zu guter Letzt werden die Kiosksysteme überwacht – eine weitere wichtige Anforderung der EES-Verordnung.

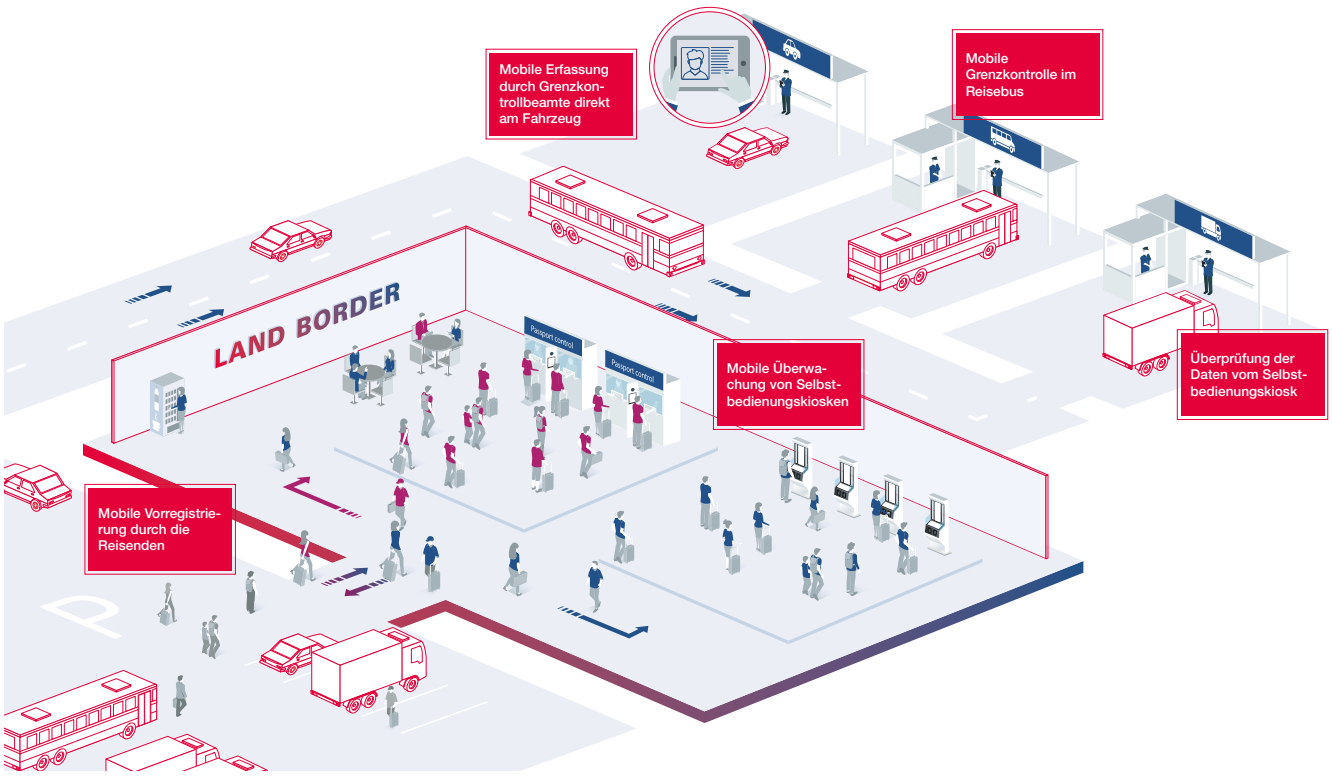
Strenge Vorgaben

Die Kiosksysteme selbst müssen strenge Anforderungen gemäß der EES-Verordnung erfüllen: Diese erstrecken sich auf Vorgaben zur Biometrie, zum Beispiel müssen Gesichtsbilder gemäß ISO/IEC 19794-5:2011 als qualitativ hochwertige Frontalaufnahmen erfasst werden. Ebenso hoch sind die Anforderungen im Bereich Überwindungssicherheit. So müssen sogenannte „Presentation Attacks“, also Betrugsversuche mittels manipulierter biometrischer Merkmale wie Masken oder gefälschter Fingerabdrücke, zuverlässig erkannt werden. Dazu gehört auch eine Lebenderkennung für Gesichtsbilder und Fingerabdrücke.

Mobile Systeme spielen eine wichtige Rolle für die Kontrolle von Reisenden im Zug oder auch bei der vorgelagerten Überprüfung von Reisenden in PKWs. Hier ist vorstellbar, dass mehrere Grenzkontrollbeamte gleichzeitig mehrere Fahrzeuge („Cluster“) kontrollieren. Dabei ist es wichtig, dass überall die gleichen strengen Anforderungen für die Aufnahme und Prüfung der biometrischen Daten sowie die Überprüfung der Identitätsdokumente gelten – egal ob die Erfassung und Verifikation stationär, mobil oder am Selbstbedienungskiosk erfolgt. Es dürfen keine Schlupflöcher entstehen.

Der Einsatz von Selbstbedienungs- und mobilen Systemen an der Landgrenze ermöglicht es, den steigenden Zeitbedarf infolge der zusätzlichen Prozessschritte, die durch die EES-Implementierung erforderlich werden, zu kompensieren. Mehr als an Flughäfen gilt es dabei, individuelle Gegebenheiten zu berücksichtigen.

Frank Steffens
frank.steffens@secunet.com



„Qualitativ hochwertige und zugleich effiziente Biometrie-Erfassung“

Im Interview: Bernd Kowalski, Abteilungsleiter Cyber-Sicherheit in der Digitalisierung und für elektronische Identitäten im Bundesamt für Sicherheit in der Informationstechnik (BSI)

Herr Kowalski, können Sie kurz die Ziele und Aufgaben der Smart-Borders-Gruppe skizzieren?

Die BSI-Projektgruppe Smart Borders ist Teil der nationalen Projektgruppe Smart Borders unter Federführung des Bundesministeriums des Innern, für Bau und Heimat (BMI). Bereits seit 2014 begleiten wir gemeinsam mit Bundespolizei und Bundesverwaltungsamt die Ausgestaltung und Umsetzung des europäischen Smart-Borders-Vorhabens. Mit Verabschiedung der Verordnung über das Europäische Ein- / Ausreiseregister (Entry-Exit-System, EES) wurde durch das BMI eine nationale, behördenübergreifende Projektorganisation eingerichtet. Die nationale Projektgruppe ist zuständig für die Umsetzung des EES und des ETIAS (European Travel Information and Authorisation System) in Deutschland. Die neuen Systeme bieten die Möglichkeit für ein umfassendes Identitätsmanagement auf Basis biometrischer Daten für sämtliche Drittstaatsreisende. Wir befassen uns zum Beispiel mit der Anbindung an die neu zu schaffenden europäischen Zentralsysteme und der Digitalisierung des Grenzkontrollprozesses an den Schengen-Außengrenzen der Bundesrepublik Deutschland. Ein weiterer Aspekt ist der Zugriff weiterer Migrations- und Strafverfolgungsbehörden im Inland auf das EES. Das BSI unterstützt dabei die operativen Polizeibehörden auf Basis seiner gesetzlichen Befugnisse.

Welche Standards und technischen Richtlinien unterstützen die optimale EES-Implementierung?

Dreh- und Angelpunkt aller Vorgaben ist die EES-Verordnung selbst. Im Gegensatz zu anderen Rechtssetzungen werden hier detaillierte Vorgaben zu Zugang und Ablauf im Rahmen der EES-Prozesse definiert. Ergänzend für die technische Umsetzung sind die delegierten als auch die Umsetzungsrechtsakte, die gemeinsam mit den Mitgliedsstaaten ausgestaltet werden. Aus Sicht der Mitgliedsstaaten sind diese Spezifikationen aber nicht ausreichend, da sie letztlich nur die Sicht des Zentralsystems auf die Datenanlieferung und -abfrage abbilden. Daher wurde das BSI beauftragt, weitere Umsetzungsspezifikationen für technische Komponenten des EES zu entwickeln. In diesem Kontext sind zuvorderst die Technische Richtlinie BSI TR-03135 für die hoheitliche Dokumentenprüfung und auch die BSI TR-03121 für die biometrischen Komponenten der Grenzkontrolle zu nennen. Daneben arbeitet das BSI derzeit gemeinsam mit den operativen Behörden an den Prozessvorgaben für das hoheitliche Identitätsmanagement im Kontext EES. Geplant ist, dass diese Spezifikation in einer europäischen Version im Jahr 2020 für alle Mitgliedsstaaten verfügbar sein wird.

Wo sehen Sie die größten Herausforderungen bei der Implementierung der Prozesse zur biometrischen Erfassung und Verifikation bei der Grenzkontrolle?

Die EES-Verordnung geht bei den Vorgaben für biometrische Daten einen interessanten neuen Weg. Anstatt auf die im Bereich der Strafverfolgung übliche Erfassung aller zehn Fingerabdrücke zu setzen, sollen stattdessen nur vier Fingerabdrücke sowie das Lichtbild erfasst werden. Damit spielt das Lichtbild eine deutlich wichtigere Rolle, wie wir sie auch aus dem Bereich der Reisedokumente kennen, wo das Lichtbild als das zentrale weltweit interoperable biometrische Merkmal etabliert ist. Die Qualität der biometrischen Erfassung an der Grenze wird daher ausschlaggebend für die Nutzbarkeit

Bernd Kowalski ist seit 2002 als Abteilungsleiter beim Bundesamt für Sicherheit in der Informationstechnik (BSI) tätig. Seit April 2019 leitet er die beiden Abteilungen „Standardisierung und Zertifizierung" sowie "Cyber-Sicherheit in der Digitalisierung und für elektronische Identitäten". Sein Aufgabenbereich umfasst dabei alle Aspekte der BSI-Zertifizierung, der Betreuung grundlegender ID-Technologien und der Unterstützung von Digitalisierungsprojekten der Bundesregierung, beispielsweise BSI-Zertifizierung nach Common Criteria, IT-Grundschutz-Zertifizierungen, den elektronischen Reisepass und Personalausweis und Cybersicherheitsaspekte in eHealth, Smart Metering/Smart Grids, Industrie 4.0, intelligente Transportsysteme und der digitalen Verwaltung.

der gewonnenen Daten im europäischen Zentralsystem sein. Im Rahmen der Technischen Richtlinie BSI TR-03121 definiert das BSI einen umfänglichen Anforderungskatalog an eine qualitativ hochwertige und zugleich effiziente Erfassung der biometrischen Merkmale im Grenzkontrollprozess. Die Industrie ist aufgefordert, im gesetzten Rahmen innovative Lösungen für alle Anwendungsszenarien zu entwickeln.

Werden sich Ihrer Einschätzung nach auch andere Mitgliedstaaten an den technischen Richtlinien des BSI orientieren?

Aufgrund der erheblichen Komplexität der europäischen Vorhaben gehen wir davon aus, dass auch andere Mitgliedsstaaten unsere Vorgaben mit großem Interesse verfolgen werden. Die Technischen Richtlinien des BSI stehen auf unserer Webseite www.bsi.bund.de zur Verfügung. Das BSI definiert Vorgaben bewusst mit einem allgemeinen Fokus und ohne spezielle deutsche Besonderheiten, sie können für den entsprechenden Einsatzzweck profiliert werden.

Bernd Kowalski
Bundesamt für Sicherheit in der Informationstechnik

Qualität ist wichtig – besonders bei biometrischen Referenzdaten

Interview mit Prof. Dr. Christoph Busch, Professor für Informatik / Biometrie am Norwegian Biometrics Laboratory (NBL), Norwegian University of Science and Technology (NTNU) und an der Hochschule Darmstadt (HDA)

Herr Busch, Sie beschäftigen sich seit langer Zeit mit Datenqualität im Bereich Biometrie. Können Sie einen kurzen Abriss Ihrer Forschung geben?

Schon seit vielen Jahren ist die Bedeutung der Bildqualität von biometrischen Referenzdaten bekannt. Als die biometrischen Pässe 2005 eingeführt wurden, hatten wir in Zusammenhang mit dem Standard ISO/IEC JTC1/SC37 Technical Reports zu dem Thema erstellt und den damaligen Stand der Technik dokumentiert. Seit 2010 konnten wir gemeinsam mit dem US-amerikanischen National Institute of Standards and Technology (NIST), dem Bundesamt für Sicherheit in der Informationstechnik (BSI), dem Bundeskriminalamt, secunet und dem Fraunhofer-Institut für Graphische Datenverarbeitung (IGD) neue Algorithmen erforschen, die die Qualität von Fingerbildern messen. Diese Entwicklung (NFIQ 2.0) wurde im Jahr 2017 internationaler Standard (ISO/IEC 29794-4) und steht als Open Source zur Verfügung.

Wie bewertet man die Qualität von biometrischen Daten?

Die Grundlage wurde schon mit dem Framework-Standard ISO/IEC 29794-1 gelegt, der für alle biometrischen Modalitäten die Vorgehensweise definiert. Der Qualitätswert („score“) soll prädiktiv für eine spätere Erkennung sein, d. h. ein guter Score sagt aus, dass eine Wiedererkennung zuverlässig möglich ist. Im NFIQ-2.0-Projekt haben wir erforscht, welche Merkmale aus dem Fingerbild relevant sind, um diese Aussage zu treffen. Die NFIQ-2.0-Software ist eine gute Lösung für optische Fingerbildsensoren.

Was sind die Besonderheiten im Umgang mit biometrischen Daten in großen Datenbanken?

Bei Identifikationslösungen bedingt die wachsende Größe der Datenbank nicht nur eine Verlängerung der Transaktionsdauer, sondern auch ein zunehmendes Risiko einer falschen Entscheidung, da naturgemäß die False-Positive-Identification-Rate (FPIR) mit der Größe der Datenbank linear wächst. Daher ist es umso wichtiger, dass nur Bilder von guter Qualität gespeichert werden.

Prof. Christoph Busch
https://christoph-busch.de/

Prof. Christoph Busch promovierte 1997 im Fachbereich Informatik an der Technischen Universität Darmstadt. Im gleichen Jahr übernahm er die Abteilungsleitung Sicherheitstechnologie für Graphik- und Kommunikationssysteme am Darmstädter Fraunhofer-Institut für Graphische Datenverarbeitung (IGD).

Für das Fraunhofer-IGD ist Christoph Busch tätig in der Standardisierung biometrischer Systeme als Obmann im DIN-NIA37. Er ist Head of German Delegation in der Plenary von ISO/IEC JTC1/SC37 (Biometrics) und leitet die Working Group 3 (Biometric Data Interchange Formats).

Prof. Christoph Busch vertritt seit dem Sommersemester 2005 das Fachgebiet System Development an der Hochschule Darmstadt. Im Herbst 2007 wurde er zudem auf eine Professur am Norwegian Information Security laboratory (NISlab) berufen. Seit 2007 lehrt er ferner an der Technical University of Denmark (DTU).

Warum sind Standards von Bedeutung für die Bewertung der Qualität von biometrischen Daten?

Die internationalen Standards bieten die Möglichkeit, nicht nur Daten einfach auszutauschen, wie wir es mit den biometrischen Pässen seit 15 Jahren praktizieren. Die Verwendung von Standards in der Qualitätsbewertung wird dazu führen, dass alle Länder, die zu einer großen gemeinsamen europäischen Biometrie-Datenbank zuliefern, ein einheitliches Qualitätsniveau erreichen können. Zudem werden problematische Vendor-Lock-in-Situationen in den EU-Mitgliedsländern, also Abhängigkeiten von bestimmten Zulieferern, vermieden.

Welche Auswirkungen hat eine schlechte Qualität von biometrischen Daten in Datenbanken?

Eine schlechte Bildqualität birgt ein großes Risiko von hohen Fehlerraten, sowohl in der Falsch-Rückweisung (dadurch wird es unkomfortabel) als auch in der Falsch-Akzeptanz (dadurch wird es unsicher). Für Fingerbilder (mit ISO/IEC 29794-4) und für Irisbilder (mit ISO/IEC 29794-6) lässt sich diese Auswirkung vermeiden. Für Lichtbilder werden wir die Standardisierung von ISO/IEC 29794-5 in diesem Sommer starten. Ich freue mich über jeden Experten, der sich daran beteiligt.

Geysire, Gletscher und elektronische Reisepässe

Mit seinen urwüchsigen Landschaften zwischen aktiven Vulkanen und ewigem Eis lockt Island immer mehr Touristen aus aller Welt an. Doch es ist nicht allein der Islandtourismus, der für die ansteigenden Passagierzahlen des Flughafens Keflavik in der Nähe der Hauptstadt Reykjavik verantwortlich ist: Der Flughafen dient auch als Drehscheibe für Interkontinentalflüge zwischen Europa und Nordamerika. Aus diesen Gründen hat Island bereits vor Jahren begonnen, eine hochmoderne Grenzkontrollinfrastruktur aufzubauen. Deren jüngste Ergänzung kommt allerdings vor allem Isländern zugute: Mit einer neuen Infrastruktur kann der Inselstaat hochsichere elektronische Identitätsdokumente (eID) an seine Bürger ausgeben und bei deren Ein- und Ausreise effizient prüfen.

Verantwortlich für das Projekt ist Registers Iceland (auf Isländisch „Þjóðskrá Íslands“), die Behörde, die das isländische Personenstandsregister betreibt. Sie suchte eine eID-Lösung, bei der die Sicherheit oberste Priorität genießt, so dass die Vertraulichkeit, Verfügbarkeit und Integrität der persönlichen Daten der isländischen Bürger jederzeit sichergestellt sind. Daher entschied sie sich, eine Public-Key-Infrastruktur (PKI) auf Basis der eID PKI Suite von secunet zu implementieren. Der hohe Sicherheitsstandard dieser Lösung ist durch die Zertifizierung des CA-Kernels – einer zentralen Komponente, die bei der Vergabe elektronischer Zertifikate maßgeblich ist – nach Common Criteria EAL 4+ dokumentiert.

Registers Iceland erhielt von secunet eine schlüsselfertige PKI-Komplettlösung, die sämtliche Softwarekomponenten zum Schutz der biometrischen Daten der isländischen Bürger und zur Regelung der Zugriffsrechte (EAC-PKI) umfasst – ebenso wie die Komponenten, die die Integrität und Authentizität der Reisedokumente sicherstellen (ICAO-PKI). Die Lösung lässt sich in großen Teilen flexibel konfigurieren, was den Administrationsaufwand im Betrieb gering hält und das System zukunftssicher macht. Der hohe Standardisierungsgrad erlaubt auch die Umsetzung zukünftiger gesetzlicher und technologischer Anforderungen.

Die neue PKI ist seit Kurzem auch an die automatisierten Grenzkontrollsysteme (eGates) angebunden, die bereits im Jahr 2017 am Flughafen Keflavik ihren Betrieb aufgenommen haben. Diese secunet easygates können von isländischen Staatsbürgern, Angehörigen des Europäischen Wirtschaftsraums sowie Schweizer Staatsbürgern genutzt werden. Sie überprüfen effizient und sicher hoheitliche Dokumente optisch wie elektronisch auf ihre Echtheit, lesen das elektronische Gesichtsbild der Reisenden aus und vergleichen die biometrischen Daten mit einem Live-Bild.

Christian Rutigliano
christian.rutigliano@secunet.com

SERVICEGEDANKE BEI DER IMPLEMENTIERUNG

„Neben der sehr guten Performance und einfachen Bedienbarkeit der PKI im operativen Betrieb sind auch der Servicegedanke und das tiefgreifende Know-how des secunet Teams bemerkenswert“, sagt Þorvarður Kári Ólafsson, Programme Manager ID and Travel Documents bei Registers Iceland. „In diesem komplexen Projekt hatten wir stets jemanden an unserer Seite, der Herausforderungen umgehend und zu unserer vollsten Zufriedenheit gelöst hat – bei Bedarf auch kurzfristig vor Ort.“

Kein Mangel an Zukunftsthemen

Im Juni 2019 fand ein Wechsel an der Spitze von secunet statt: Dr. Rainer Baumgart, mehr als 18 Jahre lang Vorstandsvorsitzender der secunet Security Networks AG, ging in den Ruhestand und übergab seine Position an Axel Deininger. secuview sprach mit dem alten und dem neuen Vorstandsvorsitzenden über die Vergangenheit und die Zukunft von secunet und der IT-Sicherheitsbranche.

secunet erlebt den ersten Wechsel eines Vorstandsvorsitzenden seit 18 Jahren. Wie groß wird der Umbruch, der damit einhergeht?

Deininger: secunet hat heute eine hervorragende Marktposition inne. Wir sind in Deutschland der führende Anbieter von hochwertiger IT-Sicherheit für Behörden und Unternehmen. Zudem bewegen wir uns in einem positiven Marktumfeld. Auch im laufenden Jahr hat sich das Geschäft bisher gut entwickelt. All das zeigt, dass es sinnvoll ist, an vielen Stellen auf Kontinuität zu setzen. Aber natürlich werden wir auch einige Kurskorrekturen vornehmen, die uns organisatorisch und inhaltlich voranbringen, denn der Markt entwickelt sich weiter und liefert uns auch neue Geschäftschancen.

In welchen Bereichen stehen Änderungen auf dem Plan?

Deininger: Zum Beispiel werden wir das Industriesegment im Kontext von Industrie 4.0 stärker adressieren. Bisher sind wir vor allem in regulierten Märkten gut aufgestellt. Für behördliche IT-Infrastrukturen etwa gelten strenge Sicherheitsvorgaben, wenn sensible oder eingestufte Informationen im Spiel sind. Solche sicherheitstechnisch anspruchsvollen Aufgaben zu lösen ist seit mehr als zwei Jahrzehnten das Kerngeschäft von secunet. Dazu gehören auch unsere Biometrie-Lösungen, die etwa bei der automatisierten Grenzkontrolle zum Einsatz kommen. Nun ist davon auszugehen, dass künftig weitere regulierte Bereiche hinzukommen werden. Bereits seit 2015 haben wir in Deutschland das IT-Sicherheitsgesetz, das Betreiber kritischer Infrastrukturen in die Pflicht nimmt, mehr für ihre Cybersicherheit zu tun. Weitere Regelungen werden folgen.

Aber auch in nicht-regulierten Märkten findet ein Umdenken statt, schließlich können IT-Sicherheitsvorfälle zu großen finanziellen Einbußen führen. Und im Zuge der Digitalisierung werden immer mehr IT-Systeme vernetzt – auch mit dem Internet –, die ursprünglich nie dafür konzipiert waren. Das beste Beispiel dafür ist die Industrie. Dort sind Maschinen zum Teil 30 Jahre und länger im Einsatz. Um die Vorteile der Digitalisierung auch dort voll auszuschöpfen, wird künftig jede Maschine und jedes Steuergerät vernetzt sein – was nur mit IT-Lösungen funktionieren kann, die das passende Sicherheitsniveau herstellen.

Ein anderes Beispiel sind internationale Märkte. Zwar ist secunet schon seit vielen Jahren auch außerhalb Deutschlands aktiv, vor allem im europäischen Ausland und im NATO-Umfeld. Doch unser Engagement in diesen Märkten ist durchaus ausbaufähig. Überall wächst der Bedarf an Cybersicherheit, und wir haben genug Referenzen, um uns auch international zu empfehlen, auch in staatlich nicht regulierten Bereichen.

Und wo ist Kontinuität zu erwarten?

Deininger: Zum einen werden wir unser starkes Geschäft mit IT-Sicherheit für öffentliche Auftraggeber auf bewährte Weise fortführen. Zum anderen hat sich secunet seit jeher auch über seine Nähe zu Universitäten und Forschungseinrichtungen definiert. Wir unterhalten zum Beispiel gute Beziehungen zum Horst-Görtz-Institut in Bochum, zum Institut für Internet-Sicherheit if(is) in Gelsenkirchen, zur Technischen Universität Dresden oder zur Technischen Universität Ilmenau, um nur einige Einrichtungen zu nennen. Diese Nähe zur Wissenschaft wollen wir unbedingt beibehalten, denn sie ist einer der Schlüssel für unsere Innovationskraft. Der andere Schlüssel ist unsere Fähigkeit, die richtigen Mitarbeiter zu gewinnen und zu binden.

Bestand aus diesen Zutaten auch das Rezept, um secunet vom Start-up zum Marktführer zu machen?

Baumgart: Sie gehörten auf jeden Fall dazu. Noch zur Zeit des Börsengangs im Jahr 1999 beschäftigte sich secunet, ursprünglich eine TÜV-Ausgründung, als einer

Axel Deininger (links) und Dr. Rainer Baumgart

Axel Deininger ist seit Januar 2018 im Vorstand der secunet Security Networks AG und übernahm im Juni 2019 den Vorsitz. Vor seiner Zeit bei secunet war er mehr als zehn Jahre für die Münchener Unternehmensgruppe Giesecke+Devrient tätig, zuletzt als Group Senior VP und Head of Division Connectivity & Devices der G+D Mobile Security GmbH. Stationen in der Karriere des Wirtschaftsingenieurs waren unter anderem Siemens AG, Infineon Technologies AG sowie Samsung Semiconductor Europe GmbH.

Dr. Rainer Baumgart war seit der Unternehmensgründung im Jahr 1997 für secunet tätig und gehörte seit der Umwandlung des Unternehmens in eine Aktiengesellschaft im Jahr 1999 dem Vorstand an, dessen Vorsitz er 2001 übernahm. Der promovierte Physiker war vor seiner Zeit bei secunet für den RWTÜV tätig und leitete ab 1995 den Bereich Informationssicherheit bei der TÜV IT GmbH in Essen.

von vielen Anbietern mit der Absicherung von IT-Netzwerken durch kryptographische Mechanismen. Indem wir die richtigen Experten an Bord holen konnten, waren wir in der Lage, unser Portfolio zu erweitern – zum Beispiel durch Public-Key-Infrastrukturen (PKI), die in staatlich geprüften Trust Centern zur Zertifikatsvergabe eingesetzt wurden. Die breitere Aufstellung half uns unter anderem, das Platzen der Dotcom-Blase zu überstehen – und uns aus der Nische zu befreien.

Anfang der Nullerjahre haben wir im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI) die Sicherheitsarchitektur SINA entwickelt – das war ein Meilenstein. SINA sorgt heute in zahlreichen Behörden für Hochsicherheit. Das Jahr 2004 brachte dann für secunet zwei bedeutsame Veränderungen: Zum einen wurden wir IT-Sicherheitspartner der Bundesrepublik. Zum anderen brachte uns der Einstieg des neuen Mehrheitsaktionärs Giesecke+Devrient weitere Stabilität. Diese Konstellation hat bis heute Bestand. Mit der Beteiligung an großen Infrastrukturprojekten öffentlicher Institutionen wie ELSTER, den „Netzen des Bundes“ (NdB) oder dem Führungsinformationssystem der Bundeswehr konnten wir unsere Fähigkeiten unter Beweis stellen.

Wichtig für secunet war und ist auch die Kooperation mit institutionellen Partnern: Mit dem BSI verbindet uns eine langjährige gute Zusammenarbeit. Auch zu der

europäischen Cybersicherheitsagentur ENISA unterhalten wir gute Beziehungen. Darüber hinaus haben uns Technologiepartner wie atmedia, S.I.E oder Siemens geholfen: Sie versetzen uns in die Lage, unseren Kunden Komplettlösungen aus Hard- und Software anzubieten.

Lässt sich die Entwicklung, die secunet genommen hat, auch auf die IT-Sicherheit als Ganzes übertragen?

Baumgart: Das kann man schon so sagen. Vor 30 Jahren war IT-Sicherheit noch etwas für Nerds. Aber die Zeit hat den Nerds Recht gegeben. Nach und nach wurde vielen Menschen bewusst, dass das Thema IT-Sicherheit in Deutschland und Europa ein entscheidender Aspekt ist, um eine nationale oder europäische Souveränität zu gewährleisten. Daher ist die noch junge IT-Sicherheitsbranche gewachsen und hat sich immer stärker professionalisiert.

Aber ich bin auch überzeugt: Wir stehen erst am Anfang, und richtig spannend wird es erst noch. Es gibt neue Herausforderungen und drängende Fragen, die gelöst werden müssen. Insbesondere die Entwicklungen rund um die Postquantenkryptographie verfolge ich mit Interesse. Wenn künftig leistungsfähige Quantencomputer verfügbar sein werden, müssen kryptographische Verfahren diesen standhalten können. Daher ist die Verschlüsselungstechnologie gerade dabei, sich noch einmal neu zu erfinden. Später wird man die letzten Jahrzehnte vielleicht als die prähistorische Phase der IT-Sicherheit einordnen. Es hat Spaß gemacht, dabei gewesen zu sein.

Herr Deininger, welche Zukunftsthemen stehen neben Postquantenkryptographie konkret auf dem To-Do-Zettel?

Deininger: Ein Thema, das direkt vor der Tür steht, ist 5G. Der neue Mobilfunkstandard bietet erstmals die Möglichkeit, kryptographische Sicherheitsmechanismen aus der klassischen IT-Welt Ende-zu-Ende im Mobilfunk einzusetzen. Auch wird Biometrie künftig noch weiter an Bedeutung gewinnen. Schließlich kann sich niemand 50 Passwörter merken! Mobile Applikationen sind ein weiteres Thema: Mit der Fahndungs-App für die Bundespolizei haben wir gezeigt, dass Apps in Bereichen, bei denen es auf hohe Sicherheit ankommt, umsetzbar sind. Darauf wollen wir aufbauen. Im Gesundheitsmarkt sind wir mit dem secunet konnektor bereits erfolgreich vertreten, die nächsten Weiterentwicklungen stehen kurz bevor. Auch das Thema Automotive Security, seit Langem ein Betätigungsfeld von secunet, wird mit der schrittweisen Realisierung des autonomen Fahrens und der immer stärkeren Vernetzung der Fahrzeuge künftig noch bedeutsamer.

Natürlich darf in dieser Aufzählung Künstliche Intelligenz nicht fehlen. KI wird ganz sicher für einige Umwälzungen in der IT und darüber hinaus sorgen. Hacker werden versuchen, sie für sich zu nutzen, aber wir werden das auch tun. Ein weiteres Thema: Cloud Security wird eine immer stärkere Rolle spielen, sowohl für Unternehmen als auch für Behörden. Daher haben wir kürzlich gemeinsam mit der Cloud & Heat Technologies GmbH das Joint Venture SecuStack gegründet, das Cloud-Lösungen für sicherheitskritische Anwendungen bietet und es damit manchen Kundengruppen erstmals ermöglicht, in die Cloud zu gehen. An zukunftsträchtigen Themen herrscht im IT-Sicherheitsumfeld kein Mangel. Auch die Industrie 4.0, die ich eingangs erwähnt habe, gehört prominent dazu. Ich freue mich darauf, all diese Themen gemeinsam mit den secunet Kolleginnen und Kollegen anzugehen und blicke optimistisch in die Zukunft.

DER NEUE SECUNET VORSTAND

Seit dem 1. Juni 2019 besteht der Vorstand der secunet Security Networks AG neben dem Vorstandsvorsitzenden Axel Deininger aus Torsten Henn, Dr. Kai Martius und Thomas Pleines. Dabei wurden Chief Operating Officer (COO) Torsten Henn und Chief Technical Officer (CTO) Dr. Kai Martius, die dem Unternehmen seit vielen Jahren angehören, neu in den Vorstand berufen. Chief Financial Officer (CFO) Thomas Pleines ist bereits seit dem Jahr 1999, als das Unternehmen in eine Aktiengesellschaft umgewandelt wurde, Vorstandsmitglied.

Herr Baumgart, welchen Ratschlag geben Sie Ihrem Nachfolger mit auf den Weg?

Baumgart: Aus meiner Sicht hat es sich immer ausgezahlt, den partnerschaftlichen Gedanken im Blickfeld zu behalten und auf eine Zusammenarbeit zwischen Privatwirtschaft, Behörden, Wissenschaft und Forschung zu setzen. Die deutsche IT-Sicherheitsbranche und die öffentlichen Instanzen in ihrem Umfeld sind durchaus von gegenseitigem Respekt und Kooperationswillen geprägt, was ich immer positiv fand. Denn so ist es einfacher, die teilweise recht komplexen Herausforderungen, vor denen wir standen und vor denen die IT-Sicherheit immer stehen wird, zu lösen.

Womit werden Sie sich in nächster Zeit beschäftigen?

Baumgart: Vor allem werde ich mehr Zeit mit meiner Familie verbringen, worauf ich mich sehr freue. Vielleicht sind meine Enkelkinder bisher etwas zu kurz gekommen. Außerdem habe ich einen alten Porsche Traktor, der dringend repariert und restauriert werden möchte. Mir wird bestimmt nicht langweilig.

Vielen Dank Ihnen beiden für das Gespräch.

DIGITALE REVOLUTION DER LANDWIRTSCHAFT

Ackerbau und IT-Sicherheit

Landmaschinen haben ein Entwicklungsniveau erreicht, das sich auf traditionellem Wege kaum mehr steigern lässt. Um sich weiterhin führend am Markt zu positionieren, fokussiert der Landmaschinenhersteller CLAAS daher auf neue und zukunftsweisende Geschäftsfelder. Dazu bietet die umfassende Digitalisierung Anlass, die die Agrarwirtschaft mittlerweile erfasst hat – zwar später als andere Sektoren, aber dafür umso gründlicher, denn sie verspricht weitere große Ertrags- und Effizienzvorteile. Um das Potenzial dieser Entwicklung voll nutzen zu können, investiert CLAAS in IT-Sicherheit und hat unter anderem eine Public-Key-Infrastruktur (PKI) als zentrale kryptographische Instanz für alle Dienste etabliert.

Schon der hohe und ständig wachsende Anteil von Elektronik und Software in den Landmaschinen zeigt es: Die digitale Revolution auf dem Acker ist in vollem Gange. Heute sind Landmaschinen untereinander, mit dem IT-Backend oder auch mit dem IT-System in der Cloud vernetzt. Dafür stimmen mittlerweile auch wichtige Rahmenbedingungen: So wurde etwa die Mobilfunkversorgung im landwirtschaftlichen Bereich stark ausgebaut.

Ein Anwendungsszenario, das die Landwirtschaft derzeit stark verändert, ist das Smart Farming oder Precision Farming. Dabei lassen sich Unterschiede der Bodenbeschaffenheit sogar innerhalb eines Feldes auswerten und durch optimale Bewirtschaftung ausnutzen. Daneben können digitale Prozesse den Alltag von Agrarbetrieben auf vielfältige Weise effizienter gestalten: Beim Parallel Driving werden Landmaschinen automatisiert und GPS-gesteuert Spur an Spur über das Feld geführt. Predictive Maintenance analysiert den Zustand von landwirtschaftlichen Geräten, so dass Wartungsarbeiten genau dann stattfinden können, wenn sie auch tatsächlich erforderlich sind. Softwareupdates oder auch die Freischaltung weiterer Dienste und Funktionen lassen sich over the air durchführen, was Zeit und Aufwand spart.

Drahtlose Datenübertragung

CLAAS bietet seinen Kunden digitale Dienste für diese und andere Anwendungsszenarien und entwickelt sie ständig weiter. Die technische Realisierung der Dienste macht es notwendig, Daten unter anderem über drahtlose Schnittstellen zu übertragen, beispielsweise per Mobilfunk oder WLAN. Diesen Datenverkehr gilt es zu schützen: Um Manipulation auszuschließen, muss jederzeit sichergestellt werden, dass die Daten von vertrauenswürdigen CLAAS Instanzen stammen. Zudem kann der Schutz personengebundener Daten und geistigen Eigentums von CLAAS eine Verschlüsselung von Daten notwendig machen. Ein weiterer wesentlicher Aspekt ist die Absicherung der CLAAS Landmaschinen gegen Hackerangriffe.

IT-Sicherheit ist aus der Welt des Internets und der Unternehmens-IT wohlbekannt – für Landmaschinen jedoch ein relativ neues Feld. CLAAS hat daher Anfang 2016 das Projekt Security@CLAAS gestartet, um den Anforderungen an die IT-Sicherheit für die vernetzten CLAAS Maschinen und Dienste gerecht zu werden. Das unternehmensweit angelegte Cybersicherheitsprogramm zielte auf die ganzheitliche Absicherung der verschiedenen digitalen Use Cases gegen unberechtigte Manipulation und den Schutz vertraulicher Daten.

Precision Farming erlaubt es Landwirten, Teilflächen eines Feldes je nach Bodenbeschaffenheit optimal zu bewirtschaften, indem sie zum Beispiel unterschiedliche Mengen von Mineraldünger ausbringen.

In secuview 2/2016 stellte Thomas Böck, Mitglied der Konzernleitung der CLAAS Gruppe und verantwortlich für das Ressort Technologie und Systeme, das Projekt Security@CLAAS im Rahmen eines Interviews vor. Interessierte können die Ausgabe unter dem folgenden Link als PDF herunterladen: http://www.secunet.com/secuview

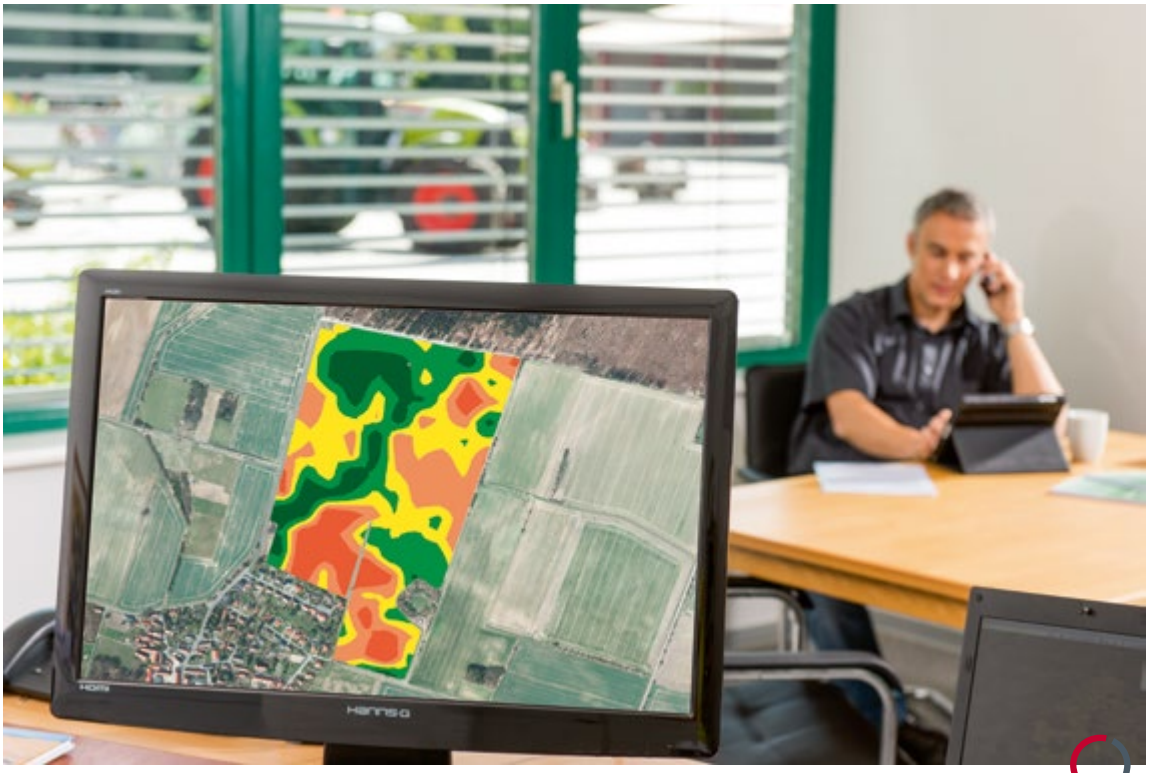
Im September 2018 konnte CLAAS das Projekt erfolgreich abschließen. „Mit Security@CLAAS haben wir einen spürbaren Veränderungsprozess im gesamten Unternehmen angestoßen“, sagt Thomas Ehl, Projektleiter bei CLAAS. „Nach der Anforderungsaufnahme in Form von Workshops, einer Risikoanalyse und der Erstellung eines Sicherheitskonzepts für die Einsatzszenarien haben wir ein Security-Manifest entwickelt und etabliert, das als unternehmensweite Norm für die Absicherung von Funktionen und Diensten fungiert.“

PKI als zentrale Technologie

Der letzte Meilenstein war die Einführung einer CLAAS Produkt-PKI (Public-Key-Infrastruktur). Dieser zentrale Dienst für kryptographische Funktionen generiert elektronische Zertifikate, die belegen, dass bestimmte Daten von einer vertrauenswürdigen Quelle stammen, und regelt den Zugriff auf diese Daten. PKI-Lösungen haben sich in anderen Bereichen, in denen es auf die Vertraulichkeit und Integrität von Daten ankommt, seit vielen Jahren bewährt: Bei der Grenzkontrolle sorgen sie beispielsweise dafür, dass die Echtheit elektronischer Identitätsdokumente zuverlässig und schnell festgestellt werden kann. Auch bei HTTPS-basierten Webservern, die zum Beispiel für Online-Banking genutzt werden, kommen PKI-gestützte Prozesse zum Einsatz. PKI-Lösungen laufen meist – so auch bei der CLAAS Lösung – automatisiert im Hintergrund ab, weitgehend unbemerkt vom Endnutzer.

Bei der Etablierung der IT-Sicherheitsmaßnahmen wurde das CLAAS Projektteam maßgeblich von secunet unterstützt. „secunet lieferte sowohl konzeptionelle Anteile als auch die Technologie für die CLAAS Produkt-PKI“, so Ehl. „Speziell die Flexibilität und leichte Integrierbarkeit dieser

Beim Parallel Driving werden Landmaschinen, hier Mähdrescher, GPS-unterstützt über das Feld geführt.



Digitale Technologien helfen bei der Kartierung von Erträgen.

Technologie in die CLAAS IT-Systeme hat hierfür den Ausschlag gegeben. Die Flexibilität zahlte sich insbesondere in der Start-of-Production-Phase der vernetzen Elektronikkomponenten aus: secunet konnte dabei noch in letzter Minute Anpassungen vornehmen. Zudem ist die Geschwindigkeit hervorzuheben, in der die CLAAS Produkt-PKI etabliert wurde: Vom Start der Implementierung bis zur Inbetriebnahme vergingen gerade einmal sechs Wochen."

Eine wichtige Voraussetzung für den Erfolg eines solchen Projekts war von Anfang an gegeben: „Wir wurden konsequent durch das CLAAS Management unterstützt", sagt Harry Knechtel, Projektleiter auf Seite von secunet. „Auch die Zusammenarbeit mit dem engagierten Projektteam und die zielorientierte abteilungsübergreifende Kooperation waren überdurchschnittlich gut."

Nur ein Ausgangspunkt

Wie so oft in der IT gilt: Der erfolgreiche Abschluss des Projekts kann kein Schlusspunkt für die Implementierung von IT-Sicherheit bei CLAAS sein. Auch die Angreifer schlafen nicht, daher muss die Messlatte ständig höher gehängt werden. Zwar wurde mit dem Projekt Security@CLAAS eine zukunftsorientierte Architektur geschaffen, die auch die Absicherung künftiger Anwendungen abdecken kann. Aber sie darf letztlich nur als Ausgangspunkt für einen kontinuierlichen Verbesserungsprozess verstanden werden, den CLAAS nun mit Leben füllen wird.

Alexander Kruse
alexander.kruse@secunet.com

AUTOMOTIVE SECURITY

Sicherheit effizient testen – durch mehr Standardisierung

Penetrationstests, auch Pentests genannt, gehören mittlerweile in den klassischen IT-Bereichen wie etwa Websites und -services oder IT-Infrastruktur nicht nur zum guten Ton, sondern stellen eine zwingend notwendige Maßnahme für den jeweiligen Betreiber dar. Nachdem sich das moderne Fahrzeug in den letzten Jahren immer stärker zu einer mobilen vernetzten Infrastruktur entwickelt hat, ist auch hier der Bedarf gestiegen, Fahrzeug-Penetrationstests entwicklungsbegleitend und regelmäßig durchzuführen. Dies ist notwendig, da sich Angriffe auf Fahrzeuge immer größer werdender Beliebtheit erfreuen.

Über einige dieser Angriffe wurde in den Medien prominent berichtet: Dazu gehören zum Beispiel die sogenannten Relay-Angriffe, die es Kriminellen ermöglichen können, Fahrzeuge mit Keyless-Go-Systemen zu stehlen, oder der berühmte Jeep Hack, bei dem Sicherheitsforscher die Kontrolle über ein gesamtes Fahrzeug übernommen haben. Daneben gibt es viele weniger bekannte Fälle: Aus den verschiedensten Gründen – Tuning, Fahrzeugdiebstahl, akademische Neugier oder Anerkennung in der Hacker-Community – haben sich Gruppen auf das Hacken aktueller Fahrzeuge spezialisiert. Da der Prestige-Schaden eines gelungenen und veröffentlichten Angriffs vor allem die Fahrzeugmarke trifft, sind es insbesondere die OEMs (Original Equipment Manufacturer, Fahrzeughersteller), die zunehmend in Cybersicherheit investieren. Zudem stehen die OEMs dem Endkunden gegenüber in der Produkthaftung.

Das vernetzte Fahrzeug ist ein attraktives Ziel für Hacker.

CONTINENTAL UND ARGUS

„Protect, Detect and React to Prevent, Understand and Respond": Entlang dieser Paradigmen bietet Continental seinen Kunden nicht nur Pentests, sondern umfassende Cybersicherheitslösungen – von Stoßstange zu Stoßstange. Um dies bis Ende 2017 zu erreichen, übernahm Continental das innovative Automotive Cyber Security Start-up Argus.

Da die Ansätze zum Schutz des Fahrzeugs, vor allem im Bereich der Verifikation – dazu zählen unter anderem Penetrationstests – jedoch von Hersteller zu Hersteller sehr unterschiedlich sind, stellt dies insbesondere die Zuliefererindustrie vor gewaltige Herausforderungen: Sie müssen die verschiedenen Vorgaben der Hersteller erfüllen. Dies ist besonders schwierig, wenn das betroffene Produkt eine Plattform darstellt, bei der die Gemeinsamkeiten in der Entwicklung erst einen Wettbewerbsvorteil im stark vom Preisdruck getriebenen Fahrzeugmarkt erzeugen.

Die Division Chassis & Safety der Continental AG ist von dieser Entwicklung bereits seit einiger Zeit betroffen. So müssen Steuergeräte, die für verschiedene Hersteller gleichartig konzipiert sind, dennoch für die meisten Hersteller (OEMs) individuell getestet werden. Dabei qualifiziert jeder Hersteller seine eigenen Werkzeuge (etwa für Robustheitstests) und fordert Continental damit nicht nur auf, diese zu erwerben, sondern auch durchgehend einsatzfähig zu halten. Auch die Schulung der Mitarbeiter für die verschiedenen Werkzeuge stellt eine Herausforderung für die Zuliefererindustrie dar. Hinzu kommen unterschiedliche Ansprüche an die Umsetzung von Penetrationstests. Während sich im Bereich der Netzwerk-Pentests mittlerweile eine allgemein anerkannte Tool-Landschaft etabliert hat, lassen im Automotive-Bereich die unterschiedliche Sichtweise der OEMs sowie die stark heterogene Technologielandschaft bisher kaum eine sinnvolle Automatisierung zu. Dabei wäre diese in Zeiten von kürzer werden Release-Zyklen und Over-The-Air-Updates nötiger denn je.

Michael Gerhard Schneider, Head Of Cyber Security in der Business Unit VED der Division Chassis & Safety der Continental AG, qualifiziert daher bereits seit Anfang 2018 auf Basis von Erfahrungen des Corporate Cyber Security Competence Center (SCC) geeignete Werkzeuge, mit denen sich die verschiedensten Anforderungen herstellerübergreifend erfüllen lassen. Ein wichtiges Kriterium ist dabei, dass solche Werkzeuge in der Lage sein müssen, durch Erweiterungen stetig neue Testfälle und Schnittstellen abzudecken und ohne Migration auch neue Trends und Technologien abzubilden.

Zu diesem Zweck arbeitet die VED (Vehicle Dynamics) Business Unit Cyber Security auch eng mit ihrem Zulieferer secunet zusammen. Die Kooperation startete bereits Mitte des Jahres 2018. Zunächst wurden die bekannten Herstelleranforderungen konsolidiert. Diese flossen in den Funktionsumfang eines Produkts ein, das sich zu dem Zeitpunkt noch in Entwicklung befand: die secunet redbox, ein Werkzeug für automatisierte Sicherheitstests in heterogenen Projektlandschaften.

Die secunet redbox baut auf der Erfahrung und Technologie auf, mit der secunet zuvor schon jahrelang OEMs bei Penetrationstests und Freigabeprozessen von Steuergeräten unterstützt hat. Das Tool bündelt damit das Automotive-Pentest-Know-how und die spezifisch für diesen Markt entwickelte Toolchain von secunet.

In einem Workshop mit Daniel Hrisca, Pentestexperte der Business Unit Vehicle Dynamics der Continental AG, konnte sich Continental ein Bild davon machen, wie sich die secunet redbox um Continental-spezifische Anwendungsfälle erweitern ließ: Mehrere Experten von secunet und Continental implementierten dafür in einem gemeinsamen dreitägigen Hackathon in Frankfurt am Main erfolgreich eine neue Continental-spezifische Schnittstelle in eine frühe Entwicklungsversion der secunet redbox. Der Beweis zur kundenspezifischen Erweiterbarkeit war damit erbracht.

Einen weiteren Meilenstein erreichte das Projekt im Frühjahr 2019. Über die Dauer von zwei Wochen demonstrierte secunet die Stärken der secunet redbox an einem kürzlich fertiggestellten Bremsensteuergerät. Die Besonderheit dabei lag darin, dass das Steuergerät unter anderem durch eine von einem OEM vorgegebene Testmethode untersucht werden musste und somit eine direkte Vergleichbarkeit mit anderen Testwerkzeugen hergestellt werden konnte. Nachdem das Steuergerät mit Unterstützung von Roopashree Dheenadayalan, Security-Testerin bei Continental, in Betrieb genommen worden war, konnte die secunet redbox mehr Findings bei der automatisierten Prüfung auf mögliche Schwachstellen aufzeigen als das zuvor eingesetzte Werkzeug.

Dieses Ergebnis überzeugte Continental. Es zeigt zudem, dass es sich lohnt, im Bereich des Security- und Robustness-Testings eine stärkere Standardisierung zuzulassen. Denn nur so kann eine starke Automotive Security Community entstehen, die sich in Zukunft herstellerübergreifend dafür einsetzen kann, die Straßen vor Cyberangriffen zu schützen.

Alexander Siegel
alexander.siegel@secunet.com

SICHERE VERNETZUNG IN DER INDUSTRIE 4.0

Am Rande des Netzwerks

Die Digitalisierung von Produktionsumgebungen ist ein zweischneidiges Schwert: Betreiber profitieren von neuen Möglichkeiten, werden aber auch unerbittlich mit neuen Herausforderungen konfrontiert. Mit secunet edge liegt eine Lösung vor, die vernetzte Maschinen absichert – und darüber hinaus weitere Fragen beantwortet, die sich in der Industrie 4.0 stellen.

Eine Folge der Digitalisierung in der Industrie ist es, dass die ursprünglich getrennten Welten der Informationstechnologie (IT) und der operativen Technologie (OT) immer stärker miteinander verzahnt sind. So werden Maschinen mittlerweile aus der Prozess-IT zentral gesteuert und überwacht, arbeiten mit IKT-Systemen aus der Business-IT zusammen und sind auf IT-Dienstleistungen außerhalb der eigenen Organisationsgrenzen angewiesen. Doch dieser hohe Konnektivitätsgrad führt unweigerlich zu neuen Herausforderungen. Heute müssen sich Betreiber mit IT-Bedrohungen auseinandersetzen, die in der früheren Arbeitswelt von Ingenieuren und Technikern nicht präsent waren.

Zudem unterstreicht der Gesetzgeber die Notwendigkeit, solchen Bedrohungen vorzubeugen, und erlässt Vorgaben, Regulierungen und Empfehlungen. Beispiele dafür sind das IT-Sicherheitsgesetz, die Verordnung zur Bestimmung Kritischer Infrastrukturen des Bundesamts für Sicherheit in der Informationstechnik (BSI-KritisV) oder die BSI-Empfehlung zur IT in der Produktion (BSI-CS 005). Mit diesen Maßnahmen wird letztlich der hohe Schutzbedarf der Komponenten in sensiblen Netzbereichen der Produktionsumgebung festgestellt. Anlagen und Maschinen erfordern demnach einen umfassenden Schutz vor IT-Einflüssen, gleichzeitig jedoch eine Vernetzung zur

Betreiber von Industrieanlagen müssen sich heute mit IT-Bedrohungen auseinandersetzen, die in der früheren Arbeitswelt von Ingenieuren und Technikern nicht präsent waren.

Umsetzung neuer datengetriebener Betriebsprozesse. Wie kann ein solch paradox erscheinender Anspruch erfüllt werden?

Lange Lebenszyklen, hohes Risiko

Für Maschinen, die in der Prozess-IT (PIT) betrieben werden, sind Lebenszyklen von mehr als 30 Jahren typisch. Untypisch dagegen sind Modifikationen von Komponenten, um Maschinen und Anlagen gegen aktuelle IT-Bedrohungen zu wappnen. Der Grund dafür ist, dass Betreiber das Ausfallrisiko durch solche Modifikationen als zu hoch einstufen. Die Devise lautet: Never change a running system. Allerdings wird dabei das Risiko, das die Vernetzung ungeschützter veralteter Technologie mit sich bringt, unterschätzt. In Gefahr gerät nicht nur der einwandfreie Betrieb der Maschine selbst. Auch andere Teilnehmer im Netzwerk sind gefährdet, zudem können sich Einfallstore für potentielle Cyberattacken öffnen. Daher besteht Handlungsbedarf, Maschinen das notwendige IT-Sicherheitsniveau zu verleihen. Wie akut dieser Handlungsbedarf ist, zeigen einige Sicherheitsvorfälle, die zuletzt bekannt geworden sind: etwa die Sicherheitslücke in der Fernwartungsfunktion aktueller sowie bereits nicht mehr mit Updates versorgter Betriebssysteme. Ein weiteres Beispiel ist die erfolgreiche Manipulation maschinenerzeugter Daten medizinischer Geräte, die durch einen fehlenden Schutz übertragener Informationen möglich wurde.

Doch es würde zu kurz greifen, den Fokus allein auf die nötige Absicherung von Maschinen zu legen. Es gibt noch weitere Baustellen: Etwa bestehen heute weitergehende Ansprüche an die Vernetzung, die so noch gar nicht bedient werden. Reicht es aus, Maschinen kabelgebunden per LAN an die Infrastruktur anzubinden oder sollte vielmehr die Mobilität der Maschine gewahrt werden, wozu eine drahtlose Verbindung per WLAN oder Mobilfunk notwendig ist? Wie können künftig neue Schnittstellen und Standards wie 5G genutzt werden? Und wie lässt sich die Anbindung von Maschinen an beliebige interne und externe Dienste oder Plattformen in den jeweils individuellen Anwendungsfällen umsetzen?

Ein ganzheitliches Konzept sollte – neben der akut notwendigen Absicherung vernetzter Maschinen – auch diese und ähnliche Fragen beantworten. Gefragt ist ein Ansatz, der folgende Aspekte vereint:

- „Protect“:
  sichere Vernetzung und reglementiertes Kommunikationsverhalten von Maschinen
- „Connect“:
  Einsatz von Software von Drittanbietern zur flexiblen Integration der Maschinen in Anwendungsfälle des Internet of Things (IoT) und der Industrie 4.0
- „Detect“:
  Security Monitoring der Maschinen und Kommunikation zur Stärkung der Abwehr von Cyberangriffen

Protect: Absicherung und sichere Vernetzung von Maschinen

Die Funktionsweise der PIT mit ihren Maschinen und Anlagen unterscheidet sich stark von der klassischen IT. Dies gilt es bei der Adaption der Sicherheitsstrategie zu berücksichtigen. Nur so kann ein angemessener Schutz vor äußeren Einflüssen erreicht werden und gleichzeitig eine kontrollierte und sichere Vernetzung stattfinden. Durch eine Entkopplung des Lebenszyklus von Maschinen und Anlagen von dem der IT-Umgebung lässt sich auch für Systeme in diesem Bereich der Infrastruktur ein hohes Sicherheitsniveau erreichen.

Daher setzt das Sicherheitssystem secunet edge, das speziell für das industrielle Umfeld konzipiert und entwickelt wurde, an der kritischen Schnittstelle zwischen der Maschine und dem Netzwerk an. Durch eine Mikro-Segmentierung des Netzwerks arbeitet die mit dem Sicherheitssystem verbundene Maschine isoliert vor äußeren Einflüssen in ihrem eigenen Netzsegment. Anders gesagt: secunet edge legt sich wie eine Schutzhülle um die Maschine. Die ein- sowie ausgehende Kommunikation nimmt stets den Weg über das Sicherheitssystem, wodurch der Datenfluss zwischen den Netzsegmenten vollständig steuer- und kontrollierbar wird. Entsprechend kann der verbundenen Maschine ein hohes Sicherheitsniveau gewährt und dieses auch stets aufrechterhalten werden. Zudem ist lediglich das gehärtete und minimierte Betriebssystem des Sicherheitssystems von schnelllebigen Update-Zyklen betroffen. Dadurch lassen sich Updates problemlos durchführen, so dass das Gesamtsystem stets auf aktuellem Stand ist, ohne dass Nebenwirkungen oder Auswirkungen auf die Verfügbarkeit der Maschine in Kauf genommen werden müssten.

Die langen Laufzeiten von Maschinen bringen es mit sich, dass deren Datenübertragung oft auf Protokollen basiert, die nicht mehr als sicher gelten. Daher lässt sich weder die Vertraulichkeit noch die Authentizität der ausgetauschten Informationen nachweisen. Dies ist problematisch, da verfälschte Informationen, die von der Maschine an eine Leitstelle gesendet werden, falsche Annahmen über den Betrieb der Maschine hervorrufen. Manipulierte Steuerbefehle, die an die Maschine übertragen werden, können sogar eine unmittelbare Gefahr für das Betriebspersonal bedeuten. Entsprechend wichtig ist der Schutz übertragener Informationen in der PIT. Allerdings ist ein Nachrüsten geeigneter Maßnahmen schwierig, gerade wenn Daten noch über veraltete Schnittstellenstandards übertragen werden. Ein in secunet edge integrierter Protokollübersetzer löst dieses Problem. Eine ungesicherte Übertragung der Daten im Netzwerk findet nur noch auf der minimalen Strecke zwischen Maschine und Sicherheitssystem (secunet edge) statt. Von dort an erfolgt die Übersetzung on-the-fly, beispielsweise vom unsicheren File Transfer Protocol (FTP) in die sicheren Protokollvarianten SFTP oder FTPS.

Connect: flexible Integration von Maschinen in IoT- und Industrie-4.0-Anwendungsfälle

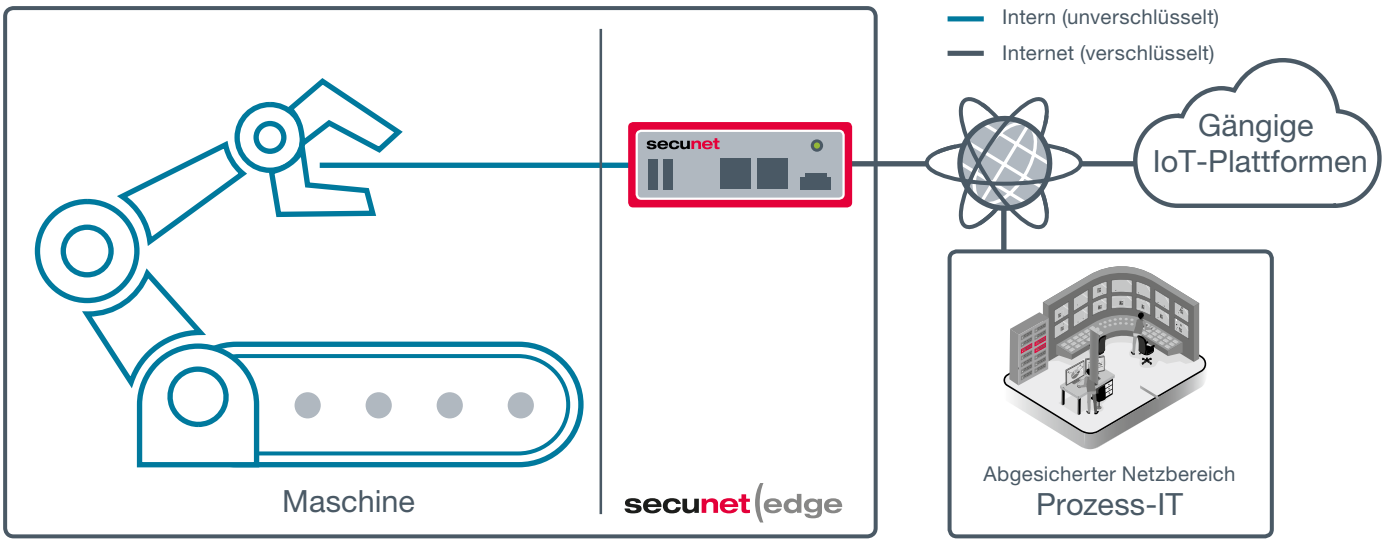
Ist eine sichere Vernetzung gegeben und damit gleichsam ein stabiles Fundament geschaffen, stehen die Betreiber vor neuen Herausforderungen. Denn nicht nur die in einer Produktionsumgebung eingesetzten unterschiedlichen Technologien, Protokolle oder Übertragungstechniken steigern die Komplexität. Auch möchten diverse Interessenten aus unterschiedlichen Gründen auf Maschinen bzw. auf deren Informationen zugreifen. Möglicherweise sollen zur Optimierung eigener Prozesse sowie zur Minimierung von Ausfallzeiten maschinenerzeugte Daten an IoT-Plattformen übertragen und analysiert werden. Oder Techniker sollen aus Kostengründen die Maschinen aus der Ferne über das Internet warten. Bei solchen Anforderungen ist eine sichere und kontrollierte Anbindung der Maschinen an interne und externe Dienste vonnöten.

Das Sicherheitssystem secunet edge enthält ein modulares Plattform-Konzept in Form einer Ausführungsumgebung für Applikationen. Anwendungen, die darin ausgeführt werden, beispielsweise Agenten von IoT-Plattformen, Anwendungen zur Datenvorverarbeitung oder zur Kommunikation mit internen Diensten, erhalten einen kontrollierten Zugriff auf Informationen verbundener Maschinen und können diese sicher und gerichtet an den jeweiligen Dienst übermitteln bzw. davon entgegennehmen. Der entscheidende Vorteil eines solch offenen und modularen Plattform-Konzepts: Die Gesamtkomplexität verringert sich durch die Bündelung benötigter Anwendungen auf einer Edge-Computing-Plattform. So benötigen individuelle IoT-Anwendungsszenarien keine Individuallösungen und lassen sich schrittweise im eigenen Tempo realisieren. Auch Entwickler sowie Anbieter von Datendiensten, beispielsweise im Bereich der künstlichen Intelligenz oder Big Data, profitieren von einem solchen Konzept. Sie können ohne tiefgreifendes Security-Know-how und ohne Einschränkungen in Hardware-Fragen ihre plattformunabhängigen Anwendungen über die Plattform secunet edge sicher anbieten.

Detect: Security Monitoring zur Stärkung der Abwehr von Cyberangriffen

Neben der grundlegenden Absicherung ist die stete Überwachung der Kommunikation von und zur Maschine zur Aufrechterhaltung eines höchstmöglichen IT-Sicherheitsniveaus entscheidend. Ein Security Monitoring macht den Informationsfluss transparent und ermöglicht die Analyse des Kommunikationsverhaltens der Maschine. secunet edge bietet hierzu eine integrierte Sensorik, die den ein- und ausgehenden Datenverkehr an der Schnittstelle zwischen Maschine und externem Netz kontinuierlich erfasst und durch ein zentrales Analysesystem auswertet.

Mit Hilfe von selbstlernenden Algorithmen erfasst das Analysesystem das Normalverhalten der Kommunikation einer Maschine. Ein plötzlich auftretendes abnormales Kommunikationsverhalten, das unter anderem durch die Infektion einer Maschine mit Malware oder durch einen nicht gewollten



Verbindungsaufbau eines Angreifers zur Maschine auftreten kann, wird so erkannt. Der Vorteil einer solchen Verhaltensanalyse: Auch bislang unbekannte Angriffstypen werden aufgedeckt. Dies ermöglicht eine unmittelbare Reaktion beim Auftritt eines Sicherheitsvorfalls, und die ungewollte Kommunikation zwischen Maschine und Netzwerk kann blockiert werden.

Hardwarebasierte Informationssicherheit

Für die unterschiedlichen Aufgaben, die secunet edge ausführt, sind kryptographische Funktionen nötig, die das System hardwaregestützt umsetzt. Das dazu fest verbaute, zertifizierte Secure Element (SE) – eine mit einer Smartcard vergleichbare Technologie – dient als Vertrauensanker und ermöglicht es beispielsweise, Verschlüsselungsmechanismen auszuführen oder kryptographische Schlüssel innerhalb eines manipulationssicheren Chips zu verwahren. Diese Sicherheitsfunktionen sind auch für externe Anwendungen nutzbar, die auf der Plattform ausgeführt werden. Ebenfalls denkbar ist es, die mit secunet edge verbundene Maschine mit einer digitalen Identität zu versehen und in eine Public-Key-Infrastruktur (PKI) zu integrieren, was eine Vielzahl weiterer Anwendungsmöglichkeiten schafft (Beispiele von PKI-Use-Cases finden sich in den Artikeln über CLAAS und ifm in dieser secuview-Ausgabe).

Vielfältige Einsatzmöglichkeiten

Mit secunet edge werden nicht nur verschiedene Anforderungsbereiche der Industrial Security bedient, sondern auch Basisfunktionen zur Umsetzung von Industrie-4.0-Konzepten bereitgestellt. Hier wird offenbar, was IT-Sicherheitsanbieter schon seit Längerem postulieren: Cybersicherheitstechnologie kann, richtig eingesetzt, zum Enabler werden.

Zudem deckt secunet edge nicht nur gegenwärtige, sondern auch künftige Anforderungen ab. Denn die Schutzhülle, die das System gleichsam um die Maschine legt, ist variabel und kann dadurch einfach an zukünftige Erfordernisse angepasst werden. Deshalb profitieren nicht nur Betreiber, die ihren Maschinenpark nachrüsten und den Digitalisierungsprozess mit einem soliden Fundament der IT-Sicherheit untermauern wollen, von secunet edge. Auch Maschinenhersteller, die neue Maschinen-Designs mit einer zukunftssicheren Schutzhülle versehen möchten – und gleichzeitig den Anforderungen ihrer Kunden zur Absicherung von Bestandsmaschinen nachkommen wollen –, gehören zu den Adressaten der Lösung. Nicht zuletzt können Systemintegratoren sich die Edge-Computing-Plattform zunutze machen und ihre IT-Dienste an die Maschine des Betreibers bringen.

Maschinen stehen zwar strukturell gesehen am Rande eines Industrie-4.0-Netzwerks – „at the edge“ –, doch nichtsdestotrotz kommt ihnen eine zentrale Rolle zu. Deshalb ist es so wichtig, sie angemessen zu schützen und ihr Potenzial durch neue Technologien auszuschöpfen.

Torsten Redlich
torsten.redlich@secunet.com

DIGITALE IDENTITÄTEN IN DER INDUSTRIE 4.0

Vertrauen zwischen Maschinen

Eine der Voraussetzungen für eine intakte Kommunikationskette ist es, dass die Kommunikationspartner darauf vertrauen, dass es sich bei den jeweils anderen tatsächlich um die Personen oder Instanzen handelt, für die sie sich ausgeben. In menschlicher Kommunikation wird dieses Vertrauen im Alltag anhand von Erfahrungswerten hergestellt oder auch verweigert; in sicherheitskritischen Kontexten nutzen Menschen Identitätsdokumente. Doch was, wenn die Kommunikationspartner Maschinen sind, so wie in der hochautomatisierten Industrie 4.0? In diesem Fall erhalten die Maschinen abgesicherte digitale Identitäten. Die ifm-Unternehmensgruppe nutzt eine Public-Key-Infrastruktur (PKI), um ihre Gateway-Komponenten zu „personalisieren“.

Gerade bei automatisierten Vorgängen im Internet der Dinge ist die Zuverlässigkeit von Daten von höchster Bedeutung. Denn anders als bei nicht- oder teilautomatisierten Prozessen, bei denen vorhandene Daten und daraus abgeleitete Handlungen durch Techniker bewertet werden können, müssen automatisierte Abläufe ohne solche Instanzen auskommen: Die übermittelten Daten werden nach festgelegten Schemata genutzt und Aktivitäten autonom umgesetzt. Es gibt weder zusätzliche Gegenprüfungen noch Interpretationsspielraum.

Wie lässt sich unter diesen Umständen Vertrauen in die Daten herstellen? Entscheidend ist die Authentizität, also die sichergestellte Identität der Datenquelle. Ist diese zweifelsfrei gegeben, kommt es im zweiten Schritt darauf an, ob mit den vorhandenen Mitteln eine unterbrechungsfreie, manipulationsgeschützte Verbindung zwischen Datenquelle und Empfänger etabliert werden kann. Ist dies der Fall, kann den übermittelten Daten vollumfänglich vertraut werden.

Die ifm-Gruppe produziert und vertreibt Sensoren, Steuerungen, Software und Systeme für die industrielle Automatisierung und Digitalisierung – sprich für die Industrie 4.0. Damit eine digitalisierte Industrie funktionieren kann, ist es zunächst wichtig, dass Komponenten wie beispielsweise Gateways in der Lage sind, sich mit der für sie relevanten IT-Infrastruktur zu vernetzen. Zudem benötigen sie eine Identität, über die sie innerhalb der Infrastruktur eindeutig zuzuordnen sind und adressiert werden können. Bildhaft spricht man von der „Personalisierung“ der maschinellen Komponenten. Nur so kann eine intakte Kommunikationskette über mehrere Komponenten hinweg entstehen, zum Beispiel vom Sensor am Anfang der Kette bis zum verarbeitenden IT-System am Ende, wobei sichergestellt ist, dass alle Elemente vertrauenswürdig sind.

PKI als Lösungsweg

Im Jahr 2018 war ifm bei der Entwicklung einer neuen Industrie-4.0-Produktlinie auf der Suche nach einer Lösung für die Personalisierung dieser Komponenten. Dafür bietet sich grundsätzlich eine Public-Key-Infrastruktur (PKI) an. PKI-Lösungen stellen die Vertraulichkeit, Authentizität und Integrität von Daten sicher, indem sie auch automatisiert digitale Zertifikate erzeugen, anwenden und verwalten. Sie laufen meist im Hintergrund ab und sind mittlerweile in vielen alltäglichen Anwendungsbereichen fest etabliert: von der Prüfung von Identitätsdokumenten bei der Grenzkontrolle über die Absicherung von Sensor- und Steuerungsdaten in der digitalisierten Landwirtschaft (vgl. den Artikel über CLAAS in dieser Ausgabe, siehe Seite 23) bis hin zum Schutz von Datenströmen in der Automotive-IT.

Auch bei dem hybriden Verschlüsselungsprotokoll TLS (Transport Layer Security), das unter anderem in HTTPS-basierten Webservern eingesetzt wird und dort alltägliche Anwendungen wie Online-Shopping absichert, handelt es sich um ein PKI-basiertes Verfahren. Im Kontext der Industrie 4.0 ist TLS dazu geeignet, Vertrauensbeziehungen zum Austausch von Daten zu schaffen. Mit TLS lassen sich Daten verschlüsselt über das Internet oder andere Netzwerke übertragen. Dabei wird zum einen durch den Einsatz von Zertifikaten die Authentizität der Kommunikationspartner sichergestellt. Zum anderen schützt eine Transportverschlüsselung die zu übermittelnden Daten vor dem unbefugten Zugriff Dritter und vor Manipulation oder Fälschung. Somit kann eine TLS-basierte Lösung die beiden oben genannten Anforderungen bei der Personalisierung der von ifm produzierten Komponenten abdecken.

So weit stand also fest, welcher Lösungsweg beschritten werden sollte. Allerdings stellte die Umsetzung für ifm eine

Die Automatisierung und Digitalisierung der Industrie, wie zum Beispiel in dieser Fabrikhalle, ist bereits weit fortgeschritten.

BEST PRACTICE: WIE SOLLTE EINE PKI FÜR DIE PRODUKTION VON INDUSTRIE-4.0-KOMPONENTEN AUSSEHEN?

PKI-Lösungen erfüllen ganz unterschiedliche Einsatzzwecke, für die jeweils typische Anforderungen gelten. Für den Einsatz bei der Produktion von Industriekomponenten sind die folgenden Anforderungen maßgeblich, die vorrangig darauf abzielen, Verzögerungen in der Produktion zu vermeiden:

- Die PKI sollte einen hohen Zertifikatsdurchsatz aufweisen, um zu vermeiden, dass bereits in der Planungsphase Einbußen im Produktionsumfang auftreten.
- Bei der Planung und Installation sollte auf Ausfallsicherheit Wert gelegt werden, so dass die Produktion der Industriekomponenten uneingeschränkt gewährleistet ist, auch wenn einmal in einer der Systemkomponenten ein Fehler auftreten oder ein Wartungseingriff erforderlich sein sollte.
- Da gegebenenfalls Zertifikatsanfragen in von Standard-IT-Systemen abweichenden Formaten durchgeführt werden müssen, sollte die PKI in Bezug auf Schnittstellen zwischen der PKI und dem Personalisierungssystem der Industriekomponenten flexibel aufgestellt sein.
- Um eine durchgehende Automatisierung zu gewährleisten, sollte die PKI automatisierte Workflows für einen reibungslosen Betrieb ohne Benutzerinteraktionen bieten.
- Die Lösung sollte erweiterbar sein, um wachsenden Produktionszahlen gerecht zu werden oder auch um individuelle Zertifikate bereitstellen zu können, die auf bestimmte Komponenten zugeschnitten sind.
- Optional sollte die PKI als Managed Security Service zur Verfügung stehen. Dies ermöglicht es dem Produktionsunternehmen, sich auf seine Kernkompetenzen zu konzentrieren.

Mit der secunet eID PKI Suite steht ein ausgereiftes Produkt zur Realisierung einer flexiblen und leistungsfähigen PKI für die Produktion im Industrie-4.0-Umfeld zur Verfügung.

Herausforderung dar, da das auf Produktion spezialisierte Unternehmen bei der Implementierung von IT-Security-Standards Neuland betreten musste. Hier erwies sich die enge Zusammenarbeit des hauseigenen Integrators ifm services gmbh mit secunet als hilfreich. Auf diese Weise konnten alle Beteiligten ihre jeweiligen Kernkompetenzen einbringen und das Projekt erfolgreich realisieren.

Integration in die Produktionsabläufe

Die Partner entwickelten auf das Anforderungsszenario hin passgenaue Vorgehensweisen und eine Integrationsplanung, um die PKI nahtlos in den Produktionsablauf einzubetten. Die Abstimmung und Implementierung der dafür benötigten Schnittstellen wurden zeitgerecht abgeschlossen, so dass ifm pünktlich zum geplanten Marktstart Gateways anbieten konnte, die bereits mit Zertifikaten personalisiert waren. Zudem übernahm secunet den fortlaufenden Betrieb der PKI-Komponenten als Managed Security Service. So musste ifm keine eigenen Kapazitäten dafür aufbauen und konnte sich weiterhin auf seine Kernkompetenzen konzentrieren.

Das hohe Tempo bei der Realisierung der ifm-Lösung ließ sich auch deswegen halten, weil sie auf einer bewährten Standardlösung basiert: der secunet eID PKI Suite. Diese modulare Infrastruktur wurde ursprünglich im Kontext der Prüfung von Identitätsdokumenten entwickelt, wird heute aber weit über diesen Bereich hinaus eingesetzt. Sie hält passende Bausteine für eine große Bandbreite von Einsatzszenarien bereit – insbesondere auch in der Industrie.

ifm-Gateway-Komponenten zur Industrieautomation wie hier im Bild erhalten digitale Identitäten, damit sie innerhalb der Infrastruktur zweifelsfrei zugeordnet werden können.
Quelle: ifm-Unternehmensgruppe

Das Projekt verlief so erfolgreich, dass derzeit eine Erweiterung in Planung ist: Künftig soll die bisher auf eine Produktlinie zugeschnittene Gerätepersonalisierung so ausgebaut werden, dass für verschiedene weitere Komponenten individuelle Zertifikate generiert werden können. Auch bei der Umsetzung dieses Elements seiner Industrie-4.0-Strategie wird ifm wieder mit secunet zusammenarbeiten.

Björn Jansen
bjoern.jansen@secunet.com

ZUM UNTERNEHMEN

Messen, steuern, regeln und auswerten – wenn es um wegweisende Automatisierungs- und Digitalisierungstechnik geht, ist die **ifm-Unternehmensgruppe** Pionier und Partner. Seit der Firmengründung im Jahr 1969 entwickelt, produziert und vertreibt ifm weltweit Sensoren, Steuerungen, Software und Systeme für die industrielle Automatisierung und Digitalisierung. Heute zählt die in zweiter Generation familiengeführte ifm-Unternehmensgruppe mit mehr als 7.000 Beschäftigten in 85 Ländern zu den weltweiten Branchenführern. Als Mittelstandskonzern vereint ifm die Internationalität und Innovationskraft einer wachsenden Unternehmensgruppe mit der Flexibilität und Kundennähe eines Mittelständlers.

PENTESTS FÜR DIE INDUSTRIE 4.0

Erst der Schrecken, dann die Lösung

Pentests – kurz für „Penetrationstests“ – decken potenzielle Einfallstore für Cyberangriffe auf. Basierend auf diesen Befunden, die für die Betreiber der IT-Systeme zunächst ein wenig erschreckend sein können, werden Lösungen zur Absicherung erarbeitet. Auch in der Industrie praktiziert man dieses Vorgehen schon seit Langem erfolgreich.

In den letzten 20 Jahren hat das secunet Pentestteam viele unterschiedliche Systemtypen geprüft: von ganz klein (Mikrokontroller) bis ganz groß (Kraftwerks-IT), von hoch kritisch (Maschinensteuerungen) bis ganz alltäglich (Bürorechner). Dabei sind den Experten auch sehr unterschiedliche (Fehl-)Verhaltenstypen der Systeme untergekommen. Hier einige Beispiele, speziell aus dem Umfeld der Prozess-IT:

- Systeme, die sich bereits bei einem Portscan tot stellen und in einen nicht-definierten Zustand verschwinden.
  `Fatal error`
- Systeme, die nach einem Test-Update mit einer angepassten Konfiguration in den Reset-Modus verfallen und nur noch mit Standard-Passwörtern auf Standard-Ports zu erreichen sind.
  `System not reachable`
- Systeme mit ungesicherten Schnellzugriffen, die – manchmal erst über Umwege – einen administrativen Zugriff erlauben. **`Welcome root`**

Doch nicht nur Maschinen und Systeme offenbaren Schwachstellen. Auch Mitarbeiter sind nicht immer fehlerfrei und geben am Telefon schon mal Login-Token an angebliche Servicetechniker heraus. **`Human error`**

Bekannte Problemzonen

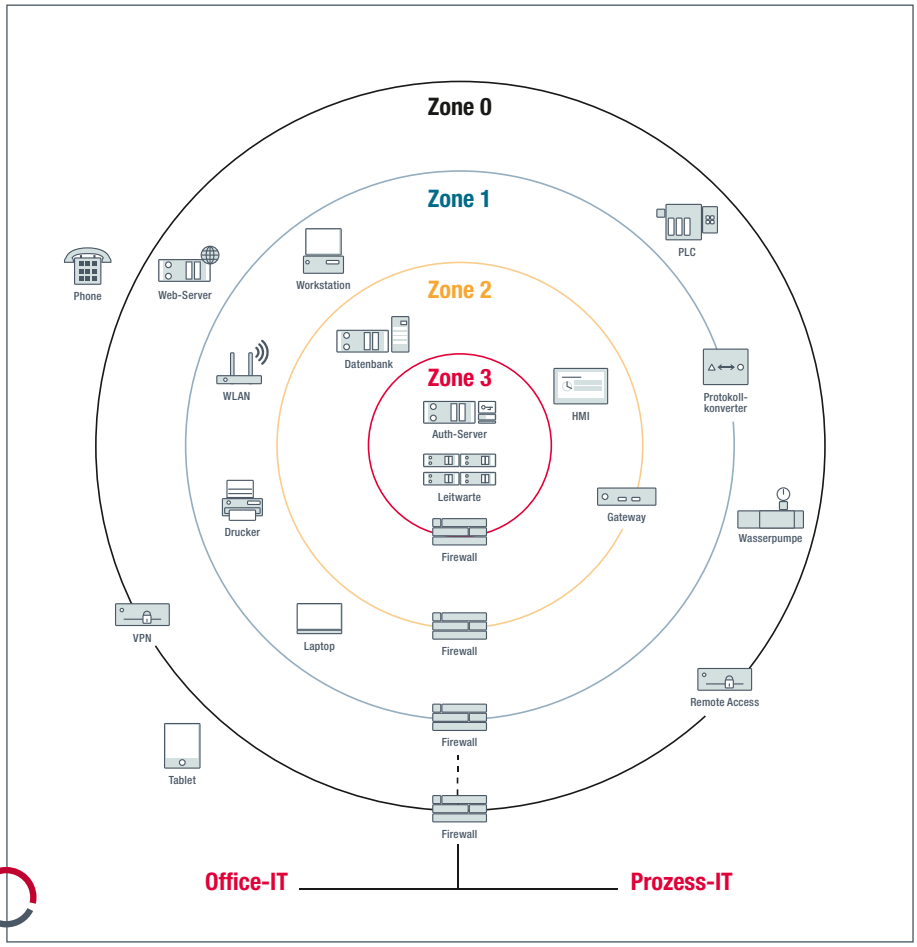
Dies sind die Top 5 der Problemzonen in Prozess-IT-Systemen aus Sicht der secunet Pentester:

1. schlechter Zugangsschutz für Systeme und Anwendungen
2. Nutzung unverschlüsselter Protokolle
3. veraltete Hard- und Softwarekomponenten
4. fehlende Systemhärtung
5. zu große und/oder unsegmentierte Netzbereiche

Diese Probleme sind alte Bekannte aus der klassischen Büro-IT. Allerdings bringt die Prozess-IT weitere, oft unterschätzte Herausforderungen mit sich:

- Der Zugangsschutz (beispielsweise über Passwörter) ist häufig trivial umgesetzt und nicht änderbar.
- Die verwendeten Transferprotokolle enthalten keine angemessenen Sicherheitsmechanismen, sie sind häufig proprietär und nicht aktualisierbar.
- Ein Patchen von Alt-Systemen ist nicht möglich oder führt zum Verlust von Service-Garantien.
- Systeme müssen wie vom Hersteller vorgegeben betrieben werden, eine Härtung ist im Nachhinein nicht möglich.

An diesem Punkt stellen sich grundsätzliche Fragen: Wie lassen sich Pentests in der Prozess-IT eigentlich durchführen, wenn die aus der Büro-IT bewährten Sicherheitsmaßnahmen nur selten anwendbar sind? Und helfen Pentests überhaupt, wenn die erwähnten Herausforderungen nicht so einfach zu lösen sind?



Im Rahmen des secunet OT-Pentest-Modells legen die Experten bei der Analyse einer Infrastruktur verschiedene Zonen oder Schalen fest – so wie in diesem Beispiel.

Das secunet OT-Pentest-Modell

Um diese Klippe zu umschiffen, wurde das secunet OT-Pentest-Modell entwickelt. Es liefert die nötige Risikoorientierung, eine valide Vorgehensstruktur sowie Analyseanwendungen, die im Umfeld der Prozess-IT bewährt sind. Das Modell teilt im ersten Schritt den zu betrachtenden Systemverbund in maximal vier Schalen auf (siehe Grafik auf Seite 35). Die äußere Schale ist oft die Firewall, die das „Drinnen" vom „Draußen" trennt. Die innere Schale weist den höchsten Schutzbedarf auf, so wie etwa die Leitwarte einer Produktionsanlage. Für jede dieser Schalen werden nun in einem zweiten Schritt die wahrscheinlichsten Angriffsvektoren bestimmt – das können zum Beispiel Angriffe über die Internetanbindung, über Schnittstellen zu Dienstleistern, über Datenkommunikationsschnittstellen mit externen Produktionsstätten oder über Schnittstellen in die Office-IT sein. Diese potenziellen Einfallstore werden dann gezielt analysiert.

Die gute Nachricht: Schlecht abgesicherte Schnittstellen lassen sich in der Regel gut behandeln, da sie meist von handelsüblichen Systemen wie Firewalls und Routern kontrolliert werden – und diese können ohne negative Auswirkungen auf die eigentlichen Steuerungssysteme angepasst werden. Ein großer Teil bekannter Angriffe wird damit wirkungslos.

Ist die äußere Schicht gesichert, werden schrittweise die weiteren Schichten geprüft. Zum Schluss haben die Experten nicht nur Angriffspotenziale auf jede einzelne Komponente identifiziert, sondern auch Maßnahmen abgeleitet, um die Risiken zu minimieren, denen diese ausgesetzt sind. Das secunet OT-Pentest-Modell definiert somit die entscheidenden Schritte auf dem Weg zur sicheren Prozess-IT.

Dirk Reimers
dirk.reimers@secunet.com

TELEMATIKINFRASTRUKTUR

E-Health: Kann Deutschland Digitalisierung?

Ein Kommentar von Markus Linnemann, Leiter der Division Kritische Infrastrukturen, secunet Security Networks AG

Der Digitalisierungsprozess im Gesundheitswesen begann bereits vor mehr als 15 Jahren. Nun, im Sommer 2019, sind die niedergelassenen Ärzte und Zahnärzte als erste von mehreren Gruppen an die Telematikinfrastruktur (TI) angeschlossen – zumindest überwiegend. Aber sind Mehrwerte für Ärzte oder Versicherte entstanden? Ist die Technologie sicher? Passt der organisatorische Rahmen? Es ist Zeit, den Status Quo zu betrachten – und auch, eine Lanze für die Technologie hinter der TI zu brechen.

Am 30. Juni 2019 lief für die erste Gruppe, die ca. 176.000 Haus-, Fach- und Zahnärzte sowie Psychotherapeuten (auch „Leistungserbringer" genannt), die Frist für die Anbindung an die Telematikinfrastruktur mit dem Konnektor ab. Wer jetzt noch nicht an das digitale Gesundheitsnetz Deutschlands angeschlossen ist, muss Strafe zahlen – und zwar laut Gesetz 1 % der Honorarkosten.

secunet hat bereits über 45.000 Konnektoren für das digitale Gesundheitsnetz ausgeliefert und ist damit sehr gut im Markt vertreten – nicht zuletzt, da es geschätzt zwischen 10.000 und 30.000 Verweigerer und Abwartende im Markt gibt, die zum Teil wohl auch eine Klage gegen die gesetzlichen Regelungen eingereicht haben und aktuell auf das Ergebnis warten.

Denn es ist nicht so, dass die Digitalisierung im Gesundheitswesen überall mit offenen Armen empfangen wird. Die Vorbehalte sind groß: Werden die Abläufe in meiner Praxis gestört? Ergibt sich überhaupt ein Mehrwert? Sind meine Patientendaten geschützt? Welche Kosten entstehen mir dadurch? Solche Fragen stellen sich viele Ärzte, und sie sind durchaus gerechtfertigt. Bei vielen Leistungserbringern herrscht Unklarheit, was die Einführung überhaupt für sie bedeutet – sei es nun im Positiven oder im Negativen.

Transformation braucht die richtige Kommunikation

Wurde also zu wenig informiert? Verschiedene Instanzen haben in zahlreichen Informationsveranstaltungen Wissen vermittelt und tun dies immer noch. Allerdings orientiert sich die Informationsvermittlung oft an technischen Fakten, die nicht zum tatsächlichen – und oft sehr unterschiedlichen – Wissensstand des Publikums passen. Wenn in einer Veranstaltung für Hausärzte darauf hingewiesen wird, dass Konnektoren Smart Cards mit Zertifikaten enthalten, die in fünf Jahren ablaufen, können die meisten

Markus Linnemann
Leiter der Division
Kritische Infrastrukturen
secunet Security Networks AG

Teilnehmer diese Information nicht einordnen. Bei ihnen bleibt vor allem hängen: „In fünf Jahren habe ich ein Problem, die Technik ist ja gar nicht ausgereift." Hier fehlt die Abstraktion von der Technik zur eigentlichen Auswirkung bei den Ärzten. Tatsächlich muss nach fünf Jahren das Zertifikat erneuert werden, aber das ist eine technisch lösbare Aufgabe, obwohl der Prozess noch nicht ganz feststeht.

Die meisten Ärzte sind keine IT-Spezialisten und wollen dies – zu Recht – auch nicht sein, schließlich liegt IT meilenweit von ihrem eigentlichen Fachgebiet entfernt. Ein Transformationsprojekt, das auf komplexer Technologie beruht, bedarf daher einer Kommunikation, die an die Zielgruppe angepasst ist. Dies erfordert eine enge Zusammenarbeit zwischen Referenten und Experten, die die komplexe Technologie auf die Lebenswirklichkeit der Ärzte abbilden können.

Ähnlich funktionieren Awareness-Projekte für IT-Sicherheit, die in Unternehmen oder Behörden Aufmerksamkeit für Informationssicherheit schaffen sollen. Durch zielgruppengerechte Kommunikation können betroffene Personengruppen von einer ursprünglich ablehnenden Haltung über rationale Akzeptanz bis hin zu Erkenntnis und Integration geführt werden, wenn es sich um ein an sich vernünftiges Projekt handelt. Diese bewährten Methoden lassen sich auch auf ein Transformationsprojekt wie die Digitalisierung im Gesundheitswesen anwenden. Die Erfahrung aus Awareness-Projekten zeigt aber auch, dass es einige Zeit dauert, bis ein Umdenken stattfindet.

Zudem besteht ein wesentlicher Unterschied zwischen IT-Sicherheit und Telematikinfrastruktur: IT-Sicherheit benötigt definitiv jeder. Bei der TI ist das aus der Perspektive vieler Ärzte noch nicht erwiesen. Erst mit künftigen Erweiterungen wie zum Beispiel der elektronischen Patientenakte ist zu erwarten, dass der Mehrwert der Digitalisierung für Leistungserbringer offenbar wird. Zumindest bis zu diesem Zeitpunkt ist weiterhin damit zu rechnen, dass dem Projekt als Ganzem auch Skepsis entgegenschlägt.

Angst vor dem „gläsernen Patienten"

Deutschland ist bekannt für seine hohen Anforderungen im Hinblick auf Sicherheit und Datenschutz. Dies schlägt sich in der Architektur der TI nieder: Deren Sicherheitsanforderungen sind sehr hoch – vermutlich sind sie im weltweiten Vergleich digitaler Gesundheits-Infrastrukturen mit Abstand die höchsten. Dennoch zweifeln verschiedene Gruppen, zum Beispiel aus dem Umfeld der Leistungserbringer, an der Sicherheit der TI.

Natürlich sind Sicherheitsbedenken grundsätzlich nichts Schlechtes – im Gegenteil. Ein IT-System in weltweite Datennetze zu integrieren bedeutet immer, statt rein lokalen potenziellen Angriffsvektoren auch globale betrachten zu müssen. Zudem gilt: Hundertprozentige Sicherheit kann es nie geben. Es ist also immer ratsam, Bedenken ernst zu nehmen und potenzielle Einfallstore zu untersuchen.

Die am weitesten verbreiteten Bedenken beziehen sich auf einen möglichen Verlust von Patientendaten und die Angst vor dem „gläsernen Patienten". Da die meisten Ärzte wie erwähnt keine IT-Experten sind und nicht jeder Arzt sich einen professionellen IT-Service mit IT-Sicherheitskompetenz

SECUNET IM GESUNDHEITSSEKTOR

secunet wurde im Dezember 2018 im digitalen Gesundheitsmarkt präsent, als der secunet konnektor von der gematik – Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH zugelassen wurde. Der secunet konnektor dient beispielsweise Arztpraxen, Apotheken oder Krankenhäusern als zentrales Element zum Anschluss an die Telematikinfrastruktur (TI).

Dem Markteintritt ging eine Entwicklungsphase voraus, die von unzähligen Gesprächen mit Kunden, Verbänden, Ärzten, dem Bundesamt für Sicherheit in der Informationstechnik (BSI), der gematik und der Politik geprägt war. Auf diese Weise hat die secunet Division Kritische Infrastrukturen einen umfassenden Einblick in den Digitalisierungsprozess im Gesundheitswesen in Deutschland und die vielfältigen damit verbundenen Herausforderungen gewinnen können.

beauftragt, ist durchaus davon auszugehen, dass einige Praxen ohne großen Aufwand angreifbar sind, da ihnen die notwendigen Sicherheitsvorkehrungen in ihrem Netzwerk fehlen. Folglich besteht ein Risiko, das allerdings immer nur auf eine Arztpraxis beschränkt ist. Die TI als Ganze mit ihrer Vielzahl von Gesundheitsdaten ist nicht in Gefahr.

Aktuell erregt in der Presse und den sozialen Medien ein Fall Aufsehen, bei dem ein Dienstleister offenbar beim Anschluss einer Praxis an die TI die vorher bestehenden Sicherheitsvorkehrungen des Praxisnetzwerks außer Kraft gesetzt und die Praxis somit unsicher hinterlassen hat. Wenn sich dies so zugetragen hat, handelt es sich um eine klare Fehlleistung des Dienstleisters. Für die betroffene Arztpraxis ist das ein Problem, aber lässt sich aus diesem Fall ableiten, die TI sei unsicher? Nein, denn erstens ist der Fehler nicht der Technologie der TI anzulasten. Zweitens hat der Fehler die Sicherheit des Praxisnetzwerks reduziert, der TI aber keinen Schaden zugefügt. Der Zugang zu dieser ist weiterhin durch den verbauten Konnektor geschützt.

Die Technik ist nicht das Sicherheitsproblem

An dieser Stelle erscheint es durchaus angebracht, eine Lanze für die Technik, die hinter der TI steckt, zu brechen. Diese Technik als unsicher oder veraltet zu bezeichnen, geht am eigentlichen Problem vorbei. Denn die Verschlüsselungstechnologien, die bei der TI eingesetzt werden, folgen höchsten Sicherheitsstandards. Aus Sicht eines Sicherheitsexperten wirken die Schutzkonzepte, die bei der TI Anwendung finden, an einzelnen Stellen sogar übertrieben. Wenn dann Geräte falsch installiert werden, ist das nicht der Technologie vorzuwerfen. Zudem können organisatorische Abläufe und Datenschutzkonzepte (etwa hinsichtlich der Art der Datenhaltung und der Zugriffsrechte) völlig unterschiedlich umgesetzt werden, mit durchaus unterschiedlichen Sicherheitsniveaus. Doch die Frage, welche Personengruppen Zugriffsrechte auf welche Daten erhalten sollen, ist keine technische, sondern eine organisatorische. Diese Aspekte können und sollten intensiv diskutiert werden.

Zudem ist zu bedenken, dass sich manche der Anforderungen widersprechen. Um die Bürger von den Vorteilen der TI profitieren zu lassen, wäre es zum Beispiel wünschenswert, dass sie ihre Patientenakte künftig auf dem Smartphone oder sogar auf der Smartwatch auslesen können. Technisch lässt sich diese Herausforderung lösen, die gematik hat bereits Spezifikationen dazu vorgelegt. Doch dabei sollte nicht vergessen werden, dass die Anbindung von Mobilgeräten prinzipiell ein höheres Risiko mit sich bringt als die Anbindung von speziell geschützten stationären Geräten wie dem Konnektor. Dieses Beispiel zeigt, dass es letztlich immer darum geht, Risiken abzuwägen. Je größer der potenzielle Schaden, desto umfangreicher sollten die Sicherheitsmaßnahmen ausfallen. Und je nach Zugriffspunkt – Handy, Arztpraxis, Krankenhaus, Krankenkasse – ist das Risiko unterschiedlich zu bewerten.

TELEMATIKINFRASTRUKTUR – WO KOMMEN WIR HER, WO GEHEN WIR HIN?

Zweck der Telematikinfrastruktur (TI) ist es, die Beteiligten im Gesundheitswesen – Ärzte, Krankenhäuser, Apotheken, Krankenkassen und weitere Instanzen – miteinander zu verbinden, um medizinische Informationen über Patienten austauschen zu können. Für den Aufbau, den Betrieb und die Weiterentwicklung der TI wurde 2005 die gematik – Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH gegründet.

Die Jahre 2006 bis 2011 waren geprägt durch Abstimmungen zwischen den Verbänden der Krankenkassen und Ärzte. Seit 2011 nahm das Projekt mit dem Rollout der elektronischen Gesundheitskarte an Fahrt auf. Ende 2017 ging die erste Praxis mit einem Konnektor online. Konnektoren (so wie der secunet konnektor) fungieren als Herzstück für die sichere Kommunikation zwischen Arztpraxis und TI.

In den kommenden Monaten wird die TI durch Fachanwendungen ergänzt, die sichtbaren Mehrwert bringen werden. Dazu zählen die qualifizierte elektronische Signatur (QES), die Kommunikation für Leistungserbringer (Kom-LE), das Notfalldatenmanagement (NFDM) und der elektronische Medikationsplan (eMP). Nach dem Terminservice- und Versorgungsgesetz (TSVG) soll am 1. Januar 2021 auch in der Fläche die elektronische Patientenakte (ePA) zur Verfügung stehen.

Parallel werden in den nächsten Monaten nach den Haus-, Fach- und Zahnärzten die Klinken und Apotheken an die digitale Datenautobahn im Gesundheitswesen angeschlossen. Auch in den übrigen Heilberufen formieren sich bereits die ersten Interessierten und prüfen die Möglichkeiten, die sich durch die Digitalisierung ergeben.

Mehrwert in Sichtweite

Die Diskussion um die TI wird zusätzlich dadurch belastet, dass echte Mehrwerte für die Beteiligten aktuell noch nicht sichtbar sind. Dies gilt insbesondere für die Versicherten: Sie können momentan durchaus den Eindruck gewinnen, für ein Mammut- und Langzeitprojekt zu zahlen, das ihnen aber unter dem Strich nichts bringt. Doch der Eindruck trügt: Mehrwerte werden sich zeigen, wenn die Applikationen eingeführt werden, die spürbare Vorteile für die Versicherten und Leistungserbringer bereithalten. Dazu gehören etwa die elektronischen Patientenakten, das Notfalldatenmanagement und der elektronische Medikationsplan.

Kann Deutschland nun Digitalisierung? Ja, wenn die beteiligten Instanzen auf eine Weise kommunizieren und organisieren, die einem tiefgreifenden Transformationsprojekt angemessen ist. Dazu müssen alle Beteiligten an einem Strang ziehen. Im Fall der TI sind die beteiligten Instanzen vielfältig, von politischen Organisationen über Krankenkassen bis hin zu Verbänden und Leistungserbringern. Es ist derzeit noch offen, ob der Dialog zwischen ihnen am Ende effizient und konstruktiv gelingt. Wünschenswert wäre dies, da die TI künftig allen Beteiligten, auch den Versicherten, echte Mehrwerte bieten kann.

SINA PRODUKT-NEWS

Client im Flüstermodus

Die speziell gehärtete SINA Workstation H R RW11 ist nun auch in einer abstrahlgeschützten Variante gemäß SDIP 27 Level A erhältlich. Dies dient der Abwehr von Angriffen, die auf das Empfangen und Auswerten elektromagnetischer Abstrahlung des Clients abzielen.

Die SINA Workstation H R RW11 ist ein universell einsetzbarer Krypto-Client für mobile und extreme Einsatzbedingungen. So bietet das Gehäuse einen hohen Schutz insbesondere gegen Schock, Vibration, Staub und Feuchtigkeit. Die SINA Workstation H R RW11 wurde gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) für die Verarbeitung, Speicherung und Übertragung von Verschlusssachen der Einstufungen bis einschließlich GEHEIM entwickelt. Im Fokus stehen dabei militärische und behördliche Hochsicherheitsnetze mit taktisch mobilen Systemanteilen.

Die neue Produktvariante erfüllt mit SDIP 27 Level A extrem hohe Anforderungen an den Abstrahlschutz. Sie ergänzt eine weitere abstrahlgeprüfte Ausführung gemäß Zone 1, die bereits seit 2017 verfügbar ist. Damit bietet das Portfolio Produktvarianten für unterschiedliche Einsatzszenarien.

Neben dem gehärteten Client befindet sich mit der SINA Workstation H Client III 27A ein weiterer maximal abstrahlgeschützter Client-Typ auf der Ziellinie. Erste Geräte werden Ende 2019 ausgeliefert.

Merlin Gräwer
merlin.graewer@secunet.com

Wunderbar together in San Francisco – secunet auf der RSA Conference 2019

Jedes Jahr im Frühjahr treffen sich die Spitzenvertreter der internationalen IT-Sicherheitsszene in Kalifornien. Mit mehr als 42.000 Besuchern, 650 Ausstellern sowie zahlreichen renommierten Experten, Keynote-Speakern und Impulsgebern gilt die RSA Conference in San Francisco als weltweit wichtigste Veranstaltung für IT-Security. Das überaus breit gefasste Konferenzprogramm aus Sessions, Keynotes und Seminaren beschäftigt sich mit Themen von Cloud-Angeboten und Kryptographie bis hin zu hoheitlichen Lösungen für IT-Sicherheit und Cyberabwehr. Auch für erfahrene Konferenzbesucher ist es aufgrund dieser Vielfalt jedes Jahr wieder eine Herausforderung, das jeweils passende Konferenzangebot nicht zu verpassen.

Wie in den Jahren zuvor war secunet auch dieses Mal auf dem deutschen Gemeinschaftsstand vertreten und präsentierte dort gemeinsam mit anderen Anbietern „IT Security made in Germany“. Die Besonderheit in diesem Jahr: Der deutsche Gemeinschaftsauftritt wurde in den Veranstaltungskalender des offiziellen, durch das Auswärtige Amt, das Goethe-Institut und den Bundesverband der Deutschen Industrie koordinierten und geförderten „Deutschland-USA-Jahres 2019“ aufgenommen – Motto dieser Initiative: „Wunderbar together“. Vor diesem Hintergrund waren auch hochrangige Vertreter des Bundesamts für Sicherheit in der Informationstechnik (BSI) sowie des Bundesministeriums des Innern, für Bau und Heimat (BMI) mit auf dem German Pavillon anwesend.

Thematischer Schwerpunkt auf dem secunet Messestand war neben SINA vor allem die Funktionalität SINA SOLID. Diese ermöglicht eine dynamische VPN-Vernetzung, die automatisch die Verbindung zwischen den einzelnen Netzknotenpunkten konfiguriert. SINA SOLID ist das Ergebnis einer Gemeinschaftsentwicklung und mehrfach prämierten Forschungsarbeit mit der TU Ilmenau. Zusätzlich wurde die sicherheitsgehärtete Cloud-Plattform SecuStack vorgestellt. SecuStack ermöglicht Unternehmen und Behörden mit sicherheitskritischen Anwendungen die Nutzung von Cloud Computing. Auf der Basis von OpenStack, dem Open-Source-Standard für Cloud-Plattformen, bietet SecuStack die aktuell weitreichendste Lösung zum Schutz und zur Kontrolle eigener Daten.

Zusätzlich zum Gemeinschaftsstand organisierte der deutsche IT-Sicherheitsverband TeleTrusT gemeinsam mit BSI, BMI und der deutsch-amerikanischen Handelskammer ein breites Rahmenprogramm, unter anderem mit dem sogenannten „German-American Security Forum“. Dr. Rainer Baumgart, Vorstandsvorsitzender der secunet, hielt dort eine Keynote mit dem Titel: “Where do we come from and where are we going? A short story about Quantum Computing”. Ebenfalls zum Programm gehörte ein Empfang im Generalkonsulat der Bundesrepublik Deutschland in San Francisco. Bei dieser Gelegenheit wurde Rainer Baumgart das vom BSI ausgestellte Deutsche IT-Sicherheitszertifikat für den secunet konnektor offiziell übergeben. Der secunet konnektor dient Leistungserbringern wie beispielsweise Arztpraxen als zentrales Element zum Anschluss an die Telematikinfrastruktur (TI) und steht seit dem erfolgreichen Abschluss des Zulassungsverfahrens bei der gematik Ende 2018 bereit für den Roll-out.

Ein weiteres Highlight außerhalb von Messe- und Konferenzhallen bot sich der secunet Delegation bei einem kleinen Abstecher vor die Tore der Stadt: beim Besuch des historischen Museums für Küstenfunk am Point Reyes in der Marconi RCA Wireless Station. Die Teilnehmer erlebten sehr anschaulich, wie die Schiffskommunikation auf dem Pazifik mit Landfunkstellen noch bis in die 1990er Jahre mittels Morsecode-Übertragung durchgeführt wurde.

Die Veranstaltung fand im Moscone Center in San Francisco statt.

LÄNDERDIALOG IT-SICHERHEIT 2019

Austausch über sichere Digitalisierung

Hartmut Beuß, CIO der Landesregierung Nordrhein-Westfalen (Mitte) mit Norbert Müller (links) und Torsten Henn von secunet beim LänderDIALOG IT-Sicherheit 2019

„Über den Tellerrand sehen“: Unter diesem Motto stand der diesjährige LänderDIALOG IT-Sicherheit, ein Forum für den Austausch über die sichere Digitalisierung in der Verwaltung auf Ebene der Bundesländer. secunet hatte die Veranstaltungsreihe im Jahr 2018 ins Leben gerufen. Nach dem Kick-off-Event in Frankfurt am Main fand die diesjährige Veranstaltung im Februar 2019 in der secunet Unternehmenszentrale in Essen statt.

Auf der Agenda standen vielfältige Themen. So referierte Hartmut Beuß, CIO der Landesregierung Nordrhein-Westfalen, über die Bedeutung von IT-Sicherheit für die Digitalisierung. Fabienne Tegeler vom Bundesamt für Sicherheit in der Informationstechnik (BSI) sprach über die Stärkung der Cybersicherheit durch Zusammenarbeit. Maren Janke-Baier vom Bayerischen Wirtschaftsministerium berichtete über den Einsatz von künstlicher Intelligenz zur kontinuierlichen Netzwerküberwachung. Das Unternehmen Materna stellte gemeinsam mit secunet den Einsatz der E-Akte für sensible Daten vor. Weitere spannende Vorträge zur Flüchtlingserfassung oder auch zum BSI-konformen Sprachanschluss rundeten das Programm ab.

Nach zwei erfolgreichen Veranstaltungen mit steigender Teilnehmerzahl plant secunet, den LänderDIALOG jährlich in wechselnden Bundesländern fortzuführen. Thematisiert werden sollen Inhalte aus der Verwaltung des jeweiligen Gastgeberlandes, aber auch Best Practices aus anderen Bundesländern. Der LänderDIALOG wird somit regelmäßig eine Gelegenheit für einen kritischen und direkten Austausch im Bereich IT-Sicherheit bieten.

Wenn Sie in einer Landesbehörde oder in der Verwaltung arbeiten und in Zukunft auch am LänderDIALOG teilnehmen möchten, registrieren Sie sich auf der folgenden Website: www.secunet.com/LaenderDIALOG

KENIAL

Spenden für bedürftige Jugendliche in aller Welt

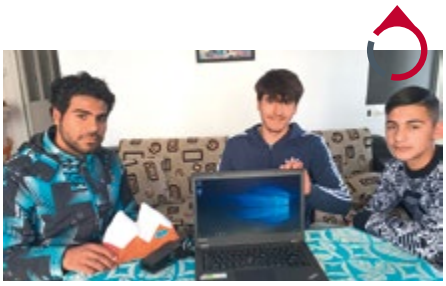
Gerade für Schulkinder und Jugendliche ist der Zugang zu Informationstechnologie wichtig, um damit an der allgegenwärtigen Digitalisierung teilhaben zu können. Leider ist dieser Zugang nicht immer vorhanden, insbesondere in weniger entwickelten Weltgegenden.

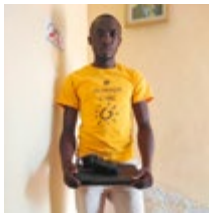
Der Verein KENIAL e. V. setzt mit seinen Projekten an diesem und vielen weiteren Problemen an: KENIAL organisiert gemeinsam mit Sportlern Kinderhilfsprojekte auf der ganzen Welt. Die beteiligten Sportler haben durch KENIAL die Chance, an die Länder, die sie für ihren Sport nutzen, etwas zurückzugeben.

Ende 2018 spendete secunet 25 Laptops an KENIAL. Die Geräte werden aktuell in diversen Einrichtungen wie einem Mutter-Kind-Heim in der Ukraine oder einem Kloster in Bhutan eingesetzt. Acht der 25 Laptops gingen an die NGO Untuzi Kwa Watoto in Nakuru, einer Stadt in Kenia. Dort wohnen mehr als 120 Waisenkinder vom Kindes- bis zum jungen Erwachsenenalter. Die Geräte werden von Schülern und Studenten genutzt, die dort aufgewachsen sind. Sie haben es selbstständig, ohne Eltern, geschafft, ihren Schulabschluss zu erreichen und blicken nun erwartungsvoll in die Zukunft. Nach Beendigung ihres Studiums werden die Laptops an die NGO zurückgegeben, um weitere Schüler und Studenten zu unterstützen.

Hier finden Interessierte mehr Informationen zu KENIAL: www.kenial.de

KENIAL nutzt die von secunet gespendeten Laptops für Hilfsprojekte in verschiedenen Ländern.





Spende an die DRK Kinderklinik in Siegen

Die Lebensqualität für Kinder verbessern – das ist das Ziel der DRK Kinderklinik in Siegen. Die Einrichtung des Deutschen Roten Kreuzes hat es sich zum Auftrag gemacht, Kinder, Jugendliche und junge Erwachsene therapeutisch, pflegerisch und medizinisch optimal zu versorgen. Jährlich behandelt die Klinik rund 6.200 Patienten stationär und über 62.000 Patienten ambulant – und das in durchgängig kinder- und familienfreundlicher Atmosphäre.

Zur Unterstützung dieser Einrichtung verzichtete der ehemalige Vorstandsvorsitzende von secunet, Dr. Rainer Baumgart, bei seinem Eintritt in den Ruhestand im Juni 2019 auf jegliche Abschiedsgeschenke. Er rief stattdessen dazu auf, an die Kinderklinik zu spenden. In diesem Rahmen konnten rund 8.800 Euro gesammelt werden, die Dr. Baumgart symbolisch übergab.

Dr. Stefan Schumann, Facharzt für Kinder- und Jugendmedizin – Arzt in der Abteilung Pädiatrie, und Dr. Rainer Baumgart nach der Spendenübergabe.

Termine – Oktober bis Dezember 2019

1. bis 2. Oktober 2019
IKT-Sicherheitskonferenz |
Fürstenfeld, Österreich

8. bis 10. Oktober 2019
it-sa | Nürnberg

15. bis 17. Oktober 2019
NIAS | Mons, Belgien

16. bis 17. Oktober 2019
ELIV | Bonn

22. bis 23. Oktober 2019
inova | Ilmenau

23. bis 24. Oktober 2019
AFCEA TechNet Europe |
Bratislava, Slowakei

28. bis 29. Oktober 2019
Digital-Gipfel | Dortmund

18. bis 21. November 2019
Defense & Security | Bangkok, Thailand

19. bis 22. November 2019
Milipol | Paris, Frankreich

22. November 2019
Automotive IT Security Workshop |
München

26. bis 27. November 2019
Berlin Security Conference | Berlin

2. Dezember 2019
Polizeitag | München

3. bis 4. Dezember 2019
StrategieTage IT & IT Security DACH |
Zürich, Schweiz

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

Design und Satz
sam waikiki, www.samwaikiki.de

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

Bildnachweis
Titel, S. 3, 11, 15, 21, 37, 39, 41, 42 unten: secunet
S. 2 oben rechts, S. 34: ifm Unternehmensgruppe
S. 2 unten links, S. 17: Bundesamt für Sicherheit in der Informationstechnik
S. 4, 5, 6: RheinEnergie AG
S. 7: Bayerisches Landesamt für Steuern
S. 8/9: iStock / baona
S. 18: Prof. Christoph Busch
S. 23, 24, 25: CLAAS KGaA mbh
S. 26, 28/29, 33: iStock
S. 40: Adobe Stock
S. 42 (außer ganz unten): KENIAL e.V.

SECUVIEW ABONNIEREN

Sie möchten secuview regelmäßig und kostenlos zugesendet bekommen? Wählen Sie zwischen der Print- und der E-Mail-Version.

Anmeldung:
www.secunet.com/secuview

Dort haben Sie auch die Möglichkeit, Ihr Abonnement zu ändern oder zu kündigen.

klimaneutral gedruckt
www.klima-druck.de
ID-Nr. 1983656
bvdm.

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

Damit Hersteller nicht plötzlich Malware produzieren.

secunet schützt Maschinen, Anlagen und kritische Netzwerke vor Cyberangriffen und Malware.

Wenn es darum geht, Maschinen und kritische Netzwerke zu schützen, steht secunet bereit. Mit unserem Portfolio aus sicheren Gateways, Quarantänesystemen und Echtzeitüberwachung isolieren wir kritische Netzwerke und verbinden sie gleichzeitig sicher mit Herstellern, Dienstleistern und Projektpartnern.

secunet – Ihr Partner für IT-Premiumsicherheit.

secunet