secuview
Das secunet Kundenmagazin
2|2019

100.000 MAL SINA WORKSTATION S

100.000 Mal modernes Arbeiten in der Verwaltung

Mit secustack zur sicheren Cloud

Wie Organisationen mit sehr strengen Sicherheitsanforderungen von Cloud Computing profitieren können

Telematik im Gesundheitswesen

Der Nächste, bitte: Nun sind die Krankenhäuser an der Reihe

9 Militärische Informationssicherheit auch unterwegs: Sicherer Fernzugriff in einer NATO-IT-Infrastruktur

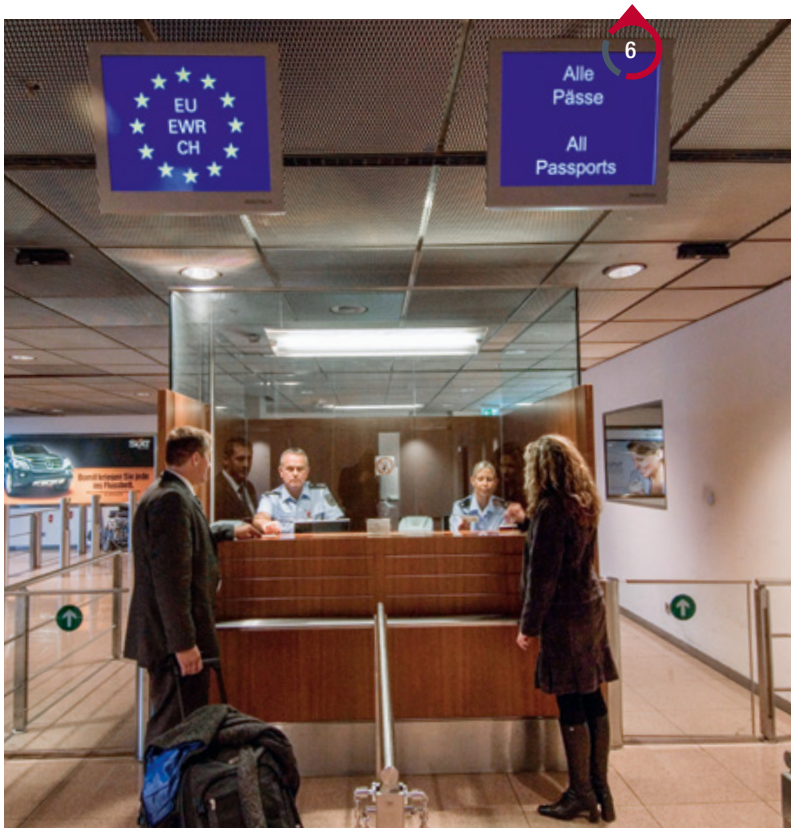
National

International

Wissenschaft

Technologien & Lösungen

Integrierte Grenzkontrollanwendung IGA 2.0 – Fit für die Grenzkontrolle der Zukunft



6

Kurz notiert

Service

Editorial

Liebe Leserinnen und Leser,

auch wenn das aktuelle Jahrzehnt streng genommen das Jahr 2020 einschließt: Wir stehen schon jetzt am Ende der umgangssprachlichen „Zehnerjahre“. Für die IT-Sicherheitsindustrie im Allgemeinen und secunet im Besonderen waren sie eine Zeit des Wandels und des Wachstums.

IT-Sicherheitstechnologie auf hohem Niveau, die ursprünglich für kleine, sehr spezielle Märkte konzipiert war, fand und findet weit darüber hinaus Verbreitung. Ein Beispiel: Vor rund zehn Jahren war der Vorläufer der späteren SINA Workstation S gerade vom Bundesamt für Sicherheit in der Informationstechnik zugelassen worden. Heute ist dieser Krypto-Client der Standard-Arbeitsplatz in zahlreichen Landes- und Bundesbehörden und hat mit seiner Mobilität und Flexibilität das Arbeiten in der Verwaltung modernisiert und digitalisiert. Im Titelthema zeichnen wir diese Entwicklung nach und zeigen, welche vielfältigen Einsatzmöglichkeiten die SINA Workstation in ihren unterschiedlichen Ausprägungen heute bietet.

Ein zweites Beispiel: Die secunet eID PKI Suite, unser Baukasten für Public-Key-Infrastrukturen und ein weiterer Eckpfeiler unseres Produktportfolios, hatte im Jahr 2010 gerade die secunet Entwicklungsabteilung verlassen. Lösungen auf Basis dieser Suite finden sich heute nicht nur in ihrem ursprünglichen Einsatzfeld der Biometrie und Identitätskontrolle, sondern auch in der Industrie oder der Energieversorgung.

Ein Ende dieser Entwicklung ist nicht in Sicht. Die fortschreitende Digitalisierung und Vernetzung erfordert es, immer mehr schützenswerte Bereiche von Staat, Wirtschaft und Gesellschaft mit hochwirksamer IT-Sicherheitstechnologie auszustatten. Öffentliche Verwaltung, Sicherheits- und Verteidigungsbehörden sind dabei schon weit vorangekommen. Immer wieder gibt es hier spannende neue Projekte, wie die Artikel über die sichere E-Akte oder über SINA Installationen in militärischen Hubschraubern zeigen.

Noch größer werden die Veränderungen in Sektoren ausfallen, die einiges aufzuholen haben. Dazu zählt vor allem die Industrie. Die Absicherung vernetzter Maschinen in Produktionsanlagen ist für die Betreiber eine große Herausforderung, für die heute schon Lösungen vorhanden sind. Mit der Gebäudeautomation umreißen wir in der aktuellen Ausgabe ein weiteres Thema mit viel Potenzial in puncto IT-Sicherheit.

Künstliche Intelligenz, 5G, autonomes Fahren – auch die Zwanzigerjahre werden von Themen mit IT-Sicherheitsbezug geprägt sein. Sie werden wohl nicht weniger spannend ausfallen.

Ich wünsche Ihnen viel Spaß beim Lesen. Kommen Sie gut ins Jahr 2020!

Ihr Axel Deininger

DIGITALISIERUNG IN DER VERWALTUNG

Endlich vereint: E-Akte und Verschlusssachen

Im Laufe der nächsten Jahre soll die Umstellung auf die E-Akte in den Ministerien und Behörden des Bundes abgeschlossen sein. Doch eine Herausforderung war bisher ungelöst: Gewöhnliche E-Akten und Verschlusssachen (VS) müssen bislang getrennt voneinander geführt werden. Das führt insbesondere dann zu Mehraufwänden und Medienbrüchen, wenn Informationen erst später in ihrem Lebenszyklus als VS eingestuft werden. Wie lässt sich diese Schwierigkeit vermeiden, ohne die Vertraulichkeit der eingestuften Informationen zu gefährden? Eine gemeinsame Lösung von Materna und secunet stellt die Interoperabilität von E-Akten und VS her und geht damit einen weiteren Schritt auf dem Weg zur Digitalisierung der Verwaltung.

Auch die öffentliche Verwaltung soll von den Potenzialen der Digitalisierung profitieren. Um das zu erreichen, wurde 2013 das E-Government-Gesetz erlassen. Dieses schreibt den meisten Bundesbehörden vor, ihre bisher papiergebundenen Akten auf elektronische Lösungen umzustellen – das Ziel ist die papierlose Verwaltung. Diese Umstellung ist bereits in vollem Gange: Zurzeit wird die sogenannte E-Akte Bund in mehreren Ministerien und Behörden in Pilotprojekten getestet. Vorreiter ist das Bundesamt für Justiz, das voraussichtlich bis Anfang 2020 die Umstellung weitgehend umgesetzt haben wird. In anderen Ministerien und Behörden wird sie im Laufe der nächsten Jahre, voraussichtlich bis 2024, erfolgen.

Die Länder sind auf einem ähnlichen Stand: Auch sie müssen die E-Akte einführen. NRW beispielsweise wird diesen Prozess mithilfe der Materna Information & Communications SE und der Ceyoniq Technology GmbH voraussichtlich 2022 abschließen.

Vertraulichkeit, Verfügbarkeit, Integrität

Noch mehr als in anderen Digitalisierungsprojekten spielt die Informationssicherheit bei der Einführung der E-Akte eine große Rolle: Erstens muss die Vertraulichkeit der darin enthaltenen Informationen sichergestellt werden, um den Schutz der persönlichen Daten von Bürgerinnen und Bürgern zu gewährleisten. Zweitens müssen die Inhalte stets verfügbar sein, um reibungslose Verwaltungsabläufe zu ermöglichen – schließlich soll die E-Akte ein wesentlicher Baustein einer effizienteren und bürgernäheren Verwaltung werden. Drittens ist die Integrität der E-Akte ganz wesentlich, um Verwaltungsvorgänge nachvollziehbar zu machen – hier geht es um nichts Geringeres als die Rechtsstaatlichkeit in deutschen Behörden.

Noch einmal zugespitzt werden diese Anforderungen in einem besonderen Bereich der Aktenführung: dem Umgang mit Verschlusssachen (VS). Informationen, deren Geheimhaltung im öffentlichen Interesse liegt, werden – je nach Schutzbedarf – in einen von vier Geheimhaltungsgraden eingestuft: VS-NUR FÜR DEN DIENSTGEBRAUCH, VS-VERTRAULICH, GEHEIM oder STRENG GEHEIM. Mitarbeiterinnen und Mitarbeitern von Behörden, die mit Verschlusssachen arbeiten, sind entsprechende Schutzgrade zugewiesen, die angeben, welche geheimen Dokumente sie einsehen dürfen. Dies wird auch als Security Clearance bezeichnet. Von VS-VERTRAULICH aufwärts müssen die Personen vor ihrer Autorisierung eine Sicherheitsüberprüfung durchlaufen. Und selbst dann, wenn eine Person für einen bestimmten Schutzgrad autorisiert ist, gilt noch der Grundsatz „Kenntnis nur, wenn nötig“: Zugriff wird nur gewährt, wenn dieser sachlich notwendig ist – und auch nicht früher und nicht in größerem Umfang als nötig. Zudem muss

Durch die gemeinsame Lösung von Materna und secunet können E-Akten zum Zeitpunkt ihrer VS-Einstufung in den gesicherten Kooperationsraum von SINA Workflow überführt werden.

juristisch belastbar und personenbezogen nachgewiesen werden können, wer wann welche eingestuften Daten eingesehen und bearbeitet hat. Festgelegt ist dies in der Verschlusssachenanweisung (VSA) des Bundes und den VSAen der Länder.

Standard für digitale Verschlusssachen

Grundsätzlich können VS heute durchgängig digital gespeichert, verarbeitet und übermittelt werden. Allerdings war dies bislang nur getrennt von der E-Akte möglich. Für den Umgang mit VS nutzen viele Bundes- und Landesbehörden die Sichere Inter-Netzwerk Architektur (SINA), die secunet im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI) entwickelt hat. Dabei kommen kryptographische Mechanismen zum Einsatz, die die Vertraulichkeit und Integrität der Daten jederzeit sicherstellen.

Bei der ebenfalls von der VSA geforderten Nachweisführung ist es allerdings noch immer eine gängige, aber sehr umständliche Praxis, auf Papierdokumente zurückzugreifen – oder auf Speziallösungen, die nicht mit der restlichen Infrastruktur verbunden sind. Um diesen Missstand zu beheben, entstand SINA Workflow. Die Lösung stellt sicher, dass jede Information im System juristisch belastbare Nachweise darüber enthält, welche Verarbeitungs- und Verwaltungsschritte damit ausgeführt wurden. SINA Workflow setzt auch das Prinzip „Kenntnis nur, wenn nötig“ digital um, indem sie Willensbekundungen der Nutzerinnen und Nutzer zur Kenntnisnahme bestimmter Informationen zweifelsfrei dokumentiert. Technisch realisiert wird SINA Workflow als Systemverbund aus sicheren Arbeitsplätzen sowie speziellen Servern mit integrierter elektronischer VS-Registratur und einem zentralen Netzwerkspeicher.

Das gesicherte Verteilungskonzept lässt sich auch behörden- und länderübergreifend anwenden. Verschiedene Sicherheitsbehörden zum Beispiel, die mit sensiblen Daten arbeiten, können sicher miteinander kooperieren. Die Zugriffsberechtigungen für die Bearbeitung eingestufter E-Akten werden durch SINA Workflow vorschriftenkonform umgesetzt.

Da allerdings bisher eine Schnittstelle zwischen SINA Workflow und den Systemen zur Bearbeitung gewöhnlicher, nicht eingestufter E-Akten fehlte, wurden die beiden Aktentypen getrennt geführt. Akten, die erst zu einem späteren Zeitpunkt in ihrem Lebenszyklus als VS eingestuft wurden, mussten dann neu angelegt werden.

Durch das E-Government-Gesetz gehören papiergebundene Akten in den meisten Bundesbehörden bald der Vergangenheit an. Doch im Hinblick auf eingestufte Dokumente müssen bei der Digitalisierung besondere Vorkehrungen getroffen werden.

Mehraufwände und Medienbrüche vermeiden

Nun haben Materna und secunet eine Lösung vorgestellt, mit der sich der Aufwand einer doppelten Dokumentenführung vermeiden lässt: SINA Workflow und die E-Akte nscale von Ceyoniq können mithilfe einer neuen Schnittstelle so integriert werden, dass ein reibungsloser Übergang einer normalen Verwaltungsakte in den eingestuften Status möglich ist.

Konkret läuft dies wie folgt ab: Eine elektronische Akte wird zu einem bestimmten Zeitpunkt als Verschlusssache eingestuft. Die neue Schnittstelle überführt sie in SINA Workflow und wendet dabei Standards für den elektronischen Austausch und die Aussonderung behördlichen Schriftguts wie XDOMEA an. Anschließend ist die eingestufte E-Akte in dem System für gewöhnliche E-Akten nicht mehr verfügbar. Sie liegt nur noch in den VS-Ablagen vor – verschlüsselt und vor unbefugtem Zugriff geschützt. Dabei gilt das Prinzip „Kenntnis nur, wenn nötig“. Der Umgang und die Weitergabe sind revisionssicher geregelt, sodass Nachverfolgung und Belegbarkeit gegeben sind. Die elektronischen VS-Dokumente können VSA-konform bearbeitet und beispielweise Mitzeichnungen unter Nutzung dieser Sicherheitsumgebung ausgeführt werden.

Behörden, die SINA Workflow einsetzen, können künftig bei der Bearbeitung von VS nicht nur durchgängig auf Papier verzichten und behörden- und länderübergreifend kooperieren. Sie profitieren auch davon, dass durch die Interoperabilität mit der E-Akte eine weitere Hürde bei der Digitalisierung der öffentlichen Verwaltung entfällt.

Norbert Müller
norbert.mueller@secunet.com

INTEGRIERTE GRENZKONTROLLANWENDUNG IGA 2.0

Fit für die Grenzkontrolle der Zukunft

Das internationale Reiseaufkommen wächst stetig, gleichzeitig steigern Terrorismus und organisierte Kriminalität die Erwartungen von Öffentlichkeit und Politik an die Qualität der Kontrollen an den Schengen-Außengrenzen. IT-Systeme können helfen, trotz umfangreicher regulatorischer Vorgaben, die Länge der Wartezeiten an den Grenzkontrollpunkten im Rahmen zu halten. Die Komplexität der IT-Systeme muss für die Beamten jedoch überschaubar bleiben, damit deren Unterstützung sich vorteilhaft auswirken kann. Ein wichtiger Schritt nach vorn ist hierbei die Integrierte Grenzkontrollanwendung (IGA) 2.0, die bereits an über 1.000 deutschen Grenzkontrollschaltern im Einsatz ist. Sie führt bisher getrennte IT-Systeme zusammen und liefert damit einen echten Effizienzgewinn.

Für Angehörige des Schengen-Raums ist das Überqueren der EU-Außengrenzen seit dem Jahr 2014 an den passagierstarken Flughäfen in Deutschland schneller und einfacher geworden: Mit dem Grenzkontrollsystem EasyPASS wird der Abgleich zwischen Person und elektronischem Identitätsdokument, konkret Reisepass oder Personalausweis, automatisiert. Reisende erledigen den Grenzkontrollprozess durch das Passieren von automatisierten Grenzkontrollschleusen – den secunet easygates – quasi in Eigenregie. Dies führt zu einer deutlich schnelleren Grenzkontrolle und kürzeren Wartezeiten.

Mehr Effizienz gefragt

Die manuelle Grenzkontrolle an den stationären Grenzkontrollschaltern blieb jedoch weiterhin aufwändig – und damit zeitintensiv für Beamte wie Reisende: Bei der Personenüberprüfung mussten die Beamten mehrere nicht miteinander vernetzte Zentralregister und Fahndungsdatenbanken manuell abfragen. Namen, Geburtsdaten und Dokumentennummern wurden in jedem System – von der Visa-Datenbank VIS bis zur Fahndungsdatenbank INPOL – einzeln abgefragt. Eine derartige Anwendungsvielfalt ist nicht nur unkomfortabel, sondern birgt grundsätzlich auch potenzielle Fehlerquellen.

Und bei aller schon bestehenden Komplexität sind weitere Anforderungen an die stationäre Grenzkontrolle bereits in Sichtweite: Bis 2022 wird – so der Beschluss des EU-Parlaments – in allen Mitgliedsstaaten das gemeinschaftliche biometrische Entry-/Exit-System (EES) der EU implementiert: Damit entfällt das bisherige Stempelverfahren für Reisende aus Drittstaaten und wird durch einen elektronischen Registereintrag ersetzt. Dazu werden die Reisenden direkt an der Schengen-Außengrenze mit vier Fingerabdrücken und einem Gesichtsbild digital erfasst. So kann später beispielsweise automatisiert kontrolliert werden, ob ein Reisender die Maximaldauer eines sogenannten Kurzaufenthaltes (90 Tage innerhalb von 180 Tagen) überschritten hat.

> Zum geplanten europäischen Entry-/Exit-System lesen Sie das Themenspecial in secuview 1/2019: www.secunet.com/secuview

Biometrie verpflichtend ab 2022

Mit der Einführung des Entry-/Exit-Systems müssen die Grenzkontrollbeamten zukünftig neben ihren originären Grenzkontrolltätigkeiten wie Dokumentenprüfung sowie Personenbefragung und -prüfung weitere Tätigkeiten übernehmen. Dazu gehört die biometrische Datenerfassung und -pflege gemäß der EES-Vorgaben. Ohne unterstützende Technik und nochmals optimierte Prozesse ist eine Bewältigung dieser Zusatzaufgaben nicht möglich – zumindest nicht ohne zeitliche Ausdehnung des vorhandenen Kontrollprozesses.

Einen ersten Aufschlag für ein unterstützendes System hatte die Bundespolizei bereits mit der in Eigenregie entwickelten Integrierten Grenzkontrollanwendung (IGA) 1.0 gemacht: Schon diese Anwendung führte alle zu dem Zeitpunkt relevanten Register und Datenbanken zusammen. Doch die Lösung ließ sich nicht oder nur umständlich um weitere

Grenzkontrollverfahren und Register erweitern, wie etwa das Entry-Exit-System, Datenbanken für Fluggastdatensätze (Passenger Name Records, PNR) oder andere polizeiliche Workflowsysteme wie Einsatzleitstellensysteme, Vorgangsverwaltungssysteme, Grenzkontrollakten, EasyPASS- oder Kiosksysteme.

IGA 2.0: Bindeglied zwischen verschiedenen IT-Systemen

Dies war der Startschuss für IGA 2.0. Die neue Anwendung musste nicht einmal von Grund auf neu entwickelt werden. Vielmehr stand mit secunet bocoa bereits eine Lösung als Baukasten zur Verfügung, mit der die Bundespolizei unter anderem im Bereich der mobilen Fahndung und in EES-Pilotprojekten bereits Erfahrungen gesammelt hatte.

IGA 2.0 führt die Ergebnisse der optischen und elektronischen Prüfung von Dokumenten, die Resultate der Hintergrundsysteme und die Analyse der biometrischen Daten geeignet zusammen und stellt sie für die Grenzkontrollbeamten übersichtlich dar. Relevante Abweichungen und Inkonsistenzen werden gefiltert und visualisiert, sodass die Beamtinnen und Beamten den Prüfvorgang auf einen Blick erfassen und bewerten können. Bei Bedarf können sie relevante Details genauer analysieren. Zudem müssen sie Daten nicht mehrfach, im Idealfall sogar überhaupt nicht mehr, manuell eingeben. Der Kontrollvorgang wird effizienter, da die Beamten sich auf die relevanteren Ausnahmefälle konzentrieren können.

Neben den aktuell bestehenden können auch zukünftig neu hinzukommende Systeme angebunden werden: so etwa das geplante EES und aktuell das Passagierdatensystem PNR.

Insgesamt dient IGA 2.0 als zentrales Bindeglied zwischen bestehenden IT-Systemen und den Grenzbeamten und sorgt darüber hinaus für einen reibungslosen Informationsfluss zwischen den involvierten Bundesbehörden – dies sind die Bundespolizei, das Bundesverwaltungsamt sowie das Bundesamt für Sicherheit in der Informationstechnik. Aktuell bewältigt die Lösung bis zu 185.000 manuelle Grenzkontrollen an deutschen Flughäfen – pro Tag.

Personal kann sich auf polizeiliche Fachaufgaben konzentrieren

Dank IGA werden Grenzkontrollbeamte von zeitintensiven Routinetätigkeiten befreit, wie der Bedienung verschiedenster dedizierter technischer Systeme und der manuellen Auswertung von Daten. Die gewonnene Zeit kann in Plausibilitäts- und Dokumentenprüfung investiert werden. Dies führt zu einem noch höheren Sicherheitsstandard.

Bei Einführung und Rollout spielte der menschliche Faktor eine wichtige Rolle: So evaluierte die Bundespolizei die Akzeptanz des Systems mittels interner Befragungen und Pilotierungsphasen. Die Ergebnisse flossen in die weitere Planungs- und Entwicklungsarbeit ein. Eine zentrale Rolle spielte auch das Design einer grafischen Nutzeroberfläche, die die Grenzkontrollbeamten in ihrer Arbeit optimal unterstützt. Auch hier wurden Anforderungen und Wünsche der Anwender berücksichtigt. Ende Oktober 2019 konnte der bundesweite Rollout abgeschlossen werden; seither trägt IGA 2.0 dazu bei, die Kontrollen an den EU-Außengrenzen zukunftssicher und effizient zu gestalten.

Eyck Warich
eyck.warich@secunet.com

IGA 2.0 befreit Grenzkontrollbeamte – so wie hier am Flughafen Hamburg – von zeitintensiven Routinetätigkeiten.

PKI BEI DER BUNDESAGENTUR FÜR ARBEIT

Vertrauen im Scheckkartenformat

Die Bundesagentur für Arbeit (BA), eine der größten Behörden Deutschlands, betreibt eine Public-Key-Infrastruktur (PKI) als Hintergrundlösung für die multifunktionalen Dienstkarten ihrer Mitarbeiterinnen und Mitarbeiter. secuview sprach mit Holger Scheetz, dem Leiter des Trustcenters der BA, welche Erfahrungen die Behörde damit gesammelt hat.

Herr Scheetz, wo ist das Trustcenter innerhalb der Organisationsstruktur der BA angesiedelt?

Das Trustcenter gehört zum Vertrauensdiensteanbieter (VDA) der BA, der eingebettet ist in das IT-Systemhaus. Dieser interne IT-Dienstleister der BA betreibt mit etwa 170.000 PC-Arbeitsplätzen eine der größten IT-Landschaften Deutschlands. Diese Arbeitsplätze gehören zur BA selbst sowie zu gemeinsamen Einrichtungen mit kommunalen Trägern, u. a. den Jobcentern.

Was ist die zentrale Aufgabe des Trustcenters?

Das Trustcenter ist für die Ausstellung und Verwaltung digitaler Zertifikate verantwortlich. Diese sind beispielsweise auf den Dienstkarten der BA aufgebracht. Mit diesen Dienstkarten authentisieren sich die Mitarbeiterinnen und Mitarbeiter unter anderem täglich an ihrem PC-Arbeitsplatz. Um die Zertifikate zu generieren und zu verteilen, betreiben wir im Trustcenter eine zentrale Public-Key-Infrastruktur (PKI). Diese Lösung besteht aus verschiedenen Komponenten wie z. B. einer Zertifizierungsstelle sowie Registrierungsstellen zur Beantragung und Ausgabe neuer Zertifikate und Dienstkarten. Diese werden regelmäßig hinsichtlich der Konformität gegenüber den Anforderungen der eIDAS-Verordnung auditiert. In Summe sorgt dies dafür, dass die in Nutzung befindlichen Zertifikate jederzeit vertrauenswürdig sind.

Was gab seinerzeit den Anstoß für die PKI-Lösung?

Die BA ist eine der größten Behörden Deutschlands. Sich den wachsenden und geänderten Anforderungen am Arbeitsmarkt anpassend, realisiert die BA zunehmend internetbasierte Anwendungen, eingebettet in die Ziele der BundOnline-Initiative. Bei vielen dieser Geschäftsprozesse werden Sozialdaten übermittelt. Um dem Schutzbedarf dieser Daten gerecht zu werden, mussten entsprechende IT-Sicherheitsmaßnahmen getroffen werden. Dieser Herausforderung wurde mit dem Einsatz kryptographischer Verfahren innerhalb einer intelligenten Lösung in Verbindung mit einer Smartcard gefolgt. Dies setzte den Aufbau einer PKI voraus.

Welche weiteren Funktionen bilden Sie über die PKI ab?

Mit den Dienstkarten können sich die Mitarbeiterinnen und Mitarbeiter nicht nur an den PC-Arbeitsplätzen anmelden, sondern mittels Single-Sign-On auch an Anwendungen. Die Mitarbeiterinnen und Mitarbeiter können mit ihren Dienstkarten außerdem Dokumente qualifiziert signieren sowie E-Mails ver- und entschlüsseln. Zusätzlich werden der Zutritt zu den Dienstgebäuden sowie die Arbeitszeiterfassung über die Dienstkarten geregelt. Die Lösung stellt also den Mitarbeiterinnen und Mitarbeitern der BA und der Jobcenter zentrale Sicherheitsfunktionen im Alltag zur Verfügung.

In der aktuellen Form kommt die PKI bereits seit 2014 zum Einsatz und wird seitdem immer wieder aktualisiert. Welche praktischen Erfahrungen haben Sie damit gesammelt?

Zunächst sind die Lösung und die durchgeführten Aktualisierungen für den Nutzer transparent und einfach anzuwenden – schon das hilft dabei, den Support- und Administrationsaufwand im Rahmen zu halten. Die aktuelle Lösung, die secunet vor fünf Jahren für uns erfolgreich konzipiert hat, ist modular aufgebaut und läuft stabil. Die bereitgestellten Schnittstellen gestatteten uns, einige Erweiterungen zu implementieren. Mit den Experten von secunet arbeiten wir inzwischen seit rund 15 Jahren konstruktiv zusammen.

Haben Sie aktuell Erweiterungen ins Auge gefasst?

Aufgrund der Laufzeit der Lösung stehen uns einige Produktaktualisierungen ins Haus. Derzeit nehmen wir außerdem gerade eine Überprüfung der Lösung hinsichtlich geänderter gesetzlicher und betrieblicher Anforderungen vor. Daraus wird sich sicher weiterer Handlungsbedarf für die Zukunft ergeben.

Holger Scheetz ist seit 2004 im IT-Systemhaus beschäftigt. Während dieser Zeit war er in vielen Bereichen der IT tätig, u. a. auch Mitglied der Projektgruppe, welche die PKI der BA aufgebaut hat. Seit September 2010 leitet er das Trustcenter und das zugehörige Betriebsteam.

IM INTERVIEW

Zentrale der Bundesagentur für Arbeit in Nürnberg

Eine Boeing E-3A (AWACS)
am NATO-Flugplatz Geilenkirchen

SICHERER FERNZUGRIFF IN EINER NATO-IT-INFRASTRUKTUR

Informationssicherheit auf militärischem Niveau – auch unterwegs

Am NATO-Flugplatz Geilenkirchen, Standort des Boeing E-3A Sentry Verbands – allgemein bekannt als AWACS-Flotte –, vertrauen die Mitarbeiter auf eine SINA Lösung, die einen Fernzugriff auf eingestufte Informationen erlaubt. secuview sprach mit Oberstleutnant Hans-Peter Kammer, dem Leiter der CIS Plans & Policy Branch (FHCP) der NATO NAEW&C (Airborne Early Warning & Control) Force.

Der NATO-Flugplatz Geilenkirchen ist der Hauptstützpunkt des NATO Boeing E-3A Sentry Verbands, einem der zwei operativen Elemente der NAEW&C-Flotte. Der Flugplatz liegt auf deutschem Territorium direkt an der deutsch-niederländischen Grenze. Ursprünglich war der Stützpunkt nach dem Zweiten Weltkrieg von der britischen Royal Air Force errichtet und betrieben worden, 1968 ging er an die Deutsche Luftwaffe. Im Jahr 1980 nahm die NATO am Flugplatz Geilenkirchen den Betrieb ihres E-3A Verbands auf. Heute sind hier rund 2.000 militärische und zivile Mitarbeiter aus 16 NATO-Mitgliedstaaten beschäftigt.

Die CIS Plans & Policy Branch (FHCP) ist verantwortlich für die Planung der strategischen Kommunikations- und Informationssysteme (CIS) der NAEW&C-Flotte sowie für Richtlinien und Beschaffungen zu deren Entwicklung und betriebsfähiger Bereitstellung.

Herr Oberstleutnant Kammer, welcher CIS-Herausforderung musste sich die NAEW&C-Flotte stellen?

Heutzutage leitet sich operativer Vorteil aus der Fähigkeit ab, einen ununterbrochenen Informationsfluss erheben, verarbeiten und verbreiten zu können. Im Jahr 2018 waren wir auf der Suche nach einer Lösung für einen sicheren Fernzugriff, um einen solchen Informationsfluss auf der Ebene der Geheimhaltungsstufe NATO RESTRICTED zu ermöglichen, und legten eine entsprechende Bedarfserklärung vor. Sie zielte darauf ab, Mitarbeitern unterwegs – hauptsächlich im Einsatz oder auf Dienstreisen – den Zugriff auf verschiedene Netzwerkressourcen und -dienste wie Einsatzplanungstools und -daten, die PILS-Anwendung (Programme Integrated Logistics System) und andere missionswichtige Informationen zu erlauben.

Rund 2.000 militärische und zivile Mitarbeiter aus 16 NATO-Mitgliedsstaaten sind am NATO-Flugplatz Geilenkirchen beschäftigt.

Welche Art von System hatten Sie im Blick?
Alles in allem sollte das neue System Benutzern den sicheren Zugriff auf das NATO RESTRICTED-Netzwerk ermöglichen, wenn sie sich physisch außerhalb ihrer jeweiligen NATO-Umgebung befinden. Konkret musste das System ein sicheres, verschlüsseltes Virtual Private Network (VPN) zur Übertragung von Daten der Geheimhaltungsstufe NATO RESTRICTED über ein nicht eingestuftes Netzwerk bereitstellen. Zudem wünschten wir uns moderne Multi-Domain-, Multi-Tenancy-Arbeitsplätze und Mechanismen zur sicheren Zugriffskontrolle, einschließlich Nutzer-Tokens. Weiterhin sollte die Infrastruktur unseren Systemadministratoren umfassende Verwaltungsfunktionen für die Clients bieten, eine Lösung zur Zuweisung und Neuzuweisung von Nutzer-Tokens bereitstellen sowie die Möglichkeit geben, die installierte Basis regelmäßig zu aktualisieren und aufzurüsten.

Das gewünschte System sollte außerdem gemäß den NATO-Sicherheitsbestimmungen und -richtlinien akkreditiert, zur Nutzung in Zusammenhang mit der Geheimhaltungsstufe NATO RESTRICTED zugelassen und im NATO Information Assurance Product Catalogue (NIAPC) gelistet sein, um Compliance zu gewährleisten.

Darüber hinaus sollte die Lösung unterschiedliche Nutzertypen unterstützen: So gibt es Nutzer auf oberster Führungsebene in der NAEW&CF-Zentrale, Nutzer innerhalb des NAEW&CF E-3A Verbands, darunter Logistik- und technische Supportmitarbeiter und aktive Einsatzkräfte, sowie sonstige Mitarbeiter, die von Zeit zu Zeit Dienstreisen unternehmen müssen, zudem Mitarbeiter im MSEC (Mission Systems Engineering Centre).

Für welche Lösung haben Sie sich letztendlich entschieden?
Im Februar 2019 entschieden wir uns für eine SINA Lösung (Sichere Inter-Netzwerk Architektur) für den sicheren Fernzugriff. Diese bewährte Multi-Domain-, Multi-Tenancy-Lösung wurde von secunet im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI) entwickelt. Unser System beinhaltet 30 SINA Workstations S (Krypto-Clients im Laptop-Format), ein Backend aus SINA L3 Boxen S (IPsec-gesicherte VPN-Gateways) und eine dazugehörige SINA Management-Lösung.

Welche Gründe sprachen für die SINA Lösung?
Auf der SINA Workstation laufen sogenannte Gastsysteme wie Windows und die zugehörigen Anwendungen in einer virtualisierten Umgebung. Der parallele Betrieb verschiedener isolierter Gastsysteme, die auch unterschiedlichen Sicherheitsdomänen zugewiesen werden können, macht es zum Beispiel möglich, mit einem Gastsystem im internen Sicherheitsnetzwerk zu arbeiten und gleichzeitig mit einem anderen System im Internet zu surfen – ohne dabei zu riskieren, dass das eigene Netzwerk durch Schadsoftware kompromittiert wird.

Der Zugriff auf verbundene Geräte und Schnittstellen, die von einem Gastsystem erkannt werden, erfolgt unter der Kontrolle des gesicherten SINA Betriebssystems. Jeder Festplattenzugriff und sämtliche Netzwerkverbindungen werden von SINA automatisch verschlüsselt. Die Nutzer können auf die verschlüsselten Daten nur mit einem PIN-geschützten SINA ID-Token zugreifen, welches die Konfigurationsdaten und Sicherheitsbeziehungen für die SINA Workstation enthält. Gleichzeitig dient es als sicherer Speicher für kryptographische Schlüssel und Zertifikate.

Als VPN-Gateway bildet die SINA L3 Box eine wichtige Komponente der zentralen IT-Infrastruktur. Der Datenaustausch zwischen den SINA Komponenten wird über verschlüsselte VPN-Tunnel sicher übertragen.

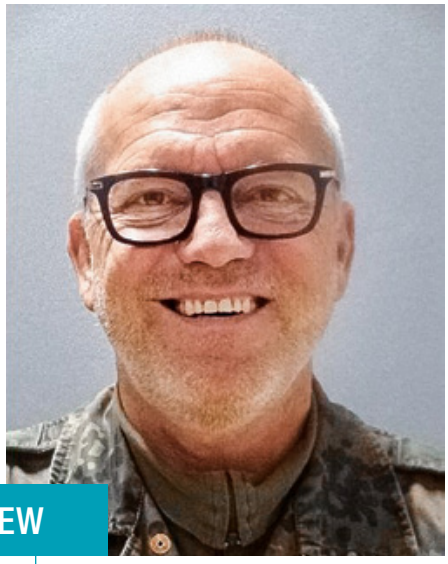
Auf zentraler Ebene wird das SINA Management zur Systemadministration, Remote-Konfiguration und Aktualisierung der SINA-Software auf allen SINA L3 Boxen im Netzwerk verwendet. Die Konfigurationsupdates beinhalten Netzwerkkonfigurationen und Sicherheitsbeziehungen. Eine integrierte Public-Key-Infrastruktur (PKI) mit zugehöriger Nutzerverwaltung unterstützt kritische Administrationsprozesse hinsichtlich der Smartcards der SINA L3 Boxen. Dies umfasst insbesondere die Personalisierung, die Erstellung und Aktualisierung von Schlüsseln und kryptographischen Parametern sowie die Verwaltung der zugehörigen PINs und PUKs.

Ein SINA Administrator kann Rechte vergeben oder entziehen sowie die Konfigurationseinstellungen aus der Ferne ändern.

Welche nächsten Schritte sind geplant?

In Anbetracht der erfolgreichen Einführung und Nutzung der SINA Lösung am NATO-Flugplatz im Jahr 2019 plant die NAEW&C-Force, im Jahr 2020 eine zweite Phase zu starten und die Lösung für den sicheren Fernzugriff auf mehr Personal sowohl inner- als auch außerhalb des Standorts auszuweiten.

Jerome Kühnert
jerome.kuehnert@international.secunet.com



IM INTERVIEW

Lt Col Hans-Peter Kammer
Head CIS Plans & Policy Branch, NATO Airborne Early Warning & Control Force

Oberstleutnant Hans-Peter Kammer wurde am 13. Mai 1961 in Würselen nahe Aachen geboren. Nach seinem Schulabschluss 1981 trat er als Rekrut der Deutschen Bundeswehr bei. Im Jahr 1982 startete er seine Laufbahn als Unteroffizier und Zugführer einer in Köln stationierten Funkstaffel. 1991 begann er ein Studium der Elektrotechnik und wurde 1994 als Offizier in Dienst gestellt. Seit 1999 dient er als Mitglied der NAEW&C-Flotte in verschiedenen Positionen. Oberstleutnant Kammer ist verheiratet und Vater von zwei erwachsenen Kindern.

Eine in Geilenkirchen stationierte Boeing E-3A, bekannt als AWACS, in der Luft

SOFTWARE INNOVATION CAMPUS PADERBORN

„Wir erforschen Software-Innovationen der Zukunft“

secunet ist seit März 2019 Mitglied des Software Innovation Campus Paderborn, kurz SICP. An der Universität Paderborn ist durch eine Kooperation zwischen Wissenschaft und Wirtschaft ein Ort der Forschung und Innovation, des Wissenstransfers und der Personalentwicklung entstanden.

Der Software Innovation Campus Paderborn (SICP) ist ein interdisziplinärer Forschungs- und Innovationsverbund, in dem Unternehmen und Wissenschaft digitale Innovationen gemeinsam erforschen und umsetzen. Dabei entwickelt der SICP Lösungen für völlig neuartige Herausforderungen in der digitalen Gesellschaft, setzt aber auch anwendungsnahe Konzepte und Systeme effizient, sicher und skalierbar um. „Mit dem Neubau der Zukunftsmeile 2 an der Fürstenallee in Paderborn, in direkter Nachbarschaft zum Fraunhofer-Institut für Entwurfstechnik Mechatronik IEM und dem Heinz Nixdorf Institut der Universität Paderborn, realisieren wir einen Forschungscampus, auf dem wir digitale Innovationen durch eine enge Vernetzung von Wissenschaft und Unternehmen besonders effektiv und agil entwickeln werden“, erläutert Dr. Stefan Sauer, Geschäftsführer des SICP und Manager des Kompetenzbereichs Software Engineering. „Die enge Zusammenarbeit zwischen Wirtschaft und Wissenschaft verstehen wir als wesentlichen Erfolgsfaktor bei der Überführung von Forschungsergebnissen in marktfähige Innovationen“, ergänzt Sauer.

Digitale Innovationen als Produkt interdisziplinärer Kooperationen

Das SICP vereint fünf Kompetenzbereiche: Cyber-Physical Systems, Digital Business, Digital Security, Smart Systems und Software Engineering. Hier entwickeln ca. 30 Arbeitsgruppen der Fakultäten für Elektrotechnik, Informatik und Mathematik, Wirtschaftswissenschaften und Kulturwissenschaften der Universität Paderborn fachgebietsübergreifend neue Konzepte, Methoden, Technologien und Tools. Die Themen reichen von großen verteilten und intelligenten Systemen und sicherer drahtloser Kommunikation über agile und menschenzentrierte Entwicklung interaktiver und sozio-technischer Systeme bis hin zu digitalen Geschäftsmodellen, datengetriebenen Entscheidungen, intelligentem Kundenmanagement und adaptiven Geschäftsprozessen. „Dabei betrachten wir digitale Innovationen immer als eine enge Verzahnung von Organisation und IT: Digitale Transformation kann nur erfolgreich sein, wenn wir Software und Systeme ausgehend vom Anwendungskontext entwickeln, organisationale Strukturen erfolgreich transformieren und Menschen zur Schaffung und Nutzung digitaler Innovationen befähigen“, erläutert Christoph Plass, Sprecher des SICP.

Der SICP-Steuerkreis (v. l. n. r.): Holger Funke (secunet Security Networks AG), Josef Tillmann (S&N Invent GmbH), Christoph Plass (UNITY AG), Prof. Dr. Gregor Engels (Universität Paderborn), Dr. Stefan Sauer (Universität Paderborn), Jörg Wehling (Atos Information Technology GmbH), Prof. Dr. Holger Karl (Universität Paderborn)

„Digital Security“ im SICP

Im Zeitalter der digitalen Transformation, von Industrie 4.0 und Internet of Things ist gerade der Sicherheitsaspekt eine der zentralen Herausforderungen unserer modernen Informationsgesellschaft. „Wir erforschen daher in unserem Kompetenzbereich Methoden, wie Sicherheit bereits in den Entwurf stärker integriert und über den gesamten Lebenszyklus gewährleistet werden kann. Unser Ziel ist es, das Thema „Digital Security“ verständlich, nachhaltig und beweisbar zu gestalten“, so Prof. Dr. Eric Bodden, Direktor des Kompetenzbereichs „Digital Security“.

Es werden zunehmend verteilte Systeme genutzt, z. B. im Cloud Computing oder in serviceorientierten bzw. Microservice-Architekturen. Das damit verbundene verteilte Rechnen und das Speichern von Daten in virtuellen Umgebungen erfordert auf der einen Seite mehr Datenkommunikation, auf der anderen Seite das Nutzen externer Anbieter. „In dieser Ausgangslage, dem Einsatz komplexer Systeme und der ständigen Konnektivität, können leicht Sicherheitslücken entstehen. Grundziele der IT-Sicherheit sind für uns daher das Aufrechterhalten der Informationssicherheit und der Schutz der Persönlichkeitsrechte“, erläutert Dr. Simon Oberthür, Manager des Kompetenzbereichs und Wissenschaftler an der Universität Paderborn. Hierfür werden am SICP unter anderem sichere IT-Architekturen, fortschrittliche kryptographische Verfahren und digitale Identitäten erforscht und gemeinsam Lösungen entwickelt. Unterstützt werden diese Themen durch die disziplinübergreifende Expertise in Themen wie agile und hybride Softwareentwicklungsmethoden, statische und dynamische Programmanalyse oder Softwarequalitätssicherung und Testen.

secunet ist Mitglied des SICP

Seit März 2019 ist die secunet Security Networks AG Mitglied des SICP und ergänzt, als einer der führenden Anbieter von IT-Sicherheit für Unternehmen und Behörden, im Besonderen den SICP-Kompetenzbereich „Digital Security“. „Wir freuen uns, mit secunet einen überaus kompetenten Partner an unserer Seite zu haben, der uns darüber hinaus beim Paderborner Tag der IT-Sicherheit, den wir seit 14 Jahren veranstalten, regelmäßig unterstützt“, so Dr. Simon Oberthür. „Mit seiner Vielzahl an Expertinnen und Experten, seinem hohen Maß an Fach- und Methodenkompetenz sowie einer großen Bandbreite an innovativen Ideen ist der SICP für uns ein ideales Forum für Austausch und Diskussion“, so Holger Funke, Principal bei der secunet Security Networks AG. Dabei baut die Mitgliedschaft auf eine schon länger existierende vertrauensvolle Beziehung und gemeinsame Aktivitäten und Projektvorhaben auf, u. a. für das Bundesamt für Sicherheit in der Informationstechnik (BSI). Ziel der SICP-Mitgliedschaft ist es, diese Beziehung weiter auszubauen, gemeinsame Projekte, Bachelor- und Masterarbeiten durchzuführen sowie hervorragend ausgebildete Studierende und Absolventen für secunet zu gewinnen.

Weitere Informationen finden Interessierte unter www.sicp.de.

Dr. Stefan Sauer, SICP
sauer@sicp.de

Holger Funke, secunet
holger.funke@secunet.com

Zukunftsmeile 2: In diesem Neubau wird der SICP ab dem nächsten Jahr untergebracht sein.
Simulation (c) Matern Architekten, Goldbeck GmbH

100.000 AUSGELIEFERTE SINA WORKSTATIONS S

100.000 Mal modernes Arbeiten in der Verwaltung

Die digitale Transformation macht auch vor Verschlusssachen und anderen sensiblen Dokumenten nicht halt. Daher entwickelte secunet im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI) eine Lösung, die die erforderliche Sicherheit bietet und gleichzeitig nutzerfreundlich ist: die SINA Workstation. Der ursprünglich als Speziallösung für besondere Einsatzzwecke konzipierte Krypto-Client hat sich mittlerweile als Standard-PC in der öffentlichen Verwaltung etabliert und ermöglicht dort ein modernes mobiles Arbeiten. Im Herbst 2019 konnte secunet einen Meilenstein vermelden. Doch die Erfolgsgeschichte geht weiter: Die Lösung wird ständig weiterentwickelt, neue Nutzeranforderungen und Technologien werden integriert.

„Die Sichere Inter-Netzwerk Architektur SINA ist ein Beispiel für eine erfolgreiche Public-Private-Partnership", so BSI-Präsident Arne Schönbohm im Oktober 2019 auf der weltgrößten Messe für IT-Sicherheit, der it-sa in Nürnberg. Axel Deininger, Vorstandsvorsitzender von secunet, traf Schönbohm aus erfreulichem Anlass: 100.000 ausgelieferte SINA Workstations S. Die Krypto-Clients sichern Arbeitsplätze in zahlreichen Behörden in Deutschland und Europa ab, unter anderem in mehreren Bundesministerien. Durch ihre Mobilität und Flexibilität haben sie das Arbeiten in Behörden, in denen der Umgang mit sensiblen oder eingestuften Dokumenten zum Alltag gehört, revolutioniert. Deren Mitarbeiter können heute trotz der hohen Sicherheitsanforderungen genauso selbstverständlich im Home Office oder unterwegs ihre Aufgaben erledigen wie das in Unternehmen der Fall ist. Das Stichwort lautet „New Work". Dabei ist die Sicherheit der sensiblen Informationen jederzeit gewährleistet. Und die Entwicklung geht weiter: „Wir werden SINA kontinuierlich an neue Nutzerbedürfnisse und Anwendungsszenarien anpassen", sagt Deininger.

SINA: Eine sichere Umgebung, vielfältige Hardware

Das Lösungsportfolio von SINA ist vielschichtig und bietet für unterschiedliche Anforderungen immer das richtige Produkt. Im Kern baut SINA mit hochentwickelter Verschlüsselungstechnologie eine sichere Umgebung auf, die dazu dient, sensible Informationen und Verschlusssachen (VS) über potenziell unsichere Netze wie das Internet zu übermitteln. Dabei kommen IPsec-gesicherte Virtual Private Networks (VPN) zum Einsatz.

Die SINA Workstation fungiert in diesen sicheren Netzwerken als Client. Sie bietet den Vorteil, dass mehrere gegeneinander abgeschottete Gastsysteme unterschiedlicher Sicherheitseinstufungen parallel auf einem Gerät betrieben werden können. Dies wird durch Virtualisierungstechnologie erreicht. Die Anwender bewegen sich einfach per Mausklick zwischen den Gastsystemen hin und her, ohne verschiedene Geräte für unterschiedliche Sicherheitslevels einsetzen zu müssen. Sie können beispielsweise in einem VS-Netz arbeiten und gleichzeitig im unsicheren Internet surfen. Zudem haben sie jederzeit Zugriff auf ihre vertraute Arbeitsumgebung (z. B. MS Windows), ohne die Sicherheit der Daten in den VS-Netzen, in denen sie parallel arbeiten, zu gefährden. Zwei-Faktor-Authentisierung und Festplattenverschlüsselung verhindern, dass Unbefugte Zugriff auf die sensiblen Daten erlangen.

Verschlusssachen von VS-NfD bis GEHEIM

So wie auch andere SINA Komponenten ist die SINA Workstation in verschiedenen Basisvarianten für unterschiedliche Sicherheitsanforderungen verfügbar: Grundsätzlich ist die SINA Workstation S (für „Standard") bis zur Geheimhaltungsstufe VS-NfD (NUR FÜR DEN DIENSTGEBRAUCH) zugelassen, die SINA Workstation E („erweitert") bis VS-VERTRAULICH und die SINA Workstation H („hoch") bis GEHEIM. Entsprechend der in verschiedenen Behörden und Institutionen vorherrschenden Sicherheitsanforderungen kommt die SINA Workstation S schwerpunktmäßig in der öffentlichen Verwaltung zum Einsatz, während die SINA Workstation H unter anderem in militärischen Kontexten eingesetzt wird. So hat sich Letztere etwa als Standard-Client im Rahmen des Bundeswehr-Programms HaFIS (Harmonisierung der Führungsinformationssysteme) etabliert.

Daneben ist die SINA Workstation in verschiedenen Formfaktoren erhältlich, etwa als Desktop, Laptop oder Tablet. Eine ganz eigene Kategorie ist das SINA Terminal. Dieser Thin Client zeigt lediglich grafische Daten an und gibt Audiosignale aus, außerdem nimmt er Maus- und Tastatureingaben entgegen. Die eigentliche VS-Bearbeitung erfolgt auf entfernten Terminal-Servern.

Die SINA Workstations E und H sind zudem als besonders robuste Varianten verfügbar, die

unter schwierigen physischen Bedingungen zuverlässig einsatzfähig bleiben: Sie sind widerstandsfähig gegenüber Hitze, Kälte, Staub, Erschütterung und Feuchtigkeit.

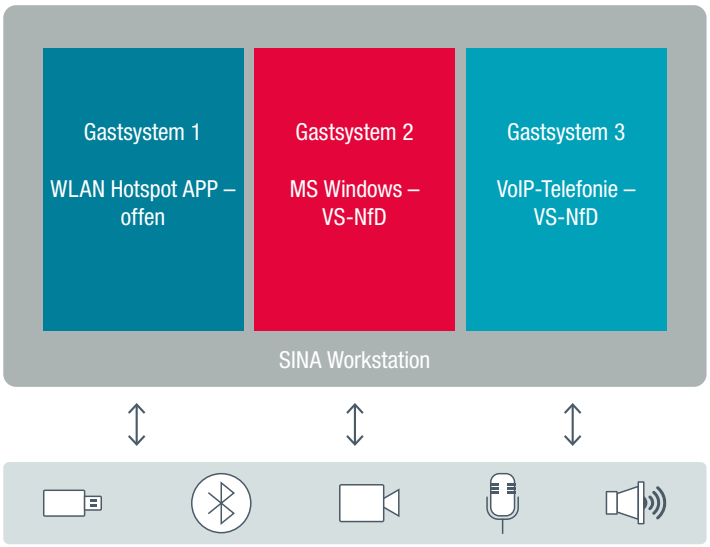
Virtualisierung: An vorderster Front der technologischen Entwicklung

Ursprünglich entstand die Projektidee für SINA aus der Forderung nach sicherer Kommunikation im Rahmen des Umzugs des größten Teils der Bundesregierung von Bonn nach Berlin. In diesem Zusammenhang wurde der Informationsverbund Berlin-Bonn (IVBB) eingerichtet, der die obersten Bundesbehörden vernetzt. Darüber hinaus bestand genereller Bedarf nach einer für den Geheimschutz geeigneten Verschlüsselung auf Internet-Protokoll-Ebene und damit einer Einsatzperspektive für sichere Kommunikation über Weitverkehrsnetze. Das BSI erstellte deshalb Ende der 1990er Jahre ein Grobkonzept für SINA. Im Dezember 1999 wurde die secunet Security Networks AG vom BSI beauftragt, die SINA Produktlinie zu entwickeln.

Zunächst, Anfang der 2000er Jahre, stellte man sichere VPN-Netze mit SINA L3 Boxen als VPN-Gateways her und schloss PCs daran an. Der nächste Schritt waren die SINA Terminals, die eine SINA L3 Box und eine Darstellungskomponente verknüpften. Mit zunehmender Verbreitung von SINA wünschten sich allerdings viele Nutzer vollständige PCs (Fat Clients), mit denen sie direkt in ihren gewohnten Windows-Umgebungen arbeiten können. secunet experimentierte daraufhin mit Virtualisierungstechnologien und entwickelte schließlich gemeinsam mit dem BSI das Konzept für die SINA Workstation. Den Durchbruch brachte eine Virtualisierungslösung des Herstellers InnoTek, die von secunet für SINA stark angepasst und weiterentwickelt wurde – und immer noch weiterentwickelt wird. InnoTek ging später an den Technologieanbieter Sun Microsystems, der dann wiederum von dem Hard- und Softwarekonzern Oracle übernommen wurde. Die Virtualisierungslösung wird unter dem Namen VirtualBox vermarktet.

› Das Erfolgsprinzip der SINA Workstation beruht auf Client-Virtualisierung. Diese Technologie treibt secunet mit der SINA Workstation maßgeblich voran, so wie Cloud Computing die Server-Virtualisierung vorantreibt. ‹

Armin Wappenschmidt, Leiter Abteilung Network & Client Security, Division Öffentliche Auftraggeber, secunet



Auf dem Weg zum Behördenstandard

Als die SINA Workstation aus der Taufe gehoben wurde, rechnete man noch mit einer Nachfrage von etwa 1.500 Arbeitsplätzen. Heute steht fest, dass sich der Markt etwas anders entwickelt hat als vorhergesagt. Mit 100.000 Installationen allein der SINA Workstation S ist die Produktfamilie zum behördlichen Standard geworden.

Ein Meilenstein auf diesem Weg war Mitte der 2010er Jahre die Vollausstattung mehrerer Bundesministerien mit SINA Workstations. Damit stellten sich wieder ganz neue Herausforderungen: Bisher stand die Sicherheit allein im Fokus, jetzt stellte sich zusätzlich die Frage, wie ein Massen-Rollout und die Administration sehr großer SINA Installationen ohne exzessiven Aufwand gelingen konnten. Die Antwort lag in der Automatisierung: Die neuen Herausforderungen wurden mit dem SINA Install Server und dem SINA Remote Admin Server angegangen. Mit deren erfolgreicher Anwendung war bewiesen, dass sich SINA für den massenhaften Rollout eignet.

Nutzer fordern vielfältige Anwendungen

Die SINA Workstation verbreitete sich recht schnell in der Behördenlandschaft Deutschlands, und so stiegen bald auch die Anforderungen der Nutzer. Diese erwarteten, dass immer mehr derjenigen Anwendungen, auf die sie im Büroalltag angewiesen waren, auch in der SINA Workstation abgebildet sein sollten: von der Anbindung von Druckern und Scannern über die USB-Unterstützung von Headsets für Audiokonferenzen bis hin zur Videotelefonie mit Skype for Business.

Anlässlich 100.000 ausgelieferter SINA Workstations S trafen sich Vertreter von BSI und secunet auf der it-sa 2019. V. l. n. r.: Dr. Günther Welsch, Arne Schönbohm (beide BSI), Axel Deininger (secunet), Dr. Gerhard Schabhüser (BSI), Dr. Kai Martius (secunet)

Die SINA Workstation ist in verschiedenen Formfaktoren erhältlich – im Bild eine Version im mobilen Laptop-Format.

Die Umsetzung dieser Anforderungen in der sicheren, virtualisierten SINA-Umgebung war oft herausfordernd, wurde aber immer wieder gemeistert.

Ein weiteres Beispiel: Seit 2015 ist SINA mit der biometrischen Middleware secunet biomiddle kompatibel. Dies ermöglicht es Fachleuten – beispielsweise bei der Grenzkontrolle – Biometrie-Hardware wie Passleser und Fingerabdruckscanner anzuschließen. Die SINA Workstation kommt so auch bei der mobilen Identitätskontrolle und der Registrierung von Personen erfolgreich zum Einsatz.

Mit den SINA Apps steht Nutzern der SINA Workstation eine Reihe von Software-Anwendungen zur Verfügung, die ursprünglich auf Wunsch einzelner Kunden hin entwickelt wurden. Diese Anwendungen können als separate Gastsysteme gestartet werden und erfüllen festgelegte Aufgaben. Ein Beispiel ist die SINA WLAN-Hotspot App. Damit können Nutzer auch an unsicheren öffentlichen Hotspots ihre sichere VPN-Verbindung aufbauen.

Komfortabel und sicher ins Netz

Oben auf der Wunschliste vieler Büro-IT-Anwender steht eine komfortable und möglichst wenig eingeschränkte Internetnutzung. Doch ein ungesicherter Internetzugang stellt eines der größten Einfallstore für Schadsoftware dar, die nicht nur das Zielsystem beeinträchtigen, sondern auch die Vertraulichkeit von Daten gefährden kann. Daher mussten viele behördliche Nutzer früher zu einem separaten PC-Arbeitsplatz wechseln, wenn sie im Internet recherchieren wollten. Andere, komfortablere Lösungen waren unter Sicherheitsaspekten stets nur ein Kompromiss.

Die SINA Workstation eröffnet hier einen eleganten Ausweg: Sie stellt eine Variante der Lösung secunet safe surfer bereit, die auf der ReCoBS (Remote Controlled Browser System)-Architektur des BSI beruht. Dabei wird der Internetbrowser nicht auf dem schützenswerten, lokalen Windows-System selbst ausgeführt, sondern in einem Quarantäne-System, das außerhalb des sensiblen Netzwerkbereichs implementiert ist – im Falle der SINA Workstation als ein weiteres virtualisiertes Gastsystem. Der Nutzer steuert den Browser innerhalb seines Windows-Arbeitsplatzes gewissermaßen fern und kann auf diese Weise mit sensiblen Daten oder kritischen Netzen arbeiten und zeitgleich auf das Internet zugreifen – ohne die bisherigen Einschränkungen. Über eine Datenschleuse sind sogar Funktionen wie Downloads und Uploads sowie eine Druckeranbindung komfortabel verfügbar.

Zusätzliche Sicherheit bietet die Möglichkeit, individuelle Windows-Anwendungen in eigenen virtualisierten Umgebungen zu starten, aus denen potenzieller Schadcode nicht ausbrechen kann. Auf diesem Prinzip beruhen spezielle Partnerlösungen wie Bromium Secure Platform, die in die SINA Workstation integriert werden können. So wird der bewährte äußere Schutz der SINA Umgebung durch einen weiteren, inneren Schutz für Windows-Anwendungen ergänzt.

Die Zukunft: klein, mobil, intuitiv

Durch die zunehmende Verbreitung der SINA Workstation kommen immer wieder neue Nutzerkreise mit ihr in Berührung. Auch aus diesem Grund geht die Entwicklung von SINA in Richtung einfacher, intuitiver Oberflächen, die spezielle Schulungen für SINA Nutzer unnötig machen. So ist etwa zurzeit eine neue grafische Benutzeroberfläche in Arbeit, die die Nutzererfahrung weiter verbessern wird. Auch der Aspekt der Barrierefreiheit steht dabei auf der Agenda.

Neben der einfachen Bedienbarkeit der SINA Workstation steht die mobile Nutzung im Fokus der Anwender. Tablet-Lösungen sind bereits verfügbar, weitere mobile Formfaktoren werden folgen.

Wie sieht also die Zukunft der SINA Workstation aus? Der alte Widerspruch zwischen Sicherheit und Komfort wird zunehmend aufgelöst. Das Ziel ist ein Krypto-Client, der sich kaum noch von herkömmlichen Anwendersystemen unterscheiden lässt, aber weiterhin hohen bis höchsten Sicherheitsanforderungen genügt.

Armin Wappenschmidt
armin.wappenschmidt@secunet.com

VERSCHLÜSSELTE VIDEOKOMMUNIKATION NICHT NUR MIT HUBSCHRAUBERN

Exklusive Liveübertragung aus mehreren Kilometern Höhe

Digitale Kommunikation hat in großem Stil Einzug in militärische Infrastrukturen gehalten. Dabei wurden die Anforderungen immer anspruchsvoller: Luftgestützte Plattformen wie Hubschrauber, Aufklärungsflugzeuge und Drohnen sollen heute nicht nur an IT-Systeme angebunden sein und etwa Bilddaten übertragen, sondern im Einsatz auch hochauflösendes Videomaterial in Echtzeit liefern – und zwar abgesichert auf VS-NfD-Level. Um dies zu realisieren, haben mehrere Hubschraubertypen der Bundeswehr die SCOTTY Communication Platform an Bord, die mit SINA Verschlüsselungstechnologie ausgestattet ist. Damit erschließt die Hochsicherheitslösung SINA, die am Boden seit Jahren den IP-Krypto-Backbone der Bundeswehr bildet, nun auch die vertikale Dimension.

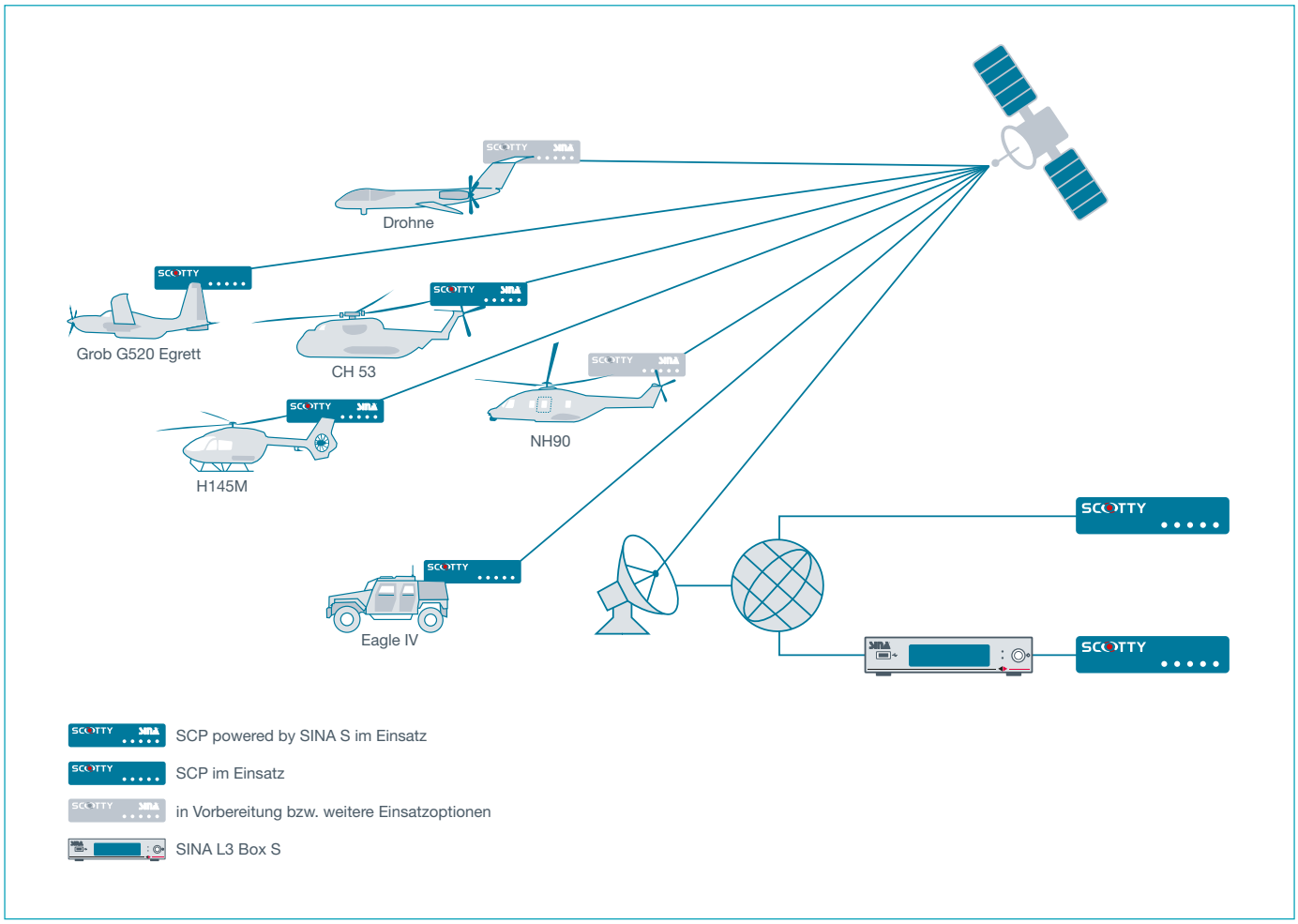
Bei den Streitkräften haben steigende Anforderungen im Hinblick auf Agilität und Flexibilität im Einsatz zu einem wachsenden Bedarf an Live-Videokommunikation geführt. Diese erlaubt es, Einsätze dynamisch zu koordinieren, zu unterstützen und zu führen. In einem konkreten Einsatz wird beispielsweise bei Aufklärungs- und Überwachungsmissionen HD-Videomaterial per Streaming live an die Kommandozentrale übertragen. Lagebeurteilungen werden dadurch wesentlich akkurater und aktueller.

Im Bereich der sanitätsdienstlichen Unterstützung erlaubt die verschlüsselte Video- und Datenübertragung in Echtzeit eine Vielzahl verschiedener Anwendungen der Telemedizin. Neben der Übertragung von Vitaldaten bei Notfällen, der Teleradiologie, Teleparasitologie und Teledermatologie ist auch die Unterstützung bei einer sonographischen Untersuchung durch einen Spezialisten im Heimatland mittlerweile in Echtzeit möglich.

Ein klassischer Anwendungsfall ist die bidirektionale Video- und Sprachübertragung in Form der Videokonferenz, die als modernes Führungsmittel eingesetzt wird. Last but not least dient das System auch zur Übertragung von Medienberichten aus dem Einsatzraum, sei es für die interne Kommunikation oder auch für die externe Berichterstattung.

Technisch realisiert werden derartige Szenarien mithilfe separater Rechnersysteme an Bord von Fluggeräten oder Fahrzeugen. Das Unternehmen SCOTTY mit Hauptsitz in Österreich stellt Lösungen zu diesem Zweck her. Die SCOTTY Communication Platform (SCP) erlaubt es, Daten, Fotos, Audio- sowie HD-Videomaterial live aus der Luft, vom Land und von hoher See aus zu übertragen – vorzugsweise per Satellitenkommunikation, da auf diese Weise eine kontinuierliche Netzverfügbarkeit sichergestellt werden kann, unabhängig von der jeweiligen Infrastruktur der Umgebung. Zusätzlich unterstützt die SCP terrestrische Netzwerke. Bei beiden Verbindungsarten ergibt sich die Herausforderung, dass die im Einsatz verfügbaren Netze meist nur moderate Bandbreite zur Verfügung stellen und hohe Latenz aufweisen. Daher bereitet die SCP die Videodaten so auf, dass sie trotz der schwierigen Bedingungen in hoher Qualität übertragen werden können. Bei Bedarf entscheiden die Anwender, ob bei der Aufbereitung eine optimale Bildschärfe oder eine optimale Bewegungsdynamik erreicht werden soll – je nach taktischem Nutzen.

Der Sikorsky CH-53 ist ein mittelschwerer Transporthubschrauber, der in den vergangenen Jahren an zahlreichen Auslandseinsätzen der Bundeswehr beteiligt war.



Die SCP besteht aus zwei Komponenten: einem Hardware-Decoder / Encoder und einer Rechnereinheit. Die Kombination dieser beiden Elemente erlaubt eine Reihe von Anwendungen, darunter bidirektionale Videokommunikation, unidirektionales Video-Streaming sowie Videoaufnahme. Auch die Übermittlung technisch weniger anspruchsvoller Informationen, die im Einsatz anfallen, etwa Audiomaterial oder einfache Daten, läuft über die SCP.

Um die Informationen nicht nur mit hoher Verfügbarkeit und in ausreichender Qualität, sondern auch abhörsicher zu übertragen, ist eine Variante der SCP mit dem Kryptosystem SINA ausgestattet. Als Bestandteil der “SCOTTY Communication Platform powered by SINA S” verlässt SINA nun den Boden und kommt an Bord von Hubschraubern der Bundeswehr in Höhen von bis zu mehreren Kilometern zum Einsatz. Die gemeinsame Lösung von SCOTTY und secunet ist für den nationalen Geheimhaltungsgrad VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) sowie international für NATO RESTRICTED sowie EU RESTRICTED / RESTREINT UE zuglassen.

Wie wird die Kommunikation konkret geschützt? Der SINA Bestandteil in der SCP im Hubschrauber fungiert als IPsec-gesichertes VPN-Gateway. Als Gegenstück werden am Boden eine (oder mehrere) SINA L3 Box S benötigt, die in die jeweilige dortige militärische IT-Infrastruktur integriert ist. Die zwischen den SINA Komponenten ausgetauschten Daten werden in verschlüsselten VPN-Tunneln sicher übertragen. Dabei ist es unerheblich, über welches potentiell unsichere Netzwerk der Datenaustausch stattfindet – zum Beispiel über das Internet oder eben im vorliegenden Fall über satellitengestützte Verbindungen.

Die Hardware-Plattform der SCP

VS-NfD-konforme Kryptographie stellt sicher, dass nur die beteiligten SINA Komponenten die Daten entschlüsseln können – und das mit hohem Datendurchsatz, um Anwendungen wie Videokommunikation zu ermöglichen.

Aktuell fliegen zwei erste Hubschraubertypen der Bundeswehr im Bestand der Deutschen Luftwaffe Einsätze mit der SCP powered by SINA S an Bord. Einer der beiden ist der Sikorsky CH-53, ein mittelschwerer Transporthubschrauber, der in den vergangenen Jahren an zahlreichen Auslandseinsätzen beteiligt war. Der CH-53 ist seit vielen Jahren das Arbeitstier der Deutschen Bundeswehr in Afghanistan. Vom Truppentransport über Verbindungsflüge, der Verlegung

SCOTTY Group Austria GmbH bietet ein umfangreiches Angebot an Kommunikationslösungen, speziell zugeschnitten auf den Einsatz in der Landesverteidigung, im Katastrophenschutz und zur Überwachung. SCOTTY ermöglicht Audio-, Video- und Datenübertragung, wo es keine Infrastruktur gibt: im Feldeinsatz, in Landfahrzeugen, in Schiffen und in der Luft.

SCOTTY wurde 1993 gegründet und verfügt über herausragende Erfahrung bei der Bereitstellung von Lösungen für kritische Anwendungen unter herausfordernden Bedingungen. Streitkräfte auf der ganzen Welt verwenden SCOTTY Equipment und vertrauen auf die langjährige Erfahrung und das Know-how, Kommunikation in entlegene und schwer zugängliche Gebiete zu bringen. SCOTTY Produkte können in Flugzeuge, Hubschrauber und Einsatzfahrzeuge integriert werden. Die Übertragung von Videoaufnahmen in Echtzeit an die Kommandozentrale macht Überwachungseinsätze, Erkundungsfahrten und -flüge effizienter und ermöglicht schnelles Handeln.

Die verschlüsselte Video- und Datenübertragung in Echtzeit erlaubt eine Vielzahl verschiedener Anwendungen der Telemedizin.
(c) SCOTTY

Die SCP ist nicht nur für den Einsatz in Hubschraubern, sondern auch für Flugzeuge (wie die Grob G520 Egrett im Bild), Landfahrzeuge sowie Schiffe konzipiert. (c) SCOTTY

von Spezialkräften in den Einsatzraum bis zur medizinischen Evakuierung wird die Plattform seit vielen Jahren für eine Vielzahl von Missionen in diesem nicht nur aufgrund der klimatischen Bedingungen schwierigen Einsatzraum genutzt.

Ein weiterer Hubschraubertyp mit SCP powered by SINA S an Bord ist der neue leichte Mehrzweckhubschrauber Airbus Helicopters H145M. Dessen Einsatzspektrum umfasst die Unterstützung landgestützter und maritimer Spezialoperationen sowie künftig auch Feuerunterstützungs-, Evakuierungs- und Aufklärungsmissionen. Die Deutsche Marine plant ebenfalls, diese IT-Sicherheitslösung einzuführen: Künftig soll die SCP powered by SINA S die Videokommunikation im neuen taktischen Marinetransporthubschrauber NH90 Sea Lion übertragen und absichern.

Als Hardware-Komponente für die Luftfahrt gelten für die SCP besondere Anforderungen: Schließlich muss die Lösung auch unter den extremen Bedingungen, wie sie im Flugzeug oder Hubschrauber herrschen, sicher funktionieren. Der Standard DO-160G legt Anforderungen für die Toleranz gegenüber Umwelteinflüssen sowie für die elektromagnetische Verträglichkeit fest. Dies beinhaltet den Temperaturbereich, in dem das System einwandfrei funktionieren muss, den Luftdruck, die Resistenz gegenüber elektromagnetischer Strahlung sowie insbesondere auch die Widerstandsfähigkeit gegenüber Vibrationen und Stößen, die vor allem bei Hubschraubern sehr extrem ausfallen können. Die SCP hat das Prüfverfahren zu diesem Standard erfolgreich durchlaufen.

Die SCP ist grundsätzlich nicht nur für die Luftfahrt, sondern auch für Landfahrzeuge und Schiffe konzipiert. Gleiches gilt für die Produktvariante mit SINA Funktionalität. Ein Projekt zur Integration des Systems in Landfahrzeuge ist aktuell bereits in Planung.

IT-Systeme sind zu integralen Bestandteilen militärischer Gesamtsysteme geworden, die deren Fähigkeiten verändern und wiederum neue Anforderungen generieren. Das wird am Beispiel der Live-HD-Videokommunikation besonders deutlich: Werden fliegende Plattformen mit dieser Funktionalität ausgestattet, erweitern sich deren Einsatzmöglichkeiten. Dies wiederum führt zu neuen Anforderungen, im konkreten Fall etwa im Hinblick auf Qualität, Verfügbarkeit und Vertraulichkeit der übertragenen Daten. Um auch künftige Anforderungen für militärische IT-Infrastruktur abzudecken, wird SINA kontinuierlich weiterentwickelt, in enger Abstimmung mit der Bundeswehr.

Dr. Michael Sobirey, secunet
michael.sobirey@secunet.com

Dr. Mario Polaschegg,
SCOTTY Group
M.Polaschegg@scottygroup.com

Dr. Michael Sobirey
Leiter Division Verteidigung, secunet

Dr. Mario Polaschegg
Head of Customization, SCOTTY Group

TELEMATIK IM GESUNDHEITSWESEN

Der Nächste, bitte: Nun sind die Krankenhäuser an der Reihe

Die Digitalisierung des deutschen Gesundheitswesens nimmt Fahrt auf. Die Telematikinfrastruktur, das digitale Rückgrat des Gesundheitssystems, wird Schritt für Schritt um weitere Anwendungen ergänzt. Gleichzeitig steht eine zweite Bauform des Konnektors in den Startlöchern: Der secunet konnektor für Rechenzentren zielt vor allem auf den Einsatz in Krankenhäusern ab.

Die Telematikinfrastruktur (TI) ist das digitale Netzwerk der Gesundheitswirtschaft, durch das die elektronische Gesundheitskarte einen digitalen Anschluss erhält. Oft als Datenautobahn für den Gesundheitssektor bezeichnet, wird die TI in Zukunft eine Reihe digitaler Prozesse unterstützen, die einen echten Mehrwert auch für die Versicherten bieten, etwa die elektronische Patientenakte oder das E-Rezept.

Als Herzstück der sicheren Kommunikation der IT-Systeme der medizinischen Leistungserbringer und der TI dient der Konnektor. Seit im November 2017 der erste Konnektor von der gematik (Gesellschaft für Telematikanwendungen der Gesundheitskarte mbH) zugelassen wurde, werden Arztpraxen in Deutschland damit ausgestattet.

Doch das war nur die erste Welle der TI-Vernetzung. Nach dem Willen des Gesetzgebers sollen bis zum 30. September 2020 auch alle Apotheken und bis Ende 2020 alle Krankenhäuser an die Datenautobahn angebunden werden.

Insbesondere im Fall der Krankenhäuser unterscheiden sich die Anforderungen bei der Vernetzung jedoch erheblich von denen einer Arztpraxis. Krankenhäuser betreiben heute große Rechenzentren. Die bisher im Markt verfügbaren Einbox-Konnektoren einschließlich des secunet konnektor weisen ein Format auf, das an einen heimischen DSL-Router erinnert. Was sich für Arztpraxen empfiehlt, passt nicht unbedingt zum Rechenzentrumsumfeld: Dort werden leistungsfähige Komponenten in geschlossenen 19“-Gehäusen erwartet, die sowohl in puncto Stromanschluss und Netzteil als auch hinsichtlich ihres Kühlkonzepts an den Rechenzentrumsbetrieb angepasst sind.

Konnektor für Rechenzentren

secunet hat sich entschieden, eine Variante für genau dieses Einsatzszenario zu entwickeln und anzubieten. Der secunet konnektor für Rechenzentren basiert technisch auf dem Einbox-Konnektor, erbringt aber die doppelte Leistung und wird zusätzlich mit einer Managementsoftware ausgestattet, die es Administratoren wesentlich erleichtert, mehrere Konnektoren im Verbund zu betreiben.

Die Zulassung der neuen Konnektor-Version wird für Dezember 2019 erwartet (so der Stand bei Redaktionsschluss der vorliegenden Ausgabe). Bleibt es bei diesem Zeitplan, kann der Rollout in Krankenhäusern bereits im Januar 2020 beginnen. Für rund 2.000 Krankenhäuser in Deutschland ist der secunet konnektor für Rechenzentren eine passgenaue Lösung, und auch für große Apotheken kann er eine interessante Alternative sein.

Die elektronische Gesundheitskarte erhält durch die Telematikinfrastruktur (TI) einen digitalen Anschluss.

Mehrwert in Sichtweite

Ausgeliefert wird die neue Konnektor-Variante vorerst mit der Software „VSDM“ (Versichertenstammdatenmanagement), bis das nächste Software-Upgrade den Zulassungsprozess durchlaufen hat. Dies wird für das zweite Quartal 2020 erwartet. Das Upgrade, das online eingespielt werden kann, wird den Konnektor um die Anwendungen elektronischer Medikationsplan (eMP), qualifizierte elektronische Signatur (QES) und Notfalldatenmanagement (NFDM) ergänzen. Die QES-Funktionalität ermöglicht dann auch den elektronischen Arztbrief über die Fachanwendung KOM-LE (Sichere Kommunikation zwischen Leistungserbringern). Die elektronische Patientenakte (ePA) wird frühestens für Ende 2020 erwartet.

Im Laufe des Jahres 2019 ist die Einführung der TI mit großen Schritten vorangekommen. Die zweite Bauform des Konnektors erleichtert nun die sichere Anbindung von Krankenhäusern und Großapotheken. Gleichzeitig erscheinen Anwendungen am Horizont, die deutlich werden lassen, warum sich das Großprojekt TI am Ende lohnt.

Markus Linnemann
markus.linnemann@secunet.com

RASANTER ROLLOUT

Der secunet konnektor für Arztpraxen (Einbox-Konnektor) wurde erst im Dezember 2018 von der gematik zugelassen, da sich secunet spät für einen Eintritt in den Gesundheitsmarkt entschieden hatte. Knapp ein Jahr danach sind bereits mehr als 45.000 Arztpraxen mit dem secunet konnektor ausgestattet. Auch im Verhältnis zum Gesamtmarkt ein durchaus hoher Wert: In Deutschland existieren grob 140.000 Arztpraxen, von denen aktuell etwa 115.000 an die TI angebunden sind.

Der secunet konnektor ist in einer Variante für Arztpraxen (rechts) und in einer Variante für Rechenzentren (oben) verfügbar, die beide für ihre jeweiligen Einsatzszenarien optimiert sind.

DATENSICHERHEIT IM CLOUD COMPUTING

Mit Joint Venture secustack zur sicheren Cloud

Die secunet Security Networks AG hat ihr Know-how mit der Dresdner Cloud & Heat Technologies GmbH vereint und ein Joint Venture gegründet. Die secustack GmbH bietet infrastrukturelle Cloud-Lösungen, die dem Nutzer die Souveränität über seine Daten zusichern. Das Angebot richtet sich vor allem an die öffentliche Hand sowie alle Unternehmen, die ihre sensiblen Daten noch nicht in der Cloud verarbeiten wollen oder dies aus Sicherheitsbedenken schlicht nicht dürfen. In diesem Interview gibt Dr. Marius Feldmann, CEO der secustack GmbH, Einblicke in die Zusammenarbeit und spricht über Ziele und Herausforderungen, die Ausschlag für die Kooperation beider Firmen gaben.

Dr. Feldmann, würden Sie bitte für unsere Leser beschreiben, was die secustack GmbH macht und wer sich dahinter verbirgt?

Die secustack GmbH ist eine gemeinsame Tochter von secunet und Cloud & Heat, welche im Mai dieses Jahres gegründet wurde. Unser Team besteht aus engagierten Cloud-Experten aus Dresden und widmet sich der Entwicklung eines Cloud-Betriebssystems, das höchsten Sicherheitsanforderungen gerecht wird und so Cloud Computing für alle Branchen nicht nur attraktiv, sondern zugleich sicher macht.

Dr. Marius Feldmann
COO Cloud&Heat Technologies GmbH, CEO secustack GmbH

Können Sie uns mehr über die Kooperation zwischen secunet und Cloud & Heat erzählen? Wie kam es zur Zusammenarbeit?

Die Zusammenarbeit begann bereits mehrere Jahre vor der Gründung unserer gemeinsamen Tochter. Mit dem initialen Ziel, den Markt hinsichtlich sicherer Cloud-Infrastrukturen zu explorieren, kamen wir zunächst ins Gespräch. Cloud & Heat war insbesondere aufgrund seiner langjährigen Erfahrungen im Betrieb OpenStack-basierter Cloud-Infrastrukturen ein interessanter Partner. Aber auch unsere Expertise bei den Themen Green IT und Nachhaltigkeit – die Technologie von Cloud & Heat erlaubt es, die Serverabwärme in Rechenzentren zum Heizen zu nutzen – erregte Aufmerksamkeit bei secunet. Während eines gemeinsamen Projekts in 2017 und 2018 identifizierten wir potenzielle Maßnahmen, die zur Sicherheitshärtung von OpenStack-Infrastrukturen beitragen und setzten diese zielgerichtet um.

Für welche Branchen ist die Lösung von secustack vor allem interessant und warum?

Der Einsatz von Cloud Computing bietet viele Vorteile bei der Reduzierung von Kosten und Komplexität und schafft durch Automatisierung hohe Betriebsstandards. Das ist eine Tatsache, der sicherlich niemand widersprechen wird. Das Problem dabei ist, dass es Branchen gibt, die aufgrund ihrer sehr strengen Sicherheitsanforderungen keine Cloud-Umgebungen nutzen. Dadurch verschenken sie jedoch essenzielle Wettbewerbsvorteile. Betroffen sind beispielsweise Organisationen, die sensible Daten verarbeiten, wie Behörden, aber auch Betreiber kritischer Infrastrukturen (kurz: KRITIS), für die ein Angriff auf die Infrastruktur katastrophale Konsequenzen haben könnte. Eine Lösung, die diesem speziellen Problem Rechnung trägt, gab es jedoch noch nicht am Markt. Zur Erhöhung der Cloud-Sicherheit und zur Bereitstellung einer Lösung, die diese Anforderungen erfüllt, wurde secustack gegründet.

Wie genau trägt secustack dazu bei, die Sicherheit moderner digitaler Infrastrukturen zu erhöhen?

secustack bietet mit seinem gleichnamigen Produkt „SecuStack“ eine Lösung, die die Speicherung und Verarbeitung von Daten nicht nur sicher, sondern auch transparenter macht. Basierend auf der Plattform OpenStack bietet SecuStack zusätzliche Mechanismen für durchgängige Verschlüsselung, Zugangskontrolle, Datenhoheit und Defense-in-Depth. Damit trägt SecuStack zu verschiedenen Sicherheitsthemen bei, wie z. B. der Sicherung des Infrastrukturzugangs oder der umfassenden Kontrolle über kryptographisches Material. Für die Umsetzung des Infrastrukturzugangs wird die bewährte SINA Technologie von secunet eingesetzt. Neben der allgemeinen Entwicklung von Sicherheitserweiterungen deckt SecuStack das gesamte Lifecycle-Management ab und bietet zudem eine Lösung zur sicheren Container-Orchestrierung.

Warum ist die Open-Source-Plattform OpenStack eine geeignete Basis für SecuStack?

Es gibt viele Möglichkeiten, eine Cloud-Umgebung aufzubauen. OpenStack ist in diesem Kontext der de-facto-Standard für Open-Source-Lösungen. Es bietet eine modulare Architektur, um eine Reihe von Kerndiensten bereitzustellen, die Skalierbarkeit und Elastizität als Kerndesigngrundsätze ermöglichen.

Dr. Feldmann ist seit 2013 für die Cloud & Heat Technologies GmbH in Dresden tätig – seit 2015 in der Rolle des Chief Operating Officer. Hier ist er für den Betrieb der OpenStack-basierten Cloud-Installationen bei Cloud & Heat verantwortlich. Aktuell begleitet er unter anderem Forschungsprojekte rund um das Thema Cloud-Sicherheit und Datenschutz in der Cloud. Dazu gehört AUDITOR, das die Entwicklung einer EU-weit gültigen Cloud-Zertifizierung anstrebt. Mit der Gründung der secustack GmbH im Mai 2019 übernahm Dr. Feldmann zusammen mit Dr. Kai Martius von der secunet Security Networks AG die Rolle des CEO des gemeinsamen Joint Ventures.

Dr. Marius Feldmann (links) und Dr. Kai Martius. Beide sind CEOs der secustack GmbH.

Open-Source-Plattformen bieten viele Argumente wie beispielsweise Flexibilität, Anbieterunabhängigkeit, die Fähigkeit zur Überprüfung und Verbesserung des Codes sowie die Umsetzung kurzfristiger Innovationen durch eine breite Gruppe von Mitwirkenden. Diese Eigenschaften tragen auch in einem hohen Maß zur Vertrauenswürdigkeit digitaler Infrastrukturen bei. Und genau dabei geht es uns ja bei secustack.

Was sind die nächsten Meilensteine und wo sieht sich secustack in fünf Jahren?

Neben der stetigen Weiterentwicklung des Security-Stacks werden wir unsere Marketing- und Vertriebsaktivitäten ausbauen. SecuStack konnte bereits jetzt in Projekten der Cloud & Heat erfolgreich in Betrieb gesetzt werden, so zum Beispiel in ihrem Rechenzentrum im Frankfurter Eurotheum. Zusammen mit Cloud & Heat sind wir bestrebt, alle künftigen Rechenzentrumsprojekte nicht nur energieeffizienter und damit nachhaltiger zu machen, sondern auch mit SecuStack-Distributionen auszustatten. Darüber hinaus wollen wir die Zusammenarbeit zwischen der secustack und ihren Müttern verstetigen. Unser übergeordnetes Ziel ist dabei, die Cloud-Welt sicherer zu machen und wir hoffen so, vielen Unternehmen branchenübergreifend den Wechsel in die Cloud zu erleichtern. In fünf Jahren sehen wir uns als etablierten Enabler für sicheres Cloud Computing mit einem starken Netzwerk.

secustack wurde im Mai 2019 vom IT-Sicherheitsspezialisten secunet Security Networks AG und dem IT-Infrastrukturanbieter Cloud & Heat Technologies GmbH gegründet. In der Zusammenarbeit bündeln die beiden Partner ihre langjährige Expertise im Bereich von IT-Sicherheitslösungen und dem Betrieb von OpenStack-basierten Cloud-Infrastrukturen. Das in Dresden ansässige Team leidenschaftlicher Cloud-Experten entwickelt Mechanismen, um ein sicheres Cloud-Betriebssystem basierend auf OpenStack bereitzustellen. Die Lösung SecuStack verfügt über verschiedene Funktionen zur Sicherung von Daten und der Cloud-Infrastruktur. Kernelement hierbei ist die strikte, funktionsübergreifende Mandantentrennung. SecuStack kann in jeder Umgebung mit sicherheitskritischen Prozessen und sensiblen Daten eingesetzt werden.

GEBÄUDEAUTOMATION

So sichert man ein Smart Building

IT-Systeme steuern zunehmend auch gewerblich oder öffentlich genutzte Gebäude. In der Gebäudeautomation (GA) herrscht aber traditionell ein anderes Sicherheitsverständnis als in der IT. Das führt dazu, dass IT-Sicherheit bis heute in der GA stiefmütterlich behandelt wird. Die daraus resultierenden Risiken für Smart Buildings werden immer größer. Ein Umdenken und vor allem interdisziplinäre Zusammenarbeit zwischen GA und IT sind notwendig.

Wohnungen, Häuser und Gebäude werden immer intelligenter: Mit Hilfe von smarten Technologien wird Energie effizienter eingesetzt und die Nutzung von Räumen aller Art komfortabler gestaltet. Smarte Lichtsteuerung passt sich an den menschlichen Biorhythmus an, Sprachassistenten ermöglichen die Steuerung von Geräten aller Art und intelligente Temperaturregelungen sorgen für Wohlfühltemperatur – wenn jemand im Raum ist.

Solche Anwendungsszenarien gibt es nicht nur im „Smart Home“. Sie haben ihre Entsprechungen im gewerblichen und öffentlichen Bereich. Dafür haben sich die Begriffe „Smart Building“ oder „Gebäudeautomation“ etabliert. Gemeint ist die Vernetzung und automatische Steuerung von technischen Anlagen der GA in Zweckgebäuden – dazu zählen Bürogebäude, aber auch Flughäfen, Krankenhäuser, Fabriken und Einkaufszentren. Die Gebäudeautomation gehört zu den komplexesten Einsatzgebieten des Internet of Things (IoT).

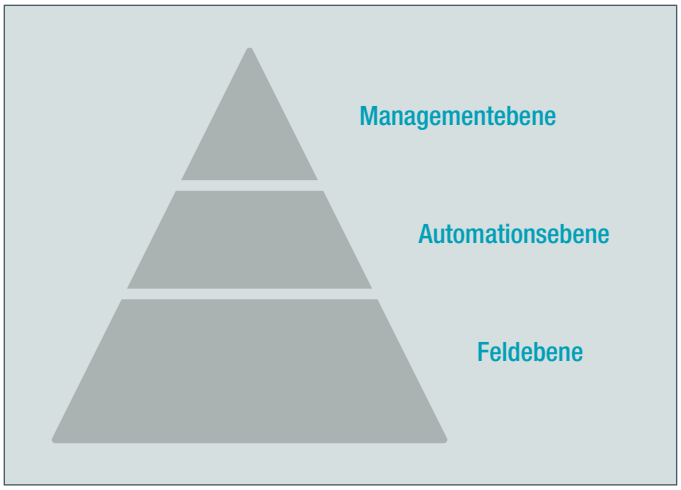
Hohe Komplexität in der Gebäudeautomation

Da Zweckgebäude in der Regel wesentlich größer sind als privat genutzte Immobilien, ist auch ihre Automatisierungstechnik wesentlich umfangreicher und komplexer. Um Struktur in die Vielzahl einzelner Elemente und Steuerungskreise zu bringen, wird häufig eine Drei-Ebenen-Einteilung verwendet, wie in der Abbildung der Automatisierungspyramide veranschaulicht wird:

Sensoren und Aktoren – beispielsweise Temperaturmesser und Heizungsregler – sind auf der untersten Ebene angesiedelt, der Feldebene. Die Geräte der Automationsebene werten die Messungen der Sensoren aus und generieren entsprechende Einstellungen der Aktoren. Auf der Managementebene ist die Leitzentrale angesiedelt, wo die Resultate dieses komplexen Zusammenspiels kontrolliert und gesteuert werden.

Die Kommunikation zwischen den Bauteilen und Geräten in einer Ebene und zwischen verschiedenen Ebenen erfolgt dabei nicht unbedingt einheitlich: Es kommen, besonders in älteren und modernisierten Gebäuden, oft verschiedene Protokolle, Bussysteme und Schnittstellen zum Einsatz. Die Nachrichtenübermittlung zwischen den verschiedenen Komponenten erfolgt überwiegend kabelgebunden, zunehmend aber auch kabellos.

Ebenso heterogen wie die Technik ist das Alter der Komponenten. Mehr noch als in anderen Einsatzgebieten digitaler Vernetzung treffen in der Gebäudeautomation teils jahrzehntealte Strukturen auf nachträglich eingebaute Technik, teilweise auch brandneue Technologien. Bei der Planung der meisten heute stehenden Gebäude hat die Möglichkeit der computergestützten Steuerung noch keine nennenswerte Rolle gespielt. Die entsprechenden Bauteile werden traditionell zum Gebiet der Automationstechnik und nicht zur Informationstechnologie gezählt – etwa die älteren verbindungsprogrammierten Steuerungselemente oder die neuere speicherprogrammierbare Steuerung. Das ist selbst bei Steuerungssystemen der Fall, deren Kern PC-Technologie mit einem PC-Betriebssystem bildet.



Was ist Sicherheit? Safety vs. Security

Während für die Fachleute in der Automationstechnik die Sicherheit im Sinne von „Safety“, also Betriebssicherheit bei Schutz von Leib und Leben, im Vordergrund steht, spielt in der IT die Sicherheit im Sinne von „Security“ (IT-Security) eine große Rolle. In deren Mittelpunkt stehen die klassischen Schutzziele Integrität, Verfügbarkeit und Vertraulichkeit von Informationen. Dies ist nicht nur eine begriffliche Unterscheidung von Sicherheit, sondern bringt auch kulturelle Unterschiede zwischen den beiden Fachgebieten mit sich.

Ob IT in der Gebäudeautomation formell zur Automationstechnik gezählt und so behandelt wird oder nicht: Es ändert sich nichts daran, dass sie in der Praxis ähnlich behandelt wird wie IT-Systeme in anderen Bereichen: Komponenten technischer Anlagen der GA werden aus verschiedensten Gründen mit dem Internet verbunden, mit Notebooks von Technikern oder Netzen der Bürokommunikation. Noch niedriger werden die Hürden der Vernetzung durch die Tatsache, dass die Kommunikationsprotokolle auch in der Gebäudeautomation immer mehr standardisiert werden – und diese Standards häufig aus der IT übernommen werden, wie etwa die Internet-Protokollfamilie (TCP/UDP/IP). „Internet Comes to Building Automation“ wurde schon 1999 verkündet und das Cloud-Management für die GA großer Gebäude ist längst kein Zukunftsmärchen mehr.

Diesem Zuwachs an Kommunikationsmöglichkeiten steht bisher nur selten ein entsprechender Zuwachs an Sicherheitsmaßnahmen gegenüber. Für GA-Systeme gilt häufig: Standard-Passwörter werden nicht geändert oder können überhaupt nicht geändert werden. Externe Laptops von Wartungstechnikern stellen eine unbekannte Größe im Hinblick auf Malware-Infektionen dar. Logdateien werden entweder nicht geschrieben oder zumindest nicht ausgewertet. Und preiswerte OEM-Komponenten aus Fernost haben nicht nur Sicherheitslücken im Sinne von unbeabsichtigten Mängeln, sondern können auch mit Spyware ausgeliefert werden.

Hier zeigt sich die Doppelrolle der Informationssicherheit für Smart Buildings:

- Zum einen wird Informationssicherheit immer wichtiger auch für die physische Sicherheit von Menschen. Unerkannte Sicherheitslücken und unberechtigte Zugangswege öffnen Tür und Tor etwa für die Manipulation von Systemen wie Brandschutzanlagen oder Heizkesseln.
- Zum anderen kann sich die Informationssicherheit der GA-Technik eines Smart Buildings bei entsprechender Vernetzung auf die Informationssicherheit der in diesem Gebäude ansässigen Parteien auswirken. Beispielsweise könnten vertrauliche Daten, mit denen etwa die Mieter eines Bürogebäudes umgehen, gefährdet werden, wenn die Schließanalage über Schwachstellen in Überwachungskameras angreifbar ist. Oder umgekehrt kann ein angegriffener Server im Büronetz zum Einfallstor für Angriffe auf die Gebäudeautomationstechnik werden. Derlei Angriffe sind keine Fiktion, sondern finden bereits heute statt.

Stufenplan für Informationssicherheit im Smart Building

Die Herausforderungen der IT-Sicherheit in der Gebäudeautomation sind also enorm. Wie lässt sich ein pragmatischer Einstieg finden? Die Fachleute von secunet orientieren sich bei einschlägigen Projekten an dem folgenden Stufenplan:

1. Dokumentation

Der erste Schritt, um die Komplexität in den Griff zu bekommen, ist eine (möglichst) vollständige und aktuelle Dokumentation aller verwendeten technischen Anlagen inklusive Standort, Vernetzung, Hersteller, Softwareversionen, Konfiguration und Parametrierung, ggf. Wartungsdienstleister. Häufig liegen dazu nur unvollständige Informationen vor, und das auch nicht an zentraler Stelle.

Einmal erstellt, sollte diese Aufzeichnung des Ist-Zustandes stets aktuell gehalten und allen befugten Personen zugänglich gemacht werden. Sinnvoll ist zudem, externe Informationsquellen zu nutzen, die beispielsweise über aktuell bekannt gewordene Sicherheitslücken in Komponenten und Software informieren.

2. Feststellung des Schutzbedarfs

In der Gebäudeautomation müssen die kritischen Prozesse wie beispielsweise Stromversorgung, Brandschutz, Klimatisierung, Leckageerkennung und Notfallevakuierung (inkl. Sicherheitsbeleuchtung) vorrangig geschützt werden. Der Schutzbedarf der kritischen Geschäftsprozesse bestimmt den Schutzbedarf der technischen Anlagen, mit denen sie umgesetzt werden. Die Bestimmung des Schutzbedarfs von Geschäftsprozessen ist eine Aufgabe der Leitungsebene.

3. Ermittlung des Handlungsbedarfs

Auf Basis des zuvor ermittelten Schutzbedarfs der Geschäftsprozesse und technischen Anlagen und unter zusätzlicher Berücksichtigung des Notfallmanagements müssen nun die erforderlichen weiteren Sicherheitsmaßnahmen festgelegt und priorisiert werden. Das können sowohl organisatorische als auch konkrete technische Maßnahmen sein. Es ist praktisch unumgänglich, bei diesem Prozess Informationen von Dienstleitern und Herstellern einzuholen.

4. Umsetzung

Je nach zuvor ermittelter Priorität und dem verfügbaren Budget muss die Umsetzung der Sicherheitsmaßnahmen erfolgen. Sie kann entweder im Zuge der regelmäßigen Wartung, bei ohnehin geplanten Modernisierungsmaßnahmen, oder außerplanmäßig, wenn dringender Handlungsbedarf besteht, geschehen.

Um die Steuerung, Kontrolle und ggf. Anpassung von Sicherheitsmaßnahmen zu gewährleisten, ist es empfehlenswert, ein Informationssicherheitsmanagementsystem (ISMS) für die GA aufzubauen, wie aus dem Kontext des IT-Grundschutzes bekannt.

IT-Grundschutz ist das Mittel der Wahl

Nicht nur ein ISMS, sondern auch andere Methoden und Prozesse des IT-Grundschutzes des Bundesamtes für Sicherheit in der Informationstechnik (BSI) sind anwendbar, um die Sicherheit in der Gebäudeautomation zu gewährleisten. Der IT-Grundschutz ist bewährt und der beste Ansatz, der aktuell verfügbar ist.

Besonders relevant sind die Bausteine zur industriellen IT des modernisierten IT-Grundschutzes, die Anforderungen an die Informationssicherheit technischer Anlagen enthalten. In zukünftigen Versionen sollen im Bereich industrieller IT noch weitere Bausteine ergänzt werden, die den IT-Grundschutz für Smart Buildings noch umfassender anwendbar machen, wie etwa die Bausteine für Leitstand und Safety-Systeme.

Praxiserfahrungen von secunet zeigen, dass eine erste Absicherung der GA eines Smart Buildings mit etwa 20 Bausteinen des IT-Grundschutz-Katalogs erreicht werden kann. Für eine umfassende Absicherung werden in der Regel um die 40 Bausteine benötigt.

In Zukunft: Safety und Security by Design

Die Anwendung des IT-Grundschutz-Katalogs ist umso effizienter und wirksamer, je früher sie im Lebenszyklus eines automatisierten Gebäudes ins Spiel kommt. Optimal ist eine Berücksichtigung der Informationssicherheit schon bei der Planung der Gebäudeautomationstechnik im Sinne der Security by Design. Sie ergänzt die Safety by Design wie etwa die frühzeitige Planung des Brandschutzes.

Kulturwandel erforderlich

Darüber hinaus sind kulturelle Faktoren von grundlegender Bedeutung: Die noch immer bestehende Scheingrenze zwischen den „Welten“ der IT und der GA in den Köpfen und die reale Grenze in den Organisationsstrukturen müssen als Problem, als Sicherheitsrisiko, erkannt und beseitigt werden. Erforderlich ist stattdessen ein holistisches Verständnis der Gebäudeautomation, das deren IT-Charakter – mitsamt der IT-Probleme und IT-Sicherheitsprobleme – nicht verdrängt, sondern immer mitdenkt. Eine grundsätzliche Verbesserung der Situation wird es nur dann geben können, wenn es zu einem echten Kulturwandel kommt.

Für die Weiterentwicklung des IT-Grundschutzes bleibt die Frage, ob seine Anwendung im Bereich der Gebäudeautomation eine ebensolche Erfolgsgeschichte wird wie im Bereich der klassischen IT. Die Grundlagen dazu sind mit dem modernisierten IT-Grundschutz gelegt. Es braucht aber auch den erwähnten Kulturwandel in der Gebäudeautomation, um die erforderliche IT-Sicherheit zu gewährleisten.

Robert A. Gehring
robert.gehring@secunet.com

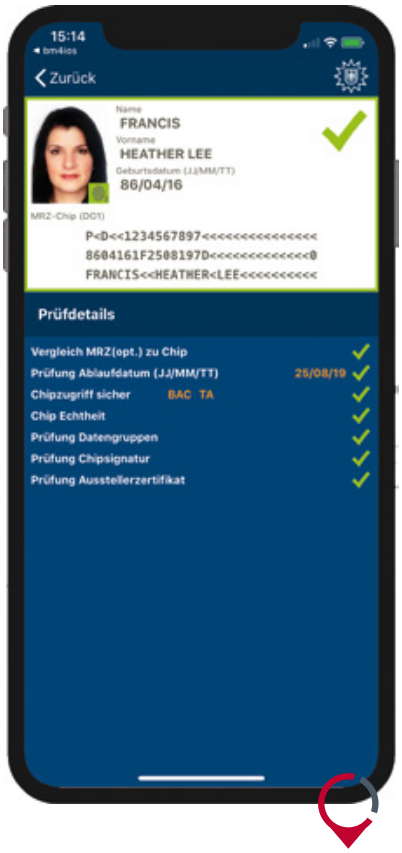
Gebäudeautomation hilft u. a. beim Energiesparen. Manche Smart Buildings kommen ohne Klimaanlage aus, stattdessen werden Sonnenblenden und Lüftung je nach Sonneneinstrahlung intelligent gesteuert.

Der Artikel basiert auf dem Vortrag „Herausforderungen der IT-Sicherheit im Bereich der Gebäudeautomation“ von **Robert A. Gehring , Christina Helbig und Markus Stark,** der beim 16. Deutschen IT-Sicherheitskongress im Mai 2019 in Bonn-Bad Godesberg gehalten wurde. Der Tagungsband zum Kongress erschien im SecuMedia Verlag und kann im Buchhandel erworben werden (ISBN: 978-3-922746-82-9).

BUNDESPOLIZEI

Mobile Dokumentenprüfung per Smartphone-App

secunet ist langjähriger Partner der Bundespolizei bei der Entwicklung einer modernen Informationsarchitektur für die digitale Polizeiarbeit. Ein herausragendes Ergebnis der Zusammenarbeit ist die Entwicklung einer Smart Police App auf Basis der Softwareplattform secunet biomiddle. Die Applikation ermöglicht einen orts- und endgeräteunabhängigen Zugriff sowie die Verarbeitung polizeilicher Informationen. Ab sofort ist die App auch für iOS verfügbar und steht den Polizeien der Länder zur Verfügung.



Mit der App „BPOL-Dokumentenprüfung“ können Bundespolizisten elektronische Identitätsdokumente (eID) unterwegs flexibel und sicher mit dem Smartphone auslesen und prüfen.

Bereits seit 2018 setzt die Bundespolizei bei Personenkontrollen in mobilen Einsätzen erfolgreich Apps zur Dokumentenprüfung und Identitätsfeststellung ein. Mit der App „BPOL-Dokumentenprüfung“ können Bundespolizisten elektronische Identitätsdokumente (eID) unterwegs flexibel und sicher mit dem Smartphone auslesen und prüfen. Darüber hinaus ist die Verifikation biometrischer Daten möglich, wie z. B. der Vergleich des im Chip gespeicherten Gesichtsbildes mit dem Livebild der Person. Die App bietet wichtige Elemente der stationären Prüfung von Reisepässen und Personalausweisen auch mobil per Smartphone an. secunet hat die App im Auftrag der Bundespolizei auf Basis der secunet biomiddle Plattform entwickelt und an die Bedürfnisse der Bundespolizei für den täglichen Einsatz angepasst. Zum Beispiel sind auch Prüfungen im Offline-Modus möglich. Insgesamt wird die Verfügbarkeit polizeilicher Informationen verbessert – ein wichtiger Beitrag zur Inneren Sicherheit.

Mit der kürzlich für Drittanbieter geöffneten NFC-Schnittstelle in iOS13 ist die App nun für alle gängigen mobilen Plattformen verfügbar und kann eIDs ohne zusätzliche Hardware auslesen. Davon profitieren Polizeibehörden, die sowohl Android- als auch iOS-Geräte im Einsatz haben und die App „BPOL-Dokumentenprüfung“ verwenden bzw. dessen Verwendung planen.

Die Bundespolizei und secunet bieten die Ergebnisse der erfolgreichen Kooperation auf Bundesebene bei der Entwicklung von Apps im Bereich der mobilen Dokumentenprüfung und biometrischen Verifikation von Personen auch den Polizeien der Bundesländer an. Mehrere Landespolizeien nutzen neben der App „BPOL-Dokumentenprüfung“ auch weitere mit secunet entwickelte Apps bereits erfolgreich im Alltag.

Alle Smart Police Apps von secunet basieren auf der gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik entwickelten Softwareplattform secunet biomiddle, welche eine breite Palette an Funktionen im Bereich Dokumentenprüfung, Biometrie und OCR bietet. Sie ist das Kernstück für vielseitige polizeiliche Anwendungen zur Dokumentenprüfung und Identitätsfeststellung. Über serviceorientierte Schnittstellen setzt secunet biomiddle die Prozesslogik anwendungsspezifisch um und steuert die für das jeweilige polizeifachliche Verfahren (zum Beispiel Fast-ID) notwendigen Komponenten sowie die Kommunikation mit Hintergrundsystemen.

Die mobile Version der secunet biomiddle Plattform kann als Software Development Kit (SDK) auch in bestehende Apps der Polizeien oder anderer Anbieter eingebunden werden, zum Beispiel für die Vorgangbearbeitung. Mit der vielseitigen Plattformunterstützung und SDK-Verfügbarkeit gelingt der Bundespolizei und secunet ein wichtiger Schritt in Richtung einheitliche mobile IT-Welt bei den Polizeibehörden.

Thomas P. Schäfer
thomas.schaefer@secunet.com

Ein weiteres Rekordjahr für die it-sa

Auch dieses Jahr konnte die it-sa mit neuen Rekorden überzeugen: Mit rund 15.600 Fachbesuchern und über 750 Ausstellern bildet die jährlich wachsende Messe den europäischen Treffpunkt für die internationale IT-Sicherheits-Community. Ein Plus von 20 Prozent an Messebesuchern aus dem Ausland und viele länderübergreifende Gemeinschaftsstände zeigen die wachsende internationale Bedeutung der Messe.

„Die it-sa ist die Messeheimat für alle, die sich dem Thema IT-Sicherheit professionell widmen. Das klare Plus bei den Aussteller- und Besucherzahlen und die erneut vergrößerte Ausstellungsfläche bestätigen die Relevanz der it-sa als führende internationale Plattform für Cybersicherheit“, erklärt Petra Wolf, Mitglied der Geschäftsleitung beim Veranstalter NürnbergMesse.

Rund 350 Forenbeiträge und 30 separate Veranstaltungen im Congress@it-sa bereicherten die Messe mit Einblicken in die IT-Sicherheit und den Datenschutz. Einen Höhepunkt bildete die Special Keynote des britischen Investigativjournalisten Misha Glenny am letzten Messetag.

Seit bereits elf Jahren beteiligt sich secunet an der mittlerweile weltweit größten Fachmesse für IT-Sicherheit. An einem neu konzipierten Messestand präsentierte secunet ein breites Spektrum von Lösungen für staatliche und militärische Organisationen, Sicherheitsbehörden, kritische Infrastrukturen, die Industrie und das Gesundheitswesen. Diverse themenübergreifende Vorträge rundeten den Messeauftritt ab. Auch in diesem Jahr konnte sich secunet wieder über einen regen Austausch mit den Standbesuchern freuen.

Dr. Kai Martius, CTO von secunet und CEO von secustack, vor seinem Vortrag über sicheres Cloud Computing

secunet CEO Axel Deininger (rechts) begrüßt Tobias Hans (Mitte), den Ministerpräsidenten des Saarlandes, am Messestand.

Der secunet Messestand auf der it-sa 2019

secunet Experte Mustafa Alaa Eddine spricht über einen sicheren Übergang von ISDN zu All-IP.

secunet Experte Jens Kulikowski erklärt, wie Maschinen im industriellen IoT-Umfeld mit secunet edge sicher vernetzt werden können.

Termine – Januar bis Juni 2020

20. Januar 2020
ELSTERdialog | München

20. bis 22. Januar 2020
Omnisecure | Berlin

4. bis 5. Februar 2020
Europäischer Polizeikongress | Berlin

11. bis 12. Februar 2020
StrategieTage IT Security |
Bergisch Gladbach

11. bis 13. Februar 2020
e-World | Essen

18. bis 20. Februar 2020
General Police Equipment Exhibition & Conference (GPEC) |
Frankfurt am Main

24. bis 28. Februar 2020
RSA Conference | San Francisco, USA

10. März 2020
SINA Anwendertag | Berlin

17. März 2020
SINA Anwendertag | Bonn

20. bis 22. März 2020
Chemnitzer Linux-Tage | Chemnitz

23. bis 24. März 2020
Rethink! IT Security | Hamburg

25. März 2020
Polizeitag | Düsseldorf

31. März bis 2. April 2020
ICAO TRIP Symposium & Exhibition |
Montreal, Kanada

31. März bis 2. April 2020
Passenger Terminal Expo |
Paris, Frankreich

1. bis 2. April 2020
AFCEA Fachausstellung | Bonn

16. bis 8. April 2020
GISEC | Dubai, Vereinigte Arabische Emirate

20. bis 24. April 2020
Hannover Messe | Hannover

21. bis 23. April 2020
DMEA | Berlin

28. bis 29. April 2020
ID@Borders Conference | Brüssel, Belgien

5. Mai 2020
ITS.Connect | Bochum

12. bis 14. Mai 2020
KELI | Bremen

3. bis 4. Juni 2020
FTE EMEA | Dublin, Irland

9. bis 11. Juni 2020
Identity Week (SDW) |
London, Großbritannien

15. bis 17. Juni 2020
Zukunftskongress Staat & Verwaltung |
Berlin

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

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.

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.

Urheberrecht
© secunet Security Networks AG. Alle Rechte vorbehalten. Alle Inhalte sind urheberrechtlich geschützt. Jede Verwendung, die nicht ausdrücklich vom Urheberrechtsgesetz zugelassen ist, bedarf der vorherigen schriftlichen Erlaubnis.

Bildnachweis
Titel, S. 5, 8, 18/19 unten, 27, 28: iStock
S. 2 unten, 7: alamy
S. 3, 6, 15, 16, 17, 19 oben, 21 unten links, 23, 24, 25, 29, 30: secunet
S. 8: Bundesagentur für Arbeit
S. 9, 10, 11: NATO
S. 12: SICP
S. 13: Matern Architekten, Goldbeck GmbH
S. 20, S. 21 oben und unten rechts: SCOTTY Group
S. 22: Fotolia

Aus Gründen der besseren Lesbarkeit wird im Magazin oft auf die gleichzeitige Verwendung weiblicher und männlicher Sprachformen verzichtet und das generische Maskulinum verwendet. Sämtliche Personenbezeichnungen gelten gleichermaßen für beide Geschlechter.

klimaneutral gedruckt
www.klima-druck.de
ID-Nr. 1986664
bvdm.

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

Damit Dienstgeheimnisse nicht in die falschen Kanäle geraten.

Mit SINA sind Behörden-Netzwerke premiumsicher.

Wo Behörden und Verwaltungen ihre Daten und IT-Infrastrukturen gegen Eindringlinge sichern müssen, steht secunet bereit. Als IT-Sicherheitspartner der Bundesrepublik Deutschland sind wir Spezialisten für den Schutz von Verschlusssachen. Expertenberatung und BSI-zugelassene SINA Technologie machen Netzwerke, Clients und Prozesse premiumsicher.

secunet – Ihr Partner für IT-Premiumsicherheit.

secunet