secuview

Das secunet Kundenmagazin 2•2021

Digitale Souveränität wahren

Dr. Sven Egyedy, CIO des Auswärtigen Amts, über die modernisierte Verschlusssachen-Kommunikation des Bundes

Zugang für alle

Auf dem Weg zur barrierefreien IT – bald auch mit SINA

Mensch oder Morph?

Schutz vor Identitätsbetrug bei der Grenzkontrolle

National

International

Technologien & Lösungen

Kurz notiert

Service

Liebe Leserinnen und Leser,

zwar dauert die Pandemie weiter an, aber immerhin hat uns das Jahr 2021 auch einige Monate beschert, in denen sich das Leben etwas normaler abspielte. Bei secunet haben wir diese Zeit genutzt: Wir haben Kontakte gepflegt, an Branchenevents wie der it-sa teilgenommen und selbst Events veranstaltet, nämlich die SINA Anwendertage. Bei solchen Gelegenheiten wurde nicht nur deutlich, wie sehr wir den persönlichen Austausch vermisst haben. Es war dann auch wieder klarer zu sehen, dass die IT-Sicherheit eine Branche ist, die vor Dynamik und Innovation brodelt.

Das liegt zum einen an ihrer Offenheit und einer gewissen Diskussionsfreude: Wer an Konferenzen teilnimmt und immer einen Fuß in der Tür der Entwickler-Communities hat, profitiert ständig von neuen Erkenntnissen und Ansätzen und gestaltet diese mit. Auch der Open-Source-Gedanke sorgt für Transparenz.

Zum anderen hat die IT-Sicherheit an vielen der großen technologischen Themen unserer Zeit teil – etwa KI, Cloud oder der vierten industriellen Revolution. Auch Home Office und Kollaboration werden stark von IT-Sicherheit getrieben, und aus diesem Grund hat die Pandemie, die vieles lähmt, die Dynamik der IT-Sicherheit eher noch angefacht.

Noch dazu geht IT-Sicherheit uns alle etwas an, als Privatpersonen oder als Bürger*innen eines Gemeinwesens. Im Gegensatz zu manchen Unternehmen, die das Thema noch immer eher stiefmütterlich behandeln, legen staatliche Organisationen großen Wert darauf, ihre – und unsere – Daten angemessen zu schützen. In diesem Zusammenhang freue ich mich insbesondere über das Titelinterview der vorliegenden Ausgabe der secuview. Dr. Sven Egyedy, Chief Information Officer des Auswärtigen Amts, erläutert darin, welche führende Rolle die Behörde künftig bei der Verschlusssachen-Kommunikation des Bundes spielen wird.

Global betrachtet muss es ein wichtiges Ziel Deutschlands und Europas sein, digitale Souveränität aufzubauen und zu schützen. Um dieses Ziel zu erreichen, wäre es sicher hilfreich, wenn die IT-Sicherheitsbranche Unterstützung in Form von Industriepolitik erhalten würde – so wenig sie den Wettbewerb auf technologischer Ebene auch scheuen muss.

Nun wünsche ich Ihnen viel Spaß bei der Lektüre und erholsame Feiertage. Auf ein möglichst coronafreies Jahr 2022. Bleiben Sie gesund!

Ihr Axel Deininger

Bundesverwaltung modernisiert Verschlusssachen-Kommunikation

„Essenzieller Beitrag für eine zukunftsfähige Sicherheitsarchitektur Deutschlands“

Gerade in Krisenzeiten wird deutlich, wie wichtig funktionierende Kommunikation ist. So hat die Corona-Pandemie ein Vorhaben beschleunigt, das schon seit längerer Zeit geplant war: Die Bundesverwaltung stellt ihre Verschlusssachen-Kommunikation neu auf. In einem ressortübergreifenden Projekt unter der Federführung des Auswärtigen Amts wurde in weniger als zwei Jahren eine neue Infrastruktur aufgebaut, die Sprach- und Videokommunikation bis zur Geheimhaltungsstufe GEHEIM ermöglicht. secunet ist eines von zwei Unternehmen, die die Technologie dafür liefern. Bereits Anfang 2022 wird das System seinen Betrieb aufnehmen. secuview sprach mit Dr. Sven Stephen Egyedy, Chief Information Officer des Auswärtigen Amts.

Herr Dr. Egyedy, wie kam es ursprünglich zu der Initiative?

Dr. Sven Egyedy: Zur Kommunikation von Verschlusssachen (VS) der Geheimhaltungsgrade VS-VERTRAULICH und GEHEIM existierte bis 2020 keine allgemeine, ressortübergreifend verfügbare elektronische Lösung in der Bundesverwaltung. Ein konkreter Handlungsbedarf in puncto Verschlusssachen-Kommunikation wurde 2016 im Rahmen einer Nato-Übung identifiziert, die aufdeckte, dass viele Systeme zur Kommunikation von sensiblen Verschlusssachen veraltet, defekt oder nur mit eingeschränktem Funktionsumfang nutzbar sind. In 2017 erfolgte die Konstituierung einer ressortübergreifenden VS-Kommunikation-Arbeitsgruppe unter Beteiligung des Bundesministeriums des Inneren, für Bau und Heimat (BMI), des Bundesministeriums für Verteidigung (BMVg), des Bundeskanzleramts (BKAmt), des Bundesamts für Sicherheit in der Informationstechnik (BSI) und des Auswärtigen Amts (AA) – die sogenannten Kernressorts der heutigen Bundesmaßnahme R-VSK. Ziel war die nachhaltige Stärkung des VS-Kommunikationsnetzes der Bundesverwaltung. Im Rahmen der IT-Konsolidierung Bund wurde 2019 die Federführung der Bundesmaßnahme R-VSK durch Beschluss an die Auslands-IT des Auswärtigen Amtes übertragen. Seither hat das gesamte Projektteam der Bundesmaßnahme R-VSK einen essenziellen

„Im Rahmen der Markterkundung stellte sich die secunet Security Networks AG als einer von zwei wegweisenden VS-IT-Anbietern heraus, um der Dual-Vendor-Strategie der Bundesmaßnahme zu entsprechen."

Beitrag für eine zukunftsfähige Sicherheitsarchitektur Deutschlands und einen modernen Staat geleistet. Innerhalb von wenigen Monaten wurde der Bereich der Geheimkommunikation in Form von Telefon- und Videokonferenztechnik auf Basis neuester Krypto-Technologie ressortübergreifend in der Bundesverwaltung aufgebaut.

Welche Rolle spielte die Coronakrise für die Finanzierung und Umsetzung des Projekts?

Als Gegenmaßnahme zur Coronakrise und daraus resultierenden wirtschaftlichen Schäden wurde das Konjunkturpaket durch die Bundesregierung beschlossen, mit einem Umfang von zehn Milliarden Euro. Diese waren unter anderem auch für eine Modernisierung und Digitalisierung der Verwaltungen vorgesehen. Davon wurden ca. 52 Millionen Euro für die Finanzierung des Projektes gesichert. Daraus resultierte die Bedingung, dass die Umsetzung des Projektes von fünf auf zwei Jahre verkürzt wird. Dies ließ sich nur durch eine ganzheitliche Neuausrichtung der Projektziele und darauf abgestimmtes Projektmanagement bewerkstelligen.

Wie sieht die Lösung im Kern aus und wie sind die Verantwortlichkeiten aufgeteilt?

Die Lösung umfasst die ressortübergreifende Kommunikation mittels Telefonie und Videokommunikation. In 2021 wurde ein Minimum Viable Product (MVP) vom Auswärtigen Amt in Zusammenarbeit mit externen Lieferanten und Dienstleistern entwickelt und in mehreren Tests erfolgreich erprobt. Derzeit befindet sich die erarbeitete Lösung in Freigabeprüfungen nach Verschlusssachenanweisung (VSA) durch das BSI, welches das Projekt von Beginn an betreut. In 2022 beginnt der Wirkbetrieb mit den Diensten Telefonie und Videokommunikation und die Skalierung der Lösung auf die gesamten Bundesbehörden wird gestartet. Ein weiterer Teil der Lösung sieht die Errichtung einer Infrastruktur für den Datenaustausch von Verschlusssachen vor. Die Kommunikation kann dabei verschlüsselt über das offene Internet wie auch über die Regierungsnetze stattfinden. Für den Betrieb wird dafür in Rechenzentren eine Cloud-Infrastruktur entwickelt. Insgesamt ist ein großes heterogenes Team Teil der Bundesmaßnahme und umfasst die Zusammenarbeit zwischen den Behörden AA, BMI, BKMVg, BMF und BSI sowie privatwirtschaftlichen Herstellern von Krypto-Komponenten und weiteren externen Dienstleistern. Dabei übernimmt die Auslands-IT des AA die Koordination und Steuerung der Bundesmaßnahme.

Warum haben Sie sich unter anderem für secunet als Technologie-Lieferant entschieden?

Innerhalb des Projektvorlaufs der Bundesmaßnahme R-VSK wurde durch die Auslands-IT des Auswärtigen Amtes eine Markterkundung für VS-IT-Kommunikationsgeräte praktiziert. In dieser Markterkundung wurde unter spezifischen Bedingungen eruiert, welche potenziellen Anbieter und Produkte für den Aufbau einer ressortübergreifenden VS-IT-Infrastruktur

Dr. Sven Egyedy

Dr. Sven Egyedy ist Chief Information Officer (CIO) des Auswärtigen Amts und Leiter der Auslands-IT. Neben Stationen im BMF, BMI und dem BMVg sowie deren Geschäftsbereichen, war er von 2011 bis 2015 Commercial Coordinator für die Bauverträge des Kernfusionsreaktors ITER bei der europäischen Joint Undertaking Fusion for Energy F4E. Dr. Egyedy ist Vorstandsvorsitzender des gemeinnützigen Vereins NExT (Netzwerk: Experten für die digitale Transformation der Verwaltung) und promovierte in den Sozialwissenschaften.

zur Verfügung stehen. Unter Berücksichtigung der Vorgaben der VSA sowie des SÜG (Sicherheitsüberprüfungsgesetz) und im Interesse der digitalen Souveränität beschränkte sich die Betrachtung auf Anbieter, deren Unternehmensanteile und Entwicklung überwiegend in Deutschland verortet sind. Im Rahmen der Markterkundung stellte sich die secunet Security Networks AG als einer von zwei wegweisenden VS-IT-Anbietern heraus, um der Dual-Vendor-Strategie der Bundesmaßnahme zu entsprechen. Das Produktportfolio von secunet beinhaltet Produkte, die speziell für IT-Sicherheitslösungen für die elektronische Verschlusssachenbearbeitung oder VS-Kommunikation entwickelt wurden und somit den spezifischen Anforderungen dieses Kommunikationszwecks gerecht werden. Beispielhaft für das Produktportfolio von secunet steht die Kryptoarchitektur „Sichere Inter-Netzwerk Architektur", kurz SINA, die im Auftrag des BSI entwickelt wurde. SINA ermöglicht die sichere Bearbeitung, Speicherung, Übertragung und Nachweisführung von Verschlusssachen. Unterschiedlich eingestufte Daten können dabei strikt getrennt werden. Die Architektur bietet eine umfangreiche Produktpalette aus Endgeräten, Krypto-Gateways und Ethernet-Verschlüsselungstechnik sowie der Systemlösung SINA Workflow (SWF).

Zudem besteht seit 2004 eine Sicherheitspartnerschaft mit der Bundesrepublik Deutschland. In verschiedenen Projekten sammelte secunet Erfahrungen in der öffentlichen Verwaltung, beispielsweise im BMI, beim BSI, beim Auswärtigen Amt, bei der Luftwaffe sowie beim Deutschen Militärischen Vertreter – beim Militärausschuss der NATO.

Wie verlief die Zusammenarbeit mit den anderen Ressorts und mit den Industriepartnern?

Wie bereits dargestellt ist die ressortübergreifende Zusammenarbeit in puncto VS-Kommunikation historisch gewachsen. Seitdem das Auswärtige Amt die Federführung der Bundesmaßnahme innehat, konnte die ressortübergreifende Zusammenarbeit nochmals intensiviert werden. Die VS-Produkte für Telefonie und Video wurden im Kernressortkreis ausgiebig getestet und wir haben konstruktive Arbeitskreise etabliert, um bereits gesammelte Erfahrungen im Umgang mit VS-IT Produkten zu bündeln und um den vorhandenen Wissensstand der Bundesverwaltung auszuschöpfen. Ferner ist der Aufbau von VS-IT-Infrastruktur hochkomplex, daher sind wir neben den Ressorterfahrungen auf die fachlichen VS-IT-Expertisen unserer Industriepartner angewiesen. Durch die unterschiedlichen VS-IT Produkte und Services, die in dem Produktportfolio der Bundesmaßnahme R-VSK zu finden sind, bündeln wir die interdisziplinären Expertisen unserer Industriepartner. Unsere Vision ist es, als Leuchtturmprojekt für eine funktionierende ressortübergreifende Zusammenarbeit unter Einbindung strategischer Industriepartner für weitere IT-Maßnahmen innerhalb der Bundesverwaltung zu dienen.

> „Vor dem Hintergrund der besonders sensiblen Natur von Verschlusssachen erlangt der Aspekt der digitalen Souveränität zusätzliches Gewicht."

Bei der Verschlüsselungstechnik und den Endgeräten kommen nur deutsche Anbieter zum Einsatz. Können Sie den Sinn dahinter kurz erläutern?

Der Markt für VS-Produkte ist speziell auf die Zielgruppe der öffentlichen Verwaltung ausgerichtet. Die Anwendungsszenarien und Rahmenbedingungen unterscheiden sich von denen der Privatwirtschaft, da hohe geheimschutzrelevante Auflagen erfüllt werden und komplexe Prüfprozesse durchlaufen werden müssen – Stichwort VSA. Vor dem Hintergrund der besonders sensiblen Natur von Verschlusssachen erlangt der Aspekt der digitalen Souveränität in der VS-Kommunikation zusätzliches Gewicht. Für den

Aufbau einer VS-IT-Infrastruktur für eine ressortübergreifende VS-Kommunikation werden Produkte und Dienstleistungen von externen Software- und Hardwareanbietern benötigt. Dabei spielen vor allem die Dimensionen der Souveränität im Umgang mit Daten sowie der technologischen Souveränität in den Bereichen Software, Hardware und Architekturen wichtige Rollen. Folglich sind hohe Anforderungen nicht nur an die eingesetzten Produkte selbst zu stellen, sondern auch an deren Anbieter. Nationale Sicherheitsinteressen müssen auch bei der Kooperation mit externen Dienstleistern und Anbietern jederzeit gewahrt bleiben. Dabei ist eine Unabhängigkeit von Drittstaaten außerhalb der EU von zentraler Bedeutung und der Fokus wurde auf Unternehmen gesetzt, die überwiegend in Deutschland angesiedelt sind.

Welche Laufzeit erwarten Sie sich in etwa von der Lösung und welche Unterstützungsleistungen sollte secunet im laufenden Betrieb erbringen?

Wir als Dienstleister der Bundesverwaltung sowie Federführer der Bundesmaßnahme möchten natürlich unseren Bedarfsträgern eine sichere, langlebige und performante VS-IT bereitstellen. Daher verbringen wir ausschließlich VS-IT auf dem neusten Stand der Technik in unseren Kundenkreis. Die Endgeräte für VS-Kommunikation unterliegen einer Update-Fähigkeit, um dynamisch auf Veränderung reagieren zu können. Unsere Industriepartner stehen uns als verlässliche Partner für das weitere Product Development zur Verfügung.

Wie geht es konkret weiter, was sind die nächsten Schritte?

Nach der Betriebsfreigabe durch das BSI werden in 2022 nach einem definierten Rollout-Plan zunächst die Nutzer*innen der Behörden auf Leitungsebene mit der Lösung versorgt. Daran anschließend werden nach und nach alle Bundesbehörden an die Lösung angeschlossen. Parallel bauen wir in Kooperation mit dem ITZBund neue Rechenzentren auf, deren georedundantes Modell die Verfügbarkeit der Cloud gewährleistet. Ab 2024 wird mit der „Diplo-Version“ auch Partnern und Verbündeten in anderen Ländern eine Lösung für direkte geschützte Informationen zur Verfügung gestellt. Die letzte Ausbaustufe erfolgt 2025 mit der „Firmen-Version“ für die geheimschutzbetreute Wirtschaft. Bei der Skalierung der Lösung ist die Integrationsfähigkeit mit anderen Plattformen sehr wichtig. Um im Sinne der Nutzerfreundlichkeit Medienbrüche zu vermeiden, müssen automatisierte Schnittstellen zu den ressortinternen Netzen geschaffen werden, um eine nahtlose VS-Kommunikation zu realisieren.

Herr Dr. Egyedy, vielen Dank für das Gespräch.

DAS ROTE TELEFON DER NÄCHSTEN GENERATION

Im Rahmen der neuen VS-Kommunikation der Bundesverwaltung stellt secunet eine hochsichere Kommunikationslösung für den Desktop-Betrieb. Die Lösung lässt das klassische „rote Telefon“ für die geschützte Kommunikation wieder aufleben. Bei der modernen Version handelt es sich allerdings um einen gehärteten All-in-One-PC mit Hörer und Bildschirm für Sprach- und Videokommunikation. Das Gerät ist bis zur Geheimhaltungsstufe GEHEIM zugelassen und basiert auf dem SINA Communicator H. Die Zwei-Faktor-Authentisierung erfolgt mittels eines Krypto-Sticks, der über eine USB-Schnittstelle angeschlossen wird.

20 Jahre Biometrics Institute

Wie eIDs und Biometrie die Grenzkontrolle effizienter und sicherer gemacht haben

Elektronische Identitätsdokumente (eIDs) und die darin gespeicherten biometrischen Daten bilden die Grundlage für automatisierte Grenzkontrollen und die bequemen Passagierabfertigungsprozesse, wie wir sie heute kennen. Wie sind wir dorthin gekommen? Anlässlich des 20-jährigen Bestehens des Biometrics Institute blicken wir zurück auf die Entwicklungen der letzten zwei Jahrzehnte.

Die Erweiterung der etablierten optischen Sicherheitsmerkmale um eine elektronische Komponente ermöglichte es, biometrische Daten auf den Chips von eIDs zu speichern. Gleichzeitig schuf die Biometrie eine einzigartige Verbindung zwischen Dokument und Dokumenteninhaber*in. Dies führte nicht nur zu einer deutlich verbesserten Fälschungssicherheit, sondern ebnete auch den Weg für die biometriegestützte automatisierte Grenzkontrolle. Biometrische Daten in eIDs und der damit verbundene Nutzerkomfort gelten mittlerweile weltweit als selbstverständlich. Der Weg zum Erfolg war allerdings gewiss nicht immer leicht, und er erforderte unzählige Schritte.

Echter Mehrwert entsteht durch Interoperabilität

Das reine Vorhandensein biometrischer Daten in eIDs bringt noch keinen Mehrwert. Zusätzlich muss sichergestellt werden, dass eIDs an den Grenzen rund um den Globus akzeptiert und verarbeitet werden können. Die Verbindung zwischen eID und Inhaber*in mittels biometrischer Daten sorgt zwar für mehr Sicherheit, erfordert aber auch neue digitale Prozesse. Zwei Aspekte unterstreichen die Bedeutung der Interoperabilität:

- Der Markt für biometrische Technologien ist dynamisch: Es gibt viele Geräte und Hersteller sowie kurze Produktlebenszyklen.
- Es existiert eine ungeheure Vielzahl von eIDs: Mehr als 150 Staaten haben bislang über eine Milliarde eIDs ausgestellt.

Automatisierte Grenzkontrollsysteme (secunet easygates) am Flughafen Sofia, Bulgarien

Bei zahlreichen Interoperabilitätstests unterstützte secunet die Hersteller von eIDs und Prüfsystemen dabei, die Komponenten zu optimieren und für den internationalen Gebrauch tauglich zu machen. Diese Tests zeigten, wie wichtig die Kooperation zwischen Staaten, hoheitlichen Behörden und der Industrie ist. In Anbetracht des wachsenden Potenzials der Biometrie waren unabhängige Organisationen wie das Biometrics Institute für den Prozess unverzichtbar, um alle Stakeholder zu vernetzen und eine Plattform bereitzustellen, über die sowohl innovative Ideen als auch Bedenken ausgetauscht werden können.

Der Schlüssel liegt in der Standardisierung

Die grundlegenden Parameter für die Nutzung biometrischer Daten in eIDs sowie die Qualitäts- und Sicherheitsanforderungen für deren Einsatz in hoheitlichen Anwendungen wurden in Standards festgelegt und weiterentwickelt. Standards regulieren viele verschiedene Aspekte. Ein Schwerpunkt ist der Schutz biometrischer Daten über den gesamten Lebenszyklus hoheitlicher eIDs hinweg, zum Beispiel während der Dokumentenausstellung, in Bezug auf die Sicherheitsmechanismen und Zugriffsrechte während der Dokumentenprüfung sowie im Hinblick auf eine verantwortungsvolle Nutzung. Letzteres schließt eine angemessene und datenschutzkonforme Handhabung ein.

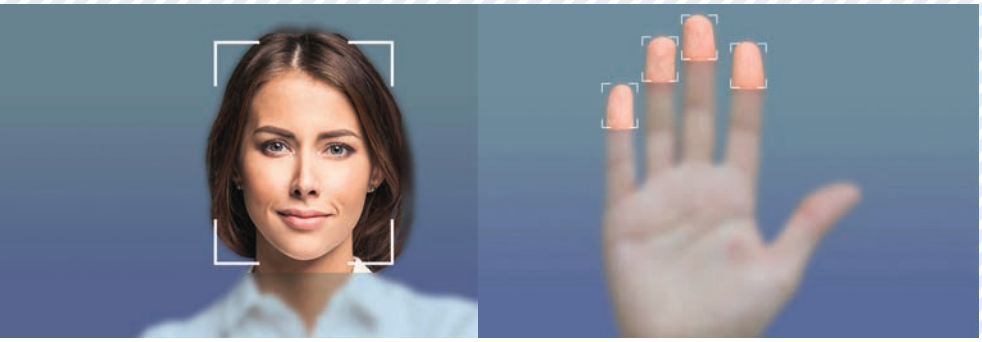
Einer der ersten bedeutenden Standards für automatisierte Grenzkontrollen war ICAO DOC 9303. Er bildete eine wichtige Voraussetzung für den umfassenden Einsatz von Biometrie in Anwendungen des öffentlichen Sektors und wird noch heute gewissermaßen als Goldstandard für eIDs angesehen.

Ein Meilenstein für den Schutz biometrischer Daten in hoheitlichen eIDs war sicher die Technische Richtlinie TR-03110 des Bundesamts für Sicherheit in der Informationstechnik, die auch heute noch Gültigkeit besitzt. secunet war an ihrer Entwicklung beteiligt. Die TR-03110 spezifiziert unter anderem die Erweiterte Zugangskontrolle (Extended Access Control, EAC) für den Zugriff auf die in eIDs gespeicherten biometrischen Daten. Sie kann als Fundament für alle Sicherheitsprotokolle für hoheitliche eIDs betrachtet werden und hatte überdies signifikanten Einfluss auf die Teile 10 und 11 von ICAO DOC 9303.

Standards sind weiterhin ein wichtiges Werkzeug für alle beteiligten Stakeholder, um gemeinsam ein konsistent hohes Sicherheitsniveau für den Umgang mit biometrischen Daten in eIDs umzusetzen – sowohl auf der Anwendungs- als auch auf der Technologieseite. Insbesondere bei biometrischen Systemen sorgt Standardkonformität auf allen Ebenen für Präzision und folglich für eine zuverlässige Nutzbarkeit. Wie wurden diese Standards entwickelt und was sind die Voraussetzungen dafür?

Umfangreiche Datenbasis

Eine Grundvoraussetzung für die Standardisierung sind Daten und Erfahrungswerte – dies ist eine unverrückbare Tatsache. Für den Einsatz von Biometrie in hoheitlichen eIDs mussten daher zunächst eine Unmenge von Daten erhoben werden. Biometrie-Kennern sind gewiss noch die Projekte



Für biometrische Verfahren werden u. a. Gesichtsbilder und Fingerabdrücke genutzt.

BioP I und II in Erinnerung: Gemeinsam mit dem deutschen Bundeskriminalamt führte secunet einen umfangreichen Praxistest am Frankfurter Flughafen durch und verglich die biometrischen Prüfalgorithmen (Gesicht, Fingerabdruck, Iris). Die Ergebnisse bildeten die Grundlage für die Auswahl der biometrischen Merkmale des elektronischen Reisepasses in Deutschland. Beide Studien waren der Auftakt für zahlreiche Folgeprojekte zur Untersuchung und Beurteilung biometrischer Verfahren, von denen der gesamte Markt in Form von Standards und technischen Richtlinien profitierte.

Diese Schritte – Datenerhebung, Standardisierung, Interoperabilität – waren wesentliche Schlüsselfaktoren für den heute üblichen, umfassenden Einsatz von Biometrie. Sie gewährleisten, dass sich die Daten zuverlässig und gemäß den Anforderungen im Hinblick auf Qualität, Sicherheit und Geschwindigkeit nutzen lassen.

Sichere eIDs im Alltag

Standards und die weltweite Verbreitung biometrischer Reisedokumente eröffneten ganz neue Möglichkeiten: Steigende Passagierzahlen konnten nun durch automatisierte Grenzkontrollen (Automated Border Controls, ABC) bewältigt werden. Abgesehen vom aktuellen Covid-bedingten Rückgang steigt die weltweite Nachfrage nach Biometrie bei der Grenzkontrolle und Passagieridentifikation.

So ist beispielsweise im Rahmen des deutschen EasyPASS-Projekts die Anzahl von ABC-Systemen von 70 genutzten eGates an vier Flughäfen im Jahr 2014 auf aktuell über 250 eGates an acht Flughäfen mit insgesamt 95 Millionen Benutzern angewachsen.

Bei der biometriegestützten automatisierten Grenzkontrolle spielt der Schutz vor betrügerischen Umgehungsversuchen eine wichtige Rolle. Aktuelle Standardisierungsanstrengungen und -entwicklungen konzentrieren sich darauf, die Verfahren zu optimieren, die Betrugsversuche erkennen und abwehren können. Dazu gehören Maßnahmen zur Erkennung sogenannter Präsentationsangriffe, etwa mit Masken (Presentation Attack Detection, PAD), oder zur Erkennung von Morphing-Angriffen (Morphing Attack Detection, MAD, siehe auch den folgenden Artikel in dieser secuview-Ausgabe).

Jede Menge Herausforderungen liegen vor uns

Biometrische Daten sind ein sensibles Gut, das es zu schützen gilt. Eine Vielzahl von Standards gibt vor, welche Daten erhoben, genutzt und gespeichert werden können. Dabei müssen Qualität, Sicherheit, Nutzbarkeit und Benutzerkomfort stets gegenüber den spezifischen Anwendungsbedürfnissen abgewogen werden. Die kontinuierliche Entwicklung von Standards ist entscheidend, um die aktuellen und künftigen Anforderungen an sichere biometrische Verfahren zu erfüllen und Versuche, diese zu umgehen, effektiv zu vereiteln. Neue Möglichkeiten, die sich beispielsweise durch Künstliche Intelligenz (KI) ergeben, werden hierbei eine entscheidende Rolle spielen – und bedeuten jede Menge Arbeit für das Biometrics Institute, secunet und andere wichtige Akteure der Biometrie-Gemeinschaft.

Das **Biometrics Institute** ist ein internationaler Verein, der zum Thema Biometrie Informationen, Schulungen, Forschung und ein Netzwerk von Experten bietet. Seine Mission liegt in der Förderung der verantwortungsbewussten und ethischen Nutzung biometrischer und damit verbundener Technologien, die den ethischen Grundsätzen des Instituts als unabhängiges und unparteiisches internationales Forum für Biometrie-Nutzer und andere interessierte Parteien entsprechen.

Das Institut wurde 2001 gegründet und stellt eine einzigartige Gemeinschaft von Stakeholdern dar, die rund um den Globus verteilt sind. Dazu gehören eine Vielzahl von Regierungsbehörden, Banken, Fluggesellschaften, Flughäfen, Biometrieexperten, Datenschutzexperten, Regulierungsbehörden, Zulieferern und Wissenschaftlern sowie internationalen Beobachtern wie Organisationen der Vereinten Nationen, EU-Institutionen und IGOs. Das Biometrics Institute bietet eine unparteiische und unabhängige Diskussionsplattform, die verschiedene Blickwinkel vereint, um eine ausgewogene Sicht auf die Biometrie zu gewinnen.

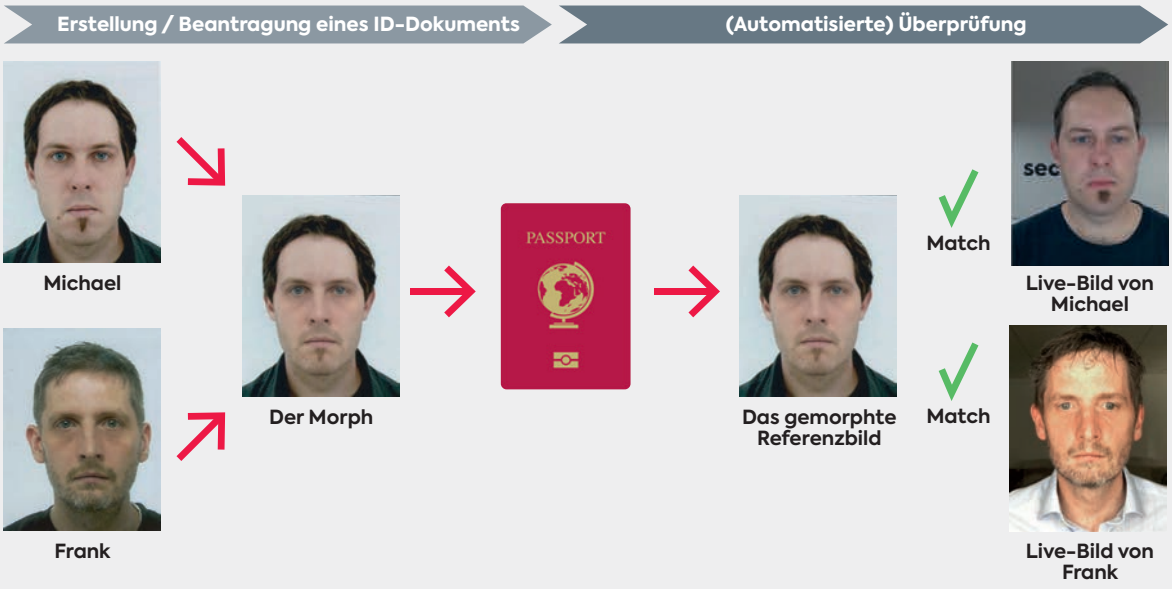
Schutz vor Identitätsbetrug bei der Grenzkontrolle

Mensch oder Morph?

Biometrie und Gesichtserkennung haben die Grenzkontrolle effizienter und sicherer gemacht. Doch es gibt Betrugsmethoden, die gleichermaßen für Grenzkontrollbeamt*innen und automatisierte Grenzkontrollsysteme eine Herausforderung darstellen. Dazu gehören vor allem die sogenannten Morphing-Attacken, bei denen die Angreifer Ausweisfotos einsetzen, die sie aus Gesichtsbildern mehrerer Personen zusammengesetzt haben. Nun gibt es einen Algorithmus, der solche Morphe mit hoher Zuverlässigkeit erkennt.

Die fiktiven Betrüger Michael und Frank verschmelzen mit einer guten Bildbearbeitungssoftware ihre biometrischen Passfotos zu einem einzigen Bild. Das Ergebnis ist ein Bild, das beiden Beteiligten ähnelt. Dieses manipulierte Bild nutzt Michael dann für seinen neuen Reisepass. Oberflächlich ist er als die Person auf dem Bild zu erkennen, daher schöpfen die Beamt*innen bei der Passerstellung keinen Verdacht. Mit seinem neuen Reisepass geht Frank dann zum Flughafen. Da der Morph gut gemacht ist, erkennt die Gesichtserkennungssoftware – oder der Mensch am Grenzkontrollschalter – ihn fälschlicherweise als die Person auf dem Bild, und identifiziert ihn folglich als Michael, den Inhaber des Reisepasses. Auf diese Weise kann Frank im hier beschriebenen Worst Case eine Grenze unter einer falschen Identität passieren.

Die Betrüger sind erfunden, aber der Tathergang ist durchaus real. Behörden aus verschiedenen Ländern haben bereits über Betrugsversuche mit Morphing berichtet, so etwa die slowenische Polizei. Der Grund für die Verbreitung dürfte sein, dass sich Morphe



So funktioniert ein Morphing-Angriff.

leicht umsetzen lassen. Es bedarf dafür keiner besonderen Expertise. Ein kommerzielles Bildbearbeitungsprogramm und ein wenig Talent genügen.

Sicherheitsfaktor Mensch

Zwar zeigen die Berichte über entdeckte Morphe, dass die Täter*innen überwiegend automatisierte Grenzkontrollsysteme ins Visier nehmen. Aber auch für Menschen stellt die Betrugsmethode eine Herausforderung dar. Untersuchungen zeigen, dass Personen im Durchschnitt nur etwa 60 Prozent der Morphe erkennen, die ihnen im Vergleich zu einem vertrauenswürdigen Bild gezeigt werden. Allerdings scheinen Menschen, die an einem solchen Test teilnehmen, im Verlauf der Untersuchung immer besser abzuschneiden. Wer sich also speziell mit dem Thema beschäftigt, erkennt später mitunter mehr Morphe.

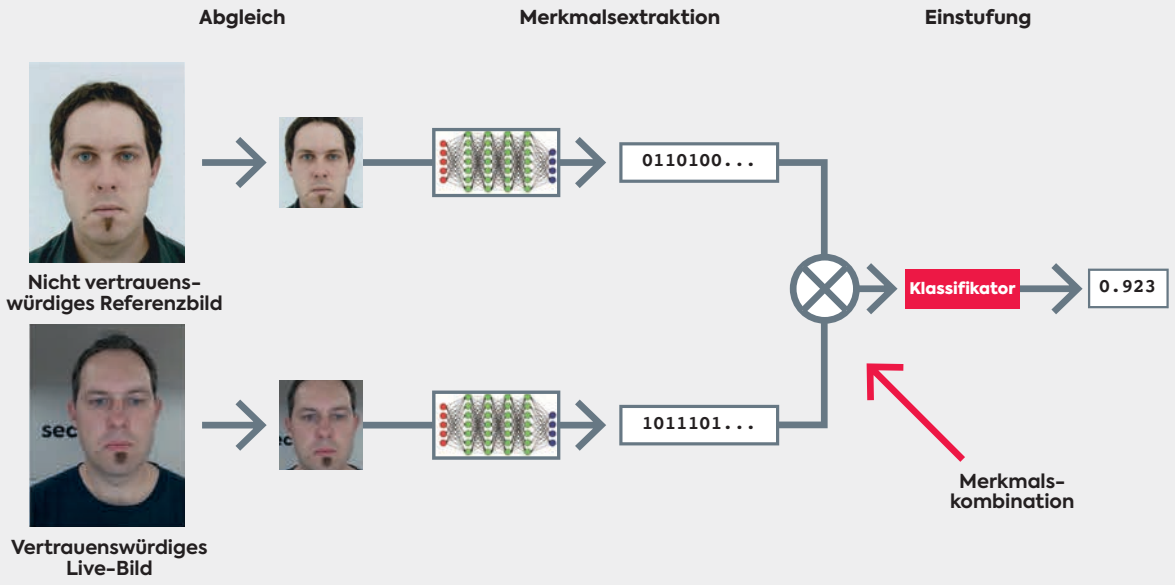
Erfassung unter Aufsicht

Trainings für Grenzkontrollbeamt*innen sind daher ein Weg, um das Problem einzudämmen. Ein anderer ist das sogenannte Live-Enrolment. Um dem Fälschen von Personenbildern in Ausweisdokumenten bereits bei der Erstellung vorzubeugen, können Behörden bei Identitätsdokumenten gänzlich auf Fotos verzichten, die die Antragstellenden selbst mitbringen. Stattdessen werden ausschließlich Bilder verwendet, die direkt vor Ort, also unter Aufsicht der Behörden, aufgenommen werden. Dies würde sicherstellen, dass keine Morphe mehr ihren Weg in die Ausweise finden. Das Problem dabei: Selbst wenn sich alle europäischen Staaten künftig auf ein solches Vorgehen einigen würden, wird es weltweit wohl immer Staaten geben, die selbst erstellte Ausweisbilder dulden. Daher wird Live-Enrolment die Morphing-Herausforderung nie vollständig lösen.

Eine Verbesserung der Situation ist allerdings von dem künftigen europäischen Einreise-/Ausreise-System (EES) zu erwarten: Bei der Einreise in die Länder des Schengen-Raums müssen sich Drittstaatsangehörige künftig mit vier Fingerabdrücken und Gesichtsbild registrieren lassen – und zwar direkt am Grenzübergang, per Live-Enrolment. Bei einer erneuten Einreise in den Schengen-Raum liegt dann nicht nur das Bild im Identitätsdokument vor, sondern auch ein vertrauenswürdiges Gesichtsbild in der Datenbank des EES. Wenn für die Bilderfassung hochwertiges Equipment wie die höhenverstellbare Gesichtsbildkamera secunet easytower verwendet wurde, lässt es sich ideal für die Grenzkontrolle im EES-Kontext nutzen.

Clevere Software

Eine weitere Sicherheitsmaßnahme sind Softwarealgorithmen, die Gesichtsmorphe bei der automatisierten Grenzkontrolle erkennen. Bereits seit einigen Jahren beschäftigen sich die Expert*innen von secunet mit Morphing Attack Detection (MAD). Genau genommen geht es dabei um „differenzielle“ MAD, womit gemeint ist, dass ein Gesichtsbild im Vergleich mit einem vertrauenswürdigen zweiten Bild geprüft wird. Beim automatisierten Grenzkontrollprozess ist eine solche vertrauenswürdige Datenquelle stets vorhanden, denn als Teil des Prozesses wird ein Live-Bild aufgenommen, das anschließend mit dem Bild im elektronischen Identitätsdokument verglichen wird. An dieser Stelle greift der Algorithmus



So arbeitet Morphing Attack Detection.

ein und erkennt gegebenenfalls Abweichungen. Voraussetzung ist, dass das Live-Bild hohen Qualitätsstandards entspricht.

Gemeinsam mit der Hochschule Darmstadt hat secunet nun einen neuen, noch wirksameren Algorithmus entwickelt.[1] Er hat sich bereits im laufenden Betrieb als alltagstauglich erwiesen. Wie bei anderen Algorithmen dieser Art lässt sich über einen Schwellenwert eine Feinabstimmung vornehmen. Stellt man ihn auf eine Falsch-Positiv-Rate von 2 Prozent ein – das heißt zwei von hundert Gesichtsbildern werden fälschlicherweise als Morphe klassifiziert und müssen manuell begutachtet werden –, erkennt der Algorithmus 85 bis 88 Prozent der tatsächlichen Morphe. Verglichen mit menschlichen Testpersonen und früheren Algorithmen ist das ein sehr guter Wert.

Portfolio mit Morphing-Schutz

Der neue Algorithmus findet im gesamten Grenzkontroll-Portfolio von secunet Anwendung. Dazu gehört neben dem automatisierten Grenzkontrollsystem secunet easygate zum Beispiel auch der Selbstbedienungskiosk secunet easykiosk für die einfache Vorerfassung von Passagierdaten und die Grenzkontrollapplikation secunet bocoa in Kombination mit der Gesichtsbildkamera secunet easytower. Diese Produkte und Lösungen liefern überdies Live-Bilder in der hohen Qualität, die notwendig ist, um sie als vertrauenswürdige Vergleichsbilder für differenzielle MAD nutzen zu können.

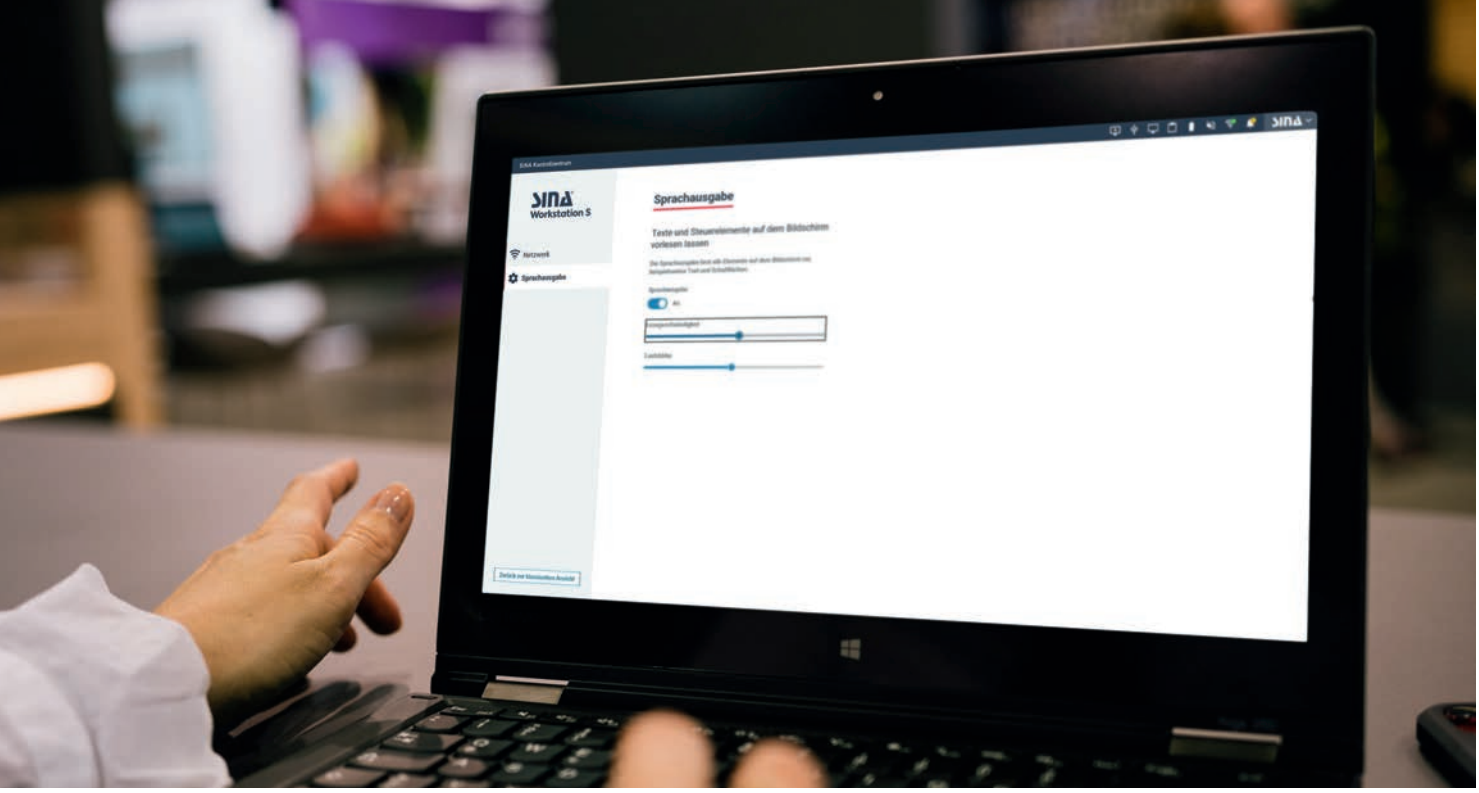
Der MAD-Algorithmus ergänzt weitere Sicherheitsmaßnahmen, über die das Grenzkontroll-Portfolio von secunet bereits verfügt. Das secunet easygate erkennt zum Beispiel mit hoher Zuverlässigkeit sogenannte Präsentationsangriffe, bei denen Betrüger*innen etwa mit Masken versuchen, eine falsche Identität vorzutäuschen.

Morphing-Erkennung, heute und in Zukunft

Durch den neuen Algorithmus ist die MAD innerhalb kurzer Zeit einen entscheidenden Schritt vorangekommen. Trotz dieses Fortschritts werden Morphing-Angriffe auf absehbare Zeit eine Herausforderung bleiben. Den Algorithmus gilt es daher ständig zu verbessern, zu erweitern und neu zu trainieren, um die Fehlerraten weiter zu reduzieren. Zudem kann softwarebasierte MAD nur ein Teil der Lösung sein. Deren andere Eckpfeiler sind Live-Enrolment und die Schulung von Grenzkontrollpersonal. Denn bei der Bekämpfung von Morphing kommt es auf Mensch und Maschine gleichermaßen an.

Michael Schwaiger
michael.schwaiger@secunet.com

[1] Die Methodik wurde in der folgenden Publikation erstmals beschrieben und anschließend von secunet weiterentwickelt: U. Scherhag, C. Rathgeb, J. Merkle, C. Busch: „Deep Face Representations for Differential Morphing Attack Detection“, in IEEE Transactions on Information Forensics and Security (2020).



Barrierefreie IT

Zugang für alle

Ist unsere Gesellschaft auf dem Weg zur Barrierefreiheit in der digitalen Welt bereits gut vorangekommen? Je nach Perspektive wird das unterschiedlich beurteilt. Einerseits gibt es immer mehr Gesetze und Vorgaben zu dem Thema und auch die Zahl der barrierefreien IT-Produkte und Dienste nimmt zu. Andererseits bleibt noch viel zu tun, Behindertenverbände kritisieren das Fortschrittstempo als zu langsam. secunet entwickelt derzeit eine barrierefreie Version der SINA Nutzeroberfläche. In dem Zusammenhang sprach secuview mit Robert Schäfer, Softwareentwickler beim Statistischen Bundesamt, der sich für Barrierefreiheit einsetzt und als einer von mehreren blinden Nutzer*innen das neue SINA User Interface getestet hat.

Herr Schäfer, wie beurteilen Sie den Stand der Barrierefreiheit in IT und digitalen Angeboten in Deutschland?

Robert Schäfer: Was die Bundesverwaltung angeht, ist aus der Perspektive der Betroffenen noch Luft nach oben. Vieles wird unter Zeitdruck umgesetzt und nicht konsequent zu Ende geführt. Nehmen wir das Beispiel E-Akte: Sie selbst ist barrierefrei, aber das Ablagesystem und die Workflows nicht.

In der Wirtschaft sind die Lücken noch größer. Onlinebanking zum Beispiel ist bisher kaum barrierefrei, teilweise kann man als Sehbehinderter nicht mal die Kundennummer eingeben. Es gibt nur zwei, drei Banken, die barrierefrei aufgestellt sind. Beim Onlineshopping ist die Situation uneinheitlich: Die Websites der großen Anbieter sind im Großen und Ganzen gut bedienbar, und teilweise gibt es Informationen und Hotlines zur Barrierefreiheit. Bei den kleineren dagegen ist das Thema oft schlicht nicht präsent. Dabei gibt es in Deutschland 10 Millionen Schwerbehinderte, wir sprechen also von einer großen Gruppe potenzieller Kunden.

Robert Schäfer

Seit dem Jahr 2000 ist Robert Schäfer beim Statistischen Bundesamt tätig und dort für Anwendungsentwicklung mit dem Schwerpunkt Barrierefreiheit zuständig. Er arbeitet seit 1991 im öffentlichen Dienst. Eine seiner früheren beruflichen Stationen war die Verwaltung des Deutschen Bundestags.

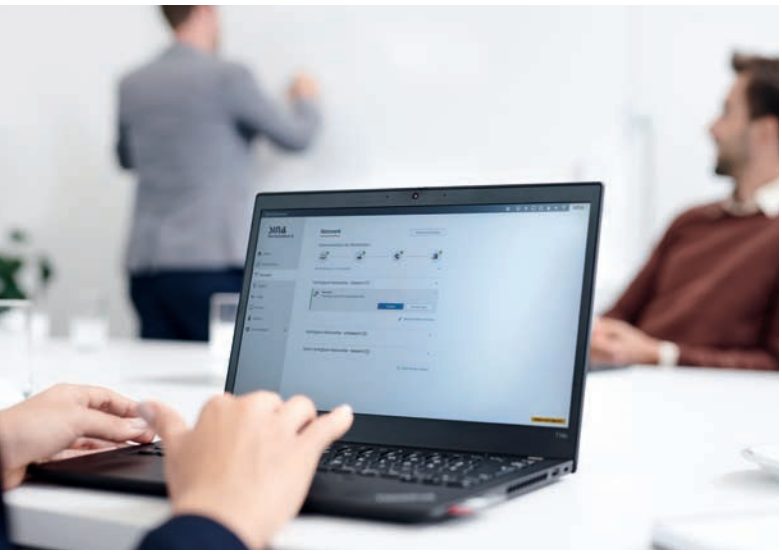
Robert Schäfer ist örtliche Vertrauensperson für die schwerbehinderten Beschäftigten des Statistischen Bundesamts in Bonn. Zudem ist er Gründungsmitglied der VSV Bund (Vereinigung der Schwerbehindertenvertretungen des Bundes) und dort Vorstandssprecher für IT-Angelegenheiten. Die VSV Bund vertritt die Interessen von schwerbehinderten Beschäftigten zahlreicher Bundesressorts und deren nachgeordneten Behörden.

Viele Menschen machen sich nicht klar, was fehlende Barrierefreiheit für die Betroffenen bedeutet: Sie werden von elementaren gesellschaftlichen Prozessen ausgeschlossen. Wir brauchen hingegen Zugang für alle. In den USA ist man übrigens deutlich weiter als hierzulande. Dort gelten auch für die Wirtschaft schärfere Gesetze in Bezug auf Barrierefreiheit.

Wie nutzen Sie die SINA Workstation?

Seit 2013 nutze ich sie in allen Lebenslagen. Ich bin Softwareentwickler. Das Tagesgeschäft läuft praktisch rund um die Uhr, dafür ist die SINA Workstation mein primäres Arbeitsgerät. Ich bin viel unterwegs und grundsätzlich kann ich die SINA Workstation überall nutzen, etwa um kleinere Programmierungen vorzunehmen. Da ich nicht sehen kann, gibt es aber unterwegs Einschränkungen. Das ist zum Beispiel der Fall, wenn das Gerät die Verbindung zum Netzwerk verliert. Die Netzwerk-Einstellungen sind für mich aktuell nicht bedienbar. Aber das ändert sich mit der neuen Version der SINA Nutzeroberfläche.

Ausblick auf die barrierefreie SINA Nutzeroberfläche, von der erste Funktionen bereits im ersten Quartal 2022 verfügbar sein werden.



Die Entwicklung der barrierefreien Version haben unter anderem Sie angestoßen. Wie war das genau?

Im Jahr 2017 habe ich bei einem SINA Expertentreffen Armin Wappenschmidt, der bei secunet für die SINA Workstation S verantwortlich ist, auf das Thema angesprochen. Mobiles Arbeiten wird ja immer wichtiger, da sollte es zumindest möglich sein, barrierefrei das Netzwerk einzustellen und die SINA Gastsystem-Sessions zu starten. secunet hat positiv auf mein Anliegen reagiert. Nun ist die neue Version der SINA Nutzeroberfläche fast fertiggestellt und ich habe an einem User-Test teilgenommen.

Wie laufen solche User-Tests ab?

Wir gehen vordefinierte Anwendungsfälle durch und probieren aus, wie gut sie sich bedienen lassen. Dann werden Rückfragen diskutiert. Nutzertests sind meiner Meinung nach aussagekräftiger als die verbreiteten BITV-Tests, bei denen nur die Punkte geprüft werden, die in der Barrierefreie-Informationstechnik-Verordnung (BITV) stehen. Ein gutes Ergebnis bei einem BITV-Test heißt noch nicht unbedingt, dass ein Angebot auch tatsächlich gut nutzbar ist.

Barrierefreiheit in IT und Telekommunikation (ITK) sollte einen gleichberechtigten Zugang für alle Menschen sicherstellen. Dies bedeutet, dass Nutzerschnittstellen und Informationen für Nutzer*innen wahrnehmbar, bedienbar, verständlich und robust gestaltet werden müssen. „Robust" bedeutet, dass Inhalte verlässlich abrufbar sind, egal welche Technologien (Browser, Hilfsmittel) die Nutzer*innen dafür einsetzen.

Barrierefreiheit in der ITK ist in der EU bereits heute teilweise verpflichtend: Websites, Apps, Intranets, Extranets und elektronische Verwaltungsabläufe sind von öffentlichen Stellen barrierefrei zu gestalten. Einheitliche Minimalforderungen hinsichtlich der Barrierefreiheit sind in der harmonisierten Europäischen Norm EN 301549 definiert. Deren Anwendung ist in Deutschland durch die Barrierefreie-Informationstechnik-Verordnung (BITV) 2.0 und das Behindertengleichstellungsgesetz (BGG) für die genannten Produkte und Dienstleistungen gesetzlich fixiert und bis spätestens Anfang 2022 umzusetzen.

Der „European Accessibility Act" (EAA) verpflichtet darüber hinaus erstmals nicht nur öffentliche Stellen, sondern auch Wirtschaftsakteure zu Barrierefreiheit. Das Barrierefreiheitsstärkungsgesetz (BFSG) ist seit Juli 2021 in Deutschland die gesetzliche Umsetzung des EAA. Da mitunter eine Übergangsfrist bis Mitte 2025 und zum Teil auch darüber hinaus vorgesehen ist, kritisierte der Deutsche Blinden- und Sehbehindertenverband e.V. (DBSV) das Gesetz allerdings als „unambitioniert".

Um welche Aspekte geht es im User Interface insbesondere? Wie gut wurden sie Ihrer Meinung nach bei SINA umgesetzt?

Entscheidend für Blinde und Sehbehinderte ist natürlich eine gute Sprachausgabe. Die ist bei SINA sehr gut gelungen. Wichtig ist auch eine logische Menüführung in Verbindung mit der Tastaturnutzung. Bei diesem Punkt haben wir im Test noch Verbesserungsbedarf festgestellt, der anschließend vom SINA Entwicklungsteam behoben wurde. Ein weiterer Aspekt ist, dass grundlegende Funktionen der SINA Nutzeroberfläche wie die Netzwerkeinstellungen bedienbar sein sollen. Das ist nun der Fall. Insgesamt wurden die wesentlichen Punkte implementiert, ich bin sehr zufrieden mit dem Ergebnis. Natürlich gibt es immer noch Dinge, die man verbessern könnte.

Was würden Sie sich noch wünschen?

Zum Beispiel ist es derzeit nicht möglich, tiefergehende Konfigurationen barrierefrei vorzunehmen, etwa bei den einzelnen Arbeitsplätzen. An dieser und einer Handvoll anderer Stellen würde ich mir für die Zukunft noch Verbesserungen wünschen. Aber verglichen mit dem früheren Zustand ist das Klagen auf hohem Niveau, grundsätzlich kann ich mit der SINA Workstation nun gut arbeiten.

Davon ließen sich auch andere überzeugen: Ich habe die SINA Workstation S bei der VSV Bund, der Vereinigung der Schwerbehindertenvertretungen des Bundes, vorgestellt. Die Reaktionen waren sehr positiv. Insbesondere in Zeiten der Pandemie löst die SINA Workstation ein großes Problem: Viele Kolleginnen und Kollegen können bisher kaum im Home Office arbeiten, weil es keine geeignete Technologie dafür gibt. Daher fahren sie entweder trotz Schwerstbehinderung ins Büro oder benötigen aufwändige Sonderlösungen. SINA ermöglicht sicheres mobiles Arbeiten ohne Sonderlösungen – und das jetzt fast ohne Einschränkungen.

Herr Schäfer, vielen Dank für das Gespräch!

Alexander Wölfel
alexander.woelfel@secunet.com

Für die SINA Workstation S wird derzeit eine barrierefreie Nutzeroberfläche entwickelt. Voraussichtlich im ersten Quartal 2022 wird eine erste Version verfügbar sein. Ergänzungen sind bereits geplant, künftig sollen möglichst alle Einstellungen für jeden bedienbar sein. Um die Barrierefreiheit nachzuweisen, wird nach deren vollständiger Umsetzung eine Konformitätserklärung nach BITV 2.0 angestrebt.

New Work und Kollaboration mit sensiblen Daten

Sicher in die neue Arbeitswelt

Unter dem Schlagwort „New Work“ war dezentrales, flexibles Arbeiten bereits seit Jahren auf dem Vormarsch, als die Pandemie im Jahr 2020 in vielen Organisationen schlagartig eine neue Form der Zusammenarbeit erzwang. Heute ist klar: Vieles davon wird bleiben. Ein zentrales Element der neuen Arbeitswelt sind Kollaborationsdienste, die Präsenzmeetings ganz oder teilweise ersetzen können. Der Umgang mit sensiblen oder eingestuften Daten ist dafür kein Hindernis, wie sichere Lösungen für Videokonferenzen, Messaging & Co. zeigen.

Arbeitszeiten werden immer flexibler organisiert, Unternehmen und Behörden wollen immer ortsunabhängiger agieren und das Home Office wird auch auf lange Sicht fester Bestandteil der Arbeitswelt bleiben. So stieg der Anteil der überwiegend im Home Office Tätigen laut Statista[1] während des ersten Lockdowns innerhalb kürzester Zeit von rund 4 auf 27 Prozent, fiel danach wieder und erreichte später, Anfang 2021, erneut einen Wert von 24 Prozent. In einer Umfrage des Bundesamts für Sicherheit in der Informationstechnik (BSI)[2] gaben bereits Ende des vergangenen Jahres 58 Prozent der Unternehmen an, ihren Mitarbeitenden auch nach der akuten Pandemie die Arbeit aus dem Home Office ermöglichen zu wollen.

Moderne Büro-IT hat für diesen Wandel den Boden bereitet. Kollaborationsdienste bieten den Rahmen für ein effektives Zusammenarbeiten auch ohne persönlichen Kontakt. Doch neben der erwünschten Flexibilität entstehen zugleich neue Angriffspunkte. Parallel zur Ausdehnung von Home-Office-Angeboten ist auch die Anzahl der Malware-Varianten weiter angewachsen. Das BSI[3] hat von Juni 2019 bis Mai 2020, also einschließlich der ersten Welle der Pandemie, einen Anstieg von mehr als 20 Prozent beobachtet.

VSA-konformer Kollaborationsarbeitsplatz

Dennoch müssen Sicherheitsbedenken die Einführung von Kollaborationsdiensten nicht ausbremsen. Seit Beginn der Pandemie hat secunet eine Vielzahl von Behörden, die mit eingestuften Daten umgehen und daher die Anforderungen der Verschlusssachenanweisung (VSA) umsetzen müssen, mit sicheren mobilen Arbeitsplätzen ausgestattet. Dabei kommt die Sichere Inter-Netzwerk Architektur (SINA) zum Einsatz. Als ganzheitliches Sicherheitssystem schützt sie nicht nur einzelne Komponenten, sondern die komplette digitale Infrastruktur.

[1] Statista 12. August 2021, Befragung zur Home-Office-Nutzung in der Corona-Pandemie

[2] Bundesamt für Sicherheit in der Informationstechnik 2020, Studie „IT-Sicherheit im Home-Office“

[3] Bundesamt für Sicherheit in der Informationstechnik 2021, Bericht zur Lage der IT-Sicherheit in Deutschland

Videokonferenzen aus dem Home Office ersetzen immer mehr physische Meetings.

SINA Lösungen sind nach Bedarf für verschiedene Geheimhaltungsgrade verfügbar. Ein zentraler Baustein vieler SINA Lösungen auf dem Schutzniveau des Geheimhaltungsgrads VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) ist der Client SINA Workstation S. Er bietet Anwender*innen trotz hoher Sicherheit einen Home-Office-fähigen digitalen Arbeitsplatz mit den üblichen Betriebssystemen und Softwareprodukten und unterstützt darüber hinaus eine sichere und moderne Zusammenarbeit über VoIP-Telefonie, Video und Messaging.

Digitale Meetings via Telefon und Videokonferenzen

Mit SINA können Meetings bequem ins Home-Office verlegt werden. VSA-konforme Telefonie mit Kolleg*innen ermöglicht der Voice-over-IP-Client, der standardmäßig als Softphone-Anwendung in der SINA Workstation S integriert ist. Auch Videokonferenzen werden unterstützt: Video-Clients können über dedizierte VPN-Kanäle in die interne Videoinfrastruktur geroutet werden. So werden die vorhandenen Bandbreiten optimal genutzt und Störungen bei der Bild- und Tonübertragung vermieden.

Die Architektur von SINA lässt es auch zu, dass Anwender*innen kommerzielle Tools wie Teams, Skype oder Zoom nutzen. Hierfür stellt die SINA Workstation S mit dem secunet Desktop einen eigenen, speziell für diese Zwecke optimierten Arbeitsplatz zur Verfügung.

Messaging ohne Sicherheitsbedenken

Mit dem sicheren Messenger stashcat können Mitarbeitende sich nicht nur via Chats sicher austauschen und vernetzen, sondern auch Kalenderfunktionen nutzen, Umfragen durchführen und Videokonferenzen umsetzen. Eine Dateiablage ermöglicht es, Dokumente in der Projektarbeit im Team oder bei Bedarf auch extern zu teilen. Alle Daten werden Ende-zu-Ende verschlüsselt und nach den Anforderungen der EU-Datenschutzgrundverordnung (DSGVO) verarbeitet. Der Messenger kann mit SINA in eine VS-Infrastruktur eingebunden werden.

Gemeinsam an eingestuften Dokumenten arbeiten

Für die Zusammenarbeit mit Verschlusssachen bietet die Lösung SINA Workflow das derzeit einzige durchgängig digitale Managementsystem: Mit wenigen Mausklicks lassen sich eingestufte Dokumente wie beispielsweise (hoch)sensible E-Akten sicher verteilen. Mit SINA Workflow können Nutzer*innen auf der SINA Workstation unter anderem Inhalte kollaborativ ausarbeiten, interne Abstimmungsprozesse mit Mitzeichnungen umsetzen sowie Dokumente sicher nach dem Prinzip „Kenntnis nur, wenn nötig“ weiterleiten.

Darüber hinaus lassen sich die Möglichkeiten der sicheren Kollaboration durch ergänzende Lösungen erweitern. Unternehmen und Behörden, die ihre sichere VoIP-Telefonie über die Grenzen des eigenen Netzes ausdehnen möchten, erhalten mit dem secunet SBC eine Lösung zur internen Netzkopplung und externen Netzanbindung. Für die hochsichere Sprach- und Datenkommunikation über IP-Netze bietet der SINA Communicator H eine passende Ergänzung zur SINA Workstation auf dem Schreibtisch. Dabei handelt es sich um ein modernes Endgerät im Telefonformat, das auch für hohe Geheimhaltungsstufen bis einschließlich GEHEIM zugelassen ist.

Ganzheitliche Sicherheit für eine neue Arbeitswelt

Moderne Kollaboration ist heute auch mit besonders schützenswerten oder eingestuften Daten möglich. Wie immer, wenn es um IT-Sicherheit geht, ist ein ganzheitlicher Ansatz ratsam. Dann können Cybersicherheit und New Work Hand in Hand gehen.

Aljona Wehrhahn-Aklender
aljona.wehrhahn-aklender@secunet.com

Ärztin im Patientengespräch per Telemedizin-Anwendung

Digitalisierung des Gesundheitswesens

Cloud für Krankenhäuser?

Im Interview: Torsten Redlich, stellvertretender Leiter der Division eHealth, secunet Security Networks AG

Welche Chancen halten Cloud-Lösungen für das Gesundheitssystem bereit?

Torsten Redlich: Aktuelle Gesetze und Investitionsprogramme des Bundes stellen derzeit die Weichen für die digitale Zukunft von Krankenhäusern und anderen medizinischen Einrichtungen. Die darin geforderten Konzepte bedeuten aber auch, dass zahlreiche Datenquellen miteinander verbunden werden müssen. Deshalb wird es nicht mehr ausreichen, Informationen in Betriebsstätten oder einzelnen Organisationen isoliert vorzuhalten. Vielmehr müssen Daten zunehmend zentralisiert bereitgestellt werden, was ohne Plattformkonzepte und Cloud-Technologien nicht umsetzbar ist. Hinzu kommen weitere Aspekte: Gesamtheitliche Cloud-Lösungen entlasten das IT-Personal, machen Datenverarbeitungsressourcen spontan abrufbar und ermöglichen es Gesundheitseinrichtungen, sich auf ihre Kern-IT zu konzentrieren. In der Forschung können kooperierende Institutionen gemeinsame Datenplattformen aufbauen. Eine entscheidende Rolle bei alldem spielt die IT-Sicherheit: Komplexe Lösungsansätze werden durch sie erst möglich, denn eine Voraussetzung ist, dass die Dateneigentümer jederzeit die Hoheit über ihre Informationen behalten.

Welche Fragen sollten sich Gesundheitseinrichtungen stellen, wenn sie Cloud-Lösungen implementieren wollen?

Zunächst einmal müssen sie sich die Frage stellen, welche Cloud-Lösungen überhaupt für sie zulässig sind. Die Gesetzgebung fordert zwar offene und verteilte Systeme, aber unter hohen Datenschutz- und IT-Sicherheitsauflagen. Das gilt insbesondere für Krankenhäuser, die als kritische Infrastrukturen eingestuft werden und demnach besonders hohen Sicherheitsstandards nachkommen müssen.

Ab wann genau diese Auflagen erfüllt sind, ist jedoch für die Einrichtungen selbst kaum ermittelbar – erst recht, wenn sie, wie für Krankenhäuser üblich, über wenig IT-Kapazitäten und Fachpersonal für solche Analysen verfügen. Auch deshalb benötigen medizinische Einrichtungen fertige Cloud-Lösungen, die umfassenden Compliance-Anforderungen „off the shelf" nachkommen.

Welche Lösungen bietet secunet, um die Anforderungen im streng regulierten Gesundheitssektor zu erfüllen und was muss ein gesamtheitliches Healthcare-Cloud-Konzept leisten können?

Es ist entscheidend, Sicherheit in den Cloud-Infrastrukturen auf allen technischen Ebenen mitzudenken. Das bedeutet unter anderem, dass bereits die Hardwarebasis abgesichert wird und die darauf aufbauende Virtualisierungstechnologie von Grund auf sicher konzipiert ist – Stichwort „Security by design". Wir von secunet setzen zudem seit Jahrzehnten auf offene Standards und Open Source. Zum einen erleichtert dies Prüfstellen und Normensetzern die Arbeit, zum anderen begeben sich Nutzer nicht in Abhängigkeit eines einzelnen Herstellers. Das gilt auch für das von uns mitentwickelte sichere Cloud-Betriebssystem SecuStack. Darin kommen transparent integrierte kryptographische Mechanismen und zahlreiche Sicherheitsmodule zum Einsatz. Speziell für den Gesundheitssektor ergänzen wir Maßnahmen wie Confidential Computing für besondere Datenklassen, Revisionssicherheit beim Einsatz von Machine Learning bzw. Datenanalyse oder auch die Anbindung an staatliche Gesundheitsdienste. So lassen sich vollumfängliche „Trusted Cloud Infrastrukturen" für medizinische Einrichtungen umsetzen.

Warum schreitet der Wandel von On-Premises-Modellen hin zu flexiblen Software as a Service-Konzepten weiter voran?

Zum einen steigt der Bedarf nach Cloud-Lösungen, um fehlende IT-Ressourcen und -Experten im Gesundheitsbereich auszugleichen. Zum anderen ist es herausfordernd, On-Premises-Lösungen mit den erforderlichen Security- bzw. Privacy-Funktionen dauerhaft auf dem Stand der Technik zu betreiben. Mit Cloud-Technologien können neue Anwendungen und geförderte Vorhaben zügig umgesetzt werden. Es gibt aber noch weitere Vorteile: Im Gegensatz zu lokalen Nutzungsmodellen bilden sich bei Cloud-Ansätzen keine Informationssilos in den einzelnen Einrichtungen. Stattdessen fördern sie den Informationsaustausch und machen die Datentöpfe über diverse Schnittstellen zugänglich. Letztendlich ist es auch unvorteilhaft, die zwingend notwendige kontinuierliche Weiterentwicklung der Software über hunderte verteilte sowie teils sehr verschiedene On-Premises-Lösungen zu realisieren. Das kostet nicht nur viel Zeit und Geld, sondern hat auch sicherheitsbedingte Nachteile. Demgegenüber kann ein ganzheitlich konzipierter Cloud-Ansatz IT-Sicherheitsaspekte durchaus positiv beeinflussen. Die Erfahrung zeigt: Beweisen sich neue Technologien unter hohen Compliance-Forderungen und überspringen die formalen Hürden, wird sich eine schnelle Verbreitung einstellen.

Torsten Redlich
torsten.redlich@secunet.com

Hochsichere multimediale Kommunikation im militärischen Umfeld

Was hat Logistik mit GEHEIM-Videokonferenzen zu tun?

Videotelefonie und Videokonferenzen sind heute alltäglich, fast jeder von uns nutzt sie beruflich und privat. Gerade die letzten beiden Jahre haben dieser Kommunikationstechnologie einen enormen Schub gegeben. Auch bei militärischen Organisationen wie der Bundeswehr sind Videokonferenzen mit vielen Teilnehmer*innen und hohen Datenmengen heute Standard, ob im Feldlager, im Einsatzgebiet oder bei multinationalen Verbänden. Dabei kommt es nicht nur auf hohe Sicherheit an, sondern auch auf Alltagstauglichkeit. SCOTTY und secunet haben nun eine Lösung entwickelt, die im Gegensatz zu vielen anderen modular nutzbar ist und in praktischen Flight Cases verschickt werden kann.

Lagebesprechungen im Einsatzführungskommando, strategische Abstimmungen zwischen Generälen und dem Bundesministerium der Verteidigung, die regelmäßige Kommunikation zwischen Gefechtsständen und Standorten der Bundeswehr – für solche und andere Einsatzszenarien haben sich Videokonferenzen im militärischen Umfeld etabliert und bewährt. Da eingestufte Informationen bis einschließlich GEHEIM im Spiel sind, müssen die eingesetzten Lösungen den entsprechenden Anforderungen der Verschlusssachenanweisung (VSA) genügen. Dafür ist hochwertige Verschlüsselungstechnologie erforderlich, zusätzlich soll beste Audio- und Videoqualität gegeben sein.

Aus den hohen Sicherheitsanforderungen ergeben sich einige praxisrelevante Herausforderungen. Die meisten Videokonferenzlösungen, die heute im GEHEIM-Umfeld im Einsatz sind, müssen aufwändig als Ganzes im Hinblick auf ihre Abstrahleigenschaften zoniert und vermessen werden, um elektronische Abhörangriffe auszuschließen. Dass die Komponenten gängiger kommerzieller Lösungen nicht individuell vermessen werden können, liegt an deren Kupferverkabelung. Ersetzt man eine Komponente und verkabelt das Gesamtsystem, können sich dessen Abstrahleigenschaften ändern. Daher muss das System bei Ausfall einer Komponente

SINA H-gesicherte Videokonferenzanlage, gut transportabel in Flight Cases verpackt

komplett ausgetauscht oder nach Reparatur neu vermessen werden. So entstehen mitunter wochenlange Ausfallzeiten, ein hoher Serviceaufwand und, je nachdem wo das System sich befindet, zusätzlich ein sehr hoher logistischer Aufwand.

Daher haben secunet und SCOTTY eine Lösung entwickelt, die unter anderem diese Herausforderungen adressiert. Sie vereint die bewährte Sicherheit von SINA mit hochentwickelter Videokonferenztechnik von SCOTTY in einem ganzheitlichen All-in-One System und ist speziell auf die logistischen Anforderungen der Bundeswehr zugeschnitten. Als Basis für den sicheren Video- und Datenaustausch dienen die integrierten Komponenten SINA Workstation H Client IIIa und SINA L3 Box H. Sie ermöglichen die Bearbeitung und Übertragung klassifizierter Daten mit einer Einstufung bis einschließlich GEHEIM/NATO SECRET. Die Videokonferenz-Komponenten sind darauf ausgelegt, auch unter widrigen Umständen und in großen Räumen mit vielen Teilnehmer*innen eine hohe Video- und Audioqualität sicherzustellen.

Innovativer modularer Abstrahlschutz

Der besondere Vorteil der neuen Lösung ist die innovative modulare Systemarchitektur, welche je nach Anwendungsfall eine Zusammenstellung vielseitiger Videokonferenz-Konfigurationen ermöglicht. Grundsätzlich werden alle Systeme in sogenannten Flight Cases geliefert. Damit lassen sich die Videokonferenzsysteme leicht an ihre vorgesehenen Standorte bringen oder bei Bedarf hin- und hertransportieren. So ist es zum Beispiel einfach, einen Anlagenpool für Auslandseinsätze und Spezialkräfte vorzuhalten und im Einsatzfall sofort zu versenden. Neben dem Schutz der Komponenten dienen die Flight Cases während des Betriebs auch als Fuß der Monitore und Audio-Komponenten. Am Aufstellungsort angekommen müssen lediglich die Flight Cases geöffnet und die Videokonferenzmodule mit optischen Netzwerkkabeln untereinander verbunden werden.

Diese Glasfaser-Verkabelung ermöglicht einen Datenaustausch bei gleichzeitiger galvanischer – also elektrischer – Trennung. Dadurch und durch die individuelle Zonierung aller Komponenten entsteht eine große Flexibilität und ein logistischer Mehrwert. Da nicht das Gesamtsystem vermessen werden muss, können nach Belieben Komponenten entnommen oder ausgetauscht werden – zum Beispiel im Servicefall oder um die Konfiguration zu ändern. Fällt zum Beispiel ein Monitor aus, kann dieser schnell durch ein Austauschgerät aus dem Depot ersetzt werden und das Videokonferenzsystem bleibt einsatzbereit.

Die **SCOTTY Group Austria GmbH** ist ein Lösungsanbieter für Video-, Audio- und Datenkommunikation für Anwendungen in der Luftfahrt, im maritimen Sektor sowie für den Land-mobilen Bereich.

SCOTTY wurde 1993 gegründet und ermöglicht Audio-, Video- und Datenübertragung, wo es keine Infrastruktur gibt: im Feldeinsatz, in Landfahrzeugen, in Schiffen und in der Luft. SCOTTY hat spezielle Erfahrung und Know-how in der Bereitstellung von Lösungen für kritische Anwendungen unter schwierigsten Bedingungen. Internationale Konzerne, friedenserhaltende Kräfte, Grenzpolizei und Katastrophenschutzbehörden setzen SCOTTY Equipment derzeit in den entlegensten und schwierigsten Umgebungen der Welt ein. SCOTTYs langjährige Erfahrung mit Satellitenkommunikation (SatCom) und seine umfangreiche Expertise im Bereich hochsicherer IT-Infrastruktur sorgen für optimierte Kommunikationslösungen, die individuell angepasst und für eine Vielzahl von Anwendungen eingesetzt werden können.

Die Abteilung Forschung & Entwicklung, die Produktion und der operative Hauptsitz von SCOTTY befinden sich in Graz, Österreich.

Flexibel konfigurierbar, von portabel bis teilmobil

Für das System sind mehrere Standard-Setups vorkonfiguriert, die sich jederzeit erweitern oder ändern lassen. Das portable Setup kommt ohne eigenen Bildschirm aus und nutzt stattdessen Equipment, das am Betriebsort bereits vorhanden ist. Diese Konfiguration kann bei Bedarf zum Beispiel zu einem teilmobilen Setup mit ein oder zwei Bildschirmen ausgebaut werden. Auch ein Beamer lässt sich zusätzlich anschließen, wodurch Videokonferenzen mit wesentlich mehr Teilnehmer*innen realisiert werden können.

Diese Flexibilität führt zu einer massiven Erhöhung der Verfügbarkeit des Videokonferenzsystems und ist die Basis für eine Einsatzbereitschaft rund um die Uhr. Künftig soll das System sogar noch flexibler werden: Geplant ist eine Anbindungsmöglichkeit für die SINA Workstation H und den SINA Communicator H. Dann können auch individuelle Arbeitsplätze sicher in das Videokonferenzsystem integriert werden.

Andreas Schmidt
andreas.schmidt@secunet.com

Das SINA H-gesicherte Videokonferenzsystem im portablen Setup (links) und in der teilmobilen Konfiguration mit zwei Bildschirmen (rechts)

Cyber-Hochsicherheit

Modern arbeiten auch im GEHEIM-Umfeld

„Wenn hohe Geheimhaltungsstufen im Spiel sind, leiden Performance und Usability“ – diese Meinung hält sich hartnäckig, schließlich muss bei der Digitalisierung von Prozessen mit Verschlusssachen (VS) der Einstufungen VS-VERTRAULICH oder GEHEIM eine Vielzahl spezieller Vorgaben berücksichtigt werden. Doch aktuelle Technologie zeigt, dass sich ein moderner digitaler Arbeitsalltag mit Videokonferenzen, Kollaboration und dergleichen auch im Hochsicherheitsbereich umsetzen lässt. Mit der SINA Workstation H Client V stellt secunet eine All-in-One-Lösung vor, die Leistungsfähigkeit, Ergonomie und Praxistauglichkeit mit einer Zulassung bis einschließlich GEHEIM verbindet. Konzipiert wurde sie mit Blick auf die digitalen Arbeitsprozesse bei modern aufgestellten Streitkräften wie der Bundeswehr sowie bei Behörden mit höchsten Sicherheitsanforderungen.

Als unmittelbar nach der Jahrtausendwende die ersten SINA Lösungen entwickelt wurden, lag das Augenmerk unangefochten auf dem Sicherheitsaspekt. Es ging vor allem darum, mit hochentwickelter Verschlüsselungstechnologie eine sichere Netzinfrastruktur aufzubauen, um VS hoher Einstufungen erstmalig über potenziell unsichere Netze wie das Internet zu übermitteln. Die ersten SINA H Endgeräte waren festplattenlose Terminals. Gleichzeitig wünschten sich die Hauptanwender*innen einen vollständigen PC bzw. Fat Client, an dem sie mit ihren gewohnten Softwareanwendungen und Betriebssystemen arbeiten konnten. Deshalb wurde die SINA Workstation entwickelt, die damals noch Virtual Workstation hieß.

Damit begann auch eine kontinuierliche Evolution hin zu mehr Nutzerfreundlichkeit. Die SINA Workstation H erlaubt es, Informationen unterschiedlicher Sicherheitseinstufungen – bis einschließlich GEHEIM – parallel auf einer Hardware zu bearbeiten. Wer zuvor für Büro-IT und eingestufte Daten zwei unterschiedliche Hardwaresysteme nutzen musste, lernt diese Funktionalität schnell zu schätzen. Bei Rollout und Administration großer SINA Installationen helfen automatisierte Tools, auch das erhöht die Praxistauglichkeit.

Die SINA Workstation H Client V im Einsatz, hier in Dual-Monitor-Konfiguration

Lange Erfolgsgeschichte

Im Laufe des vergangenen Jahrzehnts verbreitete sich die SINA Workstation H schnell. In der Gerätevariante Client III dient sie zum Beispiel als hochsicheres Endgerät im Programm „Harmonisierung der Führungsinformationssysteme" (HaFIS) der Bundeswehr. SINA Systeme bilden den IP-Krypto-Backbone der Bundeswehr, das heißt sie werden in großem Umfang dazu eingesetzt, eingestufte Daten sicher zu bearbeiten, zu speichern und über IP-basierte Netzwerke zu übertragen. Erst im Sommer 2021 verlängerte das Bundesamt für Ausrüstung, Informationstechnik und Nutzung der Bundeswehr (BAAINBw) den Rahmenvertrag für die Lieferung und Betreuung von SINA Technologie.

Unterdessen geht die Evolution weiter. Wieder sind neue Nutzerbedarfe entstanden, die überwiegend der regulären, ungeschützten Office-IT entstammen. Funktionen wie Videokonferenzen, Kollaboration und Telefonie sollen nach dem Wunsch vieler Anwender*innen auch im GEHEIM-Kontext zur Verfügung stehen. Mit der neuen SINA Workstation H Client V ist es gelungen, diese neuen Anforderungen zu integrieren – und in ein stimmiges Gesamtkonzept zu überführen. Neben der bereits vorhandenen GEHEIM-Zulassung sind entsprechende internationale Zulassungen (NATO und EU) in Planung.

„Durch den Austausch mit unseren Kunden wissen wir, dass der Wunsch nach modernem, effizientem Arbeiten mittlerweile auch im Hochsicherheitsbereich recht weit oben auf der Prioritätenliste steht", sagt Merlin Gräwer, Senior Produktmanager bei secunet. „Daher haben wir uns bei der neuen SINA Workstation H Client V neben der Sicherheit auf optimale Nutzerfreundlichkeit konzentriert. Für viele, die mit hoch eingestuften Informationen umgehen, ist Effizienz am Arbeitsplatz noch keine Selbstverständlichkeit. Das wollen wir ändern."

Kompaktes Gerätedesign

Dieses Ansinnen zeigt sich schon allein darin, dass die Lösung alle Funktionalitäten in einem einzigen kompakten Desktop vereint. Die Client-Hardware ist komplett in das Primär-Display integriert. Dies hilft, den Arbeitsplatz kabelfreier und aufgeräumt zu halten, und verbessert die Ergonomie: Zum Beispiel befinden sich sämtliche Steckplätze für Smartcards und USB-Geräte alle vorn und somit direkt in Griffweite der Nutzer*in. Mit seinen zahlreichen Schnittstellen lässt sich der Client flexibel in heterogene

Die SINA Workstation H Client V in Dual-Monitor-Konfiguration

Netzwerkinfrastrukturen integrieren. Auch ein lokaler Drucker oder Scanner kann angeschlossen werden. Das brillante, verstellbare TFT-Display erlaubt ermüdungsfreies Arbeiten mit hoher Auflösung und klarem Bild. Darüber hinaus beweist das Produktdesign, dass auch ein Hochsicherheits-Client optisch ansprechend sein kann.

Ein Faktor, der die Alltagstauglichkeit enorm erhöht, ist die hohe Leistungsfähigkeit. Trotz der aufwändigen Sicherheitsmaßnahmen, die größtenteils im Hintergrund ablaufen, können Nutzer*innen auf flüssige Performance zählen. Dies macht sich zum Beispiel beim parallelen Betrieb mehrerer Gastsysteme bemerkbar. HD-Videos laufen performant und moderne Anwendungen wie Web- bzw. Videokonferenzen und Kollaboration sind problemlos umsetzbar – auch im Zusammenspiel mit dem hochsicheren Multikrypto-Telefon SINA Communicator H, das ebenfalls bis einschließlich GEHEIM zugelassen ist.

Für Einsatzszenarien, in denen ausschließlich Daten bis zur mittleren Geheimhaltungsstufe VS-VERTRAULICH verarbeitet werden, ist der neue Client in der Variante SINA Workstation E Client V verfügbar.

„Wir sind überzeugt, dass wir IT-Beauftragten mit Modernisierungsvorhaben im Hochsicherheitsbereich genau die richtige Lösung anbieten können“, so Gräwer. „Auch für Zukunftssicherheit ist gesorgt: Mit künftigen Updates wollen wir den neuen Client Post-Quanten-Kryptographie-fähig machen – was der SINA Communicator H übrigens schon ist. Insgesamt fügen wir mit diesen beiden Produkten unserer langen, erfolgreichen Geschichte im GEHEIM-Umfeld ein neues Kapitel hinzu.“

Merlin Gräwer

info@secunet.com

Hier finden Interessierte technische Informationen zur SINA Workstation E/H Client V:

https://www.secunet.com/loesungen/sina-workstation-e/h-client-v

5G-Studie

Wie sicher ist das offene Funkzugangsnetz (O-RAN)?

Im Mobilfunk nutzt die Mehrzahl der Hersteller von Komponenten für das Funkzugangsnetz (Radio Access Network, RAN) derzeit proprietäre Schnittstellen und Funktionen. Die mangelnde Interoperabilität hat dazu geführt, dass die Mobilfunknetzbetreiber stark von einzelnen Herstellern und deren Produkten abhängig sind. Daher gibt es Bestrebungen zu mehr Modularität und damit auch Interoperabilität. Ziel ist das Open-RAN, kurz O-RAN, bei dem die einzelnen Komponenten vollständig interoperabel sind. Um einen Standard nach diesem Konzept festzulegen und zu etablieren, gründeten führende Mobilfunkanbieter die O-RAN Alliance, in deren Rahmen bereits eine Umsetzung spezifiziert wurde.

Ist das O-RAN in dieser Form mit Sicherheitsschwächen verbunden? Dieser Frage geht eine Studie nach, die im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI) vom Barkhausen Institut und der Firma AI Networks in Zusammenarbeit mit secunet erstellt wurde. Die Autor*innen stellen fest, dass von einer Vielzahl der für das O-RAN spezifizierten Schnittstellen und Komponenten mittlere bis hohe Sicherheitsrisiken ausgehen. Daher sollten jetzt Sicherheitsverbesserungen in den Standardisierungsprozess eingebracht werden. Die Studienautor*innen haben einige Vorschläge dazu formuliert. secunet wird diesen Prozess mit seiner Expertise begleiten, da diese Infrastrukturen kritisch und besonders schutzbedürftig sind.

Die Studie können Interessierte auf der secunet Website herunterladen:

https://www.secunet.com/5G

Axel Deininger zum neuen Chairman der ECSO gewählt

Axel Deininger, Vorstandsvorsitzender der secunet Security Networks AG, wurde am 27. Oktober 2021 zum neuen Chairman der European Cyber Security Organisation (ECSO) gewählt. Er wird künftig als Vorsitzender des Board of Directors die Interessen des Verbands und seiner Mitglieder insbesondere bei den EU-Institutionen vertreten. Er folgt damit auf Phillipe Vannier, der als Vertreter des französischen börsennotierten IT-Dienstleisters ATOS zuvor als Chairman der ECSO fungierte.

„Ich freue mich über meine Wahl und die große Zustimmung aus dem Board of Directors", sagt Axel Deininger. „IT-Sicherheit ist Grundvoraussetzung für eine erfolgreiche Digitalisierung. Daher ist es entscheidend, das europäische IT-Sicherheits-Ökosystem, das sich in der Mitgliedschaft der ECSO widerspiegelt, weiter zu stärken, um so die gesetzten Ziele in enger Zusammenarbeit mit den europäischen Institutionen und öffentlichen Einrichtungen zu erreichen."

secunet ist Gründungsmitglied der ECSO, die im Juni 2016 unter dem damaligen EU-Kommissar Günther Oettinger als sogenannte contractual Public-Private Partnership (cPPP) im Bereich Cybersecurity gegründet wurde, um die Zusammenarbeit zwischen dem öffentlichen und dem privaten Sektor zu fördern.

Seit der Gründung engagiert sich secunet aktiv in den verschiedenen Maßnahmen, Vorstands- und Arbeitsgremien der ECSO, wie beispielsweise bei den Startup-Veranstaltungsreihen „ECSO Cyber Investor Days" oder in der Initiative „Women4Cyber". Axel Deininger ist 2020 ins Board of Directors der ECSO gewählt worden und hat die Organisation seitdem bei zahlreichen Anlässen bereits offiziell vertreten.

Luigi Rebuffi, Generalsekretär der ECSO (links), gratuliert Axel Deininger zu seiner Wahl zum Chairman der Organisation.

Die European Cyber Security Organisation (ECSO) ASBL ist eine vollständig eigenfinanzierte, gemeinnützige Organisation nach belgischem Recht, die im Juni 2016 gegründet wurde. ECSO ist der privilegierte Partner der Europäischen Kommission für die Umsetzung der öffentlich-privaten Partnerschaft für Cybersicherheit. ECSO vereint die öffentlichen und privaten Akteure der europäischen Cybersicherheit, darunter große Unternehmen, KMU und Start-ups, Forschungszentren, Universitäten, Endnutzer und Betreiber kritischer Infrastrukturen, Cluster und Verbände sowie lokale, regionale und nationale öffentliche Verwaltungen in den Mitgliedstaaten der Europäischen Union (EU), der Europäischen Freihandelsassoziation (EFTA) und assoziierten Ländern des Programms H2020.

Weitere Informationen unter: https://ecs-org.eu/

secunet erhält das ECSO-Label „Cybersecurity made in Europe“

Zur digitalen Souveränität europäischer Behörden und Unternehmen gehört es, beim Umgang mit sensiblen Informationen unabhängiger von den weltweit dominanten IT-Anbietern zu werden. Daher hat die European Cyber Security Organisation (ECSO) das Label „Cybersecurity made in Europe“ ins Leben gerufen. secunet ist qualifizierter und geprüfter Träger dieses Labels. Ausgestellt wurde es durch das europäische Kompetenzzentrum für Sicherheit in der Informationstechnologie, eurobits e. V.

Das Label dient dazu, die internationale Sichtbarkeit europäischer IT-Sicherheitsunternehmen zu erhöhen sowie die Vertrauenswürdigkeit ihrer Produkte und Dienste zu bestätigen. Um es zu erhalten, müssen Anbieter einer Reihe von Kriterien entsprechen: Unter anderem müssen sie eine europäische Besitzstruktur aufweisen und Sicherheitsanforderungen der Agentur der Europäischen Union für Cybersicherheit (ENISA) erfüllen.

Sichere digitale Infrastrukturen sind maßgeblich für die Entwicklung digitaler Souveränität. Nur wer weiß, wo seine Daten oder Anwendungen gespeichert sind und wer darauf zugreifen kann, behält die Hoheit darüber und kann sich ausreichend vor Cyberkriminalität oder Spionage schützen. Auf europäischen Standards beruhende Siegel wie „Cybersecurity made in Europe“ tragen dazu bei, europäische digitale Souveränität herzustellen und allen Nutzer*innen Lösungen zu bieten, die den hohen europäischen Anforderungen entsprechen.

CYBERSECURITY™
MADE IN EUROPE

Initiated by ECSO. Issued by eurobits e.V.

Das von der ECSO initiierte Label wird durch autorisierte Organisationen auf lokaler Ebene verliehen. In Deutschland ist der eurobits e.V. die einzige Vergabestelle. Im Verein eurobits, der 1999 in Bochum gegründet wurde, arbeiten führende Forschungsinstitute, etablierte Unternehmen der Branche sowie junge Wachstumsunternehmen zusammen und sorgen für einen Transfer zwischen Wirtschaft und Wissenschaft im Bereich IT-Sicherheit und Informationssicherheit.

Nachwuchsförderung

Deutschland ist Europameister bei der European Cyber Security Challenge

Vom 28. Oktober bis zum 1. November hat die deutsche Nationalauswahl der Cyber Security Challenge Germany (CSCG) erfolgreich am Finale der European Cyber Security Challenge in Prag teilgenommen. Nach zwei spannenden Wettkampftagen belegte sie den ersten Platz, dicht gefolgt von Polen auf dem zweiten und Italien auf dem dritten Platz.

Die CSCG ist ein deutschlandweit ausgetragener Wettbewerb für junge IT-Security-Talente. In einer Online-Qualifikation treten dazu bis zu 1.600 Teilnehmende gegeneinander an. Die Besten dieser jungen Hacker und Hackerinnen werden anschließend zu einem deutschen Finale eingeladen, in dem sie sich in jeweils zwei Alterskategorien gegeneinander messen.

Die European Cyber Security Challenge 2021 konnte trotz der Corona-Pandemie in Prag stattfinden.

Die Aufgabenfelder erstrecken sich über die Themengebiete Binary Analysis, Reverse Engineering, Kryptografie, Web Exploitation, Steganografie und Game Hacking.

Veranstaltet wird der Wettbewerb von dem im Jahr 2020 gegründeten Verein Nachwuchsförderung IT-Sicherheit e. V. mit Sitz in Bochum. Vorsitzender des Vorstands ist secunet Mitarbeiter Falk Gaentzsch, der die CSCG bereits seit 2015 organisiert. Einst gefördert durch das Bundesministerium für Wirtschaft und Energie im Rahmen der Initiative „IT-Sicherheit in der Wirtschaft", bringt der Verein junge Talente mit Unternehmen in Kontakt. „Auch wenn das Coronavirus uns im Jahr 2020 und 2021 einen Strich durch einige Pläne gemacht hat – beispielsweise wollten wir im Rahmen des deutschen Finales eine Recruiting-Messe ausrichten – , ist der Bedarf für junge IT-Talente in Unternehmen weiterhin ungebrochen", sagt Falk Gaentzsch.

Die European Cyber Security Challenge (ECSC), die seit 2015 von ehemals drei Ländern auf mittlerweile 17 Länder angewachsen ist, ist für die deutsche Nationalauswahl eine weitere spannende Möglichkeit, ihre Fähigkeiten unter Beweis zu stellen. Die Auswahl besteht aus den zehn besten Talenten des deutschen Finales. Insgesamt 271 Teilnehmende zählte der Wettbewerb in diesem Jahr.

Die ECSC wird durch ein Steering Committee organisiert, welches sich aus den Repräsentant*innen der Teilnehmerländer sowie Vertreter*innen der Agentur der Europäischen Union für Cybersicherheit (ENISA) zusammensetzt.

Juhan Lepassaar, Geschäftsführender Direktor der ENISA, sagt zur ECSC: „Die Leistungsfähigkeit der Europäischen Union hinsichtlich Cybersicherheit hängt in hohem Maße von einer angemessenen Anzahl von Fachkräften ab, die über die richtigen Kenntnisse und Fähigkeiten verfügen. Die European Cyber Security Challenge fördert Karrieren im Bereich der Cybersicherheit. Sie zieht die jungen Talente an, die wir morgen brauchen, um die Kontinuität der EU-Bemühungen rund um die Cybersicherheit unseres digitalen Raums zu gewährleisten."[1]

Trotz der Corona-Pandemie konnte die ECSC in diesem Jahr in Tschechiens Hauptstadt Prag stattfinden. Als Gastländer waren Kanada und die Slowakei eingeladen. Warum Kanada als nicht-europäisches Land? „Wir arbeiten an konkreten Plänen, mit Unterstützung durch die ENISA eine Weltmeisterschaft auszurichten. Hierzu diskutieren wir aktuell mit afrikanischen, asiatischen, nord- und südamerikanischen Ländern, Australien sowie Indien", sagt Falk Gaentzsch.

[1] ENISA, Pressemitteilung 1. Oktober 2021: Germany wins the Cyber Security Challenge

Die Gewinner der European Cyber Security Challenge 2021 mit Vertretern des Vereins Nachwuchsförderung IT-Sicherheit e. V. (NFITS) und der ENISA.

Hintere Reihe (v.l.n.r.): Adrian Belmonte Martin (ENISA), Daniel Schüll, Maurice Dauer, Robert Reith, Thomas Lambertz, Sven Stegemann, Daniel Kilimnik, Alain Rödel, Dr. Demosthenes Ikonomou (ENISA), Niklas Breitfeld

Vordere Reihe, v.l.n.r.: Tom Dohrmann, Nils Langius, Patrick Reich (NFITS), Falk Gaentzsch (NFITS), Felipe Custodio Romero, Tim Schmidt (NFITS)

AFCEA Fachausstellung

Aufbruchsstimmung nach Zwangspause

Endlich konnte sie wieder stattfinden: die AFCEA Fachausstellung. Mit einer neuen Location im World Conference Center Bonn (WCCB) öffnete die bedeutendste Messe der IT-Community der Bundeswehr für Führungsunterstützung, Nachrichtengewinnung und Aufklärung, Geoinformationssysteme, IT-Sicherheit, Simulation, Ausbildung, Logistik und SASPF am 14. und 15. September 2021 ihre Tore. Die Zwangspause hatte fast zwei Jahre gedauert. Mit einem strengen Hygiene-Konzept und ohne Fachvorträge kamen aufgrund der Corona-Pandemie weniger Besucher auf die Messe als in den Vorjahren, dennoch begrüßte secunet sehr viele Gäste am neuen Stand und führte ausführliche Gespräche mit Kunden und Partnern.

So konnten dem Fachpublikum gleich drei weitere Produkte aus der SINA Familie präsentiert werden, die während eines von Lockdown geprägten Jahres vom Bundesamt für Sicherheit in der Informationstechnik (BSI) eine Zulassung für GEHEIM erhalten haben: SINA Workflow, SINA Workstation H Client V und das neue Multikrypto-Telefon SINA Communicator H. Darüber hinaus konnten sich die Besucher*innen anhand mehrerer Anwendungsbeispiele in Zusammenarbeit mit IGEL Technology, Esri und Systematic von den vielfältigen Einsatzmöglichkeiten der SINA Workstation überzeugen.

Reges Interesse am Stand unter erschwerten Bedingungen

Nicht zuletzt hat die neu verkündete Partnerschaft zwischen IBM, RedHat und secunet, mit dem Ziel eine hochsichere Cloud-Plattform für Verschlusssachen zu entwickeln, großes Interesse geweckt und für viele Gespräche gesorgt.

Übrigens wird die AFCEA-Fachausstellung 2022 bereits am 30. und 31. März stattfinden – save the date!

Der secunet-Messestand im neuen Look am Vorabend der Messe

Brigadegeneral Armin Fleischmann, Brigadegeneral Rainer Simon und Generalmajor Dr. Michael Färber bei der Live-Demonstration des SINA Communicator H durch Dr. Michael Sobirey und Marcel Taubert (v.l.n.r)

Im Austausch: Florian Veit, Norbert Müller, Torsten Henn, Axel Deininger (alle secunet), Prof. Dr. Andreas Meyer-Falcke, Christoph Dammermann, Sebastian Barchnicki (DIGITAL.SICHER.NRW. Kompetenzzentrum für Cybersicherheit in der Wirtschaft), Christine Skropke (secunet)

it-sa

Gelungener Neustart

Nachdem die it-sa Fachmesse in Nürnberg 2020 Corona-bedingt abgesagt werden musste, konnte sie im Oktober 2021 wieder vor Ort stattfinden. Trotz verkleinerter Ausmaße wurde die Messe allgemein als Erfolg angesehen. secunet war mit Produkten und Themen wie dem sicheren Messenger stashcat, dem GEHEIM-Telefon SINA Communicator H und seinem Portfolio für Industrial Cybersecurity präsent. Für besonders großes Interesse sorgte das Thema sichere Cloud-Infrastrukturen für Behörden und Industrieunternehmen mit SecuStack. Auch ein Flugsimulator, an dem sich die Besucher*innen von der Leistungsfähigkeit der grafikbeschleunigten SINA Workstation S überzeugen konnten, kam gut an.

Am secunet Messestand konnten wie in den Vorjahren wieder hochrangige Gäste aus dem Bereich Politik und Verwaltung zahlreich begrüßt werden. Am ersten Messetag standen unter anderem BSI-Präsident Arne Schönbohm sowie Andreas Könen, Abteilungsleiter Cyber- und IT-Sicherheit im Bundesministerium des Innern, für Bau und Heimat (BMI) für einen kurzen Austausch mit Vertretern des secunet Vorstands zur Verfügung.

Am zweiten Veranstaltungstag war der secunet Stand Schauplatz eines gemeinsamen Gesprächstermins von Vertretern des Wirtschaftsministeriums Nordrhein-Westfalen (Staatssekretär Christoph Dammermann und Landes-CIO Prof. Dr. Andreas Meyer-Falcke) und dem Innen- und Digitalministerium des Landes Baden-Württemberg, vertreten unter anderem durch den Referatsleiter für Digitalisierungsstrategie und Cybersicherheit Matthias Pröfrock. Das Gespräch wurde gemeinsam initiiert durch eurobits e. V., dem IT-Sicherheitsverband des Ruhrgebiets, und Klaus-Hardy Mühleck, Vorsitzender des Cyberbeirats für das Innenministerium Baden-Württemberg. Im Fokus standen die Digitalisierungs- und Cybersicherheitsstrategien von industriestarken Bundesländern sowie die Frage, wie Cloud-Strategien unter Berücksichtigung föderaler und kommunaler Strukturen möglichst zielgerichtet und nachhaltig zu konzipieren und umzusetzen sind.

European Cyber Week

Die europäische Dimension der Cybersicherheit

Mitte November fand die fünfte Ausgabe der European Cyber Week (ECW) in Rennes, Bretagne, im Konferenzzentrum Couvent des Jacobins statt. Die Veranstaltung wird vom „Pôle d'Excellence Cyber" und seinen Partnern mit Unterstützung des französischen Verteidigungsministeriums, des Regionalrats der Bretagne und des Rennes Métropole-Councils ausgerichtet. Die ECW will Unternehmen – von multinationalen Konzernen über KMU (kleine und mittlere Unternehmen) bis hin zu KKU (Kleinst- und Kleinunternehmen) – und Start-ups, lokale Behörden, Forschungslabors, Institutionen, Studenten und Fachleute zusammenbringen. Inhaltlich bietet die Veranstaltung eine Kombination aus wissenschaftlichen und technischen Vorträgen, Geschäftstreffen und hochkarätigen europäischen Speakern. Ziel ist es, regionale, nationale und internationale Initiativen vorzustellen.

Die europäische Dimension wurde während der gesamten dreitägigen Veranstaltung deutlich sichtbar, insbesondere dank der European Cyber Security Organisation (ECSO), die die ECW mitorganisiert. Die ECW entwickelte über die letzten Jahre ihre Rolle als grundlegende und wegweisende Veranstaltung in den strategischen Bereichen Cyberverteidigung, Cybersicherheit und KI weiter – und ist gleichzeitig ein hochwertiger Netzwerkknotenpunkt. secunet war in diesem Jahr als Teil des Gemeinschaftsstands von eurobits e. V. zusammen mit dem Hamburger Start-up Quointelligence vor Ort. Zusätzlich wirkte Christine Skropke, Leiterin Bereich Public Affairs bei secunet und Vorstandsvorsitzende von eurobits, aktiv mit an den Diskussions-Panels zu den Themen „How to build a concrete European cooperation in cyber" und „Women4Cyber".

Paneldiskussion bei der European Cyber Week 2021 in Rennes, v.l.n.r.: Gregory Wawszyniak (Dumont, Cluster Security Made in Luxembourg), Neil Sandford (Wales Government), Oliver Väärtnou (Chairman of the Estonian Information Security Association), Danilo D'Elia (Moderator / Senior Policy Manager, ECSO), Christine Skropke (Leiterin Bereich Public Affairs, secunet), Giorgio Tresoldi (Armasuisse Schweiz)

Sonnenstrahl Dresden

Krankheitsbewältigung durch Kreativität

Musiktherapie beim Sonnenstrahl e. V. Dresden

Der Sonnenstrahl e.V. Dresden ist ein durch Spenden finanzierter Verein, der sich um Kinder und Jugendliche mit Krebs sowie ihre Familien kümmert. Er arbeitet eng mit der onkologischen Kinderstation des Universitätsklinikums Dresden zusammen.

Kümmern – das bedeutet unter anderem, da zu sein während der besonders schwierigen Zeit der stationären Intensivbehandlung. Eltern mit längeren Anfahrtswegen können kostenfrei im Elternhaus des Vereins übernachten und so in der Nähe ihres Kindes bleiben. Die erkrankten Kinder erhalten auf der Station die Möglichkeit der Ablenkung und künstlerisch-kreativen Verarbeitung ihrer Krebserkrankung. Auch weitere Familienmitglieder wie zum Beispiel Geschwister unterstützt der Verein.

Die diesjährige secunet Weihnachtsspende geht an den Sonnenstrahl e. V. Dresden und wird für die Musiktherapie eingesetzt. Dabei können sich die erkrankten Kinder gemeinsam mit zwei Therapeutinnen alles von der Seele singen, trommeln, spielen und klimpern, was sie mit Worten nicht gern ausdrücken möchten oder nicht auszudrücken wissen.

Kontaktmöglichkeit zum Verein:

Sonnenstrahl e. V. Dresden
Förderkreis für krebskranke Kinder und Jugendliche
Goetheallee 13
01309 Dresden
Tel.: 0351/315 839 00
E-Mail: info@sonnenstrahl-ev.org

Termine – Januar bis Juni 2022

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

1. bis 2. Februar 2022
BSI Kongress | digital

23. Februar 2022
Darmstädter IDsmart online Workshop | digital

21. bis 23. März 2022
GISEC | Dubai, Vereinigte Arabische Emirate

30. bis 31. März 2022
AFCEA Fachausstellung | Bonn

5. bis 7. April 2022
Passenger Terminal Expo | Paris, Frankreich

6. bis 8. April 2022
Intergraf Currency+Identity 2022 | Lyon, Frankreich

26. bis 28. April 2022
DMEA | Berlin

26. bis 27. April 2022
ID@Borders Seminar | Brüssel, Belgien

4. bis 5. Mai 2022
LEA-DER | Prag, Tschechien

11. bis 12. Mai 2022
Europäischer Polizeikongress | Berlin

31. Mai 2022
SINA Anwendertag | Bonn

31. Mai bis 2. Juni 2022
GPEC | Frankfurt am Main

9. Juni 2022
SINA Anwendertag | Berlin

20. bis 22. Juni 2022
Zukunftskongress Staat & Verwaltung | Berlin

28. bis 29. Juni 2022
Identity Week | London, Großbritannien

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

Impressum

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

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

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

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

Bildnachweis
Titel, S. 2 (unten), 3–18, 20–26, 31 (oben, unten links), 32, 33: secunet
S. 2 (oben), 19: alamy
S. 27: Adobe Stock
S. 28: European Cyber Security Organisation
S. 30 (oben): Jan Bacák production
S. 30 (unten): Amy Louise Hendry
S. 31 (unten rechts): Daniel Kromberg
S. 34: Sonnenstrahl e. V. Dresden

klimaneutral gedruckt
www.klima-druck.de
ID-Nr. 21110746
bvdm.

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

Damit die nächste Krisensitzung nicht im Serverraum stattfindet.

Mit SINA Gateways werden IT-Netzwerke premiumsicher.

Wo Netzwerke wirksam gegen Cyberangriffe abgeschirmt werden müssen, steht secunet bereit. SINA Gateways von secunet schützen Netz-Infrastrukturen mit BSI-zugelassener Verschlüsselungstechnik und machen sie premiumsicher.

secunet.com protecting digital infrastructures

secunet