secuview

Das secunet Kundenmagazin 1•2020

„Wir brauchen mehr Innovationen denn je“

Prof. Dr. Andreas Pinkwart, Minister für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

Home Office mit sensiblen Daten

Wie lassen sich mobile Arbeitsplätze bereitstellen, ohne die Sicherheit zu gefährden?

Gefährlich wandelbar: Emotet

Wie können sich Großunternehmen und Behörden gegen diese Art des Angriffs schützen?

National

International

Technologien & Lösungen

Kurz notiert

Service

Liebe Leserinnen und Leser,

es ist schon viel darüber geschrieben worden, wie herausfordernd die Zeiten gerade sind – und das sind sie ohne Frage. Genauso bemerkenswert ist es aber, wie schnell sich viele Unternehmen und Behörden darauf einstellen konnten. Zu Beginn der Pandemie waren sie plötzlich mit der Anforderung konfrontiert, fast ihre komplette Belegschaft im Home Office arbeiten zu lassen – und zwar ohne Sicherheitseinbußen. Dabei stellte sich nicht nur die Frage nach der technischen Machbarkeit. Auch mussten sich über Nacht Firmenkulturen ändern.

Letzteres hat sich im Nachhinein als die größere Herausforderung erwiesen. Die Technik stand bereit. Insofern hat die Krise gezeigt, wie weit die Digitalisierung bereits fortgeschritten ist. Die vernetzte Welt und das flexible Arbeiten sind schon länger nicht mehr die Zukunftsvision, als die sie immer noch gern dargestellt werden – sie sind längst Realität. Wenn wir digital per Smartphone eine Ware bestellen, setzen wir damit eine Lieferkette in Gang, die ebenfalls digital koordiniert wird. Anschließend organisiert der Händler wiederum digital Nachschub für sein Lager. Diese Möglichkeiten bestehen schon lange, und mit dem Home Office verhält es sich ähnlich: Auch damit hatten die meisten Behörden und Unternehmen bereits vor der Corona-Krise Erfahrungen gesammelt, wenn auch nicht in dem Ausmaß, das dann erforderlich wurde. Die Krise ist zum Glück nur ein Booster für die Digitalisierung, nicht ihr Ausgangspunkt.

In den letzten Monaten ist auch deutlicher geworden, dass es ohne Sicherheit keine Digitalisierung geben kann. Denn nur wer überzeugt ist, dass digitale Infrastrukturen sicher sind, nutzt sie auch. Das gilt unabhängig von der Corona-Pandemie. Wenn die Krise abebbt, wird der digitale Wandel vom Zeitraffer wieder in ein normales Tempo wechseln. Aber er wird weitergehen und sichere Lösungen erfordern.

In der neuen secuview-Ausgabe zeigen wir einige Beispiele für solche Lösungen. Mich freut besonders, dass Professor Andreas Pinkwart, Minister für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen, in einem Interview seine Sicht auf die digitale Transformation und die Rolle, die die Corona-Krise darin spielt, erläutert.

Nebenbei bemerkt: Wir haben unser Corporate Design und unser Unternehmenslogo modernisiert. Daher erscheint auch unser Magazin secuview in einem frischen gestalterischen Gewand. Wir hoffen, dass wir Ihr Lesevergnügen dadurch auch optisch noch ein wenig steigern können.

Nun wünsche ich Ihnen viel Spaß mit der neuen Ausgabe. Bleiben Sie gesund!

Ihr Axel Deininger

SINA bei der Deutschen Rentenversicherung Bund

5.800 Mal Sicherheit bitte

Die Deutsche Rentenversicherung Bund (DRV Bund) ist eine Behörde mit fast 25.000 Mitarbeiterinnen und Mitarbeitern, die 23 Millionen Versicherte betreuen. Laut der KRITIS-Verordnung des Bundesamts für Sicherheit in der Informationstechnik (BSI) gehört sie zu den kritischen Infrastrukturen und ist somit besonders schützenswert im Hinblick auf Cyberbedrohungen. Daher entschied sich die DRV Bund im Jahr 2018, sämtliche bestehenden mobilen und Home-Office-Arbeitsplätze bis Ende 2019 auf die sichere SINA Workstation S umzurüsten. Dabei ging es immerhin um mehr als 5.800 Arbeitsplätze. Gemeinsam mit dem Technikdienstleister Samhammer AG haben secunet und die DRV Bund den Massen-Rollout termingerecht gestemmt.

Ist die Entscheidung für eine SINA Lösung bei einer großen Behörde gefallen, beginnen die Planungen für den Rollout und die Konzeption der zu errichtenden SINA Infrastruktur. Und die haben es bei solchen Größenordnungen in sich: Neben der eigentlichen Aufgabe, der Konzeption und Installation der technischen Lösung, müssen Logistik organisiert, Partner eingearbeitet, Installationsbüros eingerichtet und nicht zuletzt Schulungskonzepte für Nutzer und SINA Administratoren erstellt werden. Hier zahlt es sich für die Auftraggeber aus, das gesamte Projekt mit einem Partner planen zu können. Im Fall der DRV Bund stand secunet nicht nur als Lösungsanbieter, sondern auch als Partner für den Rollout bereit.

Die nötige Erfahrung dafür hatte das Unternehmen bereits gesammelt: Zwar war die SINA Workstation als hochwertige IT-Sicherheitslösung ursprünglich eher für kleine Nutzerkreise konzipiert worden. Doch in den letzten zehn Jahren setzte secunet zahlreiche behördliche Großprojekte mit dem Produkt um, unter anderem wurden mehrere Bundesministerien vollständig damit ausgestattet. Damit war klar, dass sich die SINA Workstation S für den massenhaften Rollout eignet. Damals wurden SINA Automatisierungstools entwickelt, die die Konfiguration größerer Installationen erleichtern. Auch bei der DRV halfen diese Tools, das Projekt effizient zu halten.

Für die DRV Bund war es nicht die erste SINA Installation. Seit 2017 betreibt sie eine SINA Lösung, mit der sich etwa 100 Administratoren der DRV auf sichere Weise mobil in die zentrale IT-Umgebung der Behörde einwählen können. Da die Erfahrungen mit dieser Installation durchweg positiv waren, stand dem Aufbau einer SINA Infrastruktur im großen Stil nichts mehr im Wege.

Hauptsitz der Deutschen Rentenversicherung Bund in Berlin

Komplexe Ausgangslage

Diesmal ging es in die Breite, und das brachte im Detail einige Herausforderungen mit sich: Die Nutzer der mobilen Arbeitsplätze, die mit SINA neu aufgesetzt werden mussten, waren auf die fünf Verwaltungsstandorte der DRV Bund, einige Außenstandorte wie Kundenkontaktcenter und Rehakliniken sowie die 19 Prüfbüros mit über 2.000 Betriebsprüfern verteilt. Außerdem gab es bundesweit etwa 900 Home-Office-Arbeitsplätze, die einzeln angefahren werden mussten, um die Geräte zu installieren und die Nutzer damit vertraut zu machen.

Ein weiteres Detail erhöhte den Termindruck: Die DRV Bund hatte sich entschieden, die SINA Installation im Rahmen einer ohnehin fälligen Migration von Windows 7 auf Windows 10 durchzuführen. Die Verknüpfung war organisatorisch sinnvoll, denn sie machte aus zwei IT-Projekten eines und sparte dadurch reichlich Aufwand für die DRV Bund. Doch sie bedeutete auch, dass es eine harte Deadline für die SINA Installation und den Rollout gab: Der Herstellersupport für Windows 7 endete um den Jahreswechsel 2019/2020, und daher mussten zu diesem Zeitpunkt alle betroffenen Nutzer bei der DRV Bund mit einer SINA Workstation S ausgestattet sein, auf der Windows 10 lief.

Umfangreiche Vorbereitungen

Nach dem Ende der Konzeptionsphase im November 2018 mit Abstimmung und Erstellung von unter anderem Betriebs-, Netzwerk-, Client-, Schulungs-, Installations- und Rolloutkonzepten blieb also rund ein Jahr. Aufgabe des Rolloutteams der DRV Bund war es, für die deutlich über 5.000 zukünftigen SINA Anwender einen Verteilungsplan zu entwickeln.

Im ersten Schritt bauten DRV Bund und secunet die neue SINA Infrastruktur auf, an die die SINA Workstations S als mobile Clients sicher angebunden werden

Mit einer **SINA** Lösung können Behörden, deren Mitarbeiter mit sensiblen oder gar eingestuften Daten umgehen, sichere mobile sowie Home-Office-Arbeitsplätze einrichten. Durch eine Vielzahl ineinandergreifender Sicherheitskomponenten sorgt SINA dafür, dass Dritte keine Daten mitlesen können, wenn sich der Nutzer per Virtual Private Network (VPN) ins Behördennetz eingewählt hat. Selbst wenn ein SINA Laptop verlorengeht, bleiben die Daten dank Zwei-Faktor-Authentisierung und Festplattenverschlüsselung geschützt.

Mehr Informationen: www.secunet.com/sina

konnten. Sie wurde hochverfügbar ausgelegt, so dass die Clients jederzeit verlässlich genutzt werden können, und skalierbar, so dass künftige Erweiterungen der Installation einfach umzusetzen sind. Bei der Realisierung der SINA Box Cluster und deren Einbindung in die bestehenden Rechenzentren der DRV ergaben sich viele Detailfragen, auf die die DRV Bund und secunet passgerechte Antworten finden mussten.

Für den geplanten Marathon – die massenhafte Installation der Clients – richtete secunet gemeinsam mit der DRV in deren Räumlichkeiten zwei Installationsbüros mit insgesamt 120 Installationsplätzen ein. Für diese Büros wie auch für das Lager musste eine Vielzahl von Fragen geklärt werden, zu Themen wie Stromzufuhr, Abwärme, dem Zugang zum Lastenfahrstuhl, Zutrittsschutz, Netzwerktechnik und mehr.

Ein umfangreicher Rollout erfordert auch ein eigenes Logistikkonzept. Die SINA Workstations wurden zunächst in diebstahlgesicherten Gitterboxen untergebracht. Daneben mussten über 11.000 Smartcards für die Authentisierung an den Clients – jeder Nutzer erhielt zwei Exemplare – zunächst beschrieben und dann sinnvoll gekennzeichnet und gelagert werden.

Ein weiterer wichtiger Bestandteil der Vorbereitungen waren die Kompatibilitätstests der Anwendungen der DRV Bund im Zusammenspiel mit Windows 10 als Gastsystem der SINA Workstation. Mit der Freigabe für sämtliche Hard- und Softwarekombinationen fiel dann der Startschuss zur Masseninstallation der SINA Workstation S.

Die Deutsche Rentenversicherung Bund ist der größte Träger der deutschen Rentenversicherung mit Hauptsitz in Berlin und Standorten in Brandenburg, Gera, Stralsund und Würzburg. Fast 25.000 Mitarbeiterinnen und Mitarbeiter kümmern sich um rund 23 Millionen Versicherte und fast zehn Millionen Rentnerinnen und Rentner im Inland und Ausland.

Dieses Installationsbüro wurde eigens für das Projekt eingerichtet.

Im Rahmen des Projekts wurden über

11.000

SINA Smartcards erstellt.

Gelungene Partnerwahl

Für die technische Umsetzung des Projekts holte secunet mit der Samhammer AG einen erfahrenen Partner an Bord. Die Samhammer Techniker führten die massenhafte Installation der SINA Workstations S in den Räumlichkeiten der DRV durch, gaben die Geräte im Rahmen von Schulungen an die Mitarbeiter der DRV Bund aus, behoben technische Störungen und schrieben die über 11.000 SINA Smartcards.

Gemäß dem von der DRV Bund erstellten Verteilungsplan verlief die Steuerung der Installation. Jederzeit war klar, welches SINA Gerät für welche Person zu installieren war, bzw. wer wann welches Gerät erhalten sollte. Der Samhammer Rolloutkoordinator übernahm dabei scheinbar nebensächliche, aber zeitraubende Tätigkeiten wie die Terminvereinbarungen mit den letztendlich ca. 1.000 Home-Office-Nutzern und den Samhammer Vorort-Technikern. Diese lieferten die Workstations einzeln an die Home-Office-Nutzer, nahmen die Geräte vor Ort in Betrieb und zeigten den Nutzern die grundlegenden Funktionen der SINA Workstation S. Anschließend kümmerten sie sich um den Abtransport der Althardware.

Um die 19 im Bundesgebiet verteilten Prüfbüros mit SINA Workstations für die ca. 2.000 Betriebsprüfer zu versorgen, wurden jeweils Sammeltransporte organisiert und von Samhammer durchgeführt. Dabei wurden diebstahlgesicherte Gitterboxen voll mit SINA Geräten angeliefert. Vor Ort tauschte dann der Betriebsprüfer sein Altgerät gegen eine neue SINA Workstation S. Zeitgleich wurde ein Abtransport der Althardware organisiert und durchgeführt.

Als Ergänzung der persönlichen Schulungen der Nutzer erstellte secunet eigens für die DRV Bund SINA Lehrfilme, die die wichtigsten Funktionen der SINA Workstation S anschaulich erklären. Eine kleine Gruppe von IT-Fachleuten der DRV erhielt über die Standard-Schulungen hinaus ein umfangreicheres, fünftägiges Training im SINA Schulungszentrum bei secunet in Dresden.

Nicht alles lässt sich planen

In jedem Massen-Rollout gibt es Unwägbarkeiten: Sind die technischen Gegebenheiten vor Ort tatsächlich so wie erwartet? Liegt die Fehlerquote bei den Windows-Installationen im üblichen Rahmen? Falls Abweichungen auftreten, kann die Projektleitung gegensteuern, indem sie zum Beispiel Prozesse anpasst. Auch bei dem DRV-Rollout mussten die Verantwortlichen manche unerwartete Herausforderung meistern. Zum vorgesehenen Termin im Dezember 2019 waren aber sämtliche betreffenden Nutzer mit einer SINA Workstation S versorgt und an die Infrastruktur angebunden – genau nach Plan. Die Nutzer arbeiten seitdem nicht nur mit Windows 10, sondern greifen auf sehr hohem Sicherheitsniveau mobil und hochverfügbar auf die IT-Infrastruktur der DRV Bund zu.

Ulrich Hoffmann
ulrich.hoffmann@secunet.com

Prof. Dr. Andreas Pinkwart, Minister für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

„Wir brauchen mehr Innovationen denn je“

Gemessen am Bruttoinlandsprodukt ist Nordrhein-Westfalen das wirtschaftsstärkste Bundesland Deutschlands. Als eine der zukunftsträchtigsten Branchen des Landes gilt die IT-Sicherheitsindustrie, die in der Rhein-Ruhr-Region stark vertreten ist. secuview sprach mit Prof. Dr. Andreas Pinkwart, Minister für Wirtschaft, Innovation, Digitalisierung und Energie des Landes NRW, über Cybersicherheit, digitale Verwaltung und aktuelle Herausforderungen in Zeiten der Covid-19-Pandemie.

Herr Minister Pinkwart, mit der Digitalisierung auch in der Wirtschaft gehen Risiken einher. Sind Unternehmen, vor allem kleine und mittelständische, aus Ihrer Sicht angemessen vor Cyberbedrohungen geschützt?
Nach meiner Wahrnehmung waren viele Unternehmen bereits in den vergangenen Jahren sehr aktiv, was den Ausbau ihrer IT-technischen Infrastrukturen und Kompetenzen angeht. Dabei wurde viel in die Hardware, aber erfreulicherweise auch in die Fähigkeiten der Mitarbeiterinnen und Mitarbeiter investiert.

Diesen Weg müssen gerade die kleinen und mittelständischen Unternehmen in unserem Land konsequent weitergehen. IT-Sicherheit muss professionell umgesetzt werden. Nur wenn die eigenen Daten gut geschützt werden und mit diesen verantwortungsvoll umgegangen wird, haben Kunden und Geschäftspartner das notwendige Vertrauen für eine langjährige und tiefgreifende Geschäftsbeziehung. Daher appelliere ich immer wieder an Vertreter aller Branchen und Unternehmen: IT-Sicherheit ist Chefsache und Investitionen in sichere digitale Geschäftsprozesse sind ein zunehmend wichtiger Faktor für den Unternehmenserfolg.

Eines Ihrer Kernanliegen als Digital-Minister ist die Digitalisierung in der Verwaltung. Sie haben sich dabei hohe Ziele gesetzt. Wie weit konnten Sie diese bereits umsetzen?
Wir ziehen die komplette Digitalisierung von 2031 auf 2025 vor und beziehen Hochschulen und nahezu alle Landesbehörden ein. Wir investieren zusätzlich 600 Mio. Euro und machen damit die Verwaltung einfacher, schneller, einheitlicher und transparenter – und damit kundenfreundlicher. Mit der Novelle des E-Government-Gesetzes führen wir Regelungen

zum Serviceportal NRW als Plattform für digitale Verwaltungsleistungen ein und schaffen damit die Grundlage für die Umsetzung des Onlinezugangsgesetzes. Das wiederum bedeutet, dass wir bis Ende 2022 einen Großteil der Verwaltungsleistungen auch elektronisch über Portale anbieten werden.

Die Modellkommunen Aachen, Gelsenkirchen, Paderborn, Soest und Wuppertal bauen aktuell servicefreundliche digitale Bürgerbüros auf und stellen ihre Lösungen abschließend den anderen Städten und Gemeinden kostenlos zur Verfügung. Die angebotenen Dienstleistungen reichen von der Anmeldung zum Offenen Ganztag, zur Schule und zur Kita, über die Abfallentsorgung bis zur Erhebung der Hundesteuer. Last but not least: Auch für Unternehmen gibt es immer mehr digitale Angebote. Das Gewerbe-Service-Portal ist ein bundesweites Vorreiterprojekt, das aktuell zum Wirtschafts-Service-Portal ausgebaut wird. Schon heute können Gründerinnen und Gründer in Nordrhein-Westfalen elektronisch und ohne Medienbruch ihr Gewerbe anzeigen, um- oder abmelden und dafür elektronisch bezahlen.

Während des Shutdowns wegen Covid-19 mussten manche Behörden innerhalb kürzester Zeit massenhaft Home-Office-Arbeitsplätze aufbauen und bereitstellen. Konnte die Cybersicherheit dabei Ihrer Einschätzung nach angemessen berücksichtigt werden? Schließlich arbeiten viele Behördenmitarbeiter mit sensiblen oder sogar eingestuften Daten.

Die Corona-Krise bedeutet für die Informationstechnik in der Landesverwaltung eine große Herausforderung. Wir haben diese Aufgabe gemeinsam und gut bewältigt, aber natürlich hat uns die Corona-Krise auch gezeigt, wo wir noch etwas lernen und unsere Prozesse optimieren können.

Insgesamt können wir stolz darauf sein, dass wir innerhalb sehr kurzer Zeit unsere Infrastrukturen erheblich ausbauen konnten, und zwar – das ist mir besonders wichtig – ohne Abstriche bei der Sicherheit und dem Datenschutz zu machen. Innerhalb von zwei Monaten wurden insgesamt mehr als 14.000 Arbeitsplätze in Ministerien und Landesbehörden zu Home-Office-Arbeitsplätzen umgestaltet.

Um diese Last zu bewältigen, erfolgte innerhalb weniger Wochen eine Verdopplung der Kapazitäten in der zentralen IT-Infrastruktur für die Telearbeit. Eine ähnliche Entwicklung haben wir auch bei den vom Land betriebenen Videokonferenz-Plattformen vollzogen: Deren Kapazitäten haben wir mehr als verdreifacht.

Wird der Shutdown die Digitalisierung sprunghaft vorantreiben, so wie derzeit stark prognostiziert wird?

Jede Krise bietet bekanntlich Chancen. Die Corona-Pandemie hat der Digitalisierung in der Verwaltung Schubkraft gegeben. Durch die in den vergangenen Jahren durchgeführten Maßnahmen zur Digitalisierung unserer Verwaltungsarbeit war es uns in den vergangenen Wochen möglich, im Wirtschafts- und Digitalministerium auch mit einer Vielzahl an Mitarbeiterinnen und Mitarbeitern im Homoffice das „Soforthilfeprogramm Corona NRW“ aufzubauen. Damit konnten wir gemeinsam mit den engagierten Kolleginnen und Kollegen in den Bezirksregierungen über 400.000 Selbstständigen und kleinen sowie mittelständischen Unternehmen schnell und unbürokratisch helfen. Dies wäre vor einigen Jahren so nicht denkbar gewesen und bestärkt mich darin, bei Unternehmen und in der Gesellschaft weiterhin für eine konsequente digitale Transformation zu werben.

eurobits Security Summit

Prof. Dr. Andreas Pinkwart übernimmt die Schirmherrschaft für eine Veranstaltungswoche von eurobits e. V., dem Europäischen Kompetenzzentrum für IT-Sicherheit: Der eurobits Security Summit bündelt vielfältige Themen rund um die IT-Sicherheit. Aufgrund der aktuellen Pandemie wurde die Veranstaltungswoche, die ursprünglich im Mai stattfinden sollte, verlegt und findet nun vom 30. November bis zum 4. Dezember 2020 statt.

In der Rhein-Ruhr-Region liegt einer der Hotspots für IT-Sicherheit in Deutschland und Europa. Wie wollen Sie diese Stärke der Region zukünftig positionieren?
Die Rhein-Ruhr-Region ist auch europaweit einer der bedeutendsten Standorte für IT-Sicherheit. Mich freut es dabei sehr, dass wir hier nicht nur von der exzellenten Wissenschaft reden, sondern auch die unternehmerische Landschaft eine herausragende Stellung einnimmt.

Gerade in der IT-Sicherheit haben Existenzgründungen aus Nordrhein-Westfalen von sich reden gemacht und wir wollen die klugen Köpfe in unserem Land weiterhin dabei unterstützen, ihre Geschäftsideen auf eigene Beine zu stellen. In Zeiten von Corona brauchen wir mehr Innovationen denn je. Die Forschungs- und Entwicklungsförderung im Bereich von IT, KI und Digitalisierung wollen wir weiterführen und damit innovative Projekte unterstützen.

Neben der direkten finanziellen Unterstützung ist mir sehr daran gelegen, den Austausch zwischen Wissenschaft und Wirtschaft voranzutreiben – dabei geht es nicht nur um den Austausch innerhalb der Branchen, sondern vor allem darum, die vielen kleinen und mittelständischen Unternehmen aller Wirtschaftszweige in unserem Land beim Thema IT- und Cybersicherheit fit zu machen. Aus diesem Grund werden wir noch in diesem Jahr ein „Kompetenzzentrum Cybersicherheit für die Wirtschaft in Nordrhein-Westfalen" ausschreiben. Unser Credo ist: Wir wollen die IT-Sicherheit in der Wirtschaft stärken und das bestmögliche Umfeld für Innovationen und Ideen schaffen. Die Verbindung von herausragender Forschung und innovativen, hochspezialisierten Unternehmen in der IT-Sicherheit wird für unser Land auch in der internationalen Wahrnehmung zunehmend ein wichtiges Standortmerkmal werden.

Im Interview

Professor Andreas Pinkwart
Minister für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen

Professor Andreas Pinkwart wurde 1960 in Seelscheid, Nordrhein-Westfalen, geboren. Nach einer Banklehre studierte er Volks- und Betriebswirtschaftslehre an der Universität Münster und der Universität Bonn, wo er 1991 promovierte. Im Jahr 1994 wurde er Professor für Volks- und Betriebswirtschaftslehre an der FH für öffentliche Verwaltung NRW in Düsseldorf. 1998 wechselte er an die Universität Siegen, um einen Lehrstuhl für Betriebswirtschaftslehre zu übernehmen. Im Rahmen eines Forschungsurlaubs von 2002 bis 2011 war Professor Pinkwart Mitglied des Deutschen Bundestages (2002–2005) und Minister für Innovation, Wissenschaft, Forschung und Technologie sowie stellvertretender Ministerpräsident des Landes Nordrhein-Westfalen (2005–2010). Im Jahr 2011 wurde Professor Pinkwart zum Rektor der HHL Leipzig Graduate School of Management ernannt und hat seitdem den Lehrstuhl des Stiftungsfonds Deutsche Bank für Innovationsmanagement und Entrepreneurship inne. Im Jahr 2017 wurde er Minister für Wirtschaft, Innovation, Digitalisierung und Energie des Landes Nordrhein-Westfalen.

IT-Sicherheit nach BSI-Anforderungen

Fit für den IT-Grundschutz 2020 – mit digitaler Hilfe

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) überarbeitet jedes Jahr das IT-Grundschutzkompendium, um es an aktuelle Gefährdungen und IT-Produkte anzupassen. Dies bedeutet mitunter einen hohen Aufwand für die Behörden und Unternehmen, die den Grundschutz anwenden. Sie müssen ihre Maßnahmen an die Neuerungen anpassen und dies in ihren Sicherheitskonzepten dokumentieren. secunet compass, die Lösung für den automatisierten IT-Grundschutz, hält nun Funktionen bereit, die diese Migration erheblich erleichtern. Zudem können die Anwender den Stand der Migration und das Sicherheitsniveau ihrer IT-Infrastruktur durch übersichtliche Reports für IT-Sicherheitsbeauftragte und Management jederzeit im Auge behalten. Die Bundespolizei, die bereits seit 2017 auf secunet compass vertraut, setzt die neuen Funktionen erfolgreich ein.

Mit dem IT-Grundschutz des BSI können Behörden und Unternehmen ihr Sicherheitsniveau effektiv und nachweisbar erhöhen. Teil der bewährten Methodik ist es, für eine Vielzahl von „Informationsverbünden" Sicherheitskonzepte zu erstellen und deren Umsetzung kontinuierlich zu überprüfen. Allerdings führen immer komplexere und schnelllebige IT-Infrastrukturen zu einem erhöhten Aufwand für den IT-Grundschutz: Immer mehr Sicherheitskonzepte müssen erstellt werden, und kaum ist das erledigt, sind sie schon wieder überholt. Um den Ressourceneinsatz dennoch in angemessenen Grenzen zu halten, setzt die Bundespolizei seit 2017 mit secunet compass den IT-Grundschutz weitgehend automatisiert um. Auch für andere Behörden und Unternehmen ist die Lösung verfügbar.

secunet compass ermöglicht es, Informationssicherheit nach den Vorgaben des IT-Grundschutzes Tool-gestützt zu etablieren. Die Lösung prüft technische Komponenten automatisiert und erstellt vollständige IT-Sicherheitskonzepte nach den Anforderungen des BSI. Kernstück sind dabei die sogenannten Sicherheitsmodule. Sie beziehen sich auf die Anforderungen der Bausteine des IT-Grundschutzkompendiums für verschiedene Zielobjekte wie etwa Systeme und Anwendungen. Diese Anforderungen sind im IT-Grundschutzkompendium recht allgemein gehalten. Die Sicherheitsmodule konkretisieren sie, und zwar auf der Grundlage von Best-Practice- und Härtungs-Empfehlungen.

Wo möglich, werden die Anforderungen auf detaillierte Konfigurationseinstellungen einzelner Produkte abgebildet, so dass sie mit einer Compliance-Software vollautomatisch geprüft werden können. Die Umsetzung von nicht technisch prüfbaren Anforderungen wird in einer Web-Anwendung durch Fragebögen mit Multiple-Choice-Antworten erfasst.

Die Bundespolizei vertraut bereits seit 2017 auf secunet compass.

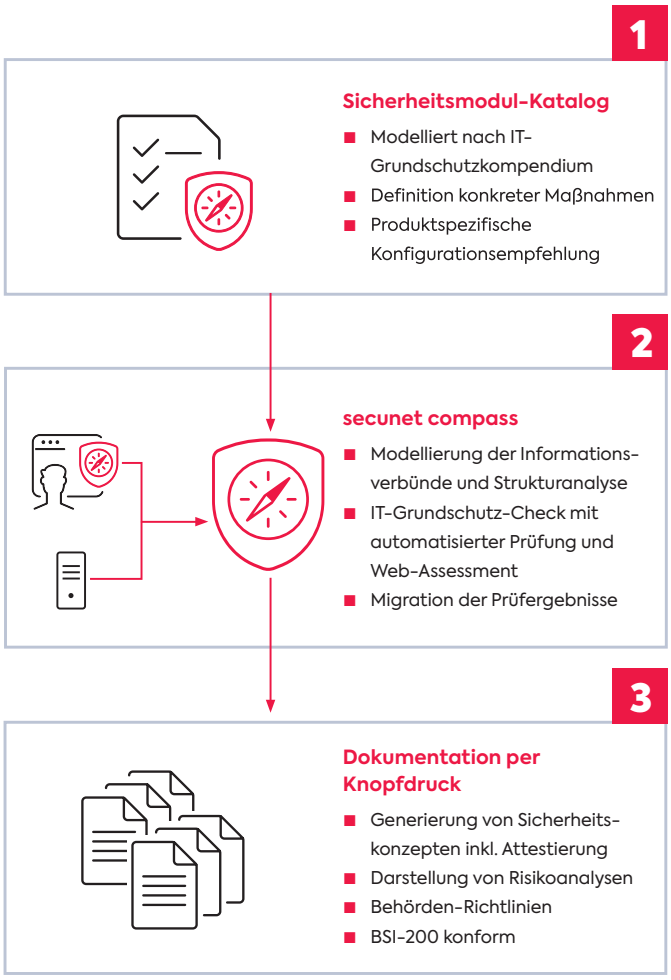
Über eine feingranulare Rollen- und Rechteverwaltung können die Fragebögen an unterschiedliche Gruppen und Personen delegiert werden. Die Ergebnisse der Umsetzungsprüfung können dann auf Knopfdruck in einem Sicherheitskonzept dokumentiert werden. Aktuell stehen in secunet compass über 90 Sicherheitsmodule für die verschiedensten Produkte und Aspekte zur Verfügung und dieser Katalog wird unter Einbeziehung der Kunden kontinuierlich erweitert.

Da sich die IT jedoch beständig weiterentwickelt – und mit ihr die Bedrohungslage –, müssen die umgesetzten Sicherheitsmaßnahmen laufend an die veränderten Gefährdungen und aktuellen Produkte angepasst werden. Das BSI aktualisiert daher jedes Jahr die im IT-Grundschutzkompendium enthaltenen Bausteine. In der aktuellen Edition 2020 wurden zahlreiche Anforderungen geändert, hinzugefügt oder entfernt. Zudem enthält sie zwei neue Bausteine. secunet compass hat die Anpassungen der Edition 2020 bereits in den Sicherheitsmodulen nachvollzogen und ist somit auf dem neuesten Stand.

Für Anwender des IT-Grundschutzes stellt die regelmäßige Aktualisierung der Anforderungen allerdings eine Herausforderung dar: Die zuvor mit viel Aufwand erhobenen Informationen zur Umsetzung müssen für alle Zielobjekte entweder von Grund auf neu erhoben oder manuell auf die geänderten Anforderungen übertragen werden. Die Ressourcen, die für diese Migration erforderlich sind, fehlen dann oft an anderer Stelle, z. B. bei der Umsetzung dringender Maßnahmen oder der Realisierung wichtiger Projekte.

Um den Aufwand für die Migration zu minimieren, bietet secunet compass eine Funktion zur Übertragung der bestehenden Prüfergebnisse und Antworten auf die neuen Sicherheitsmodule. Dabei werden für jene Anforderungen, die sich nicht geändert haben, die Ergebnisse der Umsetzungsprüfung automatisch übernommen. Für alle geänderten Anforderungen werden die alten und neuen Prüffragen sowie die Ergebnisse der Umsetzungsprüfung übersichtlich nebeneinander gestellt. Für jede Anforderung kann der Anwender dann entscheiden, ob er die Prüfergebnisse übernehmen will oder nicht. Nach diesem Migrationsschritt muss nur noch die Umsetzung der neu hinzugekommenen Anforderungen sowie von geänderten Anforderungen, für welche die Prüfergebnisse nicht übernommen worden sind, geprüft werden. Bei technisch prüfbaren Anforderungen kann diese Prüfung sogar vollautomatisch erfolgen.

Die Funktion zur Übernahme der Prüfergebnisse reduziert den Aufwand für die Umsetzungsprüfung auf ein Minimum. Trotzdem kann es notwendig sein,



für neue oder geänderte Anforderungen zusätzliche Maßnahmen umzusetzen. secunet compass bietet hierfür geeignete Funktionen zur Planung der Umsetzung, inklusive der Termine, Verantwortlichkeiten und Kosten.

Der aktuelle Stand der Umsetzung, und damit auch das aktuell erreichte Sicherheitsniveau, kann nicht nur im IT-Sicherheitskonzept eingesehen werden, sondern ist auch auf einen Blick in verschiedenen Reporting-Ansichten für die einzelnen Informationsverbünde erkennbar. Dabei stellen farbige Diagramme übersichtlich dar, welcher Anteil der Anforderungen umgesetzt wurde, nicht umgesetzt wurde, entbehrlich ist oder noch nicht geprüft wurde. In den Reports für den IT-Sicherheitsbeauftragten wird der Umsetzungsgrad für jedes Sicherheitsmodul und zusammengefasst für jede IT-Grundschutz-Schicht dargestellt. Der Management-Report verdichtet die Anzeige stärker und fasst den Stand der Umsetzung für Anforderungen an Prozesse und Systeme zusammen.

Durch die Reporting-Ansichten können die verantwortlichen Mitarbeiter jederzeit den Umsetzungsstand nachverfolgen und erkennen, wo die größten Baustellen liegen. Somit behalten sie stets den Überblick über das aktuelle Sicherheitsniveau ihrer Informationsverbünde und können die Maßnahmen, die noch umgesetzt werden müssen, optimal priorisieren.

Johannes Merkle
johannes.merkle@secunet.com

BUNDESPOLIZEI

„secunet compass ist für die Bundespolizei ein essentielles Werkzeug zur Etablierung eines einheitlichen Sicherheitsniveaus. Die Sicherheitsmodule schärfen die allgemeinen Anforderungen des IT-Grundschutzes und unterstützen somit die adressatengerechte Umsetzung innerhalb unserer dezentralen Organisation mit ihrer heterogenen Infrastruktur. Dank der neuen Visualisierungsfunktionen in secunet compass können wir den aktuellen Umsetzungsgrad des Sicherheitsniveaus umgehend erfassen und wichtige Kennzahlen als Grundlage weiterer Planungen ermitteln.“

Thomas Schonhof, Bundespolizei

Bei der Authentisierung per Smartphone ist kein zusätzliches Token erforderlich.

Onlinezugangsgesetz

ELSTER: Einfache E-Government-Anmeldung per Smartphone

Mit dem aktuellen Konjunkturpaket der Bundesregierung ist die Digitalisierung der öffentlichen Verwaltung stärker in den Fokus gerückt. So soll das Onlinezugangsgesetz (OZG) beschleunigt umgesetzt werden. Um Bürgerinnen, Bürgern und Unternehmen eine einfache Anmeldung bei einer Vielzahl von E-Government-Angeboten zu ermöglichen, soll die Steuer-ID künftig verwaltungsübergreifend zur Identifikation dienen. Das Online-Konto von ELSTER, der elektronischen Steuererklärung, erlangt damit zentrale Bedeutung für E-Government in Deutschland. ELSTER nutzt auch hier die Technologie des Partners secunet, um Nutzern eine einfache und sichere Zwei-Faktor-Authentisierung per Smartphone zu bieten.

Der neue Authentisierungsweg ist für die Nutzer besonders einfach, denn sie können ihr Smartphone als Token verwenden und brauchen keine weitere Hardware. Die Technologie basiert auf secunet protect4use, einer benutzerfreundlichen Authentisierungslösung für Webdienste, die alle relevanten Plattformen und Browser unterstützt. Dabei deckt die Lösung eine große Bandbreite von Sicherheitsanforderungen flexibel ab.

Das Onlinezugangsgesetz (OZG) verpflichtet Bund, Länder und Kommunen, bis 2022 alle staatlichen Verwaltungsleistungen digital anzubieten. Das Gesetz legt auch den Grundstein für den Portalverbund, in dem E-Government-Angebote von Bund und Ländern verknüpft werden. Sofern das ELSTER-Konto zur Anmeldung an allen Online-Angeboten des Portalverbunds verwendet wird, verfügen alle ELSTER-Nutzer bereits heute über eine digitale Identität, mit der sie viele E-Government-Dienste nutzen können. Auch ein bundesweit einheitliches Authentisierungsverfahren für Unternehmen und Organisationen wird gerade realisiert; dabei kommt ebenfalls Technologie von secunet zum Einsatz.

ELSTER ist ein Projekt der deutschen Steuerverwaltungen aller Länder und des Bundes zur Abwicklung von Steuererklärungen und Steueranmeldungen über das Internet. Bundesweiter Koordinator des Projekts und Betreiber des Portals „Mein ELSTER“ ist das Bayerische Landesamt für Steuern in München (BayLfSt). secunet leistet seit 1998 Beiträge zur sicheren Online-Authentisierung bei ELSTER.

Mehr Informationen zu secunet protect4use:
www.protect4use.de

Christian Eisenried
christian.eisenried@secunet.com

Automatisierte Grenzkontrolle

secunet easygate erstmals an einer Landgrenze

An dem ungarisch-serbischen Grenzübergang in Röszke sorgen seit April 2020 vier secunet easygates für eine effiziente Kontrolle von Busreisenden. Bei der Installation, die secunet gemeinsam mit seinem ungarischen Partner Adaptive Recognition Hungary (ARH) vorgenommen hat, handelt es sich um die ersten automatisierten Grenzkontrollsysteme (eGates) an einem Busterminal innerhalb des gesamten Schengen-Raums.

Der Grenzübergang Röszke ist Teil der Schengen-Außengrenze. Die secunet easygates dienen dazu, die dortigen Grenzkontrollbeamten zu entlasten: Freizügigkeitsberechtigte nutzen die eGates, während die Beamten den Prozess überwachen und sich ansonsten auf diejenigen Reisenden konzentrieren können, bei denen weitere Überprüfungen notwendig sind.

Das secunet easygate prüft optisch und elektronisch die Authentizität von elektronischen Identitätsdokumenten wie Reisepass und Personalausweis. Zudem liest das System das Gesichtsbild vom Chip im elektronischen Identitätsdokument aus und vergleicht die biometrischen Daten mit dem tatsächlichen Erscheinungsbild des Reisenden, das mittels einer Gesichtsbildkamera erfasst wird.

Die neuen eGates in Röszke ergänzen 14 secunet easygates, die die ungarischen Behörden bereits seit 2019 betreiben. Diese kommen an den internationalen Flughäfen in Budapest und Debrecen

An dem ungarisch-serbischen Grenzübergang in Röszke stehen Busreisenden vier secunet easygates zur Verfügung.

zum Einsatz. Insgesamt werden an internationalen Flughäfen heute bereits mehr als 350 secunet easygates eingesetzt, so z. B. in Deutschland, Österreich, Tschechien, Polen, Ungarn, Litauen und Island.

Mit secunet easygates bereiten sich Grenzkontrollbehörden in Europa auch auf die Einführung des europäischen Entry-/Exit-Systems (EES) vor, das ab dem Jahr 2022 die Grenzkontrollprozesse an den Schengen-Außengrenzen verändern wird. Von sämtlichen Angehörigen von Drittstaaten, die in den Schengen-Raum einreisen wollen, werden dann direkt an der Grenze biometrische Daten erfasst. Um den entstehenden Mehraufwand für die Grenzkontrollbeamten abzufedern, bietet es sich an, Elemente des Grenzkontrollprozesses zu automatisieren.

Mit secunet border gears bietet secunet ein komplettes Grenzkontroll-Produktportfolio, dessen Komponenten sich schnell und flexibel implementieren lassen. Sie können einzeln in bestehende Infrastrukturen integriert werden oder ergeben zusammengenommen eine verzahnte, modulare Grenzkontrollinfrastruktur, die schon heute „EES-ready" ist.

Michael Schwaiger
michael.schwaiger@secunet.com

Mehr Informationen zum europäischen Entry-/Exit-System (EES) erhalten Sie auf der folgenden Website: https://ees.secunet.com/de/

Weitere Informationen zu Adaptive Recognition Hungary (ARH) finden sich hier: https://adaptiverecognition.com/

Die neue Generation des secunet easygate

Reisen mit Stil

Das secunet easygate bewährt sich in vielen Staaten weltweit an Luft- und Landgrenzen. Über Jahre hinweg wurde das automatisierte Grenzkontrollsystem zwar kontinuierlich weiterentwickelt, änderte sein Äußeres aber kaum. Nun ist es an der Zeit für eine neue Version, die mit einem von Grund auf überarbeiteten Design besticht. Aber auch bei Technologie und Sicherheitsmechanismen gibt es Neuerungen.

Das secunet easygate entlastet die Grenzkontrollbehörden, verhilft Flughäfen zu einem größeren Passagierdurchsatz und verkürzt die Wartezeiten der Reisenden. Somit profitieren alle Beteiligten des Grenzkontrollprozesses – ohne dass Sicherheitseinbußen entstehen. Das System hat sich an großen internationalen Flughäfen bereits bei rund 100 Millionen Grenzübertritten bewährt.

Doch auch ein technisch ausgereiftes Produkt kann weiter optimiert werden. So hat das neue secunet easygate einige Verbesserungen zu bieten: Neben einem technologischen Update und Überarbeitungen in der Konstruktion haben die Entwickler von secunet Rückmeldungen, Anregungen und Wünsche von Kunden und Nutzern umgesetzt – vor allem bei Design und Sicherheit.

Modernes Design, das dem Zeitgeist entspricht

Zunächst fällt das grundlegend überarbeitete Design ins Auge. Dadurch wirkt das secunet easygate leichter und transparenter. Die Edelstahlkomponenten wurden von hellen, hochwertigen Oberflächen abgelöst und insgesamt verschlankt. Der noch großzügigere Einsatz von Glaselementen vermittelt einen einladenden, offenen und modernen Eindruck. Insgesamt ergibt sich ein hochwertiges Design, das sich perfekt in das Erscheinungsbild moderner Flughäfen einfügt und dieses aufwertet. Zudem bietet es auch Vorteile in puncto Sicherheit: So können Beamte, die die automatisierte Grenzkontrolle begleiten, den Vorgang von außen noch besser einsehen und das Geschehen in der Schleuse mitverfolgen.

Qualität bis ins kleinste Detail

Die durchdachte Konstruktion und die modularen Komponenten ermöglichen eine einfache und schnelle Installation in vorhandene Infrastrukturen. Dabei passt sich das secunet easygate seiner Umgebung an und nicht umgekehrt: Ein Umbau ist problemlos möglich, zusätzliche Komponenten können nachgerüstet werden. Somit passt das neue easygate perfekt in enge Zeitpläne und räumlich limitierte Infrastrukturen. Bei den Materialien, Motoren und Controllern und nicht zuletzt bei der Verarbeitung geht das secunet easygate keine Kompromisse ein: Es ist bis ins letzte Detail hochwertig ausgelegt für einen langen, wartungsarmen Betrieb – und wird dadurch zu einer kosteneffizienten Lösung für die Betreiber.

Sicherheit auf allerhöchstem Niveau

Auch unter dem Blickwinkel der Sicherheit hat sich das secunet easygate weiterentwickelt: Die bewährte und zuverlässige Technologie wurde in eine neue Generation mit modernsten Sicherheitskomponenten überführt. Dazu zählen beispielsweise neue Sensoren. Auch die Technologie, die sogenannte „Presentation Attacks“ erkennt – Betrugsversuche mithilfe von Gesichtsmasken oder ähnlichen Artefakten – konnte noch weiter verbessert werden. Die Farbkamera liefert qualitativ hochwertige Gesichtsbildaufnahmen und wurde nochmals auf die Anforderungen des kommenden europäischen Entry-/Exit-Systems hin optimiert. In Summe sorgen Neuerungen wie diese dafür, dass das neue secunet easygate ein bisher unerreichtes Sicherheitslevel bieten kann.

Michael Schwaiger
michael.schwaiger@secunet.com

Wer das neue secunet easygate live in Augenschein nehmen und ausprobieren möchte, vereinbart am besten einen Termin für den secunet Showroom in Essen. Bitte senden Sie uns dazu eine E-Mail an info@secunet.com.

Weitere Informationen zum Produkt finden sich unter www.secunet.com/easygate.

Das neue secunet easygate besticht mit einem Design, das sich perfekt in das Erscheinungsbild moderner Flughäfen einfügt und dieses aufwertet.

Ein Reisender nutzt den secunet easykiosk am Grenzübergang in Obrežje.

Vorregistrierung von Reisenden

Prozessbeschleuniger an der Landgrenze

In Vorbereitung auf das Einreise-/Ausreisesystem (EES) der Europäischen Union testete das slowenische Innenministerium in einem Pilotprojekt sechs Monate lang Selbstbedienungskioske – secunet easykiosk – an der Landgrenze. Das Projekt zeigte, dass Kiosksysteme den Grenzkontrollprozess nicht nur an Flughäfen, sondern auch an Landgrenzen beschleunigen.

Mit dem Pilotprojekt prüfte das slowenische Innenministerium die technische Machbarkeit für den Einsatz von Selbstbedienungskiosken an der Landgrenze. Dabei wurden die Kioske insbesondere im Hinblick darauf bewertet, ob sie sich zur Erfüllung der EES-Anforderungen eignen sowie sich in polizeiliche Hintergrundsysteme integrieren lassen. Darüber hinaus wurden die besonderen Umgebungsbedingungen der Grenzkontrolle an Landgrenzen wie Platzrestriktionen und spezifische Arbeitsabläufe berücksichtigt.

In Zusammenarbeit mit dem lokalen Partner und Generalunternehmer Cifra (Cifra komunikacijski sistemi, d.o.o.) installierte secunet den Selbstbedienungskiosk secunet easykiosk am Grenzübergang in Obrežje zwischen der Republik Slowenien und der Republik Kroatien. Als größter Grenzübergang in Slowenien wurden dort im Jahr 2018 insgesamt 45 Millionen Reisende abgefertigt. Davon waren 20 Prozent Drittstaatsangehörige (Third Country Nationals, TCN), also Personen, für die die Freizügigkeitsrechte der Europäischen Union nicht gelten.

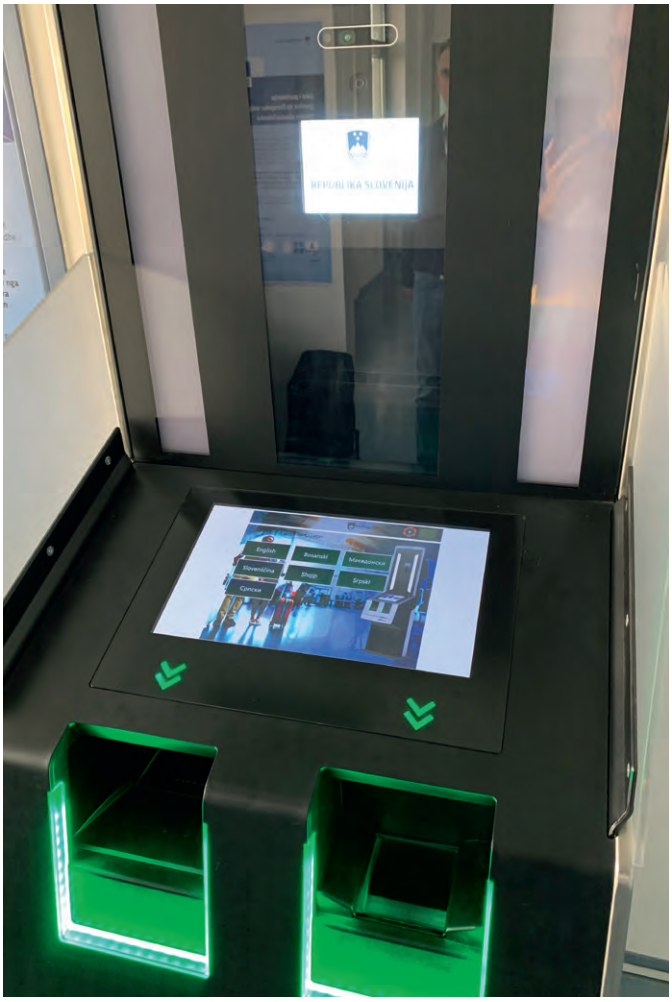
In der Pilotphase wurde der secunet easykiosk zur Vorregistrierung von TCN-Reisenden verwendet, die per Bussen die Grenze überquerten. Für die Reisenden war die Teilnahme an dem Pilotprojekt freiwillig. Entschieden sie sich für die Teilnahme, wurden sie am Selbstbedienungskiosk zunächst aufgefordert, ihre Reisepassdaten einzugeben. Die Reisenden legten dazu ihren Reisepass auf den integrierten Dokumentenleser. Darüber hinaus erfassten die Reisenden selbst ihre biometrischen Daten (Gesicht und Fingerabdrücke) am Kiosk. Dank der integrierten Kamera mit automatischer Höhenverstellung und Feedback-Bildschirm war der biometrische Erfassungprozess, der für viele Passagiere an der Landgrenze noch neu war, intuitiv und einfach zu handhaben. Über den Touchscreen konnten die Reisenden den gesamten Prozess einfach visuell verfolgen und die Vorregistrierung in Eigenregie intuitiv durchführen. Bei jedem Prozessschritt wurde am Bildschirm des Kiosks die jeweils zu verwendende Komponente hervorgehoben und die erwartete Interaktion dargestellt.

Sobald die Reisenden die Vorregistrierung am secunet easykiosk abgeschlossen hatten, wurden die vorregistrierten Daten mit Informationssystemen der Polizei abgeglichen. Dazu gehörten nationale und internationale Datenbanken, z. B. SIS, VIS und Interpol. Im Anschluss begaben sich die TCN-Reisenden zur manuellen Grenzkontrolle, wo der Grenzkontrollbeamte über eine webbasierte Grenzkontrollanwendung Zugriff auf die vorregistrierten Informationen erhielt. Mittels Dokumentenleser konnten die Grenzkontrollbeamten die Daten des maschinenlesbaren Bereichs des Reisedokuments einlesen und erhielten dann den zuvor am Kiosk erfassten Datensatz. Zur Steuerung der integrierten Hardware über die Webanwendung bei der manuellen Grenzkontrolle kam die biometrische Middleware secunet biomiddle zum Einsatz.

TCN-Reisende aus 26 Nationen nutzten die Selbstbedienungskioske freiwillig während der Pilotphase. Die Benutzeroberfläche des easykiosk wurde vom Kunden an die spezifischen Projektanforderungen angepasst. Die Dauer der verschiedenen Prozesse wurde protokolliert und für den Vorregistrierungsprozess analysiert. Die Ergebnisse zeigen, dass Kiosksysteme zur Beschleunigung des Grenzkontrollprozesses an der Landgrenze geeignet sind. Die Authentifizierung der Dokumente und die biometrische Erfassung am Selbstbedienungskiosk einschließlich weiterer Interaktionen des Benutzers (z. B. Lesen von Anweisungen, Lokalisieren der Schaltflächen auf dem Touchscreen, physische Handhabung des Dokuments) dauerte durchschnittlich 45 Sekunden.

Im Vergleich zu Pilotprojekten an Flughäfen – mit vergleichbarer Technologie und ebenfalls im EES-Kontext – waren die Ergebnisse an der Landgrenze ähnlich. Selbstbedienungskioske und automatisierte Systeme im Allgemeinen sind Prozessbeschleuniger für alle Arten größerer Grenzübergänge und verkürzen in Summe den Zeitaufwand für den Grenzkontrollprozess. Während die Prozesszeiten zwischen Vielreisenden und gelegentlich Reisenden variieren, ermöglicht der secunet easykiosk dank visueller Benutzerführung, intuitiver Prozesse und fortschrittlicher Technologien eine effiziente Dokumentenprüfung und biometrische Erfassung im Self Service-Modus.

Holger Funke
holger.funke@secunet.com



Die intuitive Benutzerführung trägt dazu bei, dass die Vorregistrierung am Kiosk nur wenig Zeit in Anspruch nimmt.

Emotet in Großunternehmen und Behörden

Gefährlich wandelbar

Seit 2014 kursiert die Schadsoftware Emotet im Netz und verursacht Schäden in Millionenhöhe. Emotet ist eine Familie von Trojanern, die sich durch einen hohen Automatisierungsgrad, Modularität und besondere Anpassungsfähigkeit auszeichnen – gewissermaßen eine intelligente Malware. Die Steuerung erfolgt über einen Command-and-Control-Server; von dort kann Emotet eine Vielzahl funktioneller Module nachladen. Angriffsziele sind bevorzugt Großunternehmen und Behörden. Die gute Nachricht: Auch gegen diese Art des Angriffs kann man sich schützen.

Eine altbekannte Gefahr im Netz: Angreifer erbeuten vertrauliche Daten von Nutzern, etwa Benutzernamen und Passwörter von Firmenaccounts oder dem Online-Banking. Bei diesem sogenannten Phishing werden gefälschte E-Mails verschickt, die scheinbar von seriösen Absendern stammen und den Empfänger dazu verleiten, auf ebenfalls gefälschten Webseiten ihre Zugangsdaten einzugeben. Die Urheber der Phishing-Mails können auf diesem Weg die wertvollen Zugangsdaten „abfischen“ und für ihre eigenen Zwecke missbrauchen.

Mit zunehmender Aufmerksamkeit in Unternehmen und bei Privatpersonen fallen immer weniger Empfänger auf schlecht formulierte, generische Phishing-Mails herein. Um im Bild des Fischens zu bleiben: Das Fischernetz hat so große Löcher, dass nur noch wenig Fang hängen bleibt.

Im Netz der Angreifer: Zugangsdaten und Passwörter

Doch die Angreifer schlafen nicht: Eine Weiterentwicklung des Phishings ist das sogenannte Spear Phishing, bei dem die Phishing-Mails nicht breit gestreut werden, sondern an sorgfältig ausgewählte Empfänger gehen. Die Inhalte sind besser recherchiert und somit wesentlich passgenauer als bei herkömmlichem Phishing, wie es der Name der Methode schon erahnen lässt (engl. „Speerfischen“).

Zumeist beziehen sich Spear-Phishing-Mails auf ein aktuelles Thema des Empfängers, so dass dieser davon ausgeht, eine legitime Mail zu erhalten, da er zum aktuellen Thema eine Mail bewusst oder unbewusst erwartet.

Naturgemäß führt der Ansatz des Spear Phishings dazu, dass ein größerer Anteil der Empfänger den Anweisungen in der gefälschten E-Mail Folge leistet als bei herkömmlichen Phishing-Mails. Er ist aber auch arbeitsintensiver: So müssen vor einem erfolgreichen Angriff ausführliche Informationen über das Angriffsziel gesammelt werden, etwa durch Social Engineering oder gar das Einschleusen eines Insiders in das Unternehmen. Spear Phishing wurde in der Vergangenheit vor allem eingesetzt, wenn das Ziel so wertvoll ist, dass sich die hohen Anfangsinvestitionen rentieren. Oft handelte es sich um Angreifer, die für staatliche oder staatsnahe Organisationen arbeiteten.

Evolution der Malware: Von Spear Phishing zu Dynamite Phishing

Emotet stellt nun die nächste Evolutionsstufe des Phishing dar: Die sorgfältige Personalisierung, die beim Spear Phishing manuell erfolgen muss, wird automatisiert. Hierzu nutzt Emotet die Adressbücher und E-Mail-Kontakte der Opfer und kann somit deren Beziehungsnetzwerke rekonstruieren. Zusätzlich verwertet die Schadsoftware automatisiert Inhalte aus realen E-Mail-Konversationen der Opfer. Dies versetzt Emotet in die Lage, neue Phishing-Mails zu verschicken, die fast perfekt in den Kontext vorhandener Arbeitsbeziehungen und E-Mail-Konversationen passen – und dies in großem Maßstab. Die Herangehensweise von Emotet wird daher auch als Dynamite Phishing (engl. „Dynamitfischen“) bezeichnet, denn sie ist großflächig anwendbar und führt zu enorm hohen Fangquoten.

Emotet: Infektion durch Makros

Eine Erstinfektion durch Emotet beginnt in der Regel durch eine gut gefälschte, seriös scheinende E-Mail mit einem Office-Dokument als Anhang. Wenn der Nutzer dieses Dokument öffnet und auf Aufforderung hin die Makros aktiviert, nimmt die Infektion ihren Lauf. Nachdem Emotet eingeschleust ist, nimmt es Verbindung zu seinem Command-and-Control-Server auf; dieser bestimmt aus der Ferne das weitere Verhalten der Schadsoftware, das abhängig von den erhaltenen Anweisungen sehr unterschiedlich sein kann.

Eine Kernfunktion von Emotet ist die weitere Verbreitung durch den Versand von Phishing-Mails innerhalb der Beziehungsnetzwerke, die es auf dem aktuell infizierten Rechner identifizieren konnte. Zum Auslesen der E-Mail-Kontakte seiner Opfer nutzt Emotet die Windows-Funktion MAPI (Messaging Application Programming Interface).

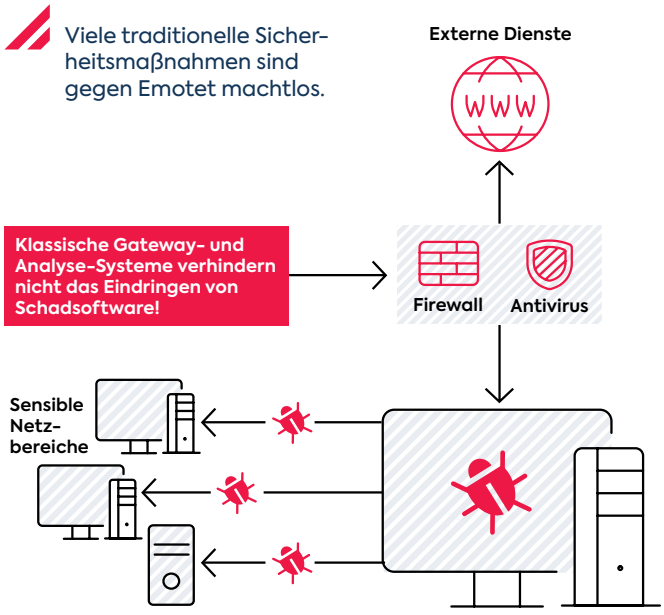
Nachladen von Modulen, Fortpflanzung als Wurm

Hat Emotet sich einmal in einem Arbeitsplatzcomputer eingenistet, kann es weitere Module in den Arbeitsspeicher nachladen, ohne dass diese als Datei abgelegt werden. Es handelt sich also um sogenannte dateilose Malware, was deren Erkennung erschwert.

Zudem funktioniert Emotet auch als Wurm und kann sich von einem infizierten Rechner auf andere im gleichen Netzwerk verbreiten, ohne dass deren Nutzer dazu aktiv beitragen müssen. Hierzu verwendet es Microsofts SMB-Protokoll (Server Message Block), liest Anmeldetoken aus dem lokalen Windows-Speicher aus und führt auch Brute-Force-Angriffe auf Benutzerkonten mittels Passwortlisten aus.

In der höchsten Eskalationsstufe einer Emotet-Infektion erkundschaften die Angreifer auch manuell das befallene System und identifizieren und entfernen beispielsweise besonders wertvolle Daten, für die dann schließlich beträchtliche Lösegeldforderungen gestellt werden. Ebenfalls eine Masche der Erpresser: Erbeutete sensible Daten werden lokal verschlüsselt und zusätzlich von den Angreifern kopiert. Zahlt das Opfer nicht, veröffentlichen die Erpresser die Daten im Internet.

Wenn es zu einem Befall des Systems kommt, vergehen unter Umständen Monate, bis dieser auffällt. Es sind Fälle bekannt, in denen Emotet und seine Module über sechs bis 18 Monate hinweg Daten im System unbemerkt verändert haben. Das Tückische daran: Werden die Daten nicht gelöscht, sondern



nur deren Inhalt modifiziert, hilft auch kein Backup. Denn es lässt sich nicht rekonstruieren, welche Daten geändert worden sind und aus dem Backup wiederhergestellt werden müssen.

Vorbeugung ist essenziell

Doch es gibt eine Reihe von Maßnahmen, die im Kampf gegen diese Art des Angriffs Erfolg versprechen. Wie bei allen Formen des Phishings kommt auch bei der Vorbeugung von Emotet-Infektionen der Aufklärung der Mitarbeiter ein hoher Stellenwert zu. Aufeinander abgestimmte Security-Awareness-Maßnahmen, etwa interne E-Mails und Plakate, steigern die Sensibilität. Spezialisierte Schulungen, zum Beispiel zum Thema E-Mail-Sicherheit, versorgen die Mitarbeiter mit dem nötigen Know-how. Aus dem vieldiskutierten „Sicherheitsrisiko Mensch" wird so der Sicherheitsfaktor Mensch, der aktiv zur Abwehr von Cyberangriffen wie Emotet beiträgt.

Um eine IT-Infrastruktur technisch gegen Emotet zu wappnen, muss erst einmal bekannt sein, wie sicher sie aktuell ist. Eine erste Annäherung bietet eine Informationssicherheits-Kurzrevision. Diese wird durch IT-Sicherheitsexperten durchgeführt und basiert unter anderem auf dem IT-Grundschutz des Bundesamts für Sicherheit für Informationstechnik (BSI). Die Experten erstellen einen Revisionsbericht mit Management-Summary und Darstellung der identifizierten Mängel als Grundlage für weitere Maßnahmen.

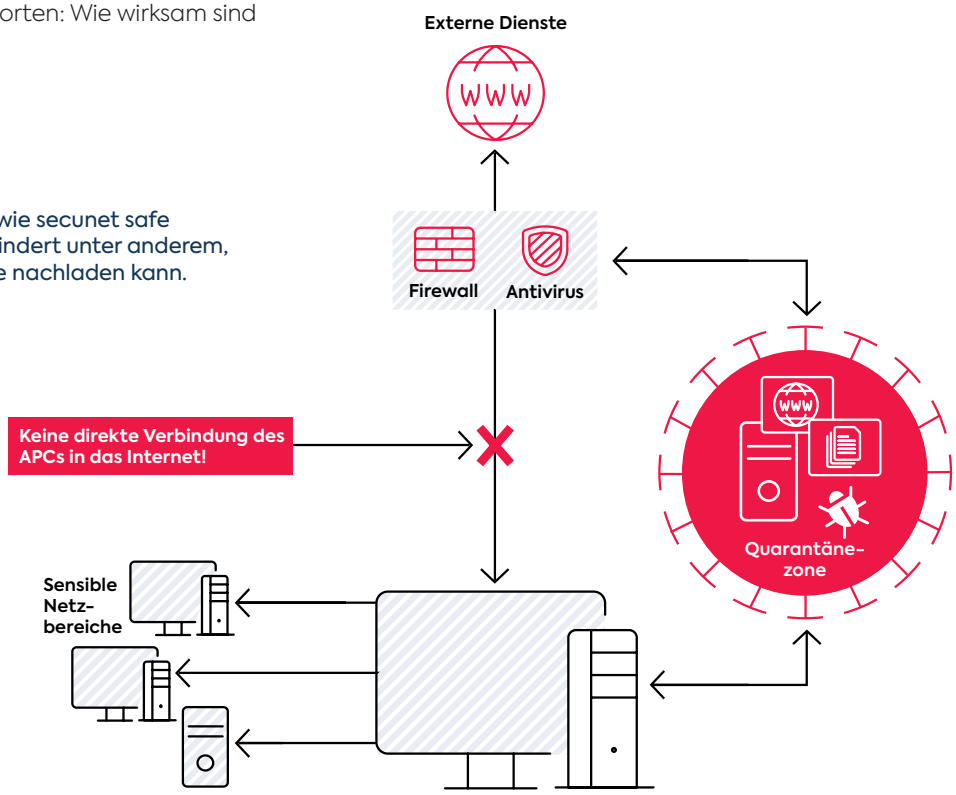
Konkrete Ansatzpunkte auf technischer Ebene liefert ein Penetrationstest. Dabei simulieren IT-Sicherheitsexperten einen Malwareausbruch, um eine Reihe von Fragen zu beantworten: Wie wirksam sind die implementierten Schutzmaßnahmen? Gibt es Schwachstellen, die kurzfristig geschlossen werden müssen? Bestehen Berechtigungen im Netzwerk, die ein Angreifer ausnutzen könnte? Auch nach Hinweisen auf eine bereits erfolgte, aber bisher nicht bemerkte Infektion suchen die Experten im Rahmen des Tests.

Um die Ausbreitung von Emotet zu erschweren, ist es generell ratsam, das Berechtigungsmanagement zu überprüfen: Kein Nutzer sollte Berechtigungen haben, die nicht notwendig sind, um seine Aufgaben zu erfüllen. Insbesondere sollte nicht flächendeckend mit Admin-Zugängen gearbeitet werden.

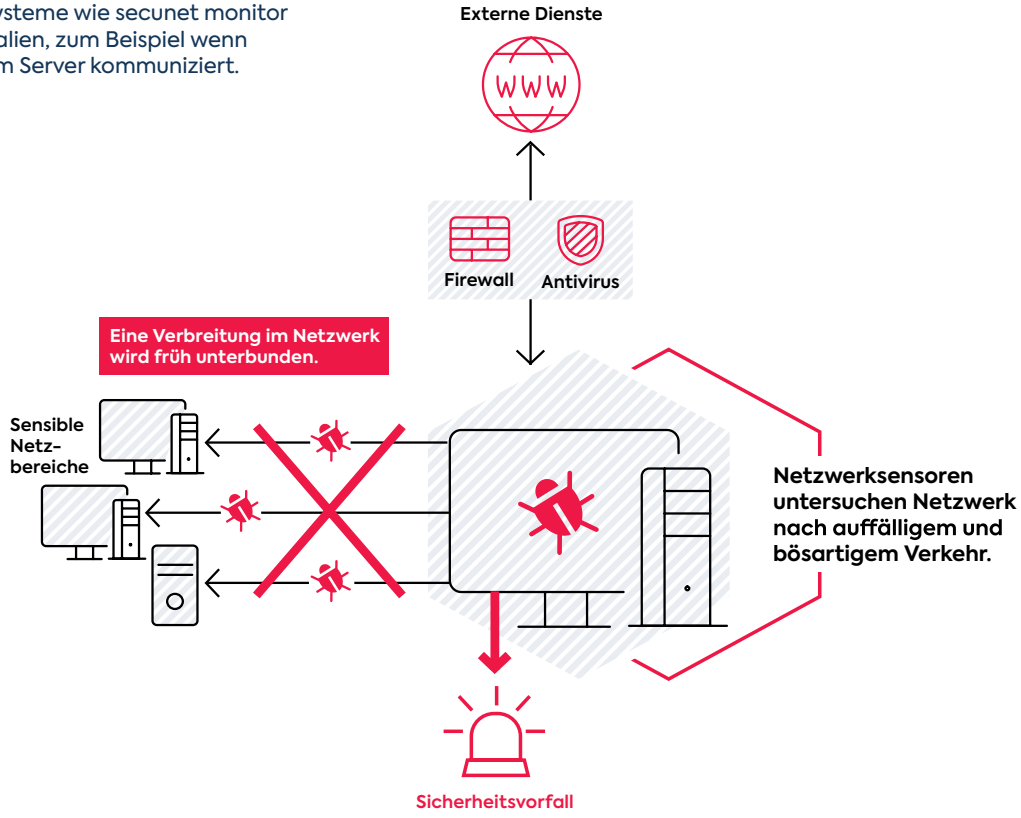
Emotet erkennen und bekämpfen

Klassische Gateway- und Analysesysteme wie Firewalls und Antivirensoftware sind gegen Emotet-Angriffe machtlos. Stattdessen sind Maßnahmen gefragt, die tiefer ansetzen – so wie das Quarantänesystem secunet safe surfer. Es verhindert, dass Emotet über einen unbedachten Klick auf einen infizierten Link auf den Rechner und damit ins Netzwerk gelangt. Mit secunet safe surfer wird die kompromittierte Website nicht in der normalen Arbeitsumgebung des Anwenders geöffnet, sondern in einem abgeschotteten Browser auf einem Quarantänesystem, den der Nutzer gewissermaßen fernsteuert. Emotet kann keinen Schaden anrichten, da die Schadsoftware das Quarantänesystem nicht verlassen kann. Mit der Zusatzfunktion safe reader lassen sich zudem infizierte E-Mail-Anhänge wirksam

Ein Quarantänesystem wie secunet safe surfer / safe reader verhindert unter anderem, dass Emotet Schadcode nachladen kann.



Früherkennungssysteme wie secunet monitor entdecken Anomalien, zum Beispiel wenn Emotet mit seinem Server kommuniziert.



abblocken. Öffnet der Nutzer einen kompromittierten Anhang mit safe reader, kann Emotet keinen Schadcode nachladen, da keine direkte Verbindung zum Internet besteht.

Zudem sollten Betreiber einer IT-Infrastruktur immer auf dem Laufenden sein, was in ihrem Netzwerk passiert und ob es Hinweise auf eine Schadsoftware-Infektion gibt. Früherkennungssysteme untersuchen die Kommunikation im Netzwerk kontinuierlich im Hinblick auf Anomalien, etwa auffällige Datenströme. Dadurch fällt es zum Beispiel auf, wenn Emotet mit seinem Command-and-Control-Server kommuniziert oder Schadsoftware nachlädt. Ist die Infektion erst einmal bekannt, kann die weitere Ausbreitung im Netzwerk verhindert werden.

Behörden und Unternehmen, die die Sichere Inter-Netzwerk-Architektur SINA einsetzen, um sensible oder gar eingestufte Daten digital verarbeiten zu können, sind auch gegenüber Emotet im Vorteil. Die SINA Workstation, die innerhalb des Systems als Client fungiert, nutzt eine Virtualisierungstechnologie, um mehrere strikt voneinander abgeschottete Gastsysteme aufzubauen. Diese Gastsysteme können gleichzeitig betrieben werden, auch wenn sie auf unterschiedlichen Sicherheitsstufen angesiedelt sind. So kann der Anwender zum Beispiel mit eingestuften Daten arbeiten und parallel im Internet surfen. Schadsoftware ist nicht in der Lage, die Grenzen zwischen den Gastsystemen zu überwinden und gelangt daher nicht ins geschützte Netzwerk.

Die Sicherheit von SINA fußt darüber hinaus auf einer Vielzahl weiterer ineinandergreifender Sicherheitsmaßnahmen: SINA Netzwerke basieren auf IPsec-gesicherten VPN-Verbindungen und bieten je nach Bedarf starke bis sehr starke Verschlüsselungen. Die Schnittstellen der SINA Workstation werden kontrolliert, um ein Eindringen von Schadsoftware über diesen Weg zu verhindern. Festplattenverschlüsselung und Zwei-Faktor-Authentisierung sorgen zusätzlich dafür, dass Unternehmens- oder Behördendaten nicht in die falschen Hände geraten.

Schutzmaßnahmen zusammenstellen

Der Evolution der Angriffsarten steht zum Glück eine Evolution der IT-Sicherheitsmaßnahmen gegenüber. So sind Behörden und Unternehmen auch Emotet nicht schutzlos ausgeliefert. Maßnahmen, die im Kampf gegen diese Art des Angriffs Erfolg versprechen, greifen in der Regel auf einer tieferen Ebene. Wie immer gilt es, im Hinblick auf die vorhandenen Gegebenheiten und den Schutzbedarf des jeweiligen Netzwerks angemessene Maßnahmen zusammenzustellen.

Christian Eisenried
christian.eisenried@secunet.com

Netzwerkanalyse bei kritischen Infrastrukturen

Wissen, was im Netzwerk passiert

Betreiber kritischer Infrastrukturen (KRITIS) sind gesetzlich verpflichtet, IT-Sicherheitsvorfälle an die Behörden zu melden. Doch dafür müssen sie in der Lage sein, solche Vorfälle überhaupt zu erkennen. Das ist gar nicht einfach, da in vielen Fällen zunächst keine merklichen Veränderungen auftreten. IT-Sicherheitsmonitoring löst dieses Problem – und hilft dabei, die Netzwerksicherheit deutlich zu erhöhen.

Gemäß dem IT-Sicherheitsgesetz, branchenspezifischen Sicherheitsstandards sowie den IT-Sicherheitskatalogen der Bundesnetzagentur müssen KRITIS-Betreiber ein Informationssicherheitsmanagementsystem (ISMS) aufsetzen und betreiben. Außerdem sind sie verpflichtet, IT-Sicherheitsvorfälle an die zuständigen Aufsichtsbehörden wie das Bundesamt für Sicherheit in der Informationstechnik (BSI) zu übermitteln.

Ein IT-Sicherheitsvorfall muss jedoch überhaupt erstmal bemerkt und erkannt werden können. Wenn es keine spür- oder sichtbaren Veränderungen gibt und kein Schaden verursacht wurde, ist das häufig nicht der Fall. IT-/OT-Sicherheitsmanager oder -Administratoren müssen schon sehr gezielt danach suchen. Und selbst wenn eine spür- oder sichtbare Auswirkung vorliegt, kann meistens nicht nachvollzogen werden, wie der Vorfall zustande kam und wie er sich weiterentwickelt hat.

Das IT-Sicherheitsgesetz fordert von den Betreibern angemessene Maßnahmen nach dem „Stand der Technik“. Dazu gehört, die Cybersicherheitslage in den IT- und OT-Netzwerken einschätzen zu können. Auch für die unternehmensinterne Berichterstattung zur Gesamtsicherheitslage sind solche Maßnahmen wichtig: In dem Bericht des IT-Sicherheitsbeauftragten oder CISO an die Unternehmensleitung sollten neben Auswertungen aus dem (IT-)Risikomanagement auch erhobene Daten aus den operativen Bereichen berücksichtigt werden. Dazu ist es sinnvoll, zentrale Kennzahlen (KPIs) auszuwerten, die unter anderem aus Beobachtungen der IT- und OT-Netzwerke resultieren.

Ein technisches IT-/OT-Sicherheitsmonitoring schafft Transparenz, um ein Lagebild zu erstellen und potenzielle Sicherheitsvorfälle schnell sichten,

bewerten, eindämmen oder direkt unterbinden zu können. Zusätzlich erleichtert es die Bewertung durch das Management und die zuständigen Behörden. Unternehmen werden in die Lage versetzt, viel zielgerichteter kurz-, mittel- und langfristige Strategien und Maßnahmen zu entwickeln und umzusetzen.

Um die Vorteile eines IT-Sicherheitsmonitorings optimal und effizient ausnutzen zu können, sollte es über ein Sicherheitslagebild-Tool verfügen. secunet hat deshalb die Lösung secunet monitor entwickelt, die aus der bisherigen Advanced Security Analytics Platform (ASAP), neuen Funktionen wie Asset-Erkennung und -Verwaltung sowie Tools von Drittanbietern besteht. Das Ergebnis ist eine modulare Lösung für Netzwerkanalyse, Detektion, Compliance und Prävention.

„IT-Sicherheitsmonitoring ohne Sicherheitslagebild-Tool ist wie eine Netzführung ohne Leitsystem."

Steffen Heyde, Division Industry,
secunet Security Networks AG

Netzwerkanalyse

Durch die fortschreitende Integration von OT-Netzen in die IT stehen die IT-Verantwortlichen vor der Herausforderung, dass sie zusätzlich zur IT nun auch die OT verstehen und verwalten müssen. secunet monitor bietet die Möglichkeit, mit dem vorhandenen Wissen der IT-Verantwortlichen ohne viel Mehraufwand und mittels der gewohnten Werkzeuge Transparenz in der OT zu erlangen.

secunet monitor ermöglicht eine automatisierte Real-Time-Analyse gängiger Protokolle aus der IT- und OT-Welt. Im Gegensatz dazu können übliche spezialisierte Lösungen zum OT-Sicherheitsmonitoring oft nur die OT-Protokolle verstehen und sind den bekannten Gefahren aus der IT, die nun immer mehr in die OT übergreift, nicht gewachsen. Die Netzwerkanalyse von secunet monitor wird standardmäßig rein passiv durchgeführt und nimmt keinen Einfluss auf die Produktionsnetze. Die Funktionsfähigkeit der jeweiligen Anlage wird nicht gestört. Zusätzlich werden dabei alle kommunizierenden Komponenten (Assets) erkannt, identifiziert und inventarisiert. Die Software leistet somit auch einen wesentlichen Betrag zum Asset-Management im Rahmen des Informationssicherheitsmanagements.

Anomalienerkennung mit
secunet monitor

Verhaltensanalyse (Detektion)

secunet monitor entdeckt Verhaltensauffälligkeiten (Anomalien) und erkennt Hinweise auf zielgerichtete Angriffe (Advanced Persistent Threats, „APTs“) im Netzwerk. Werden Angriffe und Anomalien erst einmal sichtbar, sind sie oft auch behandelbar. Die Unternehmen können schnell reagieren, Schäden reduzieren und eine weitere Ausbreitung oder gar eine Eskalation zum Not- oder Krisenfall verhindern.

Schwachstellenanalyse (Compliance)

Viele Systeme und Protokolle weisen Schwachstellen auf. Besonders problematisch ist, dass oft nicht einmal bekannt ist, wo diese kompromittierten Systeme und Protokolle überall zum Einsatz kommen. secunet monitor deckt automatisiert Schwachstellen auf, z. B. die Nutzung von älteren SMB-Protokollen oder schwachen Verschlüsselungsalgorithmen, und erzeugt einen Bericht zu deren weiterer Behandlung.

Zusätzlich identifiziert die Lösung auch unbekannte Kommunikationsverbindungen und analysiert sie.

Diese Informationen können in einen automatisiert erstellten Management-Report einfließen. In diesem Report wird die aktuelle Sicherheitslage für IT-/OT-Verantwortliche oder auch für das Management aufbereitet.

IDS/IPS (Prävention)

In Kombination mit der Industrie-4.0-Sicherheitslösung secunet edge bietet secunet monitor ein Intrusion Detection&Prevention System (IDS/IPS). Diese Funktion verhindert die Ausbreitung von Angriffen und sichert die Funktionsfähigkeit des Netzwerks.

Generell liefert secunet monitor eine umfassende Sicht auf IT- und OT-Netzwerke. Anwender können Ereignisse, die sich zu IT- oder OT-Sicherheitsvorfällen

Eine Lösung, viele Erkenntnisse

Expertensystem/-analyse

Das System ermöglicht auf Basis intelligenter Analysefunktionen eine Auswertung der im Netzwerk gesammelten Daten.

Lagebild-Auswertung

Im Rahmen des Reportings ermöglicht das System eine Aggregation und Bewertung der Events und Sicherheitsvorfälle. Die Bewertungen basieren auf vordefinierten Kriterien wie Häufigkeit und Kritikalität eines Sicherheitsvorfalls. Diese Daten können dann für den Gesamtreport weiterverarbeitet werden und stellen dem CISO und anderen Managern wichtige Entscheidungsgrundlagen bereit.

Echtzeit-Monitoring

Das System bietet eine Echtzeit-Darstellung des Netzwerkverkehrs und ermöglicht damit eine Auswertung aktueller Vorgänge im Netzwerk.

Service-Monitoring

Ein zusätzliches Modul bietet Service-Monitoring-Funktionalitäten. So lassen sich Probleme und Flaschenhälse in der IT-Infrastruktur feststellen sowie die erkannten Komponenten in der existierenden Topologie darstellen. Ein Netzwerkdaten-Logging kann z. B. für forensische Analysen verwendet werden.

Advanced Threat Detection

Unterschiedliche Vorgänge im Netzwerk können zu einer Gesamtsicht aggregiert werden. Dies erlaubt eine Auswertung hinsichtlich komplexer Angriffsszenarien wie Advanced Persistent Threats. Dabei kommt ein spezieller Sensortyp zum Einsatz, der üblicherweise die Übergänge zwischen Netzsegmenten mit unterschiedlicher Sicherheitseinstufung (IT-OT oder IT-Internet) überwacht.

entwickeln könnten, frühzeitig erkennen, schnell reagieren und ähnlichen Fällen vorbeugen. Das System bereitet Daten so auf, dass sie unmittelbar dem Management zur Verfügung gestellt werden und im Rahmen der Governance-, Risikomanagement- und Compliance-Prozesse genutzt werden können. So lassen sich deutlich schneller und präziser Entscheidungen ableiten, Maßnahmen genehmigen und deren Erfolg prüfen – das alles mit dem Ziel, die Business Continuity sicherzustellen.

Steffen Heyde
steffen.heyde@secunet.com

secunet monitor im Energieversorger-Umfeld

Ein Verteilnetzbetreiber installierte secunet monitor in mehreren Lokationen des Leitstellenverbundes. Während des Betriebs der Lösung stellte man fest, dass nur ca. 40 Prozent der Assets im vorher verwendeten Asset-Inventar erfasst waren. Zusätzlich erkannte secunet monitor Altsysteme, die Protokolle mit bekannten Schwachstellen oder veraltete Software-Versionen nutzten. Diese Systeme wurden nach der Analyse auf aktuelle Versionen umgestellt und gehärtet. Bisher nicht ins Asset-Management aufgenommene Fernwartungsschnittstellen konnten identifiziert und anschließend in die zentral administrierte Lösung überführt werden. Die Schnittstellen zur Bürokommunikation wurden überwacht und analysiert. Im Ergebnis entstand ein vollständiger Überblick über die Schnittstellen zwischen IT- und OT-Netzen. Die durch das System gewonnenen Daten werden regelmäßig aggregiert und an das Management berichtet.

secunet monitor bei Emschergenossenschaft und Lippeverband (EGLV)

Die EGLV, eines der größten Wasserwirtschaftsunternehmen Deutschlands, setzt secunet monitor as a Service ein. Ziel ist es, die eigene Infrastruktur besser zu schützen und die Vorgaben des IT-Sicherheitsgesetztes für KRITIS-Betreiber umzusetzen.

IT- oder OT-gestützte Geschäftsprozesse gehören bei der EGLV zum Standard. Ein störungsfreier sowie reibungsloser Betrieb der IT-Infrastruktur ist damit mehr denn je ein wichtiger Erfolgsfaktor. Zudem sind Angriffe auf kritische Infrastrukturen vielfältiger und professioneller geworden. Cyberangriffe können potenziell die Wasserversorgung der Bevölkerung oder auch Betriebsgeheimnisse gefährden. Angemessene Investitionen in die IT- und OT-Sicherheit sind deshalb eine notwendige Voraussetzung für die Aufrechterhaltung der Versorgungsleistung. secunet stellte der EGLV eine Lösung bereit, die mit ihrem innovativen Ansatz zum Schutz moderner IT- und OT-Systeme vertrauenswürdig und zugleich für zukünftige Anforderungen offen ist.

Ziel war es, im Hinblick auf Compliance-Anforderungen Prozesse und Aktivitäten im Zusammenhang mit Informationssicherheitsrisiken umfassender und nachhaltiger identifizieren und steuern zu können. Das System erzeugt ein Sicherheitslagebild, welches das aktuelle Sicherheitsniveau der IT-Infrastruktur sowie einiger an die IT angeschlossener Anlagen an den beiden Hauptstationen Essen und Bottrop aufzeichnet und Handlungsempfehlungen bereitstellt.

Die Lösung liefert der EGLV den Überblick über alle im Netzwerk ablaufenden Vorgänge und kann Angriffe identifizieren, analysieren und Risiken reduzieren. secunet monitor as a Service ist bei der EGLV inzwischen eine unverzichtbare Erweiterung der IT-Sicherheitsinfrastruktur geworden.

Edge Computing in der Industrie 4.0

Digitalisiert, vernetzt – und sicher

In vielen Industrieunternehmen ist eine digitalisierte und vernetzte Produktion, die mit aktuellen Technologien verknüpft ist, noch im Aufbau. Ein Mischbetrieb von Alt und Neu sowie die übereilte Einführung neuer Technologien schaffen jedoch auch Risiken, die adressiert werden müssen.

Auch im zehnten Jahr nach Stuxnet nimmt die Bedrohung von Industrieunternehmen durch Cyberangriffe weiter zu – wie an diversen zerstörerischen Ransomware-Infektionen zu beobachten ist. Gleichzeitig zeigen aktuelle Bemühungen wie das geplante IT-Sicherheitsgesetz 2.0 mit seinem Konzept der „sicheren Kernkomponenten", dass der dringende Bedarf nach zuverlässigen und wirklich sicheren Lösungen zunehmend regulatorisch erkannt wird. Für die Betreiber steigt somit der Handlungsbedarf – nicht nur durch den externen Druck, sondern auch weil sie immer stärker erkennen, wie sehr Cybersicherheit auch in ihrem eigenen Interesse liegt.

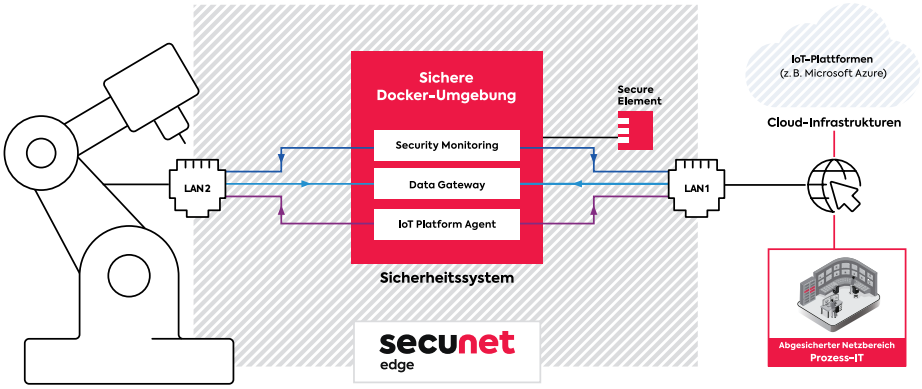
In der Industrie besteht oft ein Mix aus alten und neuen Technologien.

Wo sollte also eine sichere Gesamtlösung für die Industrie ansetzen? Ein zentrales Konzept bei der Digitalisierung von Industrieanlagen ist das Edge Computing. Dabei werden Daten nicht an den zentralen Knotenpunkten, sondern an den Rändern der Netzwerke verarbeitet und teilweise auch dort gespeichert. Ein großer Vorteil ist, dass durch die Verlagerung der Datenverarbeitung in die Peripherie Bandbreiten und Ressourcen, die oft begrenzt sind, entlastet und Reaktionszeiten beschleunigt werden. Besonders relevant ist das im industriellen Umfeld und der Operational Technology (OT).

Edge Computing ist zudem essentiell, wenn bereits bestehende Strukturen im Nachhinein digitalisiert werden sollen. Man spricht dann von einem „Brownfield" mit veralteten Legacy-Systemen, im Gegensatz zu einem frischen „Greenfield", das neu aufgebaut werden kann. Ein weiteres Einsatzfeld ist die individuelle Nachrüstung von einzelnen Systemen mit mehr Rechenleistung und aktuelleren Schnittstellen. Edge Computing ist damit ein integraler Bestandteil der Digitalisierung – als anwendungs- bzw. maschinennahe Datenverarbeitung, als Teil der Industrie 4.0 oder im Industrial Internet of Things (IIoT).

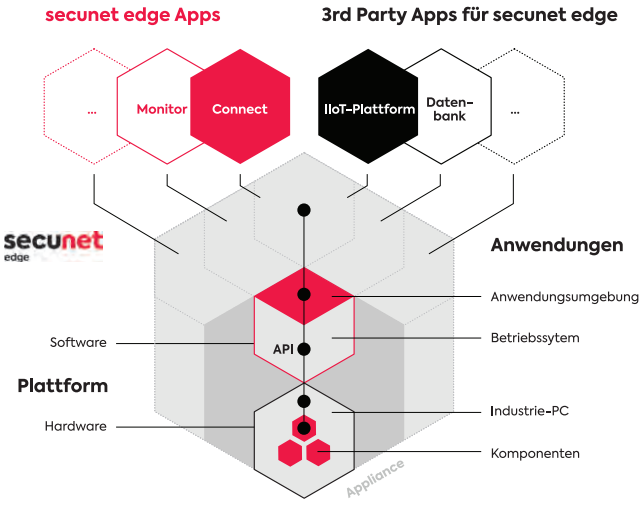
Potenzial und Risiko

Mittels Edge Computing digitalisierte und vernetze Anlagen, Maschinen, Aktoren und Sensoren schaffen



somit großes Potenzial für mehr Wertschöpfung, Profitabilität und neue Geschäftsmodelle. Zudem sorgen sie dafür, dass auch seit langem etablierte Organisationen den Anschluss an die technologische Entwicklung behalten. Gleichzeitig entstehen aber auch Angriffsvektoren für Schadsoftware und gezielte Angriffe – das Risiko von Betriebsstörungen bis hin zu existenzbedrohenden Produktionsausfällen steigt. Die neue digitale Funktionalität und Konnektivität muss daher mit einem umfassenden Schutz gegen digitale Bedrohungen abgesichert werden.

secunet edge adressiert diese Herausforderung als kosteneffiziente, komfortable und premiumsichere Gesamtlösung aus Edge-Computing-Plattform und Anwendungen. Die Plattform besteht dabei aus einem Software- und einem Hardware-Teil. Die Software umfasst ein gehärtetes Betriebssystem mit einer sicheren Anwendungsumgebung. Die Hardware basiert auf Industrie-PCs (IPCs) und darin verbauten Sicherheitskomponenten. secunet bietet Software und Hardware als kombinierte Appliance an.



Durch das Plattformkonzept können mehrere Anwendungen auf einer Appliance betrieben werden. Hinzu kommt die Möglichkeit der zentralen Administration von mehreren Apps und Appliances. Zusammen mit einem industriekompatiblen Lebenszyklus von mindestens zehn Jahren ergibt sich eine hohe Kosteneffizienz.

Durchdachte Sicherheit

Von den einzelnen Komponenten – insbesondere der patentierten CryptoCore SSD mit eingebautem embedded Secure Element (eSE) – bis zur Anwendungsebene zieht sich das Konzept der Anwendungsschnittstelle (API). Hier liegt eine große Stärke der durch secunet gestalteten und stetig weiterentwickelten Gesamtlösung: Komplexe Sicherheitsfeatures wie z. B. die Erstellung und Verwaltung von kryptographischen Schlüsseln stehen bereits als Funktionen zur Verfügung, die sich einfach und komfortabel nutzen lassen.

secunet edge ist bereits seit über zehn Jahren im Finanzsektor im Einsatz und wurde als premiumsichere Gesamtlösung nach den Prinzipien von Security by Design und Security by Default entwickelt. Wo möglich und sinnvoll wird dies auch durch entsprechende Zertifizierungen belegt (z. B. beim nach FIPS 140-2 L3 oder BSI CC L3 EAL5 zertifizierten Secure Element).

Ökosystem von Anwendungen

Wird secunet edge als Plattform für Anwendungen eingesetzt, ermöglicht dies mehrere Lösungen über eine zuverlässige und langlebige Infrastruktur. Die Anwendung Connect für secunet edge zum Beispiel übersetzt veraltete und unsichere Protokolle in aktuelle und sichere Varianten, u. a. das durch diverse Verschlüsselungstrojaner ausgenutzte SMBv1 zu SMBv3. Remote ermöglicht sichere und komfortable Fernwartung. Monitor überwacht den Netzwerkverkehr auf Schwachstellen, Angriffe und Anomalien. Neben secunet-eigenen Anwendungen entsteht rund um secunet edge ein Ökosystem von Drittanbieter-Apps, Integrationen (wie z. B. mit Microsoft Azure IoT Edge und der IIoT-Plattform PTC Thingworx) sowie von kundenspezifischen Lösungen.

Maschinen und Anlagen müssen vor schädlichen äußeren Einflüssen geschützt werden und sich gleichzeitig für eine erhöhte Konnektivität öffnen. secunet edge erfüllt diesen widersprüchlich erscheinenden Anspruch. Damit hat die Lösung großes Potenzial für die sich weiterhin rasant entwickelnde Industrie 4.0.

Aurora Monfil Herrera
aurora.monfil@secunet.com

Kooperatives Arbeiten mit eingestuften Dokumenten bis GEHEIM

Verschlusssachen sicher verteilen – mit wenigen Mausklicks

Digitales Arbeiten bringt viele Vorteile: schnell Inhalte versenden, schnell Entscheidungen treffen, einfach zusammenarbeiten und – in diesen Tagen sehr relevant – kontaktfrei arbeiten. Bislang galten diese Vorteile hauptsächlich für gewöhnliche, nicht eingestufte Daten. Wer digital mit sensiblen, hoch schützenswerten Daten oder gar Verschlusssachen (VS) arbeiten wollte, musste auf Sonderlösungen – oft ohne Zulassung – zurückgreifen, die meist an irgendeiner Stelle im Arbeitsprozess noch Papierdokumente erforderten. Erst die VS-Dokumentenmanagement-Lösung SINA Workflow, die secunet gemeinsam mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) entwickelte, hat dies geändert. Behörden können SINA Workflow nun generell für VS bis GEHEIM einsetzen, Einzelfreigaben sind nicht mehr erforderlich.

Mit SINA Workflow können Behörden die Verschlusssachenanweisung (VSA) umsetzen. Informationen lassen sich medienbruchfrei bearbeiten, verteilen und speichern – auf einem angemessen hohen und nachweisbaren Sicherheitsniveau. Im Juni 2020 erhielt die Lösung nun die Freigabeempfehlung bis zur Geheimhaltungsstufe GEHEIM durch das BSI (BSI-VSA-10158). Kunden können SINA Workflow nun einsetzen, ohne wie bisher projektspezifische Einzelzulassungen einholen zu müssen.

Wird SINA Workflow auf der Basis von SINA Workstations und unter Berücksichtigung der jeweiligen Betriebsbedingungen (SecOps) implementiert, schützt die Lösung VS und andere hochsensible Daten von der Entstehung bis zur Finalisierung. SINA Workflow unterstützt die Nutzer u.a. dabei, Inhalte kollaborativ auszuarbeiten (Zuarbeit), interne Abstimmungsprozesse mit Mitzeichnungen umzusetzen sowie Inhalte sicher nach dem Prinzip „Kenntnis nur, wenn nötig“ weiterzuleiten. Alle Funktionen und Workflows, die die Lösung anbietet, sind VSA-konform, kryptographisch gesichert und in eine umfassende Nachweisfunktion eingebettet – einschließlich eines VS-Bestandsverzeichnisses, so wie es die VSA fordert.

Im Verbund mit SINA Workstations ermöglicht SINA Workflow auch kontaktloses Arbeiten mit VS. So lassen sich eingestufte Dokumente ganz ohne den Zutritt zu Registraturen oder die Beauftragung von Kurieren verteilen. Dabei hängt es von der jeweiligen Produktvariante der SINA Workstation ab, bis zu welcher Geheimhaltungsstufe die Gesamtlösung eingesetzt werden kann: SINA Workstations S sind bis zur Stufe VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD) zugelassen, SINA Workstations E bis VS-VERTRAULICH und SINA Workstations H bis GEHEIM.

Sichere Verteilung auch außerhalb der eigenen Organisation

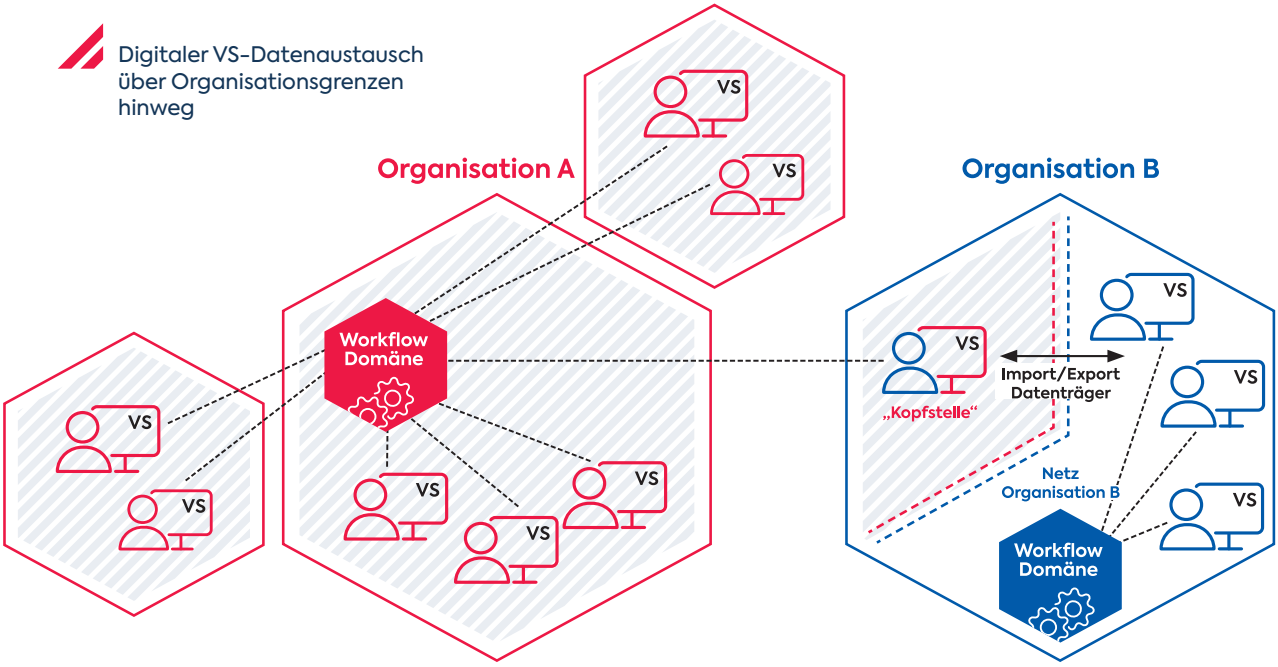
Mit Hilfe eines Kopfstellen-Modells kann SINA Workflow auch organisationsübergreifend einen digitalen VS-Datenaustausch sowie kollaboratives Arbeiten an Inhalten über Organisationsgrenzen hinweg realisieren. Eine Organisation kann damit finalisierte VS-Dokumente als Ausfertigung an eine andere Organisation senden – durchgängig digital, mit Nachweisführung und adäquatem Schutz.

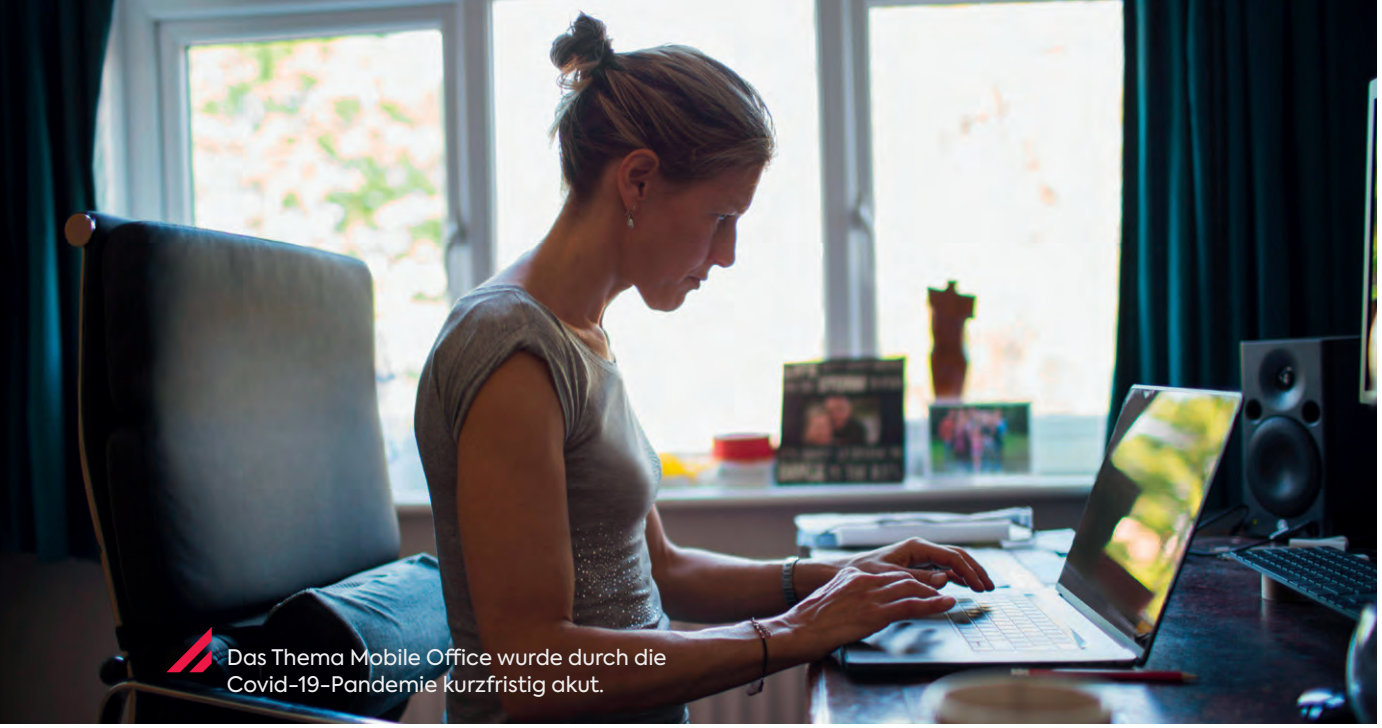
Bei dem Kopfstellen-Modell wird eine SINA Workstation mit SINA Workflow, die zu der Domäne (d.h. der SINA Infrastruktur und der SINA Workflow Registratur) von Organisation A gehört, in Organisation B aufgestellt. Mitarbeiter von B bedienen diesen SINA Workflow Arbeitsplatz. Ist eine VS von Organisation A fertiggestellt und soll an Organisation B gesendet werden, kann ein berechtigter Mitarbeiter von A einem SINA Workflow Nutzer der Organisation B (der in diesem Fall als Nutzer der Domäne von Organisation A geführt wird) die Kenntnisnahme des Dokuments anbieten. Nimmt der Nutzer von B diese an, wird das Dokument geschützt an die SINA Workstation in Organisation B übertragen und kann dort gelesen und, wenn nötig, bearbeitet werden.

Zusätzlich hat der Nutzer von B die Möglichkeit, die VS digital zu exportieren und sie so in anderen Systemen innerhalb der Organisation B weiterzuverwenden. Die Nachweisführung von SINA Workflow der Organisation A zeigt an, ab wann der Mitarbeiter von B die Kenntnisnahme angenommen hat und ob – und wenn ja, wann – eine digitale Kopie zur Verwendung außerhalb der SINA Workflow Domäne A erzeugt wurde.

Insgesamt vereinfacht SINA Workflow die digitale VS-Bearbeitung in der deutschen Verwaltung stark, der Umgang mit eingestuften Informationen wird um ein Vielfaches beschleunigt. Auch Behörden anderer Länder können von der Lösung profitieren: SINA Workflow wurde von Anfang an mit dem Ziel der Internationalisierung entwickelt.

Stefan Reuter
stefan.reuter@secunet.com





Das Thema Mobile Office wurde durch die Covid-19-Pandemie kurzfristig akut.

Home Office mit SINA

Mobiles Arbeiten – ohne Kompromisse bei der Sicherheit

Im Frühjahr 2020, zu Beginn der Corona-Pandemie, mussten viele Behörden ihren Mitarbeitern schnell und flächendeckend mobile Arbeitsplätze zur Verfügung stellen. Um die Sicherheit dabei nicht zu gefährden, setzten sie vielfach auf die SINA Workstation S. Die Migration bestehender Systeme in die sichere SINA Umgebung ist einfach.

Beim Thema Mobile Office stehen Behörden vor einem Dilemma: Unter dem Blickwinkel der Informationssicherheit gilt es, eine Vielzahl von Maßnahmen umzusetzen – was einer schnellen und einfachen Projektumsetzung zuwiderläuft. Diese Herausforderung stellt sich denjenigen Organisationen verschärft, deren Mitarbeiter regelmäßig mit Informationen umgehen, die einen hohen Schutzbedarf aufweisen oder sogar eingestuft sind. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat im März 2020 eine Sammlung von Hinweisen zum sicheren mobilen Arbeiten auf seiner Website veröffentlicht [1].

Um die nötigen Sicherheitsanforderungen umzusetzen, ist üblicherweise eine Vielzahl von Komponenten nötig, die alle einzeln administriert werden müssen. Wenn dies zu aufwändig ist, aber die Reduzierung der Sicherheit keine Option ist, können Behörden auf eine bewährte Lösung zurückgreifen: die SINA Workstation S. Sie ist Teil des Krypto-Systems SINA,

[1] https://www.bsi.bund.de/DE/Presse/Kurzmeldungen/Meldungen/Empfehlungen_mobiles_Arbeiten_180320.html

das secunet im Auftrag des BSI entwickelt hat. Bereits seit Jahren stellt die SINA Workstation S den Standardarbeitsplatz in zahlreichen Bundes- und Landesbehörden, darunter auch in mehreren Bundesministerien. Durch ihre Mobilität und Flexibilität hat sie das Arbeiten in Behörden revolutioniert. Bislang wurden bereits mehr als 100.000 Exemplare ausgeliefert.

Die Lösung erlaubt es, bestehende Systeme einfach in die sichere SINA Umgebung zu migrieren. Die Nutzer arbeiten dann ohne Einschränkungen in ihrer gewohnten Umgebung weiter, zum Beispiel in MS-Windows, und greifen sicher auf das Behördennetzwerk zu. Durch eine Vielzahl miteinander verschränkter Sicherheitsmaßnahmen wie z. B. IPsec-gesicherter VPN-Anbindung, Festplattenverschlüsselung, Zwei-Faktor-Authentisierung und Schnittstellenkontrolle sind sensible Daten jederzeit auf hohem Niveau abgesichert – egal ob sich die Mitarbeiter im Büro, zu Hause oder unterwegs aufhalten. Auch das Desktop-Telefon kann die SINA Workstation S ersetzen, indem sie sichere Telefonate per Voice over IP (VoIP) ermöglicht. Für einen schnellen Rollout und eine erleichterte Administration stehen automatisierte Tools zur Verfügung.

Die SINA Workstation S ist in verschiedenen Formfaktoren – Desktops, Laptops, Tablets – verfügbar, die alle für den Umgang mit Verschlusssachen der Einstufung VS-NfD zugelassen sind. Je nach Anforderungen steht als Alternative zum Fat Client mit vollwertigem PC-Arbeitsplatz auch eine schlanke Terminal-Server-Lösung (Thin Client) zur Wahl. Noch schlanker ist die rein softwarebasierte Lösung secunet Terminal powered by SINA, die auf jedem gängigen Windows-PC installiert werden kann und einen sicheren Zugang zu Terminalservern ermöglicht. Allen Varianten gemein ist, dass der Nutzer auch zu Hause oder unterwegs so arbeiten kann, als säße er am gewohnten Büro-Schreibtisch – und das, ohne die Informationssicherheit zu gefährden.

Christian Eisenried
christian.eisenried@secunet.com

Revival der Thin Clients

Weniger ist mehr

Beim Aufbau von IT-Infrastrukturen stehen Thin Clients derzeit wieder hoch im Kurs. Ein Setup mit schlanken Clients und starken Servern kann sich auch für Behörden oder Unternehmen lohnen, die mit sensiblen Daten oder Verschlusssachen umgehen. Das SINA Portfolio hält optimierte Hardware-Komponenten bereit, die Lösungen mit Thin Clients oder auch verschlankten Fat Clients ermöglichen – und zwar auf gewohnt hohem Sicherheitsniveau.

Auch die IT-Welt ist Moden unterworfen. Thin Clients – auf das Notwendigste reduzierte Rechner, die hauptsächlich Serverinhalte darstellen sollen – erfreuen sich mal mehr, mal weniger Beliebtheit. In den letzten Jahren setzte man eher auf das Gegenteil, den vollausgestatteten Fat Client. Doch nun schlägt das Pendel wieder leicht in die andere Richtung aus. Beides hat wirtschaftlich gesehen Vor- und Nachteile: Thin Clients können helfen, IT-Vorhaben kostengünstiger umzusetzen, etwa indem man schlankere Hardware einsetzt. Auf der anderen Seite erfordern sie eine permanente breitbandige Internetverbindung sowie eine passende Terminal-Software. Hier gilt es, die Lösung zu finden, die für das jeweilige Anwendungsszenario das optimale Kosten-Nutzen-Verhältnis bietet.

Ein Faktor, der aktuell Thin-Client-Infrastrukturen befördert, ist die Corona-Pandemie: Wenn Behörden oder Unternehmen kurzfristig für sämtliche Mitarbeiterinnen und Mitarbeiter Home-Office-Arbeitsplätze bereitstellen müssen, ist das Budget in der Regel begrenzt. Hier können Thin Clients die Lösung sein.

Um ihre besonders schützenswerten Netzwerke und Daten abzusichern, nutzen viele Behörden die Sichere Inter-Netzwerk Architektur (SINA). Die SINA Workstation, die in diesen Installationen als Client fungiert, ist in verschiedenen Varianten verfügbar. Klassischerweise wird sie als Fat Client betrieben. Dann kann sie verschiedene lokal installierte Gastsysteme ausführen, die in unterschiedlichen Sicherheitsdomänen laufen. Ein Gastsystem ist dann beispielsweise für das offene, potenziell gefährliche Internet vorgesehen und ein anderes für den Umgang mit eingestuften Informationen. Da die Gastsysteme strikt voneinander abgeschottet sind, kann der Nutzer parallel in mehreren davon arbeiten, ohne sensible Daten zu gefährden.

Doch die SINA Workstation kann auch als Thin Client eingesetzt werden. Als Hardware dafür eignet sich etwa der Nano Desktop, ein Neuling im SINA Portfolio: Mit einer Grundfläche, die kaum größer ist als die eines Smartphones, spart er Platz und Kosten. Als SINA Terminal S bietet er mehr als genug Leistung für abgesicherte Thin-Client-Anwendungen. Eine weitere Option ist ein verschlankter Fat Client: Diese Variante bietet sich zum Beispiel an, wenn zwar ein vollwertiger Office-PC gefragt ist, aber ein einziges Gastsystem ausreicht. Auch in dieser sogenannten Single-Session-Konfiguration macht der Nano Desktop eine gute Figur. Sogar eine Konfiguration für einen Fat Client mit Multi-Session-Fähigkeit, also mehreren parallel nutzbaren Gastsystemen, ist verfügbar.

Mit einer Reihe von Zusatzfunktionen sorgen SINA Clients dafür, dass im mobilen Büro keine Sicherheitseinbußen zu befürchten sind. In allen Betriebsarten, also bereits in der Thin-Client-Variante, ermöglichen sie sichere Telefonie. Dazu dient die SINA VoIP Session, die Anrufe wirksam verschlüsselt. Bei den höheren Ausbaustufen sind auch umfangreichere Collaboration-Funktionen möglich.

SINA unterstützt eine Vielzahl von Einsatzszenarien. Je nach Bedarfsfall kommen unterschiedliche Hardware-Konfigurationen in Frage. Für Interessierte erstellt secunet individuelle Konzepte.

Armin Wappenschmidt
armin.wappenschmidt@secunet.com

Nano Desktop

Smartphone

Telematikinfrastruktur im Gesundheitswesen

secunet konnektor „eHealth“ zugelassen und sofort verfügbar

Der secunet konnektor in der Softwareversion „eHealth“ hat den mehrstufigen Zulassungsprozess erfolgreich durchlaufen. Die gematik erteilte der neuen Version am 17. August 2020 die Zulassung für den Wirkbetrieb in der Telematikinfrastruktur (TI). Medizinische Leistungserbringer, die den secunet konnektor bereits nutzen, erhalten die neue Version per Online-Upgrade.

Konnektoren in der Version „eHealth“ bieten eine Reihe neuer medizinischer Anwendungen. Dazu gehören das Notfalldatenmanagement (NFDM) und der elektronische Medikationsplan (eMP). In der neuen Version sind zudem alle notwendigen Funktionen (QES) enthalten, um den Fachdienst „Kommunikation im Medizinwesen“ (KIM) nutzen zu können. Diese Anwendungen bringen echten medizinischen Mehrwert und erleichtern darüber hinaus die Arbeitsabläufe in den Praxen und zwischen medizinischen Einrichtungen.

Im Zusammenspiel mit den neuen Anwendungen hat sich der secunet konnektor „eHealth“ bereits bewährt: Ein Teil des Zulassungsprozesses war als Feldtest angelegt, in dem die teilnehmenden Leistungserbringer und deren Patienten die neuen Anwendungen erfolgreich in der Produktivumgebung nutzen konnten.

Jeder secunet konnektor, der bereits eingesetzt wird, ist für die Version „eHealth“ vorbereitet. Die Nutzer können das Online-Upgrade nun einspielen und per Lizenz die Fachmodule NFDM und eMP freischalten. Zugang zu den Lizenzen erhalten die Leistungserbringer über ihren TI-Dienstleister. Das gilt sowohl für den secunet konnektor für Arztpraxen (Einbox-konnektor) als auch für den secunet konnektor für Rechenzentren (Rechenzentrumskonnektor), der sich insbesondere für Krankenhäuser und große Apotheken eignet. Für Apotheken läuft am 30. September 2020 die Frist zur Anbindung an die TI ab.

Der secunet konnektor dient Leistungserbringern bereits seit Ende 2018 zur Anbindung an die TI und wurde in seinen beiden Bauformen gemeinsam mit der eHealth Experts GmbH entwickelt. Er zielt darauf ab, über die technischen Vorgaben hinaus auch den Ansprüchen der Kunden an Nutzbarkeit und Benutzerfreundlichkeit gerecht zu werden. secunet rechnet bis zum Jahresende 2020 mit mehr als 70.000 Installationen des secunet konnektors.

Markus Linnemann
markus.linnemann@secunet.com

Auf der elektronischen Gesundheitskarte können mit den neuen Anwendungen beispielsweise Notfalldaten hinterlegt werden.

Neue eHealth-Anwendungen

„Notfalldatensatz ist schnell erstellt und hilft im Einsatz enorm“

Im Sommer 2020 lief in der Region Westfalen-Lippe ein Feldtest für zwei wichtige Anwendungen der Telematikinfrastruktur. Rund 70 Arztpraxen, eine Notfallpraxis, einige Apotheken sowie ein Krankenhaus erprobten das Notfalldatenmanagement (NFDM) und den elektronischen Medikationsplan (eMP). Zu den Testteilnehmern zählte auch Dr. Thorsten Klüsener, leitender Notarzt im Kreis Steinfurt und Facharzt für Innere und Allgemeinmedizin sowie für Anästhesiologie.

Die hausärztliche Gemeinschaftspraxis im münsterländischen Altenberge, in der Dr. Klüsener seit 2006 tätig ist, und die Filiale in Billerbeck haben der bekennende Computer-Nerd und seine Kollegen schon vor vielen Jahren auf papierlose Prozesse umgestellt. Seit knapp zwei Jahren ist die Praxis, die das Praxisverwaltungssystem (PVS) InterARZT der InterData Praxiscomputer GmbH einsetzt, mit dem Ausstattungspaket des DGN an die Telematikinfrastruktur (TI) angebunden. Im Feldtest wurde der darin enthaltene secunet konnektor mit der Softwareversion „eHealth“ vor dem flächendeckenden Rollout erprobt.

„Als Notarzt bin ich natürlich sehr daran interessiert, die wichtigen und lebensrettenden Notfalldaten auf der elektronischen Gesundheitskarte zu hinterlegen“, sagt Dr. Klüsener. Aus seiner Sicht hätte der Chip auf der Karte schon viel früher dafür genutzt werden sollen anstatt nur für die Versichertenstammdaten. Deshalb hatte er sich bereits 2016, als das NFDM – zunächst in papiergebundener Form – entwickelt wurde, aktiv in die inhaltliche Ausgestaltung und Erprobung mit eingebracht.

Fehlbehandlungen und Zeitverlust vermeiden

Vor allem bei bewusstlosen Patienten tragen die Notfalldaten auf der elektronischen Gesundheitskarte (eGK) dazu bei, im Einsatz eine schnelle und bestmögliche Versorgung zu gewährleisten. „Wenn ich auf einen Blick sehe, welche chronischen Diagnosen und Allergien vorliegen, kann ich Fehlbehandlungen aufgrund von Unkenntnis vermeiden“, erklärt der erfahrene Notarzt. „Sind zudem die Angehörigen, die im Notfall benachrichtigt werden sollen, der Hausarzt sowie das Vorliegen einer Patientenverfügung im Datensatz vermerkt, muss ich nicht mehr auf die Suche nach den entsprechenden Unterlagen gehen und spare so wichtige Zeit.“

Der Notfalldatensatz speist sich aus der im PVS hinterlegten Patientenkartei. „Ist diese bei langjährigen Patienten mit persönlichen Daten, aktuellen Diagnosen und verschriebenen Medikamenten gut gepflegt, ist der Notfalldatensatz innerhalb von nur ein bis zwei Minuten angelegt“, berichtet Dr. Klüsener. Bei neuen Patienten müsse er etwas mehr Zeit investieren, um die entsprechenden Informationen zu erfragen.

Funktionierender Workflow

In einem Arbeitsgang wird auch gleich der Medikationsplan ohne großen zusätzlichen Aufwand mit angelegt. „Nach ein paar Startschwierigkeiten funktioniert der gesamte Workflow inzwischen einwandfrei“, zeigt sich Dr. Klüsener zufrieden. „Der Feldtest gibt mir die Möglichkeit, herauszufinden, ob das, was man sich theoretisch vorgestellt hat, in der Praxis auch wirklich läuft.“ Wichtig sei das reibungslose Zusammenspiel von Konnektor und PVS. Dank der engen Abstimmung mit InterData, dem für die technische Betreuung zuständigen Unternehmen, konnten Fehlermeldungen und Probleme schnell behoben und Abläufe optimiert werden.

Eine Hürde gilt es allerdings noch zu überwinden: Um die Notfalldaten und den Medikationsplan auf die eGK des Patienten zu schreiben, muss sich Dr. Klüsener mit seinem elektronischen Arztausweis per PIN-Eingabe am Kartenlesegerät legitimieren. Auch der Patient muss als Zeichen seines Einverständnisses die PIN seiner eGK eingeben – und genau hier liegt das Problem: Viele Patienten kennen ihre PIN gar nicht und auch spontane Nachfragen bei der Krankenkasse helfen oft nicht weiter. Grundsätzlich kann aber jeder Patient die PIN bei seiner Kasse neu anfordern.

Patienten sind überzeugt

Vor allem zu Beginn wurde der Feldtest zudem durch die Coronakrise erschwert. „Zeitweise kamen nur wenige Patienten in die Praxis, so dass wir dementsprechend wenige Notfalldatensätze und Medikationspläne anlegen konnten“, erinnert sich Dr. Klüsener. Das habe sich inzwischen aber wieder normalisiert. Bislang sind seine Patienten von der Möglichkeit, ihre Daten auf der eGK zu hinterlegen, durchweg begeistert: „Es war tatsächlich kein Patient dabei, der dies aufgrund von Datenschutzbedenken nicht wollte.“ Was die Angst vor Datenmissbrauch betreffe, gebe es wirklich eine große Diskrepanz zwischen der medialen Berichterstattung und dem, was er im Umgang mit seinen Patienten erlebe.

Nun hofft der Hausarzt, dass die beiden TI-Anwendungen möglichst bald flächendeckend zum Einsatz kommen. „Vor allem wünsche ich mir, dass die Rettungsfahrzeuge hier im Kreis ganz schnell mit einer Software zum Auslesen des Notfalldatensatzes ausgestattet werden“, so Dr. Klüsener. „Dann wird diese nützliche neue Anwendung meinen Arbeitsalltag als Notarzt wesentlich erleichtern.“

Das zugrunde liegende Interview führte Katja Chalupka (DGN Deutsches Gesundheitsnetz / InterData).

Dr. Thorsten Klüsener, leitender Notarzt im Kreis Steinfurt

Aus dem Pentest-Labor

LLMNR: Die unterschätzte Gefahr

Manche Angriffsmethoden von Cyberkriminellen sind zwar nicht neu, funktionieren jedoch immer noch viel zu häufig – und das mit teilweise katastrophalen Auswirkungen. Ein Beispiel ist der Angriff über den Dienst LLMNR.

Die Link-Local Multicast Name Resolution (LLMNR) ist ein auf dem DNS-Protokoll (Domain Name System) basierender Dienst. Wie auch der normale DNS-Dienst hat er die Aufgabe, Namen in IP-Adressen aufzulösen. Doch er geht dabei anders vor als der reguläre DNS-Dienst: Er sendet Anfragen nicht nur an einen, sondern an alle Teilnehmer im gleichen Segment. Anders gesagt: LLMNR erreicht sein Ziel nicht über eine Punkt-zu-Punkt-Verbindung, sondern über einen Broadcast.

Ein Angreifer kann diesen Umstand für sich nutzen. Im Gegensatz zu einem normalen System, das LLMNR-Anfragen ignoriert, für die es sich nicht verantwortlich fühlt, antwortet der Angreifer munter auf jedes einzelne Datenpaket. Er behauptet dabei, dass der angefragte Name unter der IP-Adresse des Angreifers zu finden sei. LLMNR ist kein authentisiertes Protokoll und die anfragenden Systeme haben somit keine Möglichkeit, die Authentizität der Antwort zu bewerten. Daher glauben sie der vom Angreifer übermittelten Information. Das Opfer baut daraufhin eine Verbindung zum Angreifer auf, in der Annahme, es handle sich um das vom Opfer gesuchte System. Falls der Angreifer nach Authentisierungsdaten fragt, werden diese vom Opfer in Form eines Hashwerts bereitgestellt. Diese Hashes kann der Angreifer dann mitschneiden und versuchen, die ursprünglichen Passworte zu rekonstruieren.

Dies ist schon schlimm genug, aber es kann noch schlimmer kommen – und zwar, wenn innerhalb des betroffenen Netzwerks das Signieren von Datenpaketen des SMB-Protokolls (Server Message Block) nicht erzwungen wird. In diesem Fall kann der Angreifer über eine Methode, die einem Man-in-the-Middle-Angriff ähnelt, noch weiter gehen und auf einem Opfersystem eine Kommandozeile mit Systemrechten starten. Mit dieser Kommandozeile kann er dann beispielsweise einen lokalen Benutzer

anlegen und in die Gruppe der lokalen Administratoren einfügen. Oder er deaktiviert den lokalen Virenschutz – was beim Windows Defender häufig mit einem einzigen Befehl erledigt werden kann. Wenn der lokale Virenschutz erst einmal deaktiviert ist, kann der Angreifer z. B. weitere Tools nutzen, die Klartextpasswörter angemeldeter Accounts auslesen. Dies betrifft sowohl lokale Nutzer als auch Domänenbenutzer.

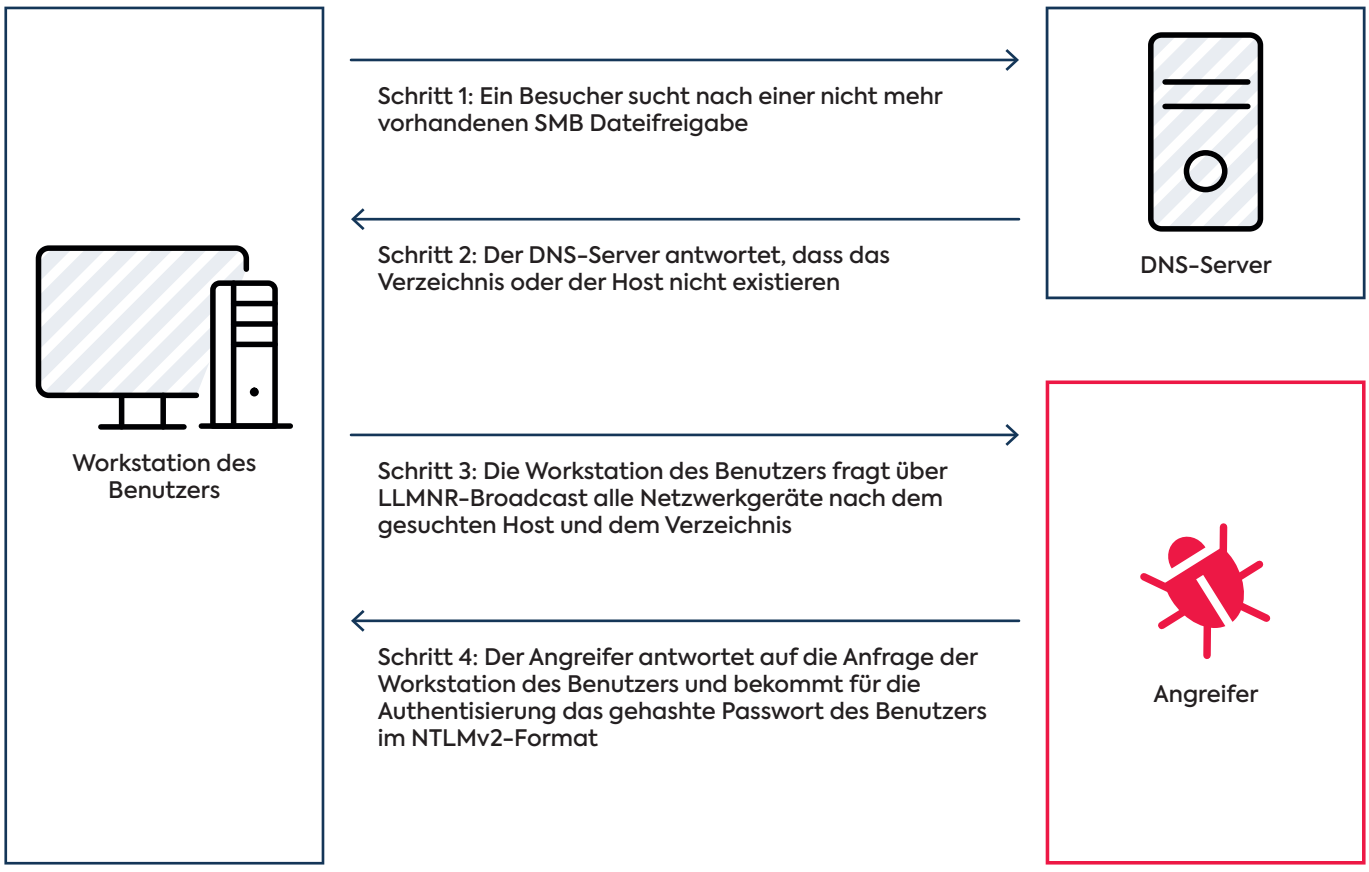
Ein Angreifer kann sich mit dieser Methode von System zu System bewegen und neue Benutzeraccounts und die zugehörigen Passwörter sammeln, bis er auf einen Benutzer in der Gruppe der Domänen-Administratoren stößt. In diesem Fall heißt es für das gesamte Netzwerk dann schnell „Game Over".

Ist der Angreifer ein beauftragter Pentester, wird er nun seinen Bericht schreiben. Handelt es sich um einen realen Angriff, bleibt zu hoffen, dass „nur" einige Festplatten verschlüsselt werden. Doch aktuell gehen Angreifer häufig darüber hinaus. Sie platzieren einen Wurm, der nach und nach Daten ändert. Diese Veränderungen fallen zunächst kaum auf. Einige Monate später stellt das betroffene Unternehmen fest, dass es den eigenen Daten nicht mehr trauen kann und die unveränderten Daten bereits aus dem Backup gefallen und damit verloren sind.

Bleibt noch ein Punkt offen: Wie können sich Unternehmen oder Behörden gegen den Angriff schützen? Das ist erstaunlich leicht: Über die Gruppenrichtlinien wird SMB-Signing als verpflichtend eingestellt und LLMNR deaktiviert. Diese Änderungen sollten vor dem Rollout allerdings gründlich getestet werden.

Dirk Reimers
dirk.reimers@secunet.com

Schema eines Angriffs über den LLMNR-Dienst.



Der Europäische Auswärtige Dienst setzt auf SINA

Der Europäische Auswärtige Dienst (EAD) stattet sein weltweites Netzwerk mit einer SINA Sicherheitslösung aus. Im Rahmen eines umfassenden IT-Projekts implementiert der EAD eine Vielzahl von SINA Komponenten. Dies ermöglicht es der Organisation, eingestufte Informationen sicher zu übertragen und zu verarbeiten, während gleichzeitig die Effizienz gesteigert und die Betriebskosten gesenkt werden können.

In erster Linie werden in dem Projekt SINA Workstations eingesetzt, die es den EAD-Mitarbeitern ermöglichen, mit nur einem Gerät sowohl auf nicht klassifizierte Büronetze als auch auf eingestufte Netzwerke zuzugreifen. Das bedeutet höhere Produktivität, niedrigere Kosten und mehr Sicherheit.

Gerd Müller
gerd.mueller@international.secunet.com

Sicheres mobiles Arbeiten: BWI beschafft SINA Workstations S für die Bundeswehr

Die BWI GmbH hat secunet mit der Lieferung von über 6.000 SINA Workstations S beauftragt. Die Krypto-Clients sind als Remote Access Service für die Bundeswehr bestimmt und ermöglichen mobiles, flexibles Arbeiten ohne Sicherheitseinbußen. Mit dem Großauftrag setzt die BWI ihre erfolgreiche Zusammenarbeit mit secunet fort: Das Unternehmen hat bereits Arbeitsplätze des Bundesministeriums für Verteidigung (BMVg) mit SINA Workstations S ausgestattet und die Bundeswehr mit SINA Lösungen für unterschiedliche Einsatzzwecke und Sicherheitsbedarfe ausgerüstet. Die aktuell georderten Geräte sind der BWI bereits termingerecht übergeben worden.

Marcel Taubert
marcel.taubert@secunet.com

ISDN adé. Hallo All-IP.

ISDN ist in Deutschland bald Geschichte: Nach den Anschlüssen für Privatkunden werden ab 2020 auch diejenigen für Geschäftskunden abgeschaltet. Behörden und Unternehmen, die noch nicht auf Voice-over-IP umgestiegen sind, vollziehen jetzt diesen Schritt. Mit der Umstellung gehen viele Vorteile einher: IP-Telefone bieten Kollaborationswerkzeuge, Zugriff auf Benutzerverwaltungsserver und vieles mehr. Mit ihren Betriebssystemen und grafischen Oberflächen gleichen sie eher Computern als klassischen Telefonen. Doch genau hier liegt das Problem: IP-basierte Telefone und Telefonnetze sind grundsätzlich genauso angreifbar wie Computer und Datennetze.

Der secunet Session Border Controller (SBC) löst dieses Problem durch Filtern von Audio- und Videoprotokollen wie z.B. SIP oder RTP. Er bewacht dabei den Netzeingang und lässt sich transparent in jede bestehende IT-Infrastruktur implementieren. Dabei arbeitet der SBC in einem isolierten Container auf der hoch performanten Firewall secunet wall, die als sichere Plattform fungiert. Diese Architektur ermöglicht eine vollständige Absicherung und Filterung der Datenströme auf Netzwerk-, Transport-, Sprach- und Applikationsebene.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bestätigt die Vertrauenswürdigkeit und hohe Qualität der Lösung: Der secunet SBC ist mit der Zertifizierungskennung BSI-DSZ-CC-1089 für die höchste Angriffsstärke CC EAL 4+ zertifiziert. Wer die Sicherheitsrisiken der IP-Telefonie eindämmt, kann uneingeschränkt von deren Vorteilen profitieren und aus der Umstellung eine Erfolgsgeschichte machen.

Mustafa Alaa Eddine
mohammed.alaaeddine@secunet.com

secuview Titel im alten (links) und neuen Design.

Evolution statt Revolution: secunet im neuen Corporate Design

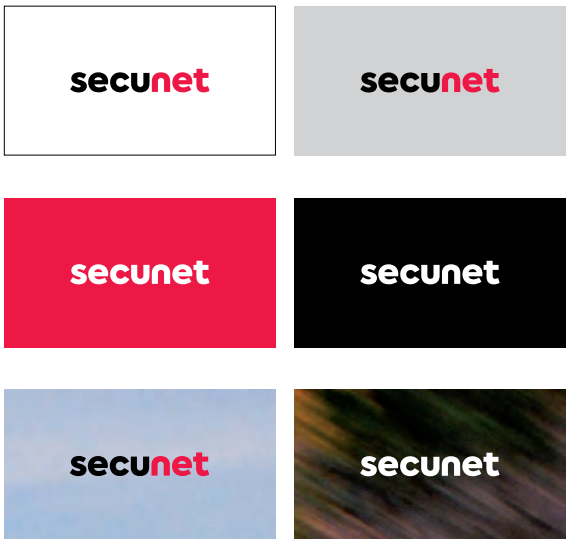
Das Corporate Design (CD) ist ein wesentlicher Bestandteil der Unternehmensidentität. Es verleiht dem Selbstverständnis des Unternehmens eine visuelle Dimension, verkörpert dessen Werte und Persönlichkeit. Im Jahr 2019 war das visuelle Erscheinungsbild von secunet in die Jahre gekommen und spiegelte daher nicht mehr den Qualitätsanspruch der Marke. Eine Überarbeitung war notwendig. Da das optische Fundament erhalten bleiben sollte, um den Wiedererkennungswert der etablierten Marke zu erhalten, entschied sich secunet für einen CD-Retouch – also eine Evolution statt einer Revolution.

Das Logo wurde typografisch überarbeitet, erhielt eine sachlichere und rationalere Anmutung. Davon ausgehend wurde die Typografie modernisiert. Die nun als Hausschrift eingesetzte Axiforma vereint optimale Lesbarkeit mit zeitgemäßer Anmutung. Die Gestaltung aller Medien, vom Produkt-Factsheet über den Messestand bis hin zum Kundenmagazin secuview, wurde ebenfalls überprüft und in der Folge vereinfacht, aufgeräumt und in eine klare Formensprache überführt.

Nicht zuletzt wurde auch die Bildwelt neu gestaltet. Große Bilder, meist Totalansichten – oft aus der Vogelperspektive – nehmen Bezug auf die Themen der secunet Zielmärkte und zeigen Städte, Industrieanlagen, Flughäfen oder Verkehrswege.

Das neue CD bringt die optische Erscheinung mit dem hohen Qualitätsanspruch des Unternehmens in Einklang und stellt die visuelle Kommunikation von secunet zukunftsfähig auf. Aktuell wird die secunet Website auf Basis des neuen CDs umfassend neu gestaltet.

Christian Reschke
christian.reschke@service.secunet.com



Termine – September bis Dezember 2020

10. September 2020
Workshop Industrial Security | München

15. bis 16. September 2020
StrategieTage IT Security | Bergisch Gladbach

7. bis 8. Oktober 2020
LEA-DER | Prag, Tschechien

27. bis 28. Oktober 2020
inova | Ilmenau

10. bis 12. November 2020
CODE Jahrestagung | München

16. bis 17. November 2020
Rethink! IT Security | Berlin

17. November 2020
Polizeitag | Kiel

19. November 2020
Informationssicherheitstag RLP 2020 | Online-Event

23. bis 25. November 2020
KELI | Bremen

24. bis 25. November 2020
Berliner Sicherheitskonferenz | Berlin

30. November bis 4. Dezember 2020
eurobits Security Summit | Verschiedene Veranstaltungsorte

1. Dezember 2020
Polizeitag | München

15. Dezember 2020
Polizeitag | Düsseldorf

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

Impressum

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

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

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

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

Bildnachweis
S. 2, 14, 20, 25, 28, 41: iStock
S. 35: iStock/LightFieldStudios
S. 5, 32: alamy
S. 3, 6, 12, 15, 17, 18, 19, 40: secunet
S. 9: Land NRW
Titel, S. 10: MWIDE NRW/E. Lichtenscheidt
S. 37: Dr. Thorsten Klüsener

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.

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.

Sicheres Arbeiten mobil und im Home Office.

Mit der SINA Workstation sind sensible Daten premiumsicher.

Die SINA Workstation bietet einen modernen und leistungsfähigen Arbeitsplatz für sicheres Arbeiten unterwegs und im Home Office. Mit Laptop oder Tablet können Nutzer ihre gewohnten Anwendungen wie Office-Programme uneingeschränkt überall nutzen und haben Zugriff auf ihre Dokumente im Firmennetzwerk.
Als IT-Sicherheitspartner der Bundesrepublik Deutschland bieten wir mit dem SINA Mobil-Portfolio premiumsichere Clients bis zur Geheimhaltungsstufe GEHEIM.

secunet.com protecting digital infrastructures

secunet