secuview

Das secunet Kundenmagazin 2•2020

Technologische Autonomie Europas

Luigi Rebuffi, Generalsekretär der ECSO, über vertrauenswürdige Cybersicherheit aus Europa

Heißer Draht in Zeiten der Krise

Sichere Audio- und Videotelefonie beim Bundesministerium für Gesundheit

Aufbruch in den Orbit

Cyber-Hochsicherheit für die Raumfahrt

National

International

Technologien&Lösungen

Kurz notiert

Service

Liebe Leserinnen und Leser,

ein Jahr geht zu Ende, das den Menschen viel abverlangt hat. Die Corona-Pandemie bringt das öffentliche Leben in manchen Bereichen nun schon zum zweiten Mal fast zum Erliegen. Bleibt zu hoffen, dass uns das Jahr 2021 eine schrittweise Rückkehr in die Normalität bescheren wird und dass die negativen Folgen für Wirtschaft und Gesellschaft nicht allzu gravierend ausfallen.

Es ist allerdings auch zu beobachten, dass die Krise eine unvermeidliche, aber in Teilen etwas verschleppte Entwicklung beschleunigt: Sie wirkt als Katalysator für die digitale Transformation. Das Paradebeispiel dafür ist der Wandel der Arbeitswelt. Seit März 2020 haben secunet Kundenteams eine Vielzahl von Behörden und Unternehmen mit Technologie ausgestattet, die sicheres mobiles Arbeiten mit vertraulichen Daten möglich macht. Sie haben einen Wandel begleitet, der ganz sicher von Dauer sein wird. Wer erlebt hat, dass die Onlinekonferenz im Home Office mitunter die gleichen Ergebnisse liefern kann wie die Geschäftsreise um die halbe Welt, der möchte nicht mehr ohne Wenn und Aber zum alten Modell zurück.

Ein weiteres Beispiel ist das eGovernment: Mit ihrem aktuellen, Corona-bedingten Konjunkturpaket zielt die Bundesregierung unter anderem auf eine beschleunigte Umsetzung des Onlinezugangsgesetzes ab. Dieses Gesetz verpflichtet Bund, Länder und Kommunen, bis 2022 alle Verwaltungsleistungen digital anzubieten. Auch hier kann die Krise also für einen Digitalisierungsschub sorgen. Die Technik für sicheres eGovernment ist längst vorhanden.

Die Krise hat auch ein Schlaglicht auf weltweite Lieferketten und außereuropäische Abhängigkeiten geworfen. Wie können wir unsere technologische Souveränität stärken? Ich freue mich, dass Luigi Rebuffi, Generalsekretär der European Cyber Security Organisation (ECSO), dieses Thema – das auch secunet seit Langem beschäftigt – in seinem Gastbeitrag in der vorliegenden secuview aufgreift.

Übrigens durchläuft auch unsere Kundenzeitschrift gerade eine digitale Transformation. Die gedruckte Version, die Sie gerade in den Händen halten, wird zwar weiterhin jedes halbe Jahr erscheinen. Doch sie wird künftig durch das neue secuview Onlineportal ergänzt, das Ihnen den gewohnten Mix aus Neuigkeiten, Hintergrundberichten, Gastbeiträgen und Interviews aus der Welt der Cybersicherheit auch digital nahebringt. Es würde mich freuen, wenn Sie öfter vorbeischauen.

Ich wünsche Ihnen – trotz der Einschränkungen – frohe Feiertage und einen guten Start ins neue Jahr. Machen Sie das Beste daraus und bleiben Sie gesund!

Ihr Axel Deininger

Sichere Audio- und Videotelefonie beim Bundesministerium für Gesundheit

Heißer Draht in Zeiten der Krise

Wie für viele Menschen, Unternehmen und Behörden ist das Jahr 2020 auch für das Bundesministerium der Gesundheit (BMG) ein Jahr mit besonderen Herausforderungen. Im Frühjahr fand sich das BMG im Zentrum der Corona-Krise wieder. Vertrauliche interne und externe Abstimmungen wurden dadurch noch wichtiger als zuvor. Innerhalb kürzester Zeit erstellte das BMG ein Sicherheitskonzept für eine benutzerfreundliche Videotelefonie-Lösung und baute diese gemeinsam mit secunet und anderen Partnern und Dienstleistern auf. Das BMG setzt die Lösung seither ständig ein – unter anderem für den täglichen Austausch mit anderen Institutionen des Gesundheitssektors.

Im März 2020 überschlugen sich die Ereignisse: Die Covid-19-Epidemie, die seit Anfang des Jahres immer stärker die Schlagzeilen dominiert hatte, wurde von der WHO am 11. März zur weltweiten Pandemie erklärt. Am 17. März setzte das Robert Koch-Institut (RKI) seine Risikobewertung für die Bevölkerung in Deutschland von „gering bis mäßig“ auf „hoch“ herauf. Am 26. März bewertete es das Risiko dann als „sehr hoch“.

Bereits als sich abzeichnete, dass eine ernste Krise vor den Toren stand, hatte man im Bundesministerium für Gesundheit mit dem Aufbau eines Lagezentrums begonnen. Dort laufen alle relevanten Informationen zusammen und finden die notwendigen Abstimmungsrunden statt. Auch mit anderen Ländern muss das BMG insbesondere in Zeiten der Pandemie ständig Kontakt halten. Für solche Zwecke ist es essenziell, dass sichere, aber auch einfach zu nutzende Kommunikations-Tools zur Verfügung stehen, auf die sich die Behördenmitarbeiter verlassen können.

Mitte März nahm das BMG Kontakt zu secunet auf, um eine neue Webkonferenz-Lösung umzusetzen. Trotz des Zeitdrucks war klar, dass die Lösung höchsten Sicherheitsanforderungen genügen musste. So gibt die Netzwerkinfrastruktur „Netze des Bundes“ (NdB), die von den Bundesbehörden in Deutschland genutzt wird, klare Standards vor.

Das Bundesministerium für Gesundheit in Berlin

Balance von Sicherheit und Nutzbarkeit

Neben der Anbindung an die NdB sollte die Lösung mit einer Vielzahl anderer bestehender Netze, Anwendungen und Technologien verbunden werden, damit sie möglichst breit nutzbar ist. Dazu gehören vom BMG bereits betriebene Videokonferenz-Anlagen, SIP-Videokonferenzsysteme sowie Videoanrufe per Browser über WebRTC. Nicht zuletzt sollte neben all den Voice-over-IP (VoIP)-basierten Anwendungen auch das traditionelle, öffentliche Telefonfestnetz angebunden werden. Das BMG legte Wert darauf, dass virtuelle Konferenzräume für die neue Lösung unkompliziert gebucht werden können. Raumnummern sowie PINs sollten dabei dynamisch für jede individuelle Konferenz vergeben werden, um eine gute Balance von Sicherheit und komfortabler Nutzbarkeit zu erreichen.

Am 23. März, wenige Tage nach der ersten Kontaktaufnahme zu diesem Thema, startete das Projekt mit einem Kick-off-Meeting. Zum Projektteam gehörten neben dem BMG und weiteren Projektpartnern auch die Firma secunet, der auf VoIP-Lösungen und VoIP-Sicherheit spezialisierte Anbieter FRAFOS sowie das Unternehmen VoIP-GO, das unter anderem technischen Support rund um VoIP-Lösungen bietet. Beide sind langjährige Partner von secunet.

Unterschiedliche Technologien, alle unter einem Hut

Neben den Einschränkungen durch die Corona-Pandemie bestanden auch technische Herausforderungen: Das Projektteam musste eine Vielzahl verschiedener Komponenten einbinden, die teilweise von verschiedenen Herstellern stammten. Netzwerk, Firewalls, vorhandene Videokonferenz-Technologie, Buchungssystem, Virtualisierungsserver, Management-Netze und einiges mehr mussten am Ende reibungslos zusammenarbeiten. Dabei zahlte es sich aus, dass ein zentraler Baustein bereits als Standardprodukt vorhanden war: der

secunet Session Border Controller (SBC). Er dient unter anderem dazu, verschiedene VoIP-Netze sicher miteinander zu verbinden und sie mittels einer integrierten Firewall vor Angriffen von außen zu schützen.

Entwicklung und Installation schritten zügig voran und am 30. März – nur eine Woche nach Projektstart – konnte das BMG mit der neuen Lösung bereits die ersten sicheren Videokonferenzen durchführen. Weitere Meilensteine erreichte das Projektteam in schneller Folge: Am 2. April standen Videoanrufe aus dem Browser über WebRTC zur Verfügung und am 6. April – nach nur zwei Wochen – nutzte das Krisenzentrum des BMG die Lösung zum ersten Mal.

Ein Sprint pro Tag

Möglich wurde dieses Tempo durch agiles Projektmanagement. Die Entwicklung erfolgte inkrementell, also in klar definierten Teilabschnitten. Die einzelnen Entwicklungszyklen – „Sprints" – waren dabei bewusst kurz gehalten: Meist gab es einen Sprint pro Tag. In täglichen Statuscalls hielt sich das Projektteam organisationsübergreifend über den Stand der Dinge auf dem Laufenden. Zudem lief nicht nur die Zusammenarbeit zwischen secunet und seinen Partnern auf der einen Seite und dem BMG auf der anderen reibungslos und partnerschaftlich, auch andere Dienstleister des BMG waren gut eingebunden – eine wichtige Voraussetzung für ein gelungenes Projekt.

Im Ergebnis erfüllt die Lösung sämtliche Anforderungen des BMG, macht keine Kompromisse bei der Sicherheit und lässt sich gleichzeitig komfortabel nutzen. Zum Beispiel sorgt ein eigens entwickelter Mechanismus für Schutz vor Brute-Force- bzw. Denial-of-Service-Angriffen, ohne zusätzliche Maßnahmen zu erfordern, die dann wieder auf Kosten der Nutzbarkeit gegangen wären. Nicht zuletzt trägt auch der 24/7-Support des secunet Partners VoIP-GO zur hohen Nutzerakzeptanz bei.

Die Lösung ermöglicht sichere und einfache Kommunikation und leistet damit einen Beitrag dazu, dass das BMG und sein Geschäftsbereich während der Corona-Krise handlungsfähig bleiben. Weitere Schritte wurden seit Projektbeginn umgesetzt. Die Webkonferenzlösung wurde sowohl hinsichtlich der Leistungsfähigkeit als auch der Funktionalität ausgebaut und wird für die Geschäftsbereichsbehörden des BMG zur Nutzung bereitgestellt.

Marcel Göhler
marcel.goehler@secunet.com

Der **secunet Session Border Controller (SBC)** sorgt für eine optimale Verknüpfung verschiedener VoIP-Netze und dient diesen als zentraler Zugangspunkt. Darüber hinaus bietet er eine Firewall-Funktionalität, die das interne Netz schützt und mit Maßnahmen zu Fraud Detection und Fraud Prevention auch Angriffe von außen abwehrt. Der secunet SBC lässt sich transparent in jede bestehende IT-Infrastruktur implementieren. Er arbeitet in einem isolierten Container auf der Firewall-Plattform secunet wall. 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: Sie ist mit der Zertifizierungskennung BSI-DSZ-CC-1089 für die höchste Angriffsstärke CC EAL 4+ zertifiziert.

Umstellung auf IPv6

ELSTER: Fit für die digitale Zukunft

Manche technologischen Umwälzungen haben durchaus weitreichende Auswirkungen, werden aber von einer breiteren Öffentlichkeit kaum bemerkt. Dazu zählt die Ablösung des jahrzehntelang maßgeblichen Internet-Protokolls IPv4 durch die Version IPv6. Für die elektronische Steuererklärung ELSTER war die langfristig unvermeidliche Umstellung ein Thema mit hoher Priorität. Die Lösung musste einem strengen Sicherheitskonzept folgen, sollte aber möglichst frühzeitig umgesetzt werden – und das im laufenden Betrieb. Gemeinsam mit secunet konnte ELSTER das Projekt planen und durchführen.

Die Geschichte von IPv6 begann bereits in den 1990er Jahren, als absehbar wurde, dass IPv4 nicht genug IP-Adressen bereitstellen konnte, um den rasant wachsenden, weltweiten Bedarf zu decken. In der Folge behalfen sich Internetprovider mit Notlösungen wie dem Verfahren „Network Address Translation“ (NAT), das die mehrfache Verwendung von IP-Adressen ermöglicht. Dadurch gelang es, das Problem der Adressknappheit noch viele Jahre aufzuschieben. Doch im Laufe der 2010er Jahre wurde klar, dass ein Wechsel auf IPv6 die einzig verbliebene Möglichkeit war.

IPv6 bietet einen wesentlich größeren Adressraum als IPv4 und darüber hinaus eine Reihe weiterer Vorteile, die etwa die Cybersicherheit und die Vernetzung mobiler Endgeräte betreffen. Übrigens war die Versionsnummer 5 schon durch eine experimentelle IP-Variante aus den frühen 1990er Jahren belegt, so dass der Nachfolger der Version 4 direkt die Nummer 6 erhielt.

Version 6 auf dem Vormarsch

Seit einigen Jahren vollzieht sich ein schleichender Übergang auf die neue Protokollversion. Google meldete für Oktober 2020 eine IPv6-Adaption in Deutschland von rund 50 %. Mittlerweile können kleinere, regionale Internetprovider keine IPv4-Netze mehr vergeben und sind daher dazu übergegangen, ihre Kunden mit IPv6-Netzen zu versorgen. Den zunächst weiterhin benötigten Zugang zu IPv4 stellen sie dann über NAT her. Das führt dazu, dass die Zahl der Endnutzer, die mit IPv6 unterwegs sind, in letzter Zeit stark anwächst. Probleme können auftreten, wenn Internetnutzer aus Deutschland etwa bei Auslandsreisen IPv6-only-Zugänge erhalten. Dann lassen sich IPv4-basierte Webdienste nicht nutzen.

ELSTER, die elektronische Steuererklärung, ist das größte und wohl erfolgreichste eGovernment-Verfahren in Deutschland.

Für Betreiber von Online-Diensten ist aus diesen Gründen der Zeitpunkt gekommen, ihre Services auf IPv6 auszurichten. Dies gilt in besonderem Maß für staatliche Stellen, die gesellschaftlich relevante eGovernment-Leistungen anbieten. Von Seiten des Bundes gibt es eine Vorgabe für deutsche Behörden, so bald wie möglich auf IPv6 zu wechseln. Eine Hürde sind jedoch die technischen Herausforderungen bei der Umstellung im laufenden Betrieb.

Gewappnet für die Übergangszeit

Das größte und wohl erfolgreichste eGovernment-Verfahren in Deutschland ist ELSTER, die elektronische Steuererklärung, die vom Bayerischen Landesamt für Steuern (BayLfSt) betrieben wird. „Uns war eine rechtzeitige IPv6-Umstellung wichtig, um allen Endnutzern weiterhin die gewohnt hohe Qualität unserer Onlinedienste bieten zu können“, so Leo Fleiner, Referatsleiter beim BayLfSt. „Dabei fassten wir eine Dual-Stack-Lösung ins Auge: Das bedeutet, dass das Portal „Mein ELSTER“ sowohl aus dem IPv6-Adressraum als auch, während einer Übergangszeit, weiterhin aus dem IPv4-Adressraum verfügbar sein sollte.“

Bei diesem Umstellungsprojekt arbeitete das BayLfSt mit secunet zusammen. Das Unternehmen leistet bereits seit 1998 Beiträge zur sicheren Online-Authentisierung bei ELSTER. Auf Basis des Adressplans des BayLfSt unterstützte secunet bei der Entwicklung eines Migrationskonzepts. Das Sicherheitskonzept der ELSTER-Umgebung wurde durch das BayLfSt und secunet den modernen Gegebenheiten angepasst, die unter anderem die sichere Konfiguration und den Betrieb von bestehenden und neuen Netzwerkkomponenten und insbesondere Firewalls erlauben.

Umsetzung Schritt für Schritt

Nun begann die Migrationsphase. Service-Ausfallzeiten sind für einen millionenfach genutzten eGovernment-Dienst naturgemäß keine Option. Das BayLfSt setzte die erarbeiteten und von secunet qualitätsgesicherten Migrationsplanungen in mehreren zeitlich gestaffelten Schritten um. Das Portal „Mein ELSTER“ stand für die Endnutzer jederzeit wie gewohnt zur Verfügung.

Eine weitere Herausforderung war die Umstellung der rechenzentrumsinternen Dienste im laufenden Betrieb mit möglichst wenig bis keinen Ausfallzeiten. Die vom BayLfSt erarbeiteten und von secunet wiederum qualitätsgesicherten Migrationsstrategien und -konzepte wurden im BayLfSt unter fachlicher Begleitung von secunet umgesetzt. So gelang eine reibungslose Migration auf einen rechenzentrumsinternen Dual-Stack-Betrieb. Zwischenzeitlich werden die internen Dienste so gut wie ausschließlich mit IPv6 betrieben. secunet führte auch interne Schulungen durch, etwa zu den Sicherheitsaspekten von IPv6.

Ende August 2020 war es dann soweit: Dem Portal „Mein ELSTER“ wurde eine öffentliche IPv6-Adresse zugewiesen. Seitdem ist der Name www.elster.de mit IPv6 auflösbar – und dank Dual-Stack-Lösung auch weiterhin mit IPv4. Das Projekt lag zudem gut in der Zeit: Mit ELSTER ist das BayLfSt die erste deutsche Behörde, die eine Komplettumstellung eines Rechenzentrums auf IPv6 vollzogen hat. „Wir haben die Umstellung auf eine Weise gelöst, die technisch anspruchsvoll ist, aber eine Reihe von Vorteilen für den kontinuierlichen Betrieb bietet“, sagt Ralf Käck vom BayLfSt.

Oliver Wolf
oliver.wolf@secunet.com

Technologische Autonomie Europas

Öffentlich-private Zusammenarbeit bei der Entwicklung vertrauenswürdiger europäischer Cybersecurity-Lösungen

Von Luigi Rebuffi, Generalsekretär der European Cyber Security Organisation (ECSO)

Eine der vorrangigen geplanten Maßnahmen der Europäischen Kommission ist es, eine „technologische Souveränität" Europas zu entwickeln. Mit diesem Begriff aus dem Brüsseler Jargon ist eigentlich „technologische Autonomie" gemeint – d.h. Europa sollte seine Autonomie im digitalen oder technologischen Bereich erhöhen.

Luigi Rebuffi

Tatsächlich hat uns die Covid-19-Krise gelehrt, dass zahlreiche Branchen in Europa – darunter auch der digitale Bereich – mehr „Autonomie" benötigen. Die Kommission erklärt in diesem Zusammenhang, dass die digitale Souveränität in Europa (und auch hier werden die Konzepte von Autonomie und Souveränität vermischt) auf drei untrennbaren Säulen ruht: Rechenleistung, Kontrolle über unsere Daten und sichere Konnektivität. Was jedoch weitaus seltener erwähnt wird, ist die Tatsache, dass auch andere strategische Technologien bei einer ganzheitlichen Betrachtung berücksichtigt werden sollten, und dass Cybersicherheit der Kitt ist, der all diese Säulen zusammenhält.

Natürlich ist es nicht einfach, in einer Welt, in der die Lieferketten eng verzahnt und geografisch weit verteilt sind, über vollständig autonome technologische Fähigkeiten auf europäischer Ebene zu sprechen. Wie können wir bestimmte Komponenten, Geräte oder Systeme kontrollieren, die in einem anderen Land (oder auf einem anderen Kontinent) produziert werden, um eine vertrauenswürdige Lieferkette aufzubauen? Die nationalen Verwaltungen in Europa könnten bestätigen, dass bestimmte Komponenten oder Geräte, die andernorts in der Welt gefertigt wurden, sowie mögliche Updates bzw. Patches (sofern sie bestimmte Regeln einhalten) den nationalen Sicherheitsgesetzen entsprechen (bei denen es sich in diesem Fall tatsächlich um Souveränitätsgesetze handelt) und dass sie daher vertrauensvoll in der Lieferkette eingesetzt werden können. Systeme oder Dienstleistungen, die auf diese Weise entstehen, können als „souverän" betrachtet werden, da sie nationale Gesetzgebungen respektieren. Dann könnten wir von „souveränen Fähigkeiten" sprechen.

Luigi Rebuffi

Luigi Rebuffi ist Generalsekretär und Gründer der ECSO (European Cyber Security Organisation) sowie Gründer und Generalsekretär der Women4Cyber Foundation. Nach seinem Abschluss in Kerntechnik am Politecnico di Milano (Italien) arbeitete er in Deutschland an der Entwicklung von Hochleistungsmikrowellensystemen für den thermonuklearen Fusionsreaktor ITER. Er setzte seine Karriere bei Thomson CSF / Thales in Frankreich fort, wo er zunehmend Verantwortung für europäische Angelegenheiten im Bereich Forschung und Entwicklung in verschiedenen Sektoren übernahm: Telekommunikation, Industrie, Medizin, Wissenschaft. 2003 wurde er Direktor für europäische Angelegenheiten für die zivilen Aktivitäten der Gruppe. Er schlug die Gründung der EOS (Europäische Organisation für Sicherheit) vor, koordinierte deren Gründung im Jahr 2007 und war 10 Jahre lang ihr CEO. Bis 2016 und sechs Jahre lang war er Berater der Europäischen Kommission für das EU-Sicherheitsforschungsprogramm und Präsident des Lenkungsausschusses für Sicherheitsforschung der französischen Förderungsorganisation ANR. Im Jahr 2016 gehörte er zu den Gründern der ECSO und unterzeichnete mit der Europäischen Kommission den cPPP zu Cybersicherheit. Im Jahr 2019 gründete er die Women4Cyber Foundation, um die Beteiligung von Frauen an der Cybersicherheit zu fördern, und wurde ihr derzeitiger Generalsekretär und Mitglied ihres Verwaltungsgremiums. Im Jahr 2020 wurde er in die Liste "IFSEC Global Influencers in Security - Executives" aufgenommen.

Die Diversifizierung von Lieferanten trägt ebenfalls zu diesem Konzept bei. Denn Souveränität bedeutet für ein Land bzw. für Europa auch, seiner Bevölkerung, der Gesellschaft oder der Wirtschaft unabhängig von (potenziell) kritischen Situationen sichere oder unverzichtbare Leistungen bereitstellen zu können. (Man denke nur an den Beginn der Covid-19-Krise, als in Europa bei medizinischem Equipment eine Abhängigkeit von nur einem Land bestand und die Anzahl der Lieferanten zu klein war).

Der Beitrag Deutschlands

Besonders jetzt, da Deutschland die Präsidentschaft im Rat der Europäischen Union innehat, sollte man erwähnen, welch führende Rolle deutsche Unternehmen und Branchenverbände bei dem Thema einnehmen. Beispielsweise setzt sich Axel Deininger, CEO von secunet, stark für das neue ECSO-Label „Cybersecurity Made in Europe" ein. Damit unterstützt secunet die Harmonisierung des europäischen Cybersecurity-Ökosystems durch diese wichtige Marketing-Innovation für kleinere IT-Sicherheitsunternehmen.

Darüber hinaus arbeiten weitere prominente deutsche Verbände wie TeleTrusT und eurobits e.V. eng mit der ECSO zusammen. eurobits war erst kürzlich ein Partner bei den ECSO Cyber Investor Days vom 30. November bis 1. Dezember in Bochum. TeleTrusT ist eines der Gründungsmitglieder der ECSO, damals unterstützt von Gerd Müller, der ebenfalls bei secunet tätig ist. Deutsche Unternehmen und Verbände sehen also einen Bedarf an echten europäischen Cybersecurity-Lösungen.

Auch auf nationaler institutioneller Ebene wird dieses Thema wahrgenommen. Die Unterstützung des Projekts GAIA-X durch das Bundesministerium für Wirtschaft und Energie zeigt – wenngleich der Fokus dabei mehr auf Daten- als auf umfassender Cybersicherheit liegt –, dass auf der Ebene der nationalen Verwaltung die Auffassung besteht, Europa müsse gemeinsame europäische Lösungen in den verschiedenen Bereichen neuer Technologien hervorbringen, um mehr Kontrolle über die nationale Sicherheit und die von der Digitalisierung vorangetriebene wirtschaftliche Entwicklung zu haben.

Insgesamt verbessert Europa seinen digitalen Reifegrad stetig weiter und gelangt zunehmend zu der Erkenntnis, dass – vielleicht in Zukunft – eine engere Kooperation erforderlich ist, bei der die Länder bereit sein müssen, etwas von ihrer nationalen Souveränität preiszugeben, um eine stärkere gemeinschaftliche Souveränität zu erlangen. Doch dieser Prozess benötigt Zeit.

Der Mehrwert eines öffentlich-privaten Dialogs

In diesem Reifeprozess ist ein öffentlich-privater Dialog entscheidend, um den Weg zu einer gemeinsamen europäischen Souveränität zu identifizieren und eine Zunahme digitaler (strategischer) Autonomie zu unterstützen – insbesondere in Verbindung mit den benötigten Investitionen und Beschaffungsregeln für sensible Anwendungen. Genau hier setzt die ECSO an, die mit ihren Mitgliedern aus dem öffentlichen und dem privaten Sektor einen hohen Mehrwert für Europa mit sich bringt.

Die ECSO hat gerade erst eine neue Arbeitsgruppe ins Leben gerufen, die sich mit Souveränität und Autonomie im Bereich Cybersicherheit (Cyber Security Sovereignty and Autonomy, CYSSA) befasst. Dabei wirken ECSO-Mitglieder mit. Auftrag dieser

Arbeitsgruppe ist es, mögliche Antworten auf einige der in diesem Artikel aufgeworfenen Fragen zu finden und zu erörtern, wo die Prioritäten liegen sollen, um die strategische Autonomie Europas in Sachen Cybersecurity zu erhöhen.

Ziel der neuen ECSO-Arbeitsgruppe ist es, gemeinsame Aussagen zu Europas Souveränität und strategischer Autonomie im Bereich Cybersicherheit zu entwickeln und zu vermitteln. Dabei sollen auch Chancen für europäische Lösungen erschlossen und das Wachstum unserer Branche gefördert werden.

Die Aktivitäten der CYSSA-Arbeitsgruppe stehen im Einklang mit den Bestrebungen der Europäischen Kommission rund um „technologische Souveränität". Auch im Zusammenhang mit dem Ansatz eines europäischen Kompetenzzentrums würden sie den institutionellen Erwartungen gerecht. Dieses Vorgehen sollte den europäischen ECSO-Mitgliedern, darunter secunet, bei der Entwicklung ihrer Märkte helfen und dazu beitragen, dass die ECSO als führende Stimme für die Autonomie und Souveränität Europas im Bereich Cybersicherheit wahrgenommen wird und als solche mehr Unterstützung und Teilnahme von Branchenakteuren und den Verwaltungen in Europa erfährt.

Durch den Dialog mit dem öffentlichen Sektor wird die bestmögliche Balance zwischen Souveränitätsgesetzen und technischen (zunehmend autonomen) Lösungen ermöglicht. Dabei wird auch berücksichtigt, dass es notwendig sein kann, Lösungen von außerhalb der EU zu verwenden, wenn keine europäischen Lösungen verfügbar sind. Bei nicht-sensiblen Anwendungen liegt möglicherweise auch keine Notwendigkeit vor, diese Art von Lieferanten einzuschränken. Dagegen sollten bei sensiblen Anwendungen (nach Definition der nationalen Verwaltungen) EU-fremde Lösungen, die in den jeweiligen Systemen oder Diensten implementiert sind, durch die nationalen Verwaltungen bewertet und mit einer Art „Souveränitätsvalidierung" versehen werden.

Die Zukunft der Cybersicherheit Europas in einer sich schnell verändernden Welt

Viele Fragen sind noch offen: Welche strategischen Technologien / Komponenten / Geräte / Systeme / Dienste werden benötigt, um die nationale Sicherheit (entsprechend der Leitlinien der nationalen Verwaltungen) zu gewährleisten und strategisches Wirtschaftswachstum zu fördern? Welche Fähigkeiten und Kapazitäten sind in Europa vorhanden? Welche fehlen? Welche könnten oder sollten entwickelt werden und wann? Welche Investitionen sind dazu nötig? Was sollte von außerhalb eingekauft und dann als vertrauenswürdig eingestuft werden (durch Validierung bzw. Zertifizierung, sofern erforderlich)?

In dieser komplexen Zukunft wird die ECSO auch weiterhin die öffentliche und private Cybersecurity-Community in Europa zusammenführen, die Wettbewerbsfähigkeit ihrer Mitglieder und des europäischen Cybersecurity-Ökosystems weiterentwickeln und die Zunahme der digitalen Autonomie Europas fördern.

Wir stehen an einer kritischen Wegmarke im globalen technologischen Wettbewerb. Wir brauchen mutige, radikale und transformative Maßnahmen, um sicherzustellen, dass die Cybersicherheit Europas auch in Zukunft gewahrt bleibt. Wir müssen im Rahmen von öffentlich-privaten Foren zusammenarbeiten, damit wir gemeinsame Probleme gemeinschaftlich in Angriff nehmen und eine gemeinsame Sprache sprechen. Nur so können wir die europäische Cybersecurity-Community zusammenbringen und dafür sorgen, dass Europa in der Lage ist, eigene Cybersecurity-Lösungen zu entwickeln, um seine Zukunft in dieser unsicheren Welt zu schützen.

SECUNET: ECSO-MITGLIED DER ERSTEN STUNDE

Am 5. Juli 2016 wurde als Teil der Cybersicherheitsstrategie der EU eine Public Private Partnership zwischen der Europäischen Kommission und der neu gegründeten ECSO geschlossen. secunet war maßgeblich an der Gründung der ECSO beteiligt und unterstützt deren Aktivitäten bis heute.

Axel Deininger
- seit September 2020 Mitglied im Board of Directors

Gerd Müller
- für TeleTrusT (bis August 2020): Vice Chairman im Board of Directors, Mitglied im Partnership Board, Mitwirkung im Financial Committee und Strategy Committee
- seit September 2020 für eurobits e.V. Bochum: Mitglied im Board of Directors

Peter Rost
- Vice Chair Working Group (WG) 2 Market deployment, investments und darüber hinaus im Strategy Board, Mitarbeit WG 3 und 4

Christine Skropke
- Mitglied Council Women4Cyber und Partnership Board sowie Mitarbeit in WG 4 SME / Regions

Flughafen Sofia

Europäische Grenzkontrolle in Bulgarien

SSARM und secunet setzen das europaweit erste EES-Projekt um

In Vorbereitung auf das geplante europäische Einreise-/Ausreisesystem (Entry/Exit-System, EES) hat sich Bulgarien für Grenzkontrolltechnologie von SSARM und secunet entschieden. Die Gesamtlösung wird die bulgarischen Behörden entlasten und den zusätzlichen Aufwand abfedern, der künftig durch die Erfassung biometrischer Daten an der Grenze entsteht.

Im Rahmen der Smart Borders Initiative hat das EU-Parlament die Einführung des gemeinsamen biometrischen Einreise-/Ausreisesystems EES zur Registrierung aller Reisenden aus Drittstaaten (Third Country Nationals, TCN) beschlossen. TCN müssen sich demnach ab 2022 bei der Einreise in Länder des Schengen-Raums an Land-, See- und Luftgrenzen mit vier Fingerabdrücken und Gesichtsbild registrieren lassen.

Das bulgarische Innenministerium hat im Rahmen einer Ausschreibung die Firma SSARM als Generalunternehmer mit der Implementierung des europaweit ersten EES-Projekts beauftragt. secunet liefert und

installiert als Subunternehmer von SSARM 20 secunet easygates für die automatisierte Grenzkontrolle einschließlich Gesichts- und Fingerabdruckverifikation sowie acht Selbstbedienungskioske – secunet easykiosk – für die Vorerfassung von TCN. Für stationäre Grenzkontrollschalter stellt secunet 66 secunet easytowers sowie Fingerabdruckscanner für eine qualitativ hochwertige biometrische Erfassung von Gesichtsbildern und Fingerabdrücken bereit. Die EES-Komponenten werden an den Flughäfen in Sofia, Varna und Burgas installiert.

Automatisierte Systeme und Selbstbedienungssysteme spielen eine Schlüsselrolle, um den zusätzlichen Aufwand zu kompensieren, den das EES durch die biometrische Erfassung an der Grenze erfordert. Der Grenzkontrollprozess wird durch die Lösungen sowohl vereinfacht als auch beschleunigt. Mit den EES-Lösungen aus der Produktfamilie secunet border gears wird Bulgarien die neuesten Technologien für eine zukunftsfähige, sichere und effiziente Grenzkontrolle implementieren.

Zum Einsatz kommt die neue Generation des secunet easygate. Sie bietet modernste Gesichts- und Fingerabdruckverifikation sowie die neuesten Schutzmechanismen für die Erkennung von Täuschungsversuchen, sogenannten Präsentationsangriffen.

secunet easykiosk und secunet easytower gewährleisten die ISO-konforme, qualitativ hochwertige Erfassung von Gesicht und Fingerabdrücken. In Anbetracht der Größenordnung des EES mit geschätzten 300 Millionen Einträgen von TCN ist dies eine Grundvoraussetzung für die zuverlässige und effiziente Identifizierung bei Grenzkontrollen.

SSARM ist in der Rolle des Generalunternehmers für das Projektmanagement verantwortlich und stellt Installations- und Supportdienstleistungen. Die Installation beginnt am Flughafen Sofia. Aktuell rechnen die beteiligten Unternehmen mit einem Abschluss des gesamten EES-Projekts noch vor dem Sommer 2021.

Walter von Weber
walter.vonweber@international.secunet.com

QUALITÄT UND TEMPO FÜR DIE BIOMETRISCHE ERFASSUNG AN DER STATIONÄREN GRENZKONTROLLE

Der secunet easytower sorgt bei der stationären Grenzkontrolle für eine schnelle und hochwertige Gesichtsbildaufnahme. Dabei garantiert er höchste biometrische Datenqualität gemäß der EU-Verordnung 2017/2226. Mithilfe einer Höhenanpassung der Kamera sowie einer zusätzlichen diffusen Beleuchtung wird die Aufnahmequalität des frontalen Gesichtsbilds nach ISO 19794-5:2011 sichergestellt. Somit sind sämtliche EES-Qualitätsanforderungen erfüllt.

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

Michael Schwaiger
michael.schwaiger@secunet.com

Cyber-Hochsicherheit für die Raumfahrt

Aufbruch in den Orbit

Seit einigen Jahren geben innovative Technologien der Raumfahrt neuen Schub: Raketen und Satelliten werden immer kleiner. Dadurch werden sie preiswerter als ihre großen, komplexeren Vorläufer und können flexibler und in größerer Stückzahl in die Erdumlaufbahn gebracht werden. Dort übernehmen sie nützliche, teils lebenswichtige Funktionen, die aus unserem Alltag nicht mehr wegzudenken sind. Da Trägerraketen, Satelliten und Raumfahrzeuge sensible Informationen mit ihren Bodenstationen und untereinander austauschen, führt auch im Weltraum kein Weg an der Cybersicherheit vorbei. Allerdings müssen die Sicherheitstechnologien für die extremen Bedingungen im Orbit angepasst werden.

Raumfahrt macht wieder verstärkt Schlagzeilen. Erst im November 2020 ging die Nachricht um die Welt, dass das US-Raumfahrtunternehmen SpaceX im Rahmen der ersten regulären bemannten Mission eines Privatunternehmens vier Astronauten zur Internationalen Raumstation ISS gebracht hat. Doch wer sich für innovative Raumfahrtprojekte interessiert, muss nicht unbedingt über den Atlantik blicken. Auch in Europa, insbesondere in Deutschland, findet eine dynamische Technologieentwicklung statt, die immer wieder von sich reden macht und auch international Beachtung findet.

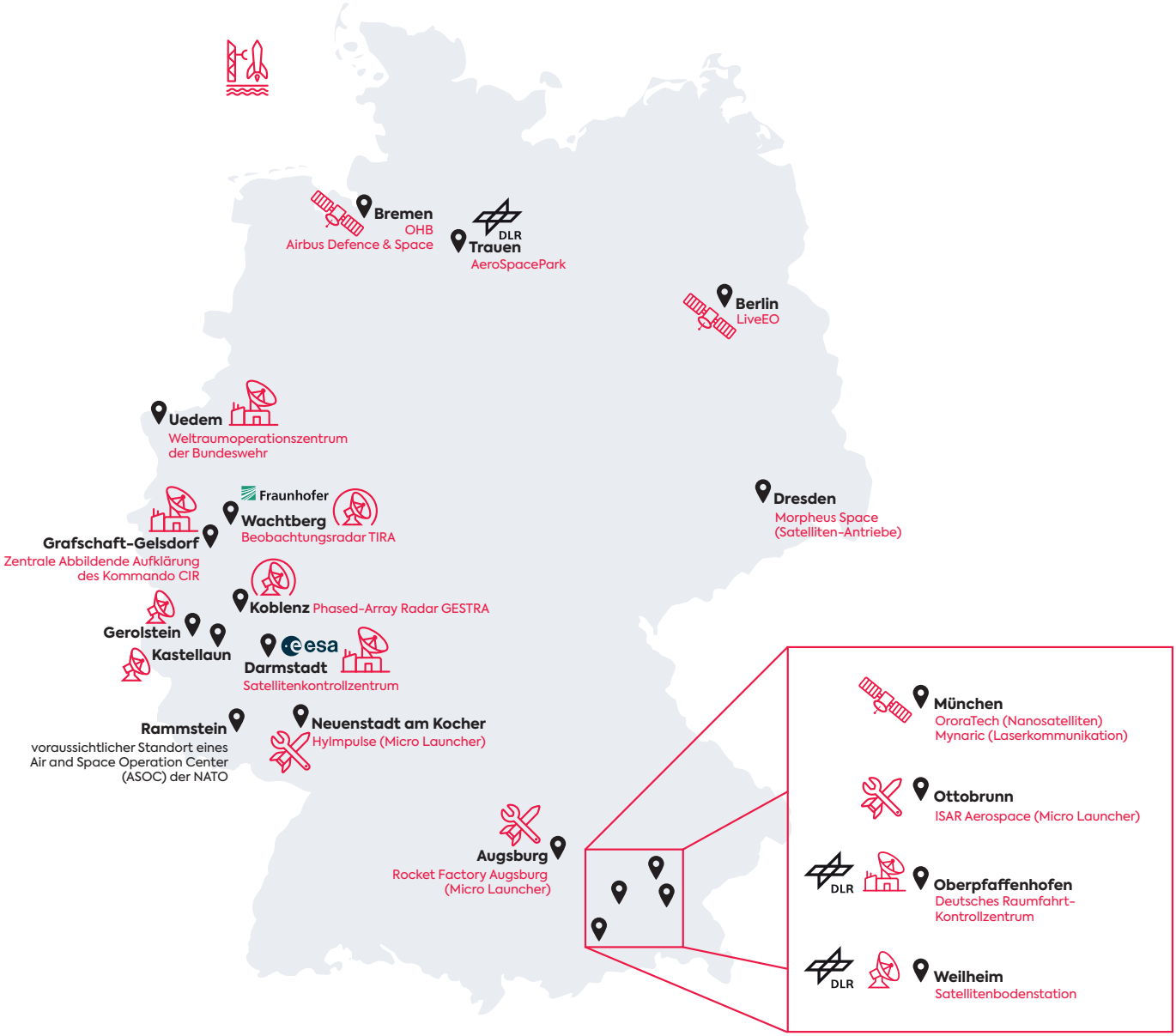
Dabei hat sich neben den traditionellen Größen wie der Europäischen Weltraumorganisation ESA, dem Deutschen Zentrum für Luft- und Raumfahrt (DLR) und den einschlägigen Konzernen ein quirliges Ökosystem von Weltraumtechnik-Startups gebildet. In

Augsburg, München oder Neuenstadt am Kocher haben sich junge Firmen niedergelassen, die leistungsfähige kleinere Raketen entwickeln. Andere Startups oder Forschungsinstitutionen bauen Satelliten, die Klimaphänomene oder Waldbrände analysieren oder die Internetversorgung verbessern. Diese „New Space"-Szene glänzt durch Innovation und treibt die etablierten Großen technologisch voran.

Mini, mikro, nano, pico, ...

Ein Trend, dem sämtliche Akteure Rechnung tragen müssen, ist die Miniaturisierung von Weltraumtechnik. Aktuelle Nano-, Cube- und Cluster-Satelliten sind zum Teil nicht größer als ein Schuhkarton. Ihre wahre Größe spielen sie dann im Verbund aus, wenn sie in großer Anzahl, als sogenannte Konstellationen, unterschiedlichste Aufgaben übernehmen. Ihre kompakten Abmessungen und ihr relativ geringes Gewicht haben einen weiteren Vorteil: Für viele aktuelle Satellitenprojekte reichen moderater dimensionierte Trägerraketen, sogenannte Micro Launcher. Diese sind weniger aufwändig und kostspielig als die klassischen großen Trägerraketen wie beispielsweise die europäische Ariane. Das macht die

Exemplarische Raumfahrt-relevante Standorte in Deutschland



neue Weltraumtechnik deutlich agiler – ein enormer Vorteil für zivile wie militärische Anwendungsszenarien. Satelliten werden immer vielfältiger und decken immer mehr Funktionen ab, die für unser tägliches Leben wichtig sind. Das europäische Satellitennavigationssystem Galileo etwa spielt (neben dem US-amerikanischen Global Positioning System) zur Positionsbestimmung in Navigationsgeräten von Fahrzeugen oder Mobiltelefonen eine große Rolle und erbringt darüber hinaus Zeitdienste, die beispielsweise für die Synchronisierung dezentraler Energienetze genutzt werden.

Auch militärische Organisationen setzen verstärkt auf Weltraumtechnik, insbesondere zur Aufklärung, Kommunikation, Navigation, zeitlichen Synchronisation und Frühwarnung. Der erste Satellit der Bundeswehr startete 2006 ins All, und zwar als einer von fünf Kleinsatelliten des Aufklärungssystems SAR-Lupe, das licht- und wetterunabhängig hochauflösende Aufnahmen von der Erdoberfläche liefert. Das leistungsstärkere Nachfolgesystem SARah wird voraussichtlich im Jahr 2021 in den Orbit gebracht.

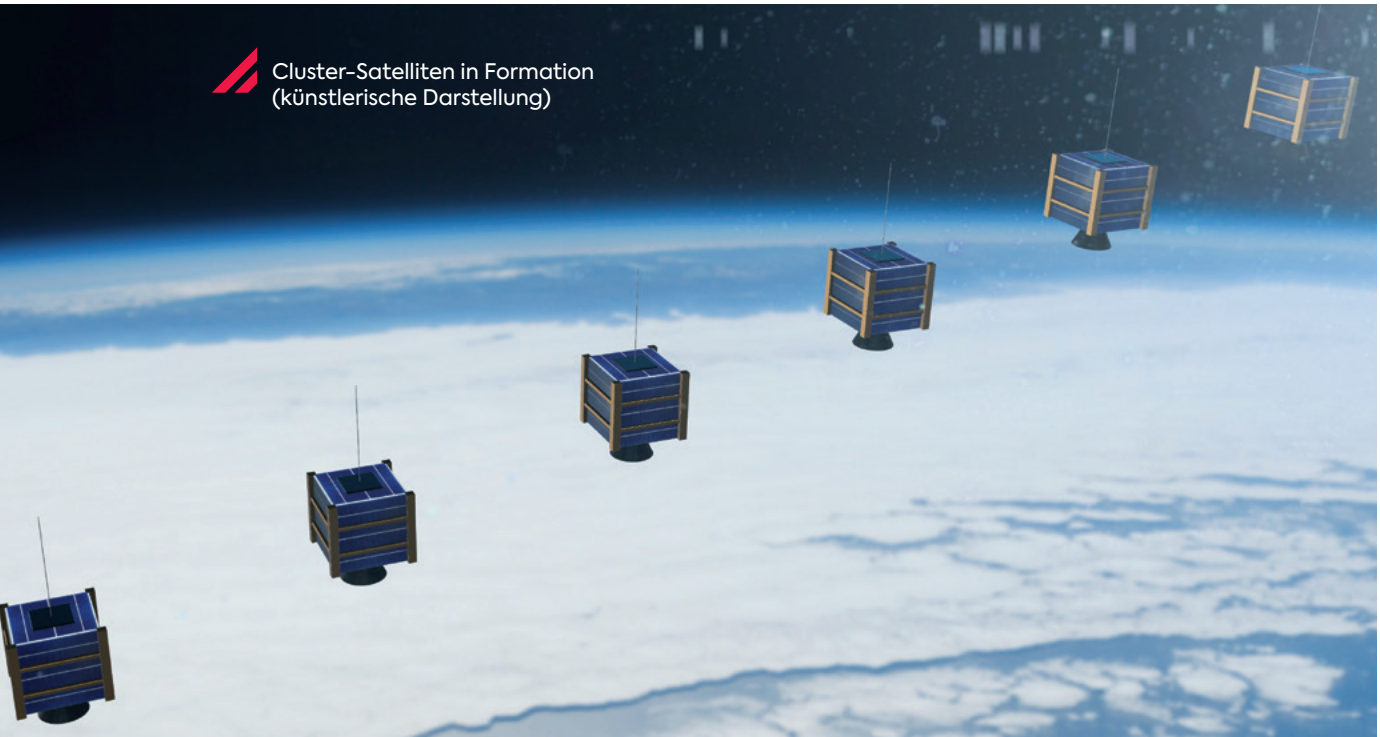
2009 und 2010 wurden die beiden Kommunikationssatelliten COMSATBw-1 und -2 gestartet, die die Bundeswehr insbesondere bei internationalen Einsätzen unabhängiger von kommerziellen Anbietern machten. Beide Satelliten ermöglichen unter anderem weltweit abhörsichere Telefongespräche, Videokonferenzen sowie Internetzugang. Zudem wird für den BND ein elektrooptischer Aufklärungssatellit entwickelt, von dem zwei Exemplare geplant sind.

Strategische Dimension

Heute wird die Raumfahrt weithin als Schlüsseltechnologie betrachtet. Die Investmentbank Morgan Stanley schätzt, dass sich der globale Raumfahrtmarkt bis 2040 verdreifachen wird, auf mehr als 1,1 Billionen US-Dollar. Weltraumgestützte Systeme leisten wesentliche Aufgaben zur Krisenfrüherkennung und damit zur außen- und sicherheitspolitischen Handlungsfähigkeit der Bundesregierung. In der aktuellen Raumfahrtstrategie der Bundesregierung heißt es: „Die innere und äußere Stabilität unseres Landes hängt zunehmend vom Funktionieren unserer im Weltraum positionierten Infrastruktur ab."

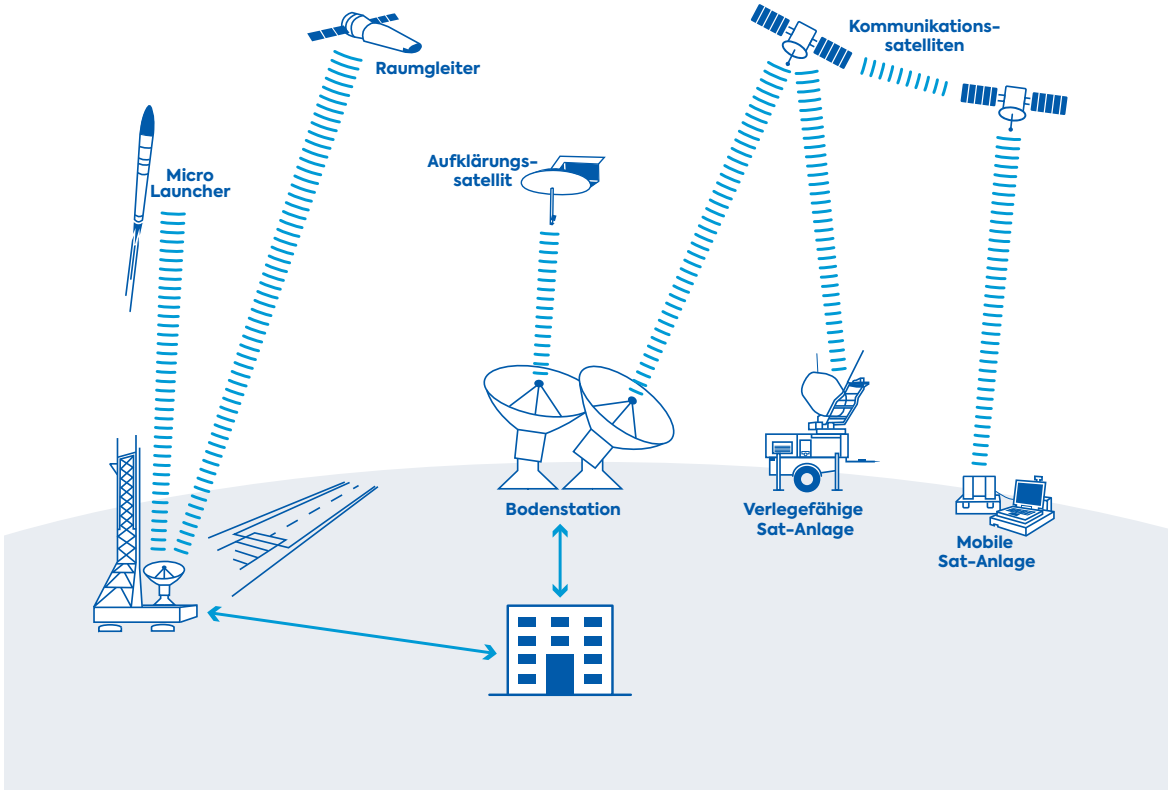
Die Technik im Orbit kann schnell zur Achillesferse werden und benötigt daher angemessenen Schutz. Ein plötzlicher Ausfall eines Satellitensystems durch Kollision, gezielte Störung, Manipulation oder gar Übernahme könnte gravierende Konsequenzen haben.

Den Schutz militärischer wie ziviler deutscher Weltraumtechnik hat das Weltraumoperationszentrum der Bundeswehr im Blick. Dort werden erdnahe Objekte im Weltraum überwacht und bei Bedarf aufgeklärt. Dazu gehören nicht nur Satelliten und andere Raumflugkörper, sondern auch Weltraumschrott, größere Meteoriten und Asteroiden, die in die Atmosphäre eintreten. Darüber hinaus umfasst das Aufgabenspektrum neuerdings auch die Planung und Durchführung von Weltraumoperationen.



Cluster-Satelliten in Formation (künstlerische Darstellung)

Grober schematischer Aufbau einer Weltrauminfrastruktur



Eigenständige Handlungsfähigkeit

Daneben verfolgt die Bundeswehr neue Ansätze, um ihre Infrastruktur im Orbit gegen Störungen und Angriffe zu wappnen – und setzt fortan auch auf miniaturisierte Weltraumtechnik. Künftig sollen ausgefallene Systeme schnell funktional wiederhergestellt oder ersetzt werden können, indem beispielsweise Klein- oder Kleinstsatelliten innerhalb kurzer Zeit in den Orbit gebracht werden. Dieser Ansatz nennt sich „Responsive Space".

Dafür wäre neben eigenen, national verfügbaren Trägerraketen auch ein eigener Startplatz von Vorteil – als Ergänzung zu den internationalen Startoptionen für leistungsstärkere Trägerraketen. Derzeit werden einige Standortkandidaten evaluiert. Auch über eine schwimmende Offshore-Plattform in der Nordsee wird dabei nachgedacht.

Neben Weltraumbeobachtung und agiler Handlungsfähigkeit wird auch Cybersicherheit künftig eine wesentliche Rolle bei der Absicherung der Infrastruktur im Orbit spielen. Zivile und militärische Weltraumtechnik wird nicht nur durch physische Einwirkung bedroht, sondern zunehmend auch durch fremdstaatliche Hackerangriffe – mit ähnlichen Konsequenzen. Manipulieren Angreifer die zwischen Satelliten und Bodenstationen ausgetauschten Steuerungsdaten, können sie schnell beträchtlichen Schaden anrichten – zumal es im Orbit immer unübersichtlicher wird: Aktuell umkreisen mehrere tausend aktive und ausgediente Satelliten die Erde, und deren Anzahl wächst stark an.

Wie lässt sich Cybersicherheit im Orbit realisieren? Ein Teil der Antwort ist, dass dazu dieselben Technologien infrage kommen, die am Boden seit vielen Jahren erfolgreich in Hochsicherheitsnetzen verwendet werden. Um sensible digitale Informationen zu kommunizieren, nutzen Behörden und Bundeswehr die Sichere Inter-Netzwerk Architektur SINA, die von secunet im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI) entwickelt wurde. Sie bietet Lösungen für sehr unterschiedliche Sicherheitsanforderungen. Die am stärksten abgesicherten SINA H-Systeme mit Zulassungen des BSI bis zum Einstufungsgrad GEHEIM werden bereits heute in großem Umfang in nationalen Hochsicherheitsinfrastrukturen eingesetzt. Auch Anbieter von Raumfahrttechnologie nutzen sie, um eingestufte Informationen zu verarbeiten. Darüber hinaus werden seit vielen Jahren größere Datenmengen, die die Bundeswehr satellitenbasiert überträgt, hochsicher mit SINA H verschlüsselt.

Extreme Betriebsbedingungen

Wer nicht nur via, sondern auch mit Satelliten oder Raumfahrzeugen hochsicher kommunizieren will, muss Verschlüsselungstechnologie an Bord der Flugobjekte integrieren. Die Anforderungen, denen Hightech-Equipment unter diesen Bedingungen genügen muss, haben es in sich. Das fängt schon beim Raketenstart an, bei dem starke Vibration und Beschleunigungskräfte auf die Hardware einwirken. In der Erdumlaufbahn angekommen, sind die Geräte sehr großen Temperaturschwankungen sowie hoher Strahlenbelastung ausgesetzt. Die nicht vorhandene Atmosphäre erfordert andere thermische Konzepte und Gerätedesigns.

Für Satellitensysteme ist hohe Zuverlässigkeit essenziell. Der partielle Ausfall einzelner Baugruppen kann ganze Weltraum-Missionen beeinträchtigen. Sind Systeme erst einmal im Orbit, bestehen nicht mehr viele Optionen für ihre Wartung und erforderliche Reparaturen. Daher sollten sie remote updatefähig und möglichst flexibel rekonfigurierbar sein. Außerdem sollten besonders wichtige Elemente von vorn herein redundant ausgelegt werden.

Noch dazu besteht mit der Miniaturisierung eine Anforderung, die sich bis auf die Ebene von Baugruppen und Modulen erstreckt. Das gilt auch für Sicherheitsmodule. Um darüber hinaus unerwünschte physische Einwirkung im Weltraum auszuschließen oder zumindest signifikant zu erschweren, sollten Satellitensysteme manipulationsgeschützt designt werden.

secunet ist seit vielen Jahren für Kunden aus dem Raumfahrtbereich tätig und verstärkt nun sein Engagement für weltraumqualifizierte Cyber-Hochsicherheitstechnologie. Als sichtbares Zeichen wird die secunet Division „Defence“ ab Januar 2021 zur Division „Defence&Space“.

Blick nach vorn

Bereits heute heben SINA Systeme in militärischen Hubschraubern ab und sorgen dort für verschlüsselte Videoübertragung und -kommunikation aus mehreren Kilometern Höhe – wir berichteten darüber in secuview 2/2019. Für diesen Einsatzfall wird eine spezielle Hardwareplattform verwendet. Was darüber hinaus auf dem Weg in den Weltraum noch zu tun bleibt, ist technisch noch anspruchsvoller, aber machbar.

Raumfahrt und Cybersicherheit sind zwei einander ergänzende, zukunftsorientierte Hochtechnologiefelder, die künftig noch stark voneinander profitieren werden. Ihr gemeinsamer Weg hat gerade erst begonnen.

Dr. Michael Sobirey
michael.sobirey@secunet.com

Start einer Vega-Trägerrakete der ESA
(c) ESA – S. Corvaja

Cloud Computing, KI und verteiltes Rechnen

Cloud: Sicher genug für die medizinische Forschung

Lange Zeit galt Cloud Computing als kosteneffizient, aber potenziell unsicher. Wo besonders hohe Sicherheitsanforderungen herrschen, war die Cloud daher bislang keine Option. Das ändert sich gerade – dank des sicheren Cloud-Betriebssystems SecuStack. Beispiel Gesundheitswesen: SecuStack ermöglicht maschinelles Lernen (ML) mit vertraulichen Patientendaten, die Cloud-basiert und sicher über verschiedene Institutionen hinweg genutzt werden. So lassen sich neue medizinische Erkenntnisse gewinnen, ohne den Datenschutz zu gefährden. Um solche Anwendungsszenarien zu realisieren, setzt SecuStack auf eine Zusammenarbeit mit Intel und Scontain.

Künstliche Intelligenz (KI) wurde von Branchenkennern längst zum „Megathema" ausgerufen, das die IT-Welt prägen und unsere Alltagswelt verändern wird. Eine große Rolle spielt dabei das adaptive und sich selbst ständig verbessernde maschinelle Lernen (ML). Seit einigen Jahren explodiert die Zahl der Anwendungsszenarien für ML. Eine dieser Einsatzmöglichkeiten ist die medizinische Forschung: Mittels maschinellem Lernen werden Patientendaten aggregiert und analysiert. So entstehen ML-Modelle, durch die die Forscher medizinische Erkenntnisse gewinnen können. Das Problem dabei: Die benötigten Rohdaten müssen institutsübergreifend, also von anderen medizinischen Einrichtungen wie etwa Krankenhäusern, zusammengetragen werden. Da es sich um sensible Informationen handelt, sprechen häufig Datenschutzgründe dagegen. Somit droht die KI-gestützte Forschung oft an einem mangelnden Zugang zu Rohdaten zu scheitern.

Die Lösung für dieses Problem liegt in einer Technologie, die schon seit vielen Jahren ein weiteres Megathema der IT-Welt darstellt – aber bis vor kurzem selbst noch als Unsicherheitsfaktor galt: Cloud Computing. Das Cloud-Betriebssystem SecuStack hat einen neuen Sicherheitsstandard gesetzt.

Kombiniert man die Lösung mit Hardware-basierter Technologie von Intel und Scontain, lassen sich zudem neuartige Cloud-Anwendungen in den Bereichen ML und verteiltes Rechnen (Multi-Party Computing) realisieren. So können etwa ML-Modelle über die Cloud Zugriff auf verschlüsselte Daten beteiligter medizinischer Einrichtungen erhalten, während dies anderen Parteien, zum Beispiel dem Cloud-Provider, sicher verwehrt bleibt.

Wodurch wird die Cloud sicher?

Cloud Computing funktioniert bekanntermaßen nach dem „as-a-service"-Prinzip. Typischerweise bieten Cloud-Provider ihren Kunden Dienste und Anwendungsprogrammierschnittstellen (APIs), legen aber die Software und den Quellcode nicht offen. Wer Cloud-Dienste nutzt, muss daher dem Provider zu einem gewissen Grad vertrauen. Für öffentliche Institutionen und stark regulierte privatwirtschaftliche Unternehmen wie Energieversorger oder Gesundheitsdienstleister kommt das nicht in Frage. Ohne Transparenz und vollständige Kontrolle über die Daten war es für solche Organisationen bisher nahezu ausgeschlossen, auf Cloud-Dienste zurückzugreifen.

Um dies zu ändern, entwickelte ein Joint Venture der Unternehmen secunet und Cloud&Heat das Cloud-Betriebssystem SecuStack, das auf der Open-Source-Software „OpenStack" basiert. Sein hohes Sicherheitsniveau erreicht SecuStack vor allem dadurch, dass die Daten durchgängig mit den gleichen Sicherheitsbausteinen verschlüsselt werden, die secunet seit vielen Jahren im Hochsicherheitsbereich einsetzt. Diese kryptographischen Mechanismen sind transparent integriert. So können Anwender auf Basis prüfbarer Software „made in Germany" eigene Cloud-Infrastrukturen für sensible Daten aufbauen. Die Hoheit über die Daten und Anwendungen verbleibt jederzeit beim Anwender.

Enklaven sorgen für zusätzliche Hardwaresicherheit

Für bestimmte Anwendungen ist es sinnvoll, die Cloud-Infrastruktur mit einer zusätzlichen, Hardware-seitigen Absicherung zu versehen. Aus diesem Grund standen die Entwickler von SecuStack schon früh mit Experten von Intel in Kontakt. Im Blick hatten sie dabei die Intel Software Guard Extensions (SGX). Prozessoren, die mit dieser Technologie ausgestattet sind, können kritische Infrastrukturdienste innerhalb von vertrauenswürdigen, hardwaregeschützten Bereichen, sogenannten „Enklaven", ausführen. Dadurch erhöht sich die Hürde für Angreifer enorm.

Mit den skalierbaren Intel Xeon Prozessoren der dritten Generation (Codename „Ice Lake") ermöglicht es Intel, bis zu ein Terabyte an Code und Daten während der Nutzung in Enklaven zu schützen. Intel SGX wird in das gesamte Spektrum der Ice-Lake-Plattformen integriert. So können Partner auf Basis von Ice Lake eigene Lösungen entwickeln, die bestehende Risiken im Zusammenhang mit dem Datenschutz und der Einhaltung von Vorschriften in streng regulierten Bereichen – wie dem Gesundheitswesen – reduzieren. Durch die Kombination von SecuStack und Intel SGX-Enklaven entsteht der umfassendste Schutz für die Cloud, der heute verfügbar ist.

Die Verbindung der beiden Technologien wird über die SCONE Plattform von Scontain realisiert. Mit SCONE lassen sich Dienste in Intel SGX-Enklaven einfach integrieren und ausführen. Auf diese Weise können in SecuStack kritische Funktionen wie Laufzeitverschlüsselung, Secrets Management und Autorisierung besonders sicher in Intel SGX-Enklaven umgesetzt werden.

Sicheres verteiltes Rechnen

Neben der Infrastruktur-Absicherung haben die Intel SGX-Enklaven für SecuStack noch einen weiteren Vorteil: Mit ihnen lassen sich neuartige Verfahren aus den Bereichen KI und ML umsetzen, bei denen es auf einen sicheren Datenaustausch ankommt – so wie in dem eingangs beschriebenen Anwendungsszenario aus der medizinischen Forschung. Das Verfahren, das dort zum Einsatz kommt, funktioniert so: Über das Cloud-Betriebssystem SecuStack und abgesichert in Intel SGX-Enklaven werden Anwendungsdienste verteilt ausgeführt, d.h. über voneinander isolierte Ressourcen hinweg. Orchestriert, also zu einem Verbund kombiniert, werden die Dienste mit dem Open-Source-System Kubernetes. Auf diese Weise kann verteiltes Rechnen in einem sicheren Kontext stattfinden. Mit dem Verfahren können ML-Modelle krankenhausübergreifend mit Patientendaten trainiert werden, ohne dass die sensiblen Daten das Krankenhaus, zu dem sie gehören, verlassen müssen.

Der Ansatz nennt sich „Confidential Federated Machine Learning" – vertrauliches maschinelles Lernen im Verbund. Dabei spielt eine alte Herausforderung des Cloud Computing keine Rolle mehr: Ob die beteiligten Anwender dem Cloud-Provider vertrauen oder nicht, ist unerheblich. Daten, Code und Modelle bleiben jederzeit vor dem Zugriff des Providers geschützt. Für den Datenschutz ist somit gesorgt, und die medizinische Forschung kann das Potenzial des maschinellen Lernens voll ausschöpfen. Im besten Fall entstehen dadurch Erkenntnisse, von denen alle profitieren.

Dr. Kai Martius
kai.martius@secunet.com

Aus dem Pentest-Labor

Fatales Zusammenspiel

Erfolgreiche Angriffe auf IT-Systeme rühren meist nicht daher, dass ein Angreifer nur eine einzelne Schwachstelle ausnutzen konnte. Vielmehr ist es das Zusammenspiel mehrerer Faktoren, das einen Angriff zu einer Katastrophe macht. Ein Beispiel: Ein Angreifer findet in einem Web-Portal eine Command-Injection – also eine Schwachstelle, die es ihm erlaubt, eigene Befehle einzuschleusen, die das System dann ausführt. Wenn die Schwachstelle in einem isolierten Bereich hinter einer Firewall lokalisiert ist, die sowohl den eingehenden als auch den ausgehenden Traffic filtert, ist das bereits ein unschöner Sicherheitsvorfall. Wenn aber der Web-Server-Prozess mit Root-Rechten läuft, für Updates frei ins Internet kommunizieren kann und gleichzeitig Daten von einer internen Datenbank erhält, kann sich die Kombination der Schwachstellen so weit aufbauen, dass ein Advanced Persistent Threat (APT) im internen Local Area Network (LAN) platziert werden kann, der nach und nach das komplette Unternehmen ausspäht oder – was noch schlimmer wäre – nach und nach die Werte zentraler Datenbanken ändert.

Um einer solchen fatalen Kombination von Angriffspunkten entgegenzuwirken, sollten IT-Sicherheitsexperten eingebunden und Unit-Pentests durchgeführt werden. Ist den Analysten bekannt, in welcher Umgebung ein Web-Portal betrieben wird und welche Schnittstellen dieses Portal zu anderen Systemen hat, können bereits in der Planungsphase Angriffspunkte identifiziert und eliminiert werden. Dabei können die Experten etwa Firewall- und Datenbankaudits nutzen, um Angriffe zu simulieren, bei denen erste Schutzmechanismen überwunden wurden.

Erfolgreiche Angriffe basieren oft nicht nur auf fehlenden Patches oder Systemhärtungen – diese Punkte können häufig, aber nicht immer, auch nach Abschluss des Projekts angepasst werden. Ein typischer Entwickler trifft Entscheidungen aufgrund des Pflichtenhefts der Anwendung. Viele dieser Entscheidungen basieren auf Vermutungen, wie Benutzer die neu zu erstellende Anwendung verwenden wollen und sollen. Ausgehend von dieser Vermutung werden Komponenten entwickelt und funktionale Tests erarbeitet, die die zentrale Funktion der Entwicklung prüfen.

Ein guter Pentester prüft dann genau diese Vermutungen, nur dass er eben genau so reagiert, wie ein Benutzer nicht reagieren würde. Zum Beispiel verwendet er unlogische Wertebereiche, manipuliert von der Webseite übertragene Inhalte, löscht existierende Parameter oder erzeugt neue. Je nach Robustheit der Anwendung führen diese Manipulationen zu internen oder externen Fehlern, werden durch Standardwerte kompensiert oder führen zum Absturz. Je früher im Entwicklungsprozess diese Tests durchgeführt werden, desto leichter ist es, die Entwicklung anzupassen. Auch die Implementierung zusätzlicher funktionaler Tests, die absichtlich fehlerhafte Daten enthalten, kann vorangetrieben werden, so dass in Summe eine robustere Anwendung entsteht.

Gleiches gilt für die Systeme, die von dem zu prüfenden Webportal genutzt werden, wie etwa Datenbanken, Reverse-Proxies oder Firewalls. Je früher den Systembetreibern verdeutlicht wird, dass sich keine der Komponenten darauf verlassen kann, dass die jeweils andere Komponente zu 100 % vertrauenswürdig ist, desto höher wird die Resilienz des Gesamtsystems. Damit wächst auch die Fähigkeit der Einzelkomponenten, trotz möglicherweise vorhandener Fehler in sicherer Weise zu agieren.

Dirk Reimers
dirk.reimers@secunet.com

Hochsichere Sprachkommunikation mittels VoIP und SCIP

Abhören zwecklos

Das Ende von ISDN zieht sich ein wenig, aber das ändert nichts daran, dass der digitale Telefonie-Standard ausgedient hat. Die deutschen Netzbetreiber schalten das 1989 eingeführte „Integrierte Sprach- und Datennetz“ in naher Zukunft ab, IP-Telefonie wird dann endgültig an seine Stelle treten. Eine Herausforderung bedeutet das für Behörden, die auf geheime Sprachkommunikation angewiesen sind, denn für diesen Zweck kommen heute noch flächendeckend ISDN-basierte Verschlüsselungssysteme zum Einsatz. Mit dem SINA Communicator H stellt secunet nun eine kompakte und einfach zu nutzende Schreibtischlösung vor, die IP-Telefonie hochsicher macht – und zwar bis zum Einstufungsgrad GEHEIM.

Vor allem in der öffentlichen Verwaltung und bei der Bundeswehr kommen derzeit noch Telefonie-Verschlüsselungslösungen auf Basis des ISDN-Standards zum Einsatz. Um die Lebensdauer dieser Lösungen zu verlängern, setzen manche auf ISDN-IP-Gateways. Da die beiden zugrundeliegenden Technologien ISDN und IP aber sehr unterschiedlich sind – ISDN arbeitet leitungsorientiert, IP paketorientiert –, bestehen Kompatibilitätsprobleme, die sich nie ganz ausgleichen lassen. Die Gateway-Lösungen können zwar den Übergang erleichtern, mittelfristig müssen sie aber durch neue Sicherheitstechnologie ersetzt werden, die speziell für IP-Telefonie konzipiert wurde.

secunet nahm sich dieser Herausforderung bereits vor einigen Jahren an. Dabei war es klar, auf welcher Grundlage die neue Lösung aufsetzen konnte: Die Sicherheitsarchitektur SINA, die secunet im Auftrag

Mit dem SINA Communicator H wechseln Nutzer einfach zwischen verschiedenen Geheimhaltungsgraden.

des Bundesamts für Sicherheit in der Informationstechnik (BSI) entwickelt hatte, ist im Kern ein Konzept zur Absicherung von IP-basierten Netzwerken. Mittlerweile hat sich SINA über viele Jahre hinweg in zahlreichen Bundes- und Landesbehörden bewährt und ist zur führenden Sicherheitsarchitektur der Bundesrepublik Deutschland geworden. Auch in anderen Staaten gibt es SINA Installationen. Für unterschiedliche Einsatzszenarien und Sicherheitsanforderungen sind vielfältige Varianten verfügbar, mit Zulassungen für Geheimhaltungsstufen von VS-NfD bis GEHEIM.

Auf dieser Basis entwickelte secunet eine hochsichere Telefonie-Lösung für die Zeit nach ISDN: den SINA Communicator H. Als Schreibtisch-Endgerät im Telefonformat konzipiert, dient die Lösung zur Sprach- und Datenkommunikation und ist für den Einstufungsgrad GEHEIM sowie vergleichbare internationale Level zulassungsfähig. Der SINA Communicator H kann sowohl innerhalb von Behördennetzen als auch direkt am Internet betrieben werden. Er nutzt bewährte Internetstandards für Voice-over-IP (VoIP) und unterstützt damit vorhandene, kommerziell beschaffte, Session Initiation Protocol (SIP)-fähige Vermittlungsinfrastrukturen. Zusätzlich setzt er Protokolle der NATO um, wie etwa das Secure Communication Interoperability Protocol (SCIP), und ermöglicht so eine abgesicherte Kommunikation mit internationalen Bündnispartnern.

„Der SINA Communicator H kombiniert die Anforderungen geheimer Sprachkommunikation mit den Gewohnheiten des modernen Arbeitsalltags."

Jan Leduc, Senior Produktmanager bei secunet

Dank der Multilevel-Fähigkeit des SINA Communicator H wechseln Nutzer einfach zwischen verschiedenen Geheimhaltungsgraden wie VS-NfD, VS-VERTRAULICH und GEHEIM im nationalen Umfeld sowie RESTRICTED, NATO SECRET oder EU SECRET/SECRET UE im internationalen Umfeld. Auch native Telefonanrufe können entgegengenommen werden. „Der SINA Communicator H kombiniert die Anforderungen geheimer Sprachkommunikation mit den Gewohnheiten des modernen Arbeitsalltags", sagt Jan Leduc, Senior Produktmanager bei secunet. „Damit zeigen wir einmal mehr, dass Hochsicherheit und Nutzerfreundlichkeit keine Gegensätze sein müssen. Sobald sich ein Nutzer per Token und PIN authentisiert hat, stehen die Funktionen komfortabel per Touch-Bedienung zur Verfügung."

Das 10,1 Zoll große Display ermöglicht neben der reinen Sprachkommunikation zahlreiche weitere Anwendungen. Für spätere Ausbaustufen sind zum Beispiel Textkommunikation, Videotelefonie und sogar eine Thin-Client-Funktionalität vorgesehen – optional mit externem Monitor. Ergänzend können weitere Anwendungen je nach Belieben und Bedarf hinzugefügt werden, zum Beispiel Web Clients, operative Fax-Unterstützung, Datei- und Dokumentenaustausch oder Mehrparteien-Messaging.

Die Migration von ISDN-Lösungen zum SINA Communicator H lohnt sich für Behörden zusätzlich durch den Umstand, dass sich die neue Telefonie-Lösung funktional in bestehende SINA Installationen integrieren lässt. „Bereits heute kann man mit der SINA Workstation S und H über eine abgesicherte IPsec-Verbindung bis GEHEIM mittels VoIP kommunizieren", erklärt Leduc. „In den SINA Communicator H lässt sich diese Funktion ebenfalls integrieren, so dass er mit den VoIP-Anwendungen der SINA Workstation S und H abwärtskompatibel ist. Auch die zentrale Administration über das SINA Management, das in einer Behörde meist schon vorhanden ist, erhöht die Effizienz und erleichtert die Migration. Insgesamt war es unser Ziel, dem SINA Communicator H für unsere Kunden so viel Mehrwert wie möglich mitzugeben – aus meiner Sicht haben wir das Ziel erreicht."

Jan Leduc
jan.leduc@secunet.com

Business Continuity Management

Nichts geht mehr – wie geht es trotzdem weiter?

Der Strom fällt aus, ein wichtiger Dienstleister kann nicht mehr liefern, in Büroräumen werden Schadstoffe entdeckt: Nicht erst seit der Covid-19-Pandemie gibt es Ereignisse, die den Betrieb eines Unternehmens oder einer Behörde von jetzt auf gleich lahmlegen können. In solchen Notfällen sind Organisationen im Vorteil, die ein Business Continuity Management etabliert haben. Im Fall der Fälle können dann die betroffenen zeitkritischen Geschäftsprozesse in den geregelten Notbetrieb gehen. Die handelnden Personen haben wichtige Zeit gewonnen, um das Ereignis zu bewältigen.

Flughafen Hamburg, Juni 2018: Ein Kabelbrand an einer Hauptstromleitung führt vormittags zum Stromausfall. Auch die Reserveeinspeisung ist betroffen, da an der Schadstelle die Normal- und Notstromversorgung in einem gemeinsamen Schacht verlaufen. Der gesamte Flughafen wird geräumt. Nach der Reparatur in der Nacht kann am Folgetag der Betrieb wieder aufgenommen werden.

Norddeutscher Rundfunk (NDR), November 2018: Bei Umbauarbeiten in einem Bürohochhaus kommt ein zuvor eingeschlossenes Füllmaterial mit Luft in Verbindung. Messungen in den betroffenen Büros ergeben Asbestpartikel in der Luft. Die Geschäftsleitung lässt das Gebäude sicherheitshalber komplett schließen. Für 300 Beschäftigte werden innerhalb von 18 Stunden Ausweicharbeitsplätze bereitgestellt. Im September 2019 wird die Entscheidung zum Ersatzneubau bekannt gegeben.

Das dritte Beispiel kennt jeder: Die Covid-19-Pandemie sorgte im Frühjahr 2020 dafür, dass weltweit unzählige Büroarbeitsplätze innerhalb kurzer Zeit nicht mehr genutzt werden konnten. Schnell mussten in großer Anzahl Mobile-Office-Arbeitsplätze eingerichtet werden. Seitdem ist die Aufmerksamkeit für das Thema Business Continuity Management (BCM) deutlich gestiegen.

Wer ein BCM etabliert hat, ist für Szenarien wie diese besser gerüstet. Zunächst wird in einer Business-Impact-Analyse ermittelt, welche Geschäftsabläufe auch im Notfall unbedingt fortgeführt werden müssen.

Abb. 1: Standard-Ausfallszenarien für Geschäftsprozesse

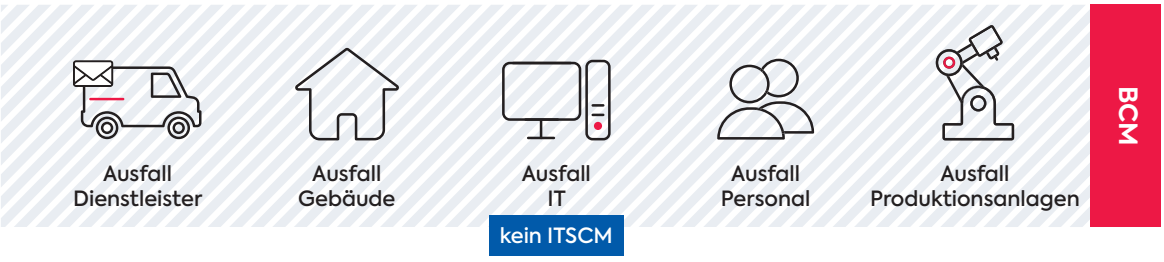


Abb. 2: Beispielhafte GFP-Übersicht für den Notfallstab

	zeitkrit. GP HelpDesk	zeitkrit. GP EPOS Verwaltung	zeitkrit. GP Token-Herstellung	GP Reporting
Ausfall Dienstleister	**x** (Risikoübernahme)	–	✓	Kein GFP notwendig
Ausfall Gebäude	✓	✓	✓	
Ausfall IT	x	x	x	
Ausfall Personal	x	x	x	
Ausfall Produktionsanlagen	–	–	✓	

✓ = Plan vorhanden **x** = Plan notwendig, fehlt aber (ggf. Grund warum keine Erstellung)
– = unzutreffend / nicht notwendig

Dies sind die sogenannten „zeitkritischen Geschäftsprozesse“ (GP). Anschließend werden für die so ermittelten GP jeweils „Geschäftsfortführungspläne“ (GFP, engl. Business Continuity Plans) konzipiert, in denen geregelt ist, was im Fall der Fälle getan werden muss, damit die GP weiterlaufen können. Doch wie kommen Behörden und Unternehmen zu zielführenden Geschäftsfortführungsplänen?

An dieser Stelle ist es notwendig, einige Abgrenzungen vorzunehmen. Das BCM oder auch „Notfallmanagement“ ist ein System zur Organisation und Sicherstellung der Geschäftsfortführung einer Institution auf Geschäftsprozessebene. Je nach Ansatz ist die Rechenzentrums-Ebene mit abgedeckt (so wie teilweise im kommenden Standard 200-4 des Bundesamts für Sicherheit in der Informationstechnik, BSI) oder sie ist in einem eigenständigen Managementsystem als IT Service Continuity Management (ITSCM (ITIL)) bzw. IT-Notfallmanagement organisiert. Im Folgenden werden ausschließlich Ausfallszenarien für die Geschäftsprozessebene vorgestellt.

Vom individuellen GFP zu GFP mit standardisierten Ausfallszenarien

Die traditionelle Vorgehensweise im BCM ist es, pro GP einen GFP zu erstellen. Dabei werden Fokus und Umfang oft für jeden GFP individuell festgelegt, je nach Kapazitäten oder Fachabteilungswünschen. Tritt dann der Notfall ein, sind oft Außenstehende involviert, die sich zum ersten Mal im Detail mit dem Dokument auseinandersetzen. Nicht selten stehen sie dann vor Überraschungen. Sie müssen Zeit aufwenden, um die Logik des individuell erstellten GFP zu verstehen – Zeit, die im Notfall sinnvoller genutzt werden sollte.

Zudem sind manche GFP für den konkreten Fall lückenhaft oder gar nicht anwendbar. Ein Beispiel: Eine Fachabteilung regelt in ihrem detailverliebten GFP, wie die Geschäftsfortführung nach (A) einem Bürobrand mit (B) anschließendem Ausfall einer Spezialsoftware am bezogenen Ausweichstandort und (C) ausbleibendem Vor-Ort-Support des Softwareherstellers abläuft. Für diese eskalierende Reihe liegt ein funktionierender GFP vor. Aber was ist, wenn nicht die Software, sondern die Hardware einen Defekt hat und der Ersatzdienstleister nicht nur am Ausweichstandort benötigt wird?

Aus diesen Gründen hat sich eine alternative Vorgehensweise entwickelt, die mit standardisierten Ausfallszenarien arbeitet. Diese werden einmal definiert und gelten dann für alle GP. Etabliert haben sich die Ausfallszenarien „Dienstleister“, „Gebäude“, „IT“, „Personal“ und „Produktionsanlagen” (Abb. 1).

Diese Vorgehensweise bietet eine Reihe von Vorteilen. Erstens können sich alle Beteiligten auf ein **gleichwertiges Abdeckungslevel** verlassen: Ist ein Thema als Standard-Ausfallszenario abgegrenzt und definiert, wird es für sämtliche GP angewendet. Die Vorgaben, etwa im Hinblick auf Fokus und Umfang, erfolgen zentral und werden mit Blick auf die gesamte Institution festgelegt.

Zweitens lassen sich die GFP nach dem **Baukastenprinzip** nutzen. Ausfälle können individuell kombiniert werden und bei Bedarf einem Eskalationsablauf folgen.

Drittens ist die **Vergleichbarkeit der Pläne** gegeben, denn je Ausfallszenario gibt es nur eine Dokumentenvorlage. So sind z. B. alle GFP für das Szenario „Ausfall Dienstleister“ identisch aufgebaut. Der Austausch unter den Fachabteilungen wird gefördert und spätere Notfallteams können GFPs verschiedenster Fachabteilungen schnell anwenden.

Viertens ist jederzeit die **Transparenz des Umsetzungsstandes** gewährleistet: Es lässt sich jederzeit auf einfache Weise überprüfen, für welche Ausfallszenarien der GP aktuell gerüstet ist. So kann kein Thema versehentlich ausgelassen werden. Die Hürde, für eine Kontrolle die Pläne im Detail inhaltlich sichten zu müssen, entfällt. Auch wenn der Notfall eingetreten ist, kann der Notfallstab schnell – ohne inhaltliche Kenntnis – erkennen, wofür ein bestimmter GFP vorliegt. Zudem wird transparent dargestellt, wo zwar Handlungsbedarf besteht, aber aus bestimmtem Grund kein GFP vorliegt (siehe Abbildung 2).

Grundprinzipien, auf denen der Erfolg beruht

Die Vorgehensweise mit Ausfallszenarien basiert auf einer Reihe von Grundannahmen:

- Alle GP werden neutral und **einheitlich analysiert**, unabhängig von der Aufbauorganisation. Es werden immer die gleichen Ausfallszenarien bearbeitet.
- Ausfallszenarien sind **ursachenneutral**: Die Planung setzt immer mit dem Fakt ein, dass der zeitkritische GP ad hoc durch eine geeignete Kontinuitätsstrategie kompensiert werden muss. Die Ursache wird ausgeblendet und ist nicht relevant. Beim Szenario „Ausfall Dienstleister" kommt es zum Beispiel nicht darauf an, ob der Dienstleister wegen eines Maschinenbrands, eines Unwetters, einer Insolvenz oder ungenügender Produktqualität aktuell nicht zur Verfügung steht.
- Planungsgrundlage ist der **Worst-Case-Ansatz**. So wird verhindert, dass der Notfallstab durch Eskalationen von Ausfallursachen, die anfangs noch begrenzt erscheinen, überrascht wird. Bei dem Szenario „Ausfall Gebäude" wird unterstellt, dass das betreffende Gebäude samt mittelbarer Umgebung nicht mehr zur Verfügung steht. Für die Planungen sollte ein Sperrkreis (z. B. ein Kilometer) angenommen werden. Ein zweites Gebäude auf der gleichen Liegenschaft kommt daher nicht als verlässliche Ausweichoption infrage. Zudem sollte davon ausgegangen werden, dass nach dem Verlassen eines Gebäudes praktisch keinerlei Arbeitsmaterialien wie beispielsweise Laptops oder Papier-Passwortlisten zur Verfügung stehen – so wie das bei Ereignissen mit akuten Gesundheitsgefahren tatsächlich der Fall sein kann. Bei dem Szenario „Ausfall Personal" wird unterstellt, dass ausnahmslos alle an diesem GP Beteiligten nicht mehr verfügbar sind. Jede Stellvertretungsregelung innerhalb dieser Gruppe greift ins Leere. Es steht niemand für Rückfragen zur Verfügung.

Für alle Ausfallszenarien kann eine Vielzahl unterschiedlicher Kontinuitätsstrategien (einschließlich mehrerer Varianten) für den Auswahlprozess definiert werden. Sämtliche zu entwickelnden Kontinuitätsstrategien leiten sich von den vier abstrakten Grundintentionen in der Tabelle unten ab.

Grundintentionen der Kontinuitätsstrategien

Intention	Ableitung auf Ausfallszenarien
Diversifikation	**>> produktiver Betrieb läuft mit aktiver Aufteilung**
	Dienstleister: z. B. vergebene Auftragslose 50:50
	Gebäude: z. B. zwei entfernte Gebäude gleichzeitig genutzt
	IT: z. B. aktive Georedundanz mit Synchronisation
	Personal: z. B. Personal arbeitet auf zwei Standorte aufgeteilt
Replikation	**>> fertig vorbereitet (Nutzung: sofort)**
	Dienstleister: z. B. alternativer Dienstleister wartet (Vertrag)
	Gebäude: z. B. Ausweichstandort komplett eingerichtet
	IT: z. B. RZ-Container steht eingerichtet bereit
	Personal: z. B. anderes Personal wird immer voll mitgeschult
Standby	**>> gleichwertig bzw. rudimentär vorbereitet (Nutzung: längere / unbekannte Vorlaufzeit)**
	Dienstleister: z. B. alternativer Dienstleister bekannt
	Gebäude: z. B. leeres Gebäude könnte umgerüstet werden
	IT: z. B. gelagerte Hardware könnte konfiguriert werden
	Personal: z. B. ähnliches Personal könnte angeleitet werden
Neubeschaffung nach dem Ereignis	**>> Beschaffung / Auswahl erst nach Ereignis angehen**
	Dienstleister: z. B. Dienstleister suchen und um Angebot bitten
	Gebäude: z. B. Gebäude neu anmieten
	IT: z. B. Hardware kaufen und Backups aufspielen
	Personal: z. B. Personaldienstleister beauftragen; neues Personal ausbilden

Einstieg ins BCM mit einer Reihe von Fragen

Wer sich einen ersten Überblick über den Stand der Dinge hinsichtlich BCM-relevanter Themen in der eigenen Behörde oder im eigenen Unternehmen verschaffen möchte, sollte sich die folgenden Fragen stellen:

- Gibt es Geschäftsprozesse, die unbedingt weiterlaufen müssen und damit zeitkritische Geschäftsprozesse sind?
- Kann der Zugriff zu zeitkritischen IT-Systemen in wenigen Minuten wiederhergestellt werden?
- Ist dokumentiert, welche konkrete Arbeitsumgebung für einen zeitkritischen Geschäftsprozess wie z.B. die Finanzbuchhaltung bereitzustellen ist, wenn diese ad hoc „auf der grünen Wiese" neu aufgebaut werden muss (Anzahl der Arbeitsplätze, Vernetzung, Anwendungen, geschaltete Telefonnummern, etc.)?
- Sind zeitkritische Dienstleister bei Bedarf auch abends erreichbar und werden sie dann Unterstützung leisten – und zwar so lange der Notfall andauert?
- Wer entscheidet ganz konkret nach einem Brand im Serverraum am Sonntagnachmittag, wer was wann wie zu tun hat?

secunet verfügt über langjährige Erfahrung mit dem Thema Business Continuity Management und unterstützt Unternehmen wie auch Behörden dabei, zielführende Geschäftsfortführungspläne aufzubauen. Der Aufwand für diesen Prozess lohnt sich, wenn im Notfall wertvolle Zeit gewonnen werden kann.

Christian Bergmann
christian.bergmann@secunet.com

Beispiele für konkrete Kontinuitätsstrategien für das Szenario „Ausfall Gebäude"

- **Umnutzung: Ausweichen in regulär für andere Aufgaben genutzte Räume (Besprechungsräume, Kantine, Büros nicht-zeitkritischer Abteilungen)**
- **Arbeitsumgebungsdienstleister: reservierte Räume, gemeinsam genutzte Räume (z.B. first come – first serve)**
- **Entfernter Ausweichstandort: Nutzung entfernter organisationseigener Flächen**
- **Vereinbarung auf Gegenseitigkeit: Partner halten fest definierte Flächen zur gegenseitigen Nutzung bereit**
- **Anlieferung von Ressourcen: Externer Vertragspartner liefert (teil-)fertige Umgebungen (Bürocontainer, Leichtbauhallen)**
- **Telearbeit: Arbeit aus dem Home Office oder an mobilen Orten**
- **Arbeitszeitfenster: Optimale Auslastung begrenzt zur Verfügung stehender Arbeitsplatzkapazitäten (Randzeiten, Wochenende)**
- **Robuster Betrieb: dauerhafte, dezentrale Aufteilung eines GP auf mehrere Standorte**

SINA Workstation S mit optimierter Grafikleistung

Turbo fürs sichere Home Office

Das weltweit grassierende Coronavirus hat unsere Arbeitswelt verändert. Gleichermaßen ändern sich die Anforderungen an das technische Equipment. Da Videokonferenzen nun an der Tagesordnung sind, ist Grafikleistung in diesen Zeiten besonders gefragt. Darauf hat secunet schnell reagiert und gemeinsam mit dem Partner Cyberus Technology die SINA Workstation S weiterentwickelt. Tor Lund-Larsen, CEO von Cyberus, erläutert im Gespräch mit Armin Wappenschmidt, Leiter der Abteilung Network&Client Security bei secunet, wie der sichere Client optimiert wurde und welche Vorteile sich daraus für die Nutzer ergeben.

Welche konkreten Anforderungen stellen Nutzer heute? Und welche Vorteile bietet die optimierte SINA Workstation S für sie?

Wappenschmidt: Die Ansprüche erweitern sich stetig. Auch bei der hohen Sicherheit, die die SINA Workstation S bietet, wollen die Nutzer sie für alle Einsatzszenarien des modernen Arbeitslebens verwenden. Das bleibt nicht unbeantwortet: Wir sind immer mit der Zeit gegangen und haben unsere Lösungen der Arbeitsweise der Nutzer angepasst. Anfangs stand die SINA Workstation S beispielsweise nur als Desktop zur Verfügung, heute ist sie mobil und sehr flexibel einsetzbar. Dann kam die Unterstützung von USB-Audio-Headsets und Videokameras. Zuletzt spielte die Grafikleistung, die unter anderem für Videokonferenzen benötigt wird, eine immer wichtigere Rolle. Das ist nicht erst seit der Corona-Pandemie so, dennoch treibt sie diese Entwicklung derzeit stark voran: Präsenz-Meetings fallen aus, die Leute arbeiten im Home Office. Darauf haben wir in den letzten Monaten schnell mit technischen Verbesserungen reagiert.

Lund-Larsen: Die optimierte SINA Workstation S bietet zugleich mehrere Vorteile für den Nutzer. Videos und andere Bewegtbild-Anwendungen wie Videokonferenzen laufen nun flüssig und in hoher Qualität ab, ohne dass die hohen Sicherheitsanforderungen von SINA S reduziert werden müssen.

Wie haben Sie das technisch umgesetzt?

Lund-Larsen: Die Integration der Cyberus Virtualisierungsplattform ist eine bedeutende Erweiterung der Architektur der SINA Workstation S. Sie erforderte eine sehr enge und intensive Entwicklungszusammenarbeit zwischen secunet und Cyberus Technology.

Die Lösung setzt unterhalb des SINA Software Stacks an. Die Trennung der verschiedenen Gastsysteme, die für die Sicherheit der SINA Workstation S so

wichtig ist, wird nun nicht mehr durch den Linux Kernel gewährleistet, sondern durch die unterliegende Virtualisierungsplattform.

Dies ermöglicht auch neue funktionale Erweiterungen wie zum Beispiel Grafik-Virtualisierung. Weil die verschiedenen Gastsysteme der Workstation früher aus Sicherheitsgründen nicht auf eine gemeinsame Grafikkarte zurückgreifen konnten, musste die virtualisierte CPU, vereinfacht gesagt, die Grafikberechnungen mitübernehmen. Die neue Systemarchitektur entlastet die CPU bei Grafikleistungen. Damit wird das System effizienter, was sich auch positiv auf die Akkulaufzeit auswirken kann.

Die Virtualisierungsplattform basiert auf unserem quelloffenen „Hedron" Micro-Hypervisor, dessen Wurzeln zur TU Dresden zurückreichen – also Technologie „Made in Germany", wie bei SINA üblich.

Wappenschmidt: Cyberus besitzt tiefgreifendes Know-how zu Virtualisierung, Low-Level-Hardware, CPU-Design und Software-Testautomatisierung – eine ziemlich einzigartige Mischung. Deshalb ist Cyberus der richtige Partner für uns. Übrigens spielte das Cyberus-Team in den Jahren 2018 und 2019 eine große Rolle bei der Entdeckung der bekannten „Meltdown"- und „Spectre"-Sicherheitslücken in x86 Prozessoren und stellte damit seine Erfahrung gerade im CPU- und Low-Level-Bereich unter Beweis. Wir planen, noch weitere Projekte gemeinsam umzusetzen.

Gab es bei der Entwicklungsarbeit Herausforderungen, die Sie lösen mussten?

Lund-Larsen: Als die Zusammenarbeit mit secunet begann, ging es zunächst nicht um die Grafikleistung – sondern um zusätzliche Systemsicherung durch Virtualisierung. Die sogenannte „Trusted Compute Base" (TCB) sollte weiter verringert werden – also die Menge an Code, dem vertraut werden muss. Wir waren dabei schon gut vorangekommen, als eines Tages Armin anrief und das

Im Interview

Armin Wappenschmidt
Leiter Network & Client Security,
secunet Security Networks AG

Tor Lund-Larsen
CEO Cyberus Technology GmbH
Foto: Tommy Sauer
(info@tommysauerphotography.de)

Cyberus Technology

Das 2017 gegründete Dresdner Unternehmen Cyberus Technology ist auf Software für Cybersicherheit spezialisiert. 2018 entdeckten dessen Mitarbeiter gravierende Sicherheitslücken („Meltdown“ und „Spectre“) bei Mikroprozessoren, von denen nicht nur Unternehmen und Behörden, sondern auch private Computernutzer betroffen waren. Zwei weitere Kernbereiche von Cyberus Technology bilden die Virtualisierungstechnologie und die Testautomatisierung von Software während ihrer Entwicklung. Mehr Informationen dazu gibt es unter www.cyberus-technology.de.

Thema Grafikleistung ins Spiel brachte, das aufgrund der Corona-Pandemie auf einmal auf der Prioritätenliste ziemlich nach oben gerückt war. Also schotteten wir unsere Projektentwickler komplett von allen anderen Aufgaben ab – und das für ein knappes Jahr und unter Pandemie-Bedingungen! Wir freuen uns, dass wir jetzt unser Ziel erreicht haben, secunet eine einzigartige Grafiklösung für die SINA Workstation S Plattform anzubieten, ohne dass wir dabei das ursprüngliche Ziel, die TCB zu verringern und die Systemsicherheit zu erhöhen, aus den Augen verloren haben.

Welche Verbesserungen werden wann verfügbar sein?

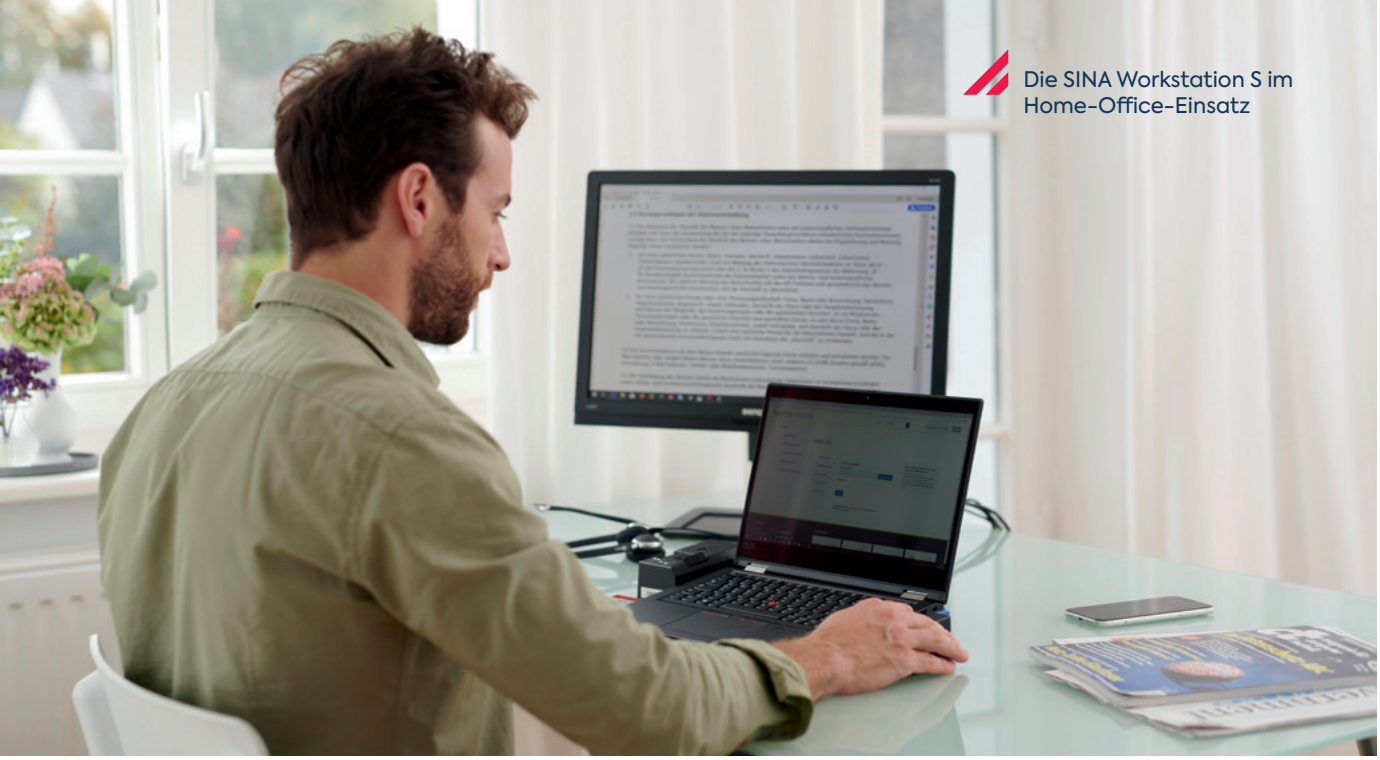
Wappenschmidt: Die erste Version der grafikbeschleunigten SINA Workstation S erscheint schon im Dezember 2020. Sie legt den Fokus auf die Nutzung der Grafikhardware in einem Gastsystem. Aufgrund der aktuellen Situation wollten wir den Nutzern dafür schnell eine Lösung präsentieren. Für den kommenden Sommer ist dann ein weiteres Release geplant, das zusätzliche Performance-Verbesserungen und eine optimierte Abstimmung aller Systemressourcen mitbringen wird. In diesem Release werden Features wie beispielsweise die Unterstützung von Multi-Monitor-Szenarien und 4K-Monitorauflösung, die unseren Kunden schon länger zur Verfügung stehen, auch für die grafikbeschleunigte SINA Workstation S kommen.

Lund-Larsen: Wir freuen uns darauf, die Zusammenarbeit weiter zu vertiefen und wissen es sehr zu schätzen, dass secunet uns bis hierher so viel Vertrauen entgegengebracht hat. Unser Unternehmen ist zwar klein, dafür können wir aber mit einer hochspezialisierten Expertise aufwarten, die wir gern für secunet einsetzen.

Armin Wappenschmidt
armin.wappenschmidt@secunet.com

Selbst Gaming ist mit der grafikbeschleunigten SINA Workstation S kein Problem…

Foto: Tommy Sauer (info@tommysauerphotography.de)



Die SINA Workstation S im Home-Office-Einsatz

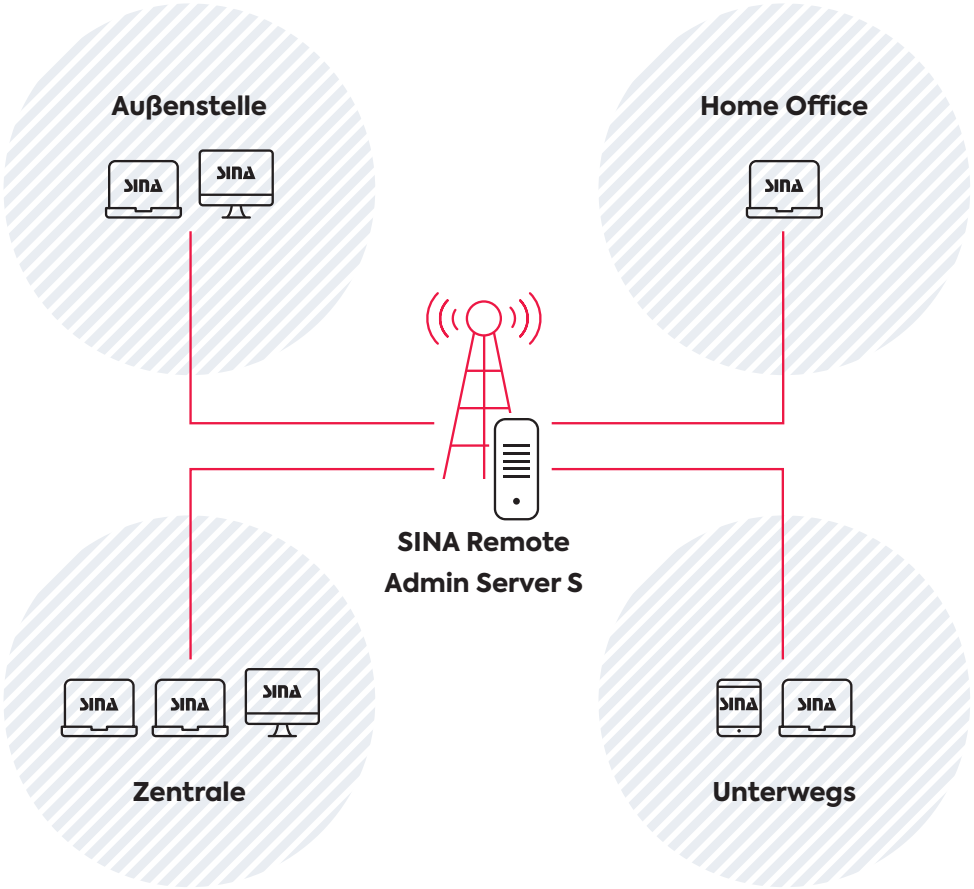
Zentrale Administration der SINA Workstation S

Bereit für den Massen-Rollout

Gerade jetzt, da Abstandhalten wichtig ist und Home Office bevorzugt wird, statten viele Behörden und Unternehmen ihre Mitarbeiterinnen und Mitarbeiter mit der SINA Workstation S aus. Sie bietet eine sichere und dennoch komfortable Alternative zu einem herkömmlichen Arbeitsplatz-PC – und das bei hoher Mobilität, denn die Nutzer können von jedem möglichen Zugangspunkt, auch von zu Hause aus, sicher auf das IT-Netz ihrer Organisation zugreifen. Bei der Verwaltung großer Installationen mit vielen SINA Workstations S hilft IT-Verantwortlichen der SINA Remote Admin Server S, den secunet kontinuierlich weiter optimiert.

Je komplexer die IT-Infrastruktur, desto mehr wird der Verwaltungsaufwand zum Thema. Das gilt auch für sichere SINA Infrastrukturen. Für Administratoren und IT-Support sind die Herausforderungen besonders groß, wenn sie keinen physischen Zugang zu Infrastrukturkomponenten haben und wenn Mitarbeiterinnen und Mitarbeiter zunehmend von zu Hause aus arbeiten und nur über das Internet mit ihrem Behörden- oder Firmennetz verbunden sind.

In Zeiten der Corona-Pandemie kann der Home-Office-Anteil bis zu 100 Prozent betragen und das über einen längeren oder jedenfalls schlecht planbaren Zeitraum hinweg. Servicezeiten für die Komponenten können dann nur noch über Remote-Zugriffe eingehalten werden. Reguläre Änderungen wie Softwareaktualisierungen oder Konfigurationsverbesserungen lassen sich normalerweise problemlos auf diese Weise durchführen. Werden aus der Ferne jedoch Sicherheitsupdates installiert oder Betriebsstörungen behoben, können durchaus Risiken entstehen.



Ein gutes Beispiel dafür ist eine Softwareaktualisierung, die auf sämtlichen Geräten durchgeführt werden muss. Jeder kennt es aus eigener Erfahrung: Die Aufforderung zum Neustart kommt im Arbeitsalltag immer zum falschen Zeitpunkt und wird daher gern möglichst lange aufgeschoben oder weggeklickt. Aber was macht der Administrator, wenn einige Nutzer auch nach mehrmaligem Bitten den erforderlichen Neustart nicht durchführen?

Die Lösung für dieses Problem liefert die Fernwartungs-Software SINA Remote Admin Server S (SINA RAS). Damit kann sich der Administrator zunächst einen Überblick verschaffen, welche über das Netzwerk erreichbaren SINA Workstations S mit welcher Softwareversion arbeiten. Bei Bedarf kann er dann eine zentral gesteuerte Softwareaktualisierung erzwingen. Mit der Inventarisierungsfunktion hat der Administrator darüber hinaus viele weitere Parameter im Blick.

Ein **Softwareupdate** kann wichtige Sicherheitspatches enthalten und sollte daher grundsätzlich schnellstmöglich eingespielt werden – gerade dann, wenn es für die Erhaltung der Zulassung des Bundesamtes für Sicherheit in der Informationstechnik (BSI) notwendig ist. Selbst wenn das Update für den weiteren Betrieb nicht zwingend notwendig sein sollte, bringt es in der Regel den Anwendern Vorteile. Zudem vereinfacht ein homogener Softwarestand auf allen Geräten die administrative Systempflege.

Komfortable Fernwartung

Hauptaufgabe des SINA RAS ist es, Konfigurationen an SINA Clients im laufenden Betrieb zu erleichtern. Updates von SINA Apps, Änderungen von Zugriffsberechtigungen oder die Anlage neuer Netzwerkprofile – Aufgaben wie diese können Administratoren mit dem Tool zentral umsetzen, egal wo sich die Clients gerade befinden.

Der Startschuss für den SINA RAS fiel Mitte der 2010er Jahre, als mehrere Bundesministerien eine Vollausstattung mit der SINA Workstation S umsetzten. Damals stellte sich erstmals die Frage, wie der ursprünglich als Speziallösung konzipierte sichere Client massenhaft ausgerollt und verwaltet werden konnte. Die Antwort lag in Automatisierung und Fernwartung.

Zunächst startete der SINA RAS als reines Installationsskript für den initialen Rollout von SINA Workstations S. In kurzer Zeit hat er sich dann zu einem flexiblen Werkzeug für die Fernwartung von SINA S Komponenten entwickelt. Seitdem wird er kontinuierlich erweitert und an neue Versionen der SINA Workstation S angepasst.

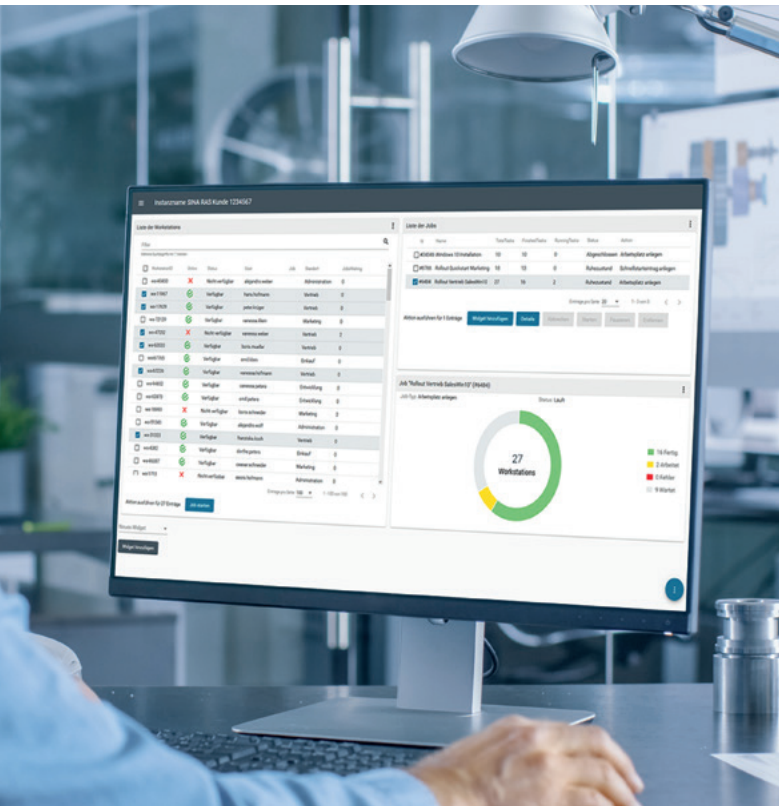
Über das CLI (Command Line Interface) können die RAS-Befehle in einen Automatisierungsworkflow eingebunden werden, der genau den Anforderungen der jeweiligen Organisation entspricht. Da der SINA RAS eine Skriptsprache (Groovy) nutzt, lassen sich die einzelnen Funktionen feingranular für eine Automatisierung in den organisationseigenen Abläufen anpassen. Es können sogar neue Skripte erstellt und verwendet werden.

Zukunftssicherheit für die Infrastruktur

Der SINA RAS wurde mit dem Ziel entwickelt, die Administration einer großen Anzahl von SINA Workstations S zu ermöglichen, ohne dass dafür zusätzliches Personal eingesetzt werden muss. Ein weiteres Ziel war es, Power-Usern praktikable Automatisierungsschnittstellen zu bieten. Mit den wachsenden Anforderungen der Nutzer verändert sich aber auch der Funktionsumfang des SINA RAS. Im nächsten Release wird es beispielsweise mit dem RAS Wartungsmodus eine Hilfestellung für die Administration laufender virtualisierter Arbeitsplätze geben.

So manche technische Optimierung ist für Anwender unsichtbar, macht das System aber robuster und verlässlicher. In diese Kategorie fallen einige derzeit geplante Maßnahmen, die künftig die Testlast zum Entwicklungsende reduzieren und damit den Releasefluss für die Umsetzung spezifischer Anforderungen beschleunigen werden. Für die Anwender bedeutet dies, dass benötigte Funktionen zukünftig schneller und agiler als Produktversion bereitgestellt werden können – was insbesondere für den Betrieb komplexer Infrastrukturen entscheidend sein kann.

Künftig verfügt der SINA Remote Admin Server S über eine grafische Benutzeroberfläche.



Die verbesserte Testautomatisierung ist die Voraussetzung für schnellere Erweiterungen und zukünftige Redesigns. In einem nächsten Schritt wird die interne Schnittstelle zur SINA Workstation S optimiert, um die Geräteadministration noch übersichtlicher und die Bedienung aufgabenorientierter zu gestalten. Dafür erhält der Administrator künftig Zugang zu einer flexiblen High Level API und einer darauf aufsetzenden grafischen Benutzeroberfläche (GUI). Mit der High Level API wird eine Abstraktionsschicht eingeführt, die einen einfacheren Zugang zur Steuerung des SINA RAS bietet – entweder manuell durch den Administrator oder automatisiert eingebunden in Kundenprozesse. Die GUI ermöglicht demnächst eine intuitivere, schnellere Bedienung und erleichtert Nutzern, die nur einen kleinen Bestand an SINA Workstations betreuen oder diesen ausbauen wollen, den Einstieg in die Fernadministration.

Die SINA Workstations werden in der GUI übersichtlich dargestellt und können über ihre Parameter gefiltert bzw. sortiert werden, so dass notwendige administrative Eingriffe leichter durchgeführt werden können. Administratoren, die wenig Erfahrung mit Linux-basierten Systemen haben oder grundsätzlich wenig Shell-basiert arbeiten, profitieren künftig von der benutzerfreundlichen Oberfläche ebenso wie Nutzer, deren hauptsächliche Domäne die Windows Administration ist oder die SINA Workstations nur am Rande mitbetreuen.

Der SINA RAS soll zukünftig mit anderen SINA Administrationswerkzeugen in einem SINA Management Center (SMC) zusammengeführt werden. Mit diesen Optimierungen wird die zentrale Administration von SINA noch funktionaler und komfortabler. Aber bereits jetzt gibt der SINA Remote Admin Server S Nutzern das notwendige Werkzeug an die Hand, SINA S Komponenten zuverlässig und einfach zu administrieren.

Andreas Rach
andreas.rach@secunet.com

Der **RAS Wartungsmodus** ist eine Erweiterung, die die flexible Funktionalität des SINA RAS nutzt, um Änderungen an virtuellen Gästen der SINA Workstation durchführen zu können – auch Remote, ohne Eingriffe des Anwenders.

Neuer ENISA Threat Landscape Report verfügbar

Im Oktober 2020 hat die Agentur der Europäischen Union für Cybersicherheit (ENISA) den 8. jährlichen ENISA Threat Landscape (ETL) Report 2020 veröffentlicht. Er identifiziert und bewertet die wichtigsten Cyberbedrohungen für den Zeitraum Januar 2019 bis April 2020. Die diesjährige Veröffentlichung ist in 22 einzelne Reports unterteilt, die im PDF-Format und als E-Book verfügbar sind. Insgesamt zeigt der Report auf, wie die von Covid-19 beeinflusste Transformation der digitalen Welt die Bedrohungslandschaft gegenüber der von 2018 verändert hat. Während der Pandemie wurde deutlich, dass Cyberkriminelle ihre Fähigkeiten weiterentwickeln, sich schnell anpassen und relevante Opfergruppen gezielter angehen.

Der ENISA Threat Landscape Report 2020 kann auf der ENISA Website heruntergeladen werden: **www.enisa.europa.eu**

Sterntaler Bonn: „Sozialsponsoring“ für Kinder

Für viele Kinder ist ein liebevolles Zuhause, in dem sie gepflegt und in ihrer Entwicklung gefördert werden, selbstverständlich. Für viele aber auch nicht. Dieses Problem geht der Verein Sterntaler Bonn e. V. an. Er bietet bedürftigen Kindern in Bonn mehr Bildung, Förderung und Teilhabe: Hausaufgabenbetreuung in Familienzentren, gesunde Mahlzeiten, Projekte zur Gewaltprävention, Förderung von Psychomotorik, Sprach- und Musikentwicklung – mit diesen und ähnlichen Angeboten verhilft der Verein Kindern zu einem besseren Start ins Leben. Für seine Tätigkeit hat er einen treffenden Begriff gefunden: „Sozialsponsoring“.

Die diesjährige secunet Weihnachtsspende geht an Sterntaler Bonn. „Wir sind überzeugt, dass jedes Kind angemessene Förderung verdient“, sagt Bill Mockridge, Schirmherr von Sterntaler. Arndt Hilse, Vorsitzender des Vereins, ergänzt: „Für viele unserer Maßnahmen sind wir neben dem Engagement unserer Mitglieder auch auf Geldmittel angewiesen. Daher freuen wir uns sehr über die Unterstützung.“

Kontaktmöglichkeit Verein:

Sterntaler Bonn e. V., Sudetenstr. 24, 53119 Bonn

Arndt Hilse, Vorsitzender

Mail: vorsitzender@sterntaler-bonn.de

Telefon: 0157 39398654

Arndt Hilse (links) und Bill Mockridge von Sterntaler Bonn e. V.

Termine – Januar bis Juni 2021

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

2. bis 3. Februar 2021
17. Deutscher IT-Sicherheits-kongress | digital

23. Februar 2021
Polizeitag | Kiel

13. bis 15. April 2021
DMEA | Berlin

27. bis 28. April 2021
ID@Borders Conference | Brüssel, Belgien

3. bis 5. Mai 2021
Omnisecure | Berlin

5. bis 6. Mai 2021
LEA-DER | Prag, Tschechien

17. Mai 2021
RSA Conference | digital

18. bis 19. Mai 2021
Berliner Sicherheitskonferenz | Berlin

19. bis 20. Mai 2021
AFCEA Fachausstellung | Bonn

25. bis 28. Mai 2021
ICAO TRIP Symposium and Exhibition | Montreal, Kanada

29. Juni bis 1. Juli 2021
Passenger Terminal Expo | Amsterdam, Niederlande

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

Impressum

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

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

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

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

Bildnachweis
Titel, S. 9, 10: ECSO
S. 2 (oben), 14, 16, 19, 21: Adobe Stock
S. 2 (unten), 8, 27, 33: iStock
S. 3, 13, 22, 23, 29 (links), 31: secunet
S. 5: BMG/Akthar
S. 12: alamy
S. 18: ESA – S. Corvaja
S. 29 (rechts), 30: Tommy Sauer
S. 34: Sterntaler Bonn e.V.

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.

Wenn es um die Sicherheit der Grundversorgung geht, steht secunet bereit. Als IT-Sicherheitspartner der Bundesrepublik Deutschland beraten wir Betreiber kritischer Infrastrukturen zu Sicherheitskonzepten und implementieren premiumsichere Schutzmaßnahmen.

secunet.com protecting digital infrastructures

secunet