secuview

Das secunet Kundenmagazin 2023

„Unsere größte Herausforderung war die Zeit“

Mohamed Kiwan, CEO von EgyptTrust, über die Implementierung einer PKI-Lösung für digitale Identitäten und Signaturen

Effizienz ohne Abhängigkeit

Die souveräne Cloud für Behörden und Verwaltung

Kryptografie 2.0

Sicherheit vor Quantencomputern

National

International

Technologien & Lösungen

Perspektive

Richtlinien & Standards

Kurz notiert

Service

Liebe Leserinnen und Leser,

das Spannende an der IT-Branche ist, dass sie sich ständig erneuert. Aktuell stehen wir vor einer Reihe von IT-Revolutionen, die unser aller Leben verändern werden – zum Beispiel künstliche Intelligenz (KI), die Cloud-Transformation oder autonomes Fahren. Das Spannende wiederum an secunet ist, dass wir als Cybersecurity-Unternehmen die Möglichkeit haben, an allen diesen Umwälzungen in der einen oder anderen Form mitzuwirken.

Das gilt sicherlich für die Cloud-Transformation, die zwar im privaten und geschäftlichen Alltag schon seit längerer Zeit spürbar ist, vor dem wichtigen Bereich der öffentlichen Verwaltung aber bisher aus Sicherheitsgründen Halt gemacht hat. Das ändert sich mit den souveränen Cloud-Angeboten, die aktuell in Deutschland aus dem Boden sprießen. secunet treibt den Wandel zur sicheren Cloud voran und investiert, um in diesem Markt ein sehr besonderes eigenes Angebot zu platzieren. Was daran so besonders ist, erklärt Norbert Müller, der für secunet Cloud Solutions verantwortlich ist, in der vorliegenden secuview.

Zu den vieldiskutierten Veränderungen, die KI mit sich bringen wird, gehören deren Anwendungen in der inneren Sicherheit. Diese bringen nicht nur große Chancen, sondern auch Herausforderungen mit sich. Statistische Verzerrungen in der Datengrundlage von KI-Modellen, die zu Sicherheitszwecken eingesetzt werden, können sich folgenschwer auswirken, indem die KI zum Beispiel bestimmte Personengruppen bevorzugt oder benachteiligt. In der aktuellen Ausgabe beschreiben wir einen Ansatz, der einem solchen Szenario entgegenwirkt.

Auf dem Weg zum autonomen Fahren ändert sich nicht nur das Fahrzeug selbst, die fortschreitende Vernetzung sorgt schon heute dafür, dass wir aus der Perspektive der Cybersicherheit die gesamte, zunehmend digitale Verkehrsinfrastruktur in den Blick nehmen müssen. Der Automotive-Cybersecurity-Experte Manuel Wurm spricht im Interview über diesen Paradigmenwechsel.

Schließlich vollzieht sich in der Kryptografie ein tiefgreifender Wandel, der jenseits der Fachwelt trotz weitreichender Auswirkungen nur selten thematisiert wird. Als Reaktion auf die Fähigkeiten künftiger Quantencomputer muss die Kryptografie sich neu erfinden, unter anderem damit die Sicherheit von Staatsgeheimnissen weiterhin sichergestellt werden kann. Auch darum geht es in der vorliegenden Ausgabe.

Bei all dem Wandel steht secunet auch künftig für den bestmöglichen Schutz digitaler Infrastrukturen, Daten und Anwendungen. Auf dieser Basis sind wir für jede IT-Revolution gewappnet.

Ich wünsche Ihnen viel Spaß bei der Lektüre!

Ihr Axel Deininger

Die souveräne Cloud für Behörden und Verwaltung

Effizienz ohne Abhängigkeit

Die Digitalisierung der Verwaltung ist nur nachhaltig, wenn sie Effizienz, Souveränität und Sicherheit zusammen denkt. Das gilt besonders für die Cloud-Transformation, die aktuell oben auf der Agenda vieler Behörden steht. Da die Cloud-Angebote der großen Hyperscaler häufig Fragen rund um Transparenz und Datenschutz offenlassen, besteht ein großer Bedarf nach Cloud-Lösungen „made in Germany“. Diese sollen Sicherheit und digitale Souveränität vereinen. secunet baut derzeit ein Ökosystem vertrauenswürdiger Lösungen und Services auf, welches die Cloud-Nutzung auch in sicherheitssensiblen Bereichen ermöglicht und durchaus mit Lösungen von Hyperscalern kombiniert werden kann. Norbert Müller, der für die secunet Cloud Solutions verantwortlich ist, spricht im Interview über Sinn und Zweck der souveränen Cloud, die Rolle von Open Source und den neu gegründeten Branchenverein ALASCA.

Herr Müller, warum streben Behörden überhaupt in die Cloud?

Norbert Müller: Im Privatleben und in der Geschäftswelt sind digitale Prozesse bereits Alltag und basieren überwiegend auf Anwendungen, die in der Cloud laufen. Behörden und Verwaltungen blieben bislang aus Sicherheitsgründen weitgehend ausgeklammert. Doch auch sie wünschen sich die Flexibilität und Effizienz, die neue Cloud-Dienste mitbringen. Damit können sie ihre IT agiler aufstellen und so dem großen Digitalisierungsdruck begegnen, der auf deutschen Behörden lastet: Prozesse sollen beschleunigt werden, zudem wünschen sich Bürger*innen und Unternehmen mehr digitale Angebote. Doch es bleibt die Herausforderung, dass Behörden bei der Cloudifizierung keine Kompromisse bei der Sicherheit eingehen können. Personen- oder Steuerdaten sind hochsensibel und müssen lückenlos geschützt werden. Erst recht gilt das für Staatsgeheimnisse, die als Verschlusssachen eingestuft werden. Zudem gibt es das Thema der digitalen Souveränität.

Norbert Müller
Vice President Cloud
Solutions bei secunet

Warum muss die Cloud für Behörden nicht nur sicher, sondern auch souverän sein? Ist digitale Souveränität vielleicht ein bloßes Buzzword, wie manche Beobachter meinen?

Der Wert der digitalen Souveränität wird klar, wenn man sich das Gegenteil vorstellt, nämlich digitale Abhängigkeit – etwa von bestimmten Anbietern, die einen Wechsel zu einem anderen Anbieter erschweren, oder auch von den international dominanten IT-Unternehmen. Problematisch kann das zum Beispiel dann werden, wenn Anbieter unter US-Gesetzgebung arbeiten, deren Einfluss auf die Datensicherheit mindestens unklar ist. Aus diesen und ähnlichen Gründen entsprachen herkömmliche Cloud-Lösungen, etwa die der Hyperscaler, oft nicht den Anforderungen von Behörden und sicherheitssensiblen Unternehmen. Souveräne Cloud-Angebote hingegen wollen genau dies ändern. Digitale Souveränität macht also durchaus einen zentralen Unterschied für Behörden und Verwaltungen aus.

Was sind die wichtigsten Bausteine einer souveränen Cloud?

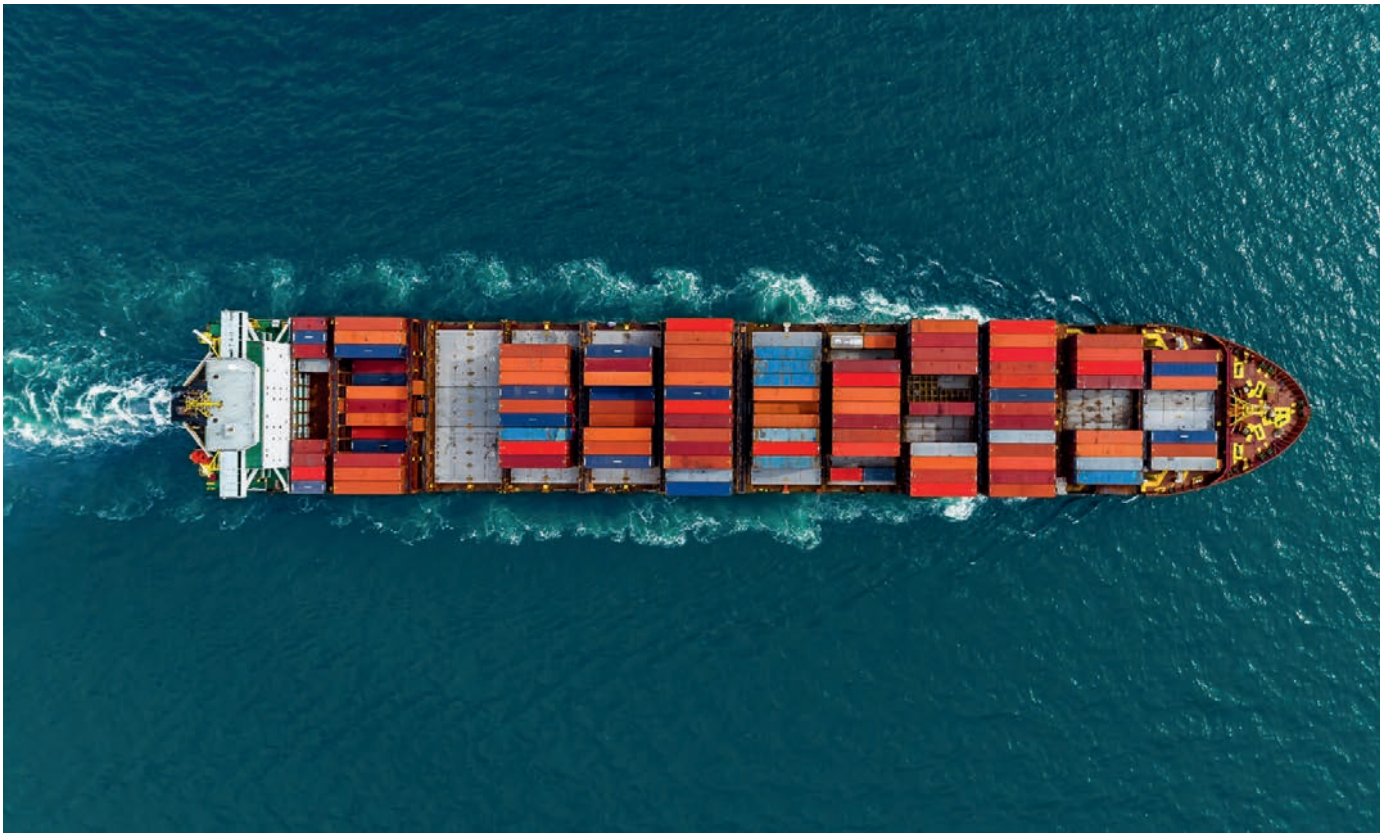
Zunächst einmal muss als Grundvoraussetzung natürlich das Sicherheitslevel stimmen. Jede Cloud-Lösung, die für Behörden in Frage kommt, sollte mit hochsicherer Verschlüsselungstechnologie arbeiten. Sie sollte modular sein und verschiedene Betriebsmodelle umfassen und kombinieren – von „on premise“ bis „as a service“. Zum Beispiel können besonders schützenswerte Daten in der eigenen IT-Infrastruktur liegen, während andere Anwendungen komplett ausgelagert werden. Die Standardisierung von Ressourcen in sogenannten Containern und deren Orchestrierung in Kubernetes sorgen dann dafür, dass alle Teile der Cloud-Infrastruktur nahtlos ineinandergreifen. Für Behörden ist darüber hinaus wichtig, dass die Infrastruktur sowohl nach IT-Grundschutz und dem Cloud-Kriterienkatalog C5 des Bundesamts für Sicherheit in der Informationstechnik (BSI) zertifiziert als auch für Verschlusssachen zugelassen werden kann. Ein weiterer wichtiger Punkt ist die Verwendung von Open-Source-Bausteinen.

Der Open-Source-Gedanke impliziert eine gemeinsame Softwareentwicklung in einer anbieterübergreifenden Community. Was haben die Cloud-Kunden davon?

Dabei geht es vor allem um Transparenz und Nachprüfbarkeit. Eine proprietäre Software, die vom Anbieter geheim gehalten wird, ist für die Cloud-Kunden wie eine Black Box. Ob sie wirklich sicher ist oder nicht, kann niemand außer dem Anbieter beurteilen. Darauf kann sich keine Behörde in sicherheitssensiblen Bereichen einlassen. Open-Source-Software hingegen ist frei zugänglich und kann von jedem jederzeit überprüft werden. Aus diesem Grund beteiligen wir bei secunet uns übrigens schon lange an Open-Source-Technologie und leisten Beiträge zu deren Weiterentwicklung – auch jenseits der Cloud.

Was ist der Kern des secunet Cloud-Portfolios und wann wird es verfügbar sein?

Wir werden den Kunden ein unabhängiges Cloud-Angebot aus einer Hand bieten, das zudem sehr breit aufgestellt ist, so dass es unterschiedlichste Kundenanforderungen hinsichtlich des Technologie-Stacks wie auch des Betriebsmodells bedienen kann.



Bei der Cloud-Transformation können Ressourcen in sogenannten Containern standardisiert werden. Mittels Kubernetes werden diese Container dann über alle Teile der Cloud-Infrastruktur hinweg orchestriert.

Zudem ist es darauf angelegt, alle Sicherheitsniveaus von DSGVO-konform bis hin zur hohen Geheimhaltungsstufe GEHEIM abzudecken. Das Portfolio wird eine Kombination aus deutschen Public- und Private-Cloud-Angeboten in den Bereichen Infrastructure as a Service (IaaS), Platform as a Service (PaaS) sowie Software as a Service (SaaS) umfassen.

Die Basis der secunet Cloud ist bereits heute verfügbar: Unsere sicherheitsgehärtete Cloud-Plattform SecuStack haben wir im Jahr 2018 vorgestellt. Im Jahr 2022 haben wir den Cloud-native-Spezialisten SysEleven akquiriert, der besondere Expertise bei der Orchestrierung standardisierter Container mittels Kubernetes sowie eine eigene Infrastruktur mit Rechenzentren in Deutschland mitbringt. Das darauf basierende Public-Cloud-Angebot hat sich bereits bei mehreren Hundert Kunden bewährt. Das secunet Cloud-Portfolio wird nun Baustein für Baustein über die nächsten ein bis zwei Jahre ausgebaut. Die Bausteine sind modular und interoperabel, deshalb sprechen wir von einem Ökosystem. Als nächste Meilensteine peilen wir die allererste Zulassung eines Cloud-Stacks für Verschlusssachen durch das BSI an, und zwar bis einschließlich GEHEIM, sowie ein Testat nach C5.

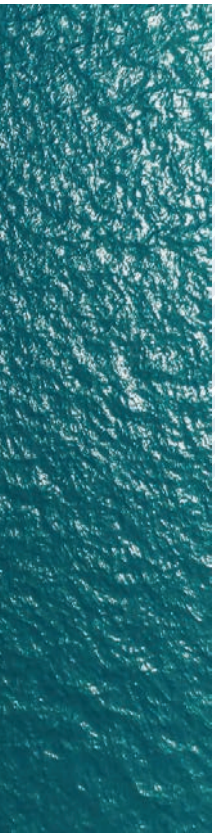
Können auch Angebote von Dritten integriert werden?

Unser Angebot ist als Hybrid-Cloud-Ökosystem konzipiert, das auf sichere Weise Lösungen von Partnern einbeziehen und zu resilienten Multi-Cloud-Angeboten verbinden kann. Dabei können sogar Lösungen von Hyperscalern eine Rolle spielen, etwa in weniger sicherheitssensiblen Bereichen. So entsteht optimale Wahlfreiheit für die Kunden – aber auf einem hohen Sicherheitslevel und mit großer Transparenz.

In welcher Form fließt die Expertise von secunet in der klassischen IT-Sicherheit ein?

Wir sichern seit über 25 Jahren besonders schützenswerte digitale Infrastrukturen, zum Beispiel in Ministerien und Sicherheitsbehörden. Dabei haben wir ein einzigartiges Know-how rund um hochwertige Verschlüsselungstechnologie aufgebaut, das nun die Grundlage für die secunet Cloud bildet.

Zudem bezieht unser Cloud-Angebot etablierte secunet Lösungen ein: So ermöglichen wir Kunden mit unserer Hochsicherheitslösung SINA, die in Behörden und der öffentlichen Verwaltung den De-facto-Standard für sichere Netzwerke und Arbeitsplätze darstellt, auch die Zugangspunkte zur Cloud abzusichern.



„In einigen Jahren werden viele IT-Sicherheitsprodukte, die heute noch auf Hardware-Boxen basieren, ‚as a service' verfügbar sein."

Somit sind wir gewissermaßen in der Lage, eine gesamte IT-Infrastruktur aus einer Hand anzubieten.

Mit ALASCA hat secunet gemeinsam mit anderen europäischen IT-Unternehmen einen neuen Verein gegründet, der Open Source im Cloud-Kontext befördern will. Was hat es damit auf sich?

Rund um die souveräne Cloud ist in den letzten Jahren eine innovative Branche entstanden, die der Gesellschaft etwas Entscheidendes anbieten kann. Nun ist der Zeitpunkt gekommen, um – bei allem nötigen Wettbewerb – Synergien zu nutzen, die Open-Source-Community zu stärken und die Technologieentwicklung dadurch weiter voranzutreiben. Zudem sollten die Akteure der neuen Branche bisweilen mit einer Stimme sprechen, damit sich das Wissen über die souveräne Cloud verbreitet. Dies sind die Ziele des neuen Vereins. ALASCA steht für „Alliance for Sovereign Cloud Infrastructures". secunet ist eines der sieben Gründungsmitglieder. Der Verein steht weiteren europäischen Unternehmen offen, die den Leitgedanken von Open Source im Cloud-Umfeld sowie digitaler Souveränität leben.

Wie wird die behördliche IT-Landschaft in fünf Jahren aussehen?

Die Cloud wird dann ein selbstverständlicher, zentraler Bestandteil der Behörden-IT geworden sein. IT-Verantwortliche werden ganz unterschiedliche Cloud-Angebote nach den jeweiligen Technologie- und Sicherheitsanforderungen auswählen und in die bestehende Multi-Cloud integrieren. Das Nutzererlebnis wird dennoch nahtlos sein. Darüber hinaus werden in einigen Jahren auch viele IT-Sicherheitsprodukte, die heute noch auf Hardware-Boxen basieren, „as a service" verfügbar sein. Die Cloud-Transformation ist vollständig, wenn sie alle Bereiche von Staat, Wirtschaft und Gesellschaft durchdringt.

Norbert Müller
norbert.mueller@secunet.com

Norbert Müller ist für secunet Cloud Solutions verantwortlich. Zuvor war er maßgeblich an dem erfolgreichen Ausbau der Zusammenarbeit von secunet mit der öffentlichen Verwaltung hinsichtlich klassischer Cybersicherheit beteiligt.

Public Key Infrastructure

„Unsere größte Herausforderung war die Zeit“

Im modernen digitalen Alltag werden Geschäftsprozesse zunehmend elektronisch abgebildet, vertrauliche Informationen über offene, internetbasierte Plattformen ausgetauscht. Dass solche Vertrauensbeziehungen funktionieren, ist oft einer Public Key Infrastructure (PKI) zu verdanken, die im Hintergrund die Authentizität digitaler Identitäten sicherstellt. Im Interview erläutert Mohamed Kiwan, CEO von EgyptTrust, warum sein Unternehmen auf eine PKI-Lösung von secunet setzt und wie die Implementierung verlief.

Herr Kiwan, welche Dienstleistungen bietet Ihr Unternehmen an und wer sind Ihre wichtigsten Kunden?

Mohamed Kiwan: EgyptTrust bietet digitale Signaturen und digitale Identitäten für alle elektronischen Dienste an. Wir sind hauptsächlich in Ägypten aktiv, da wir von der ägyptischen Regierung für die Bereitstellung digitaler Identitäten und digitaler Signaturen lizenziert sind. Unsere Kunden sind sowohl Unternehmen als auch Privatpersonen in Ägypten.

Wie kam es zu der Zusammenarbeit mit secunet?

Da wir nur begrenzte Zeit für das Projekt hatten, suchten wir einen erfahrenen Partner mit einer sicheren PKI-Lösung, die sich bereits bewährt hatte. Deshalb haben wir uns für secunet entschieden. Seit über einem Jahr arbeiten wir nun erfolgreich mit secunet zusammen.

In welcher Weise helfen Ihnen die PKI-Komponenten von secunet, zuverlässige und sichere Vertrauensdienste bereitzustellen? Gibt es Unterschiede zu PKI-Komponenten anderer Anbieter, die Sie bisher eingesetzt haben?

Im Vergleich zu den PKI-Lösungen anderer Anbieter, mit denen wir arbeiten, zeichnet sich die secunet PKI durch ihre einfache Nutzbarkeit sowohl für uns wie auch für die Anwender*innen aus. Darüber hinaus hebt sich die secunet Lösung durch ihre hohe Performance von anderen Anbietern ab: Auch wenn mehrere Prozesse gleichzeitig laufen, bleibt die PKI konsistent und vertrauenswürdig.

Mohamed Kiwan,
CEO von EgyptTrust

Für welche Anwendungsszenarien werden die PKI-Komponenten von secunet derzeit eingesetzt?
Unsere Dienstleistungen, die auf secunet Produkten basieren, finden sich in Anwendungen, die im ägyptischen Alltag eine entscheidende Rolle spielen. So müssen beispielsweise alle Unternehmen sowie Selbstständige wie Anwält*innen und Steuerberater*innen die elektronische Rechnungsstellung nutzen. Dies funktioniert mit unseren digitalen Signaturdiensten und der secunet PKI. Eine weitere wichtige Anwendung ist die Zollabfertigung für Lieferungen und Waren, die nach Ägypten kommen. Alle Waren, die per Schiff, Flugzeug oder auf anderem Wege in Ägypten ankommen, müssen deklariert werden. Die dafür erforderlichen Dokumente müssen ebenfalls über digitale Dienste bereitgestellt werden.

Wie lief die Implementierung?
Unsere größte Herausforderung war die Zeit. Wir mussten die Systeme schnell implementieren, weil die ägyptische Regierung uns eine Deadline gesetzt hatte. Und diese Deadline konnten wir einhalten. Zwischen unserem ersten Treffen und der erfolgreichen Umsetzung vergingen nur vier Monate.

„Unsere Dienstleistungen, die auf secunet Produkten basieren, finden sich in Anwendungen, die im ägyptischen Alltag eine entscheidende Rolle spielen."

Sind weitere gemeinsame Projekte geplant?
Wir planen bereits ein weiteres Projekt mit secunet und der Registrierungsstelle in Ägypten. Darüber hinaus diskutieren wir die Einsatzmöglichkeiten von Remote-Signing-Lösungen, da wir bis Ende dieses Jahres eine entsprechende Plattform fertigstellen wollen.

Gerd Schneider
gerd.schneider@secunet.com

WIE FUNKTIONIERT EINE PKI?

Zur Authentisierung von Personen und technischen Komponenten sowie zum Signieren und Verschlüsseln von Daten und Nachrichten werden digitale Zertifikate eingesetzt. Eine typische PKI besteht aus einer Reihe von Elementen, die digitale Zertifikate automatisiert ausstellen, verteilen und prüfen. Dazu gehören zum Beispiel eine sogenannte Certification Authority (CA), die die Zertifikate signiert, eine Registration Authority (RA), die die Benutzer in der CA registriert und ein Verzeichnisdienst (Directory oder DIR), der unter anderem eine Liste ungültiger öffentlicher Schlüssel enthält. In der Summe stellen diese und andere Elemente sicher, dass die im Umlauf befindlichen Zertifikate jederzeit vertrauenswürdig sind.

Da eine PKI in der Regel einen hohen Komplexitätsgrad aufweist, haben sich vor allem Anwendungsfälle durchgesetzt, bei denen die Endnutzer*innen nicht direkt mit der PKI in Berührung kommen und die Lösung automatisiert im Hintergrund abläuft. Ein gutes Beispiel dafür ist das Verschlüsselungsprotokoll TLS (Transport Layer Security), das in HTTPS-basierten Webservern eingesetzt wird. Von den Nutzer*innen weitgehend unbemerkt verwendet der Browser die PKI beispielsweise für sicheres Onlinebanking und Onlineshopping.

Bei der Grenzkontrolle prüft eine PKI die Authentizität elektronischer Identitäten. Ebenso kommen PKIs bei intelligenten Stromzählern, in vernetzten Automobilen oder bei der Interaktion von Maschinen im Umfeld des Internet of Things (IoT) zum Einsatz.

secunet eID PKI SUITE

secunet hat sein Know-how aus mehr als 350 PKI-Projekten in der secunet eID PKI Suite gebündelt. Die verschiedenen Softwarebausteine der eID PKI Suite ergeben zusammengenommen ein hochleistungsfähiges Gesamtsystem, können aber genauso gut einzeln in eine bestehende Systemarchitektur integriert werden. Alle relevanten Standards und Protokolle werden unterstützt. Für Einsatzgebiete mit besonderen Sicherheitsanforderungen ist die eID PKI Suite auch in einer nach Common Critera EAL4+ zertifizierten Variante verfügbar.

Aus dem Portrait einer realen Person (groß im Bild) und einer weiteren realen Person (oben rechts) lässt sich mit Bildbearbeitungssoftware ein Morph (oben links) erstellen, der zu kriminellen Zwecken eingesetzt werden kann.

Bekämpfung von Identitätsbetrug bei der Grenzkontrolle

Schlechte Chancen für Morphs

Biometrische Daten und automatisierte Gesichtserkennung haben die Grenzkontrolle effizienter und sicherer gestaltet. So genannte Morphing-Angriffe stellen jedoch eine Herausforderung dar, und zwar gleichermaßen für Beamte wie auch für Softwaresysteme. Dabei verwenden Betrüger ID-Fotos, die aus den Passbildern mehrerer Personen zusammengesetzt – „gemorpht" – sind. Die Morphing-Methoden entwickeln sich stetig weiter. Die differentielle Morphing Attack Detection von secunet tut das ebenfalls – und schnitt beim FRVT-MORPH-Test der US-amerikanischen Normierungsbehörde NIST beim Erkennen hochwertiger Morphs deutlich besser ab als alle anderen Verfahren.

Morphing-Angriffe zählen aktuell zu den größten Bedrohungen der Grenzkontrolle. Gelingt es den Angreifern, zwei oder mehr biometrische Passfotos mittels Bildbearbeitungssoftware zu einem überzeugenden „Morph" zusammenzufügen und auf diese Weise biometrische Software oder auch Grenzkontrollbeamte zu täuschen, können mehrere Personen dasselbe Ausweisdokument für einen Grenzübertritt verwenden – nämlich alle, deren Bilder an dem Morph beteiligt sind. Sicherheitsmaßnahmen wie „Live Enrolment", bei dem Passbilder vor Ort und unter Aufsicht von Beamten aufgenommen werden müssen, oder die Schulung der Grenzbeamten wirken den kriminellen Methoden entgegen, können das Problem aber nicht gänzlich beseitigen.

Mit Algorithmen gegen Identitätsbetrug

Daher setzen die Grenzkontrollbehörden auch auf intelligente Software, um den Betrügern das Handwerk zu legen. Bei der sogenannten Morphing Attack Detection (MAD) handelt es sich um Software-Algorithmen, die Gesichtsmorphs bei der automatisierten Grenzkontrolle erkennen können. Dabei nutzen sie unterschiedliche Methoden. secunet bietet einen Algorithmus an, der nach dem Prinzip der differentiellen MAD arbeitet. Dabei wird ein potenziell gemorphtes Gesichtsbild gegen ein zweites, in der Regel live aufgenommenes und damit vertrauenswürdiges Bild geprüft.

Die Zuverlässigkeit von MAD-Algorithmen wird im Rahmen des unabhängigen und international anerkannten „Face Recognition Vendor Test (FRVT)-MORPH" des US-amerikanischen National Institute of Standards and Technology (NIST) ermittelt. Dabei sind vor allem zwei Werte entscheidend: Die Bona Fide Presentation Classification Error Rate (BPCER), oder auch Falsch-Alarm-Rate genannt, gibt an, wie oft der Algorithmus echte IDs fälschlicherweise als Morph erkannt hat. Die Attack Presentation Classification Error Rate (APCER), auch Morph-Miss-Rate genannt, gibt dagegen an, wie viele Morphs nicht erkannt wurden. Eine niedrige APCER bedeutet also, dass viele Morphs erfolgreich entdeckt wurden. Die Algorithmen lassen sich auf einen niedrigen BPCER-Wert einstellen, doch dann steigt in der Regel der APCER-Wert. Daher kommt es auf ein gutes Finetuning je nach den jeweiligen Anforderungen an.

Differentielle MAD mit hervorragenden Ergebnissen

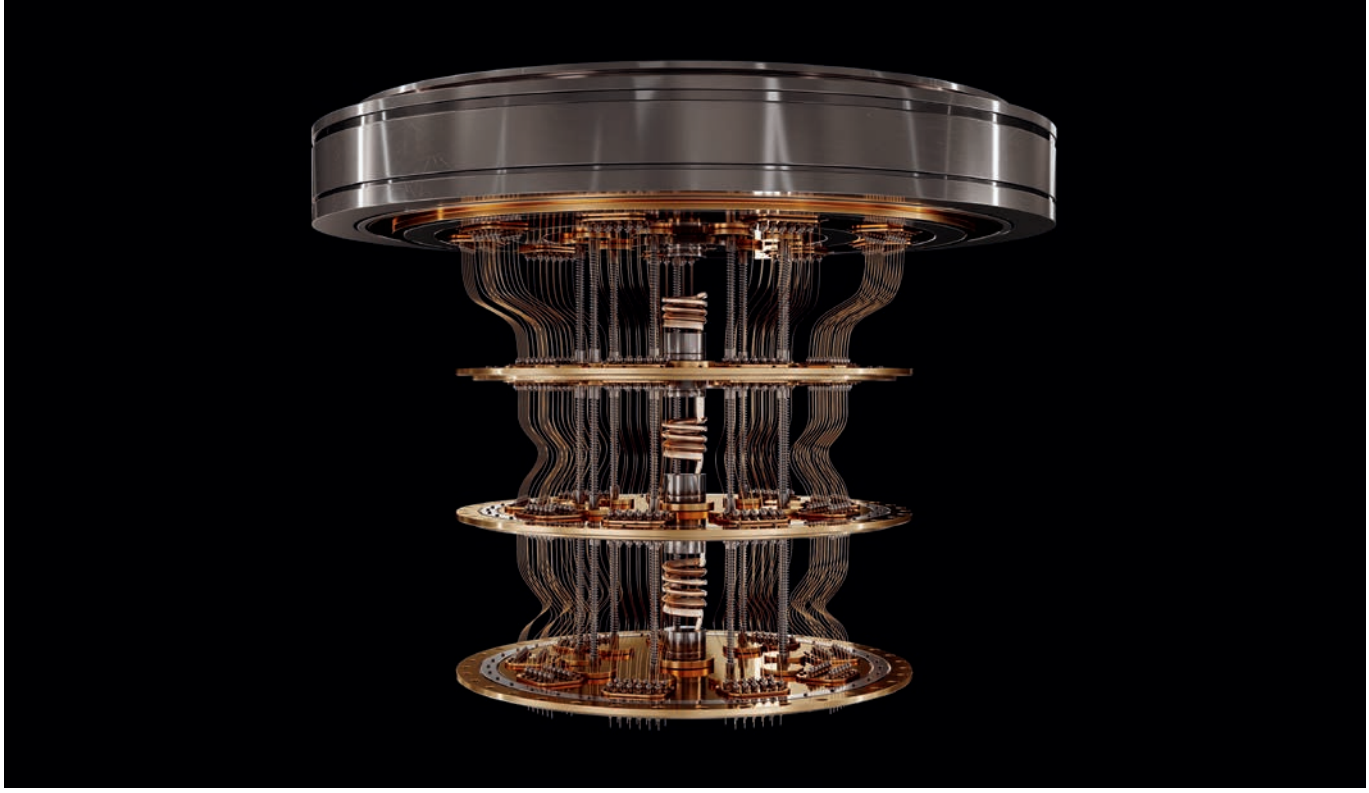
In dem FRVT-MORPH-Testdurchgang von November 2022 konnte der verbesserte Algorithmus sein bisher bestes Ergebnis erzielen: Bei einer BPCER von 0,01 wurden über alle Datensätze hinweg nur 9 Prozent bis 36 Prozent der Morphs (APCER) nicht erfolgreich erkannt. Mit einer BPCER von 0,02 sinkt die Morph-Miss-Rate sogar auf 4 Prozent bis 22 Prozent.

Insbesondere in der Kategorie der High Quality Morphs konnte der secunet Algorithmus punkten. Obwohl solche Morphs für versierte Angreifer nicht besonders schwer herzustellen sind, sind sie besonders schwer zu erkennen. Zu dieser Kategorie gehört das Data Set „Printed and Scanned", bei dem die Morphs – wie bei Passbildern üblich – ausgedruckt und wieder eingescannt wurden, wodurch praktisch keine Spuren der Manipulation im Bild verbleiben. Der secunet Algorithmus erkannte bei diesem Data Set schon bei einer moderaten BPCER von 0,01 ganze 84 Prozent der Morphs und bei einer etwas höheren BPCER von 0,02 sogar 93 Prozent. Mit diesen Ergebnissen verwies er sämtliche anderen der mehr als 30 Verfahren, die an dem Test teilnahmen, auf die Plätze – und das mit großem Abstand. Auch im Vergleich zu menschlichen Testpersonen, die Untersuchungsergebnissen zufolge in der Regel lediglich 60 Prozent der Morphs erkennen, sind die Ergebnisse interessant, denn sie zeigen, welch großen Beitrag MAD zur Bekämpfung von Identitätsbetrug am Grenzübergang leisten kann.

Nichtsdestotrotz bleibt die Morphing-Erkennung eine Herausforderung. Die MAD-Algorithmen müssen auch in Zukunft kontinuierlich verbessert, erweitert und neu trainiert werden, um den Betrügern immer einen Schritt voraus zu sein und die Fehlerquoten weiter zu senken.

Michael Schwaiger
michael.schwaiger@secunet.com

Das automatisierte Grenzkontrollsystem secunet easygate, hier eine Installation am Flughafen Wien, verfügt über Morphing Attack Detection.



Sicherheit vor Quantencomputern

Kryptografie 2.0

Zukünftige Quantencomputer stellen eine erhebliche Bedrohung für kryptografisch geschützte Daten dar. Das betrifft nicht nur die alltägliche Kommunikation im Internet, in Gefahr sind insbesondere hochsensible Daten bis hin zu Staatsgeheimnissen. Abhilfe versprechen neuartige, Quantencomputer-resistente Algorithmen, die in den letzten Jahren entwickelt wurden. Mit dieser Post-Quanten-Kryptografie (PQC) hat secunet sich schon früh befasst. Heute sind bereits mehrere SINA Komponenten, die von Behörden und Bundeswehr für den Umgang mit Verschlusssachen eingesetzt werden, mit PQC ausgestattet. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat diese Geräte für die hohe Geheimhaltungsstufe GEHEIM zugelassen. Somit ist Deutschland in Europa Vorreiter in puncto PQC.

Die Sicherheit digitaler Infrastrukturen beruht maßgeblich auf kryptografischen Algorithmen und Protokollen. Gängige Verschlüsselungsverfahren wie der in vielen Internet-Protokollen wie Transport Layer Security (TLS) und Internet Key Exchange (IKE) verwendete Diffie-Hellman-Schlüsselaustausch setzen voraus, dass bestimmte mathematische Probleme aufgrund limitierter Rechenkapazitäten praktisch nicht lösbar sind. Digitale Signaturen mit dem Verfahren RSA, die zum Beispiel zur Authentifizierung in Webbrowsern genutzt werden, gelten als sicher, solange kein effizienter Algorithmus zur Faktorisierung existiert.

Darauf konnte man sich jahrzehntelang verlassen. Doch als Experten vor einigen Jahren die ersten Konzepte für Quantencomputer diskutierten, wurde schnell klar, dass die Tage der herkömmlichen Kryptografie gezählt sind. Bis die neuartigen Rechner den gängigen Algorithmen gefährlich werden können, wird es voraussichtlich noch einige Zeit dauern.

Bislang existieren Quantencomputer nur als raumfüllende Versuchsaufbauten in Forschungslaboren, und ihre Leistungsfähigkeit beschränkt sich derzeit auf das Lösen einfacher Rechenaufgaben. Doch es wird erwartet, dass weiterentwickelte Quantencomputer schon in wenigen Jahren klassischen Rechnern in vielen Bereichen deutlich überlegen sein werden. Dazu gehört eben auch das Lösen mathematischer Probleme, die der konventionellen Kryptografie als Grundlage dienen.

Rechnen mit Qubits

Quantencomputer basieren auf einer völlig anderen Technologie als herkömmliche Systeme. Statt sich wie diese auf das binäre Rechnen mit Nullen und Einsen zu beschränken, können ihre fundamentalen Informationseinheiten, die Qubits, auch mit Abstufungen dazwischen arbeiten. Das liegt daran, dass die Qubits auf quantenmechanischen Zuständen basieren und daher nicht eindeutig einen der Werte Null oder Eins annehmen müssen. Vielmehr können sich die beiden Werte überlagern, wobei dann unterschiedliche Wahrscheinlichkeiten für sie gelten. Verbindet man zahlreiche Qubits, können logische Operationen durchgeführt werden, die allerdings eher den Prozessen in neuronalen Netzen gleichen als dem seriellen Rechnen in klassischen Computern.

Quantencomputer gehen nicht Schritt für Schritt vor, sondern beschreiten viele mögliche Lösungswege gleichzeitig und finden gegebenenfalls auch mehrere Lösungen. Dann müssen Algorithmen die Rechenoperationen sinnvoll eingrenzen, so dass verwertbare Ergebnisse herauskommen.

Sobald absehbar war, dass die neue Art des maschinellen Rechnens die herkömmliche Kryptografie bedrohen würde, begann die Suche nach alternativen Kryptoverfahren, die resistent gegenüber Quantencomputern sind. Denn nicht nur aufgrund der raschen Entwicklung der neuen Technologie ist Eile geboten. Die Herausforderung besteht auch darin, dass Angreifer bereits heute verschlüsselte Daten mitschneiden und speichern können, um sie erst später, wenn hinreichend leistungsfähige Quantencomputer verfügbar sind, zu entschlüsseln. Das ist ein sehr ernstzunehmendes Szenario, weil besonders sensible Daten, etwa mit der Einstufung GEHEIM, mitunter nicht nur für Jahre, sondern für Jahrzehnte unter Verschluss bleiben sollen. Somit ist der Quantencomputer bereits heute, bevor seine Entwicklung überhaupt den erforderlichen Reifegrad erreicht hat, eine signifikante Bedrohung für die Informationssicherheit auch von Staaten und internationalen Organisationen.

Die SINA L3 Box H (links), die SINA Workstation H Client V (hinten) und der SINA Communicator H (rechts) arbeiten bereits mit PQC-Elementen.

PQC im Einsatz

Um dieser Bedrohung zu begegnen, führt die US-amerikanische Normierungsbehörde National Institute of Standards and Technology (NIST) derzeit einen Prozess zur Standardisierung von PQC durch und hat kürzlich die ersten Algorithmen ausgewählt, die bis 2024 standardisiert werden sollen. Da jedoch mögliche Angriffe nach dem Muster „jetzt mitschneiden und später entschlüsseln" sofortige Präventivmaßnahmen erfordern, hat sich secunet in Abstimmung mit dem BSI entschieden, PQC bereits vor der Standardisierung durch das NIST zu implementieren.

Als IT-Sicherheitspartner der Bundesrepublik stellt secunet Technologie her, die hoch eingestufte Daten bis zum Grad GEHEIM schützt und unter anderem von der Bundeswehr sowie von Bundesministerien mit besonderen Sicherheitsanforderungen wie zum Beispiel dem Bundesministerium für Verteidigung genutzt wird. Insgesamt wurden seit dem Jahr 2002 in Deutschland und anderen EU- bzw. NATO-Staaten rund 30.000 für GEHEIM bzw. SECRET zugelassene SINA Verschlüsselungsgeräte ausgeliefert. In Deutschland stellt SINA den De-facto-Standard für Verschlüsselungen auf diesem hohen Sicherheitslevel dar. Drei zentrale Produkte dieses Portfolios hat secunet bereits mit PQC-Elementen ausgestattet: den SINA Communicator H, der abhörsichere Sprachkommunikation sowie viele weitere moderne Kommunikationsfeatures bietet, das hochsichere VPN-Gateway SINA L3 Box H sowie den Arbeitsplatzrechner SINA Workstation H Client V, der eine einzigartige Kombination von performanter Kryptografie und hoher Rechenleistung liefert.

Das BSI hat diese drei SINA Komponenten als erste Verschlüsselungsprodukte mit PQC in Deutschland für die Geheimhaltungsstufe GEHEIM zugelassen. Im europäischen Vergleich ist Deutschland damit Vorreiter bei Kryptogeräten, die bereits heute mit PQC arbeiten. Und mit der SINA Workstation H R RW14 steht die neueste Generation von gehärteten Laptops, die für den Einsatz unter extremen Bedingungen konzipiert sind, bereits in den Startlöchern für den Eintritt ins PQC-Zeitalter.

Hybride Verfahren

In den bisher drei SINA Komponenten mit PQC wird der Schlüsselaustausch quantenresistent umgesetzt. Was bedeutet das? Um die Vertraulichkeit von Daten bei der Übertragung gegenüber Quantencomputern zu gewährleisten, müssen sowohl der Verschlüsselungsalgorithmus als auch das Schlüsselaustauschverfahren, das zur Ableitung des Schlüssels verwendet wird, quantenresistent sein. In der Regel ist der Verschlüsselungsalgorithmus bereits quantenresistent, wenn er mit ausreichend großen Schlüsseln verwendet wird. Die konventionellen Schlüsselaustauschverfahren sind jedoch gegenüber Quantencomputern potentiell anfällig. Da sich die PQC-Algorithmen noch in der Endphase der Standardisierung befinden, empfiehlt das BSI die Verwendung von so genannten Hybridverfahren: Durch die Kombination von konventioneller Kryptografie und PQC müsste ein Angreifer jeden Algorithmus brechen, um die Hybridlösung zu knacken. Die drei SINA Produkte mit PQC unterstützen einen hybriden quantenresistenten Schlüsselaustausch mit dem vom BSI empfohlenen Algorithmus FrodoKEM. Perspektivisch, im Laufe der nächsten Jahre, wird secunet alle kritischen Funktionalitäten des gesamten SINA Portfolios für die Stufe GEHEIM, aber auch für niedrigere Geheimhaltungsstufen wie VS-NUR FÜR DEN DIENSTGEBRAUCH (VS-NfD), mit PQC realisieren.

Dabei können Hybridmodi nicht nur als vorübergehende Migrationsstrategie in Richtung PQC dienen, sondern als Beitrag zu langfristiger Sicherheit und Agilität hinsichtlich der Verschlüsselungsverfahren. Generell beginnt mit dem Einsatz von PQC eine neue kryptografische Ära, die nicht nur durch Resistenz gegenüber Quantencomputern, sondern auch durch eine erhöhte kryptografische Agilität gekennzeichnet ist. Als Reaktion auf die Bedrohung erfindet die Kryptografie sich also neu – und gewinnt an Stärke hinzu.

Leonie Bruckert
leonie.bruckert@secunet.com

Biometrie und künstliche Intelligenz

Fairness, Robustheit und Sicherheit für KI

Künstliche Intelligenz (KI) birgt großes Potenzial für Anwendungen im Bereich der inneren Sicherheit. Ein Beispiel ist die Live-Analyse von Gesichtsbildern zur Gefahrenabwehr, etwa an Flughäfen. Dabei gibt es allerdings eine große Herausforderung: Statistische Verzerrungen bei der Datengrundlage können dazu führen, dass KI tendenziöse Ergebnisse liefert, die im schlimmsten Fall bestimmte Personengruppen benachteiligen oder bevorzugen können. secunet erforscht Lösungen, die diesem gefährlichen und folgenschweren Effekt entgegenwirken und so dazu beitragen, dass KI-Anwendungen fair arbeiten und vertrauenswürdig sind.

Um die Sicherheit und Fairness von KI-Anwendungen zu garantieren, erarbeitet die EU derzeit den sogenannten EU AI Act, welcher Anwendungen von Künstlicher Intelligenz in verschiedene Risikokategorien einteilen und bestimmte Prüfungen vorschreiben wird. In Deutschland hat das Bundesamt für Sicherheit in der Informationstechnik (BSI) mit dem AIC4 Kriterienkatalog frühzeitig ein Rahmenwerk für Prüfkriterien von KI-Anwendungen aufgestellt.

Ein wichtiger Bestandteil solcher Prüfungen ist die Frage, ob und in welchem Maße ein trainiertes KI-Modell statistischen Verzerrungen – einem sogenannten Bias – unterliegt. Ein Bias entsteht beispielsweise durch unzureichend ausgeglichene Trainingsdaten oder durch eine Überrepräsentation bestimmter Merkmalskombinationen, die dann vom KI-Modell gelernt und verallgemeinert werden. So kann es im ungünstigsten Fall passieren, dass bei der Anwendung des KI-Modells bestimmte Gruppen von Menschen oder auch Individuen benachteiligt oder bevorzugt werden. Insbesondere bei KI-Anwendungen, die mit Bildern oder Videos von Menschen arbeiten, hätte ein Bias schwerwiegende Konsequenzen.

Das Problem sitzt durchaus tief: Bildverarbeitende KI-Modelle mit Architekturen wie CNNs (Convolutional Neural Networks) sind dazu konzipiert, Muster zu erkennen. Auch wenn Merkmale wie Alter, Geschlecht oder ethnische Zugehörigkeit nicht explizit in den Trainingsdaten gekennzeichnet sind, kann

Diese synthetischen Gesichter wurden aus einer Vielzahl möglicher Merkmale zusammengesetzt und anschließend als Grundlage für virtuelle Bilder verwendet, welche die Gesichter in verschiedenen Situationen zeigen. Auch bei der Prüfung von KI-Modellen auf einen Bias kommen solche Bilder zum Einsatz.

ein KI-Modell eine indirekte Repräsentation solcher oder ähnlicher Merkmale auf der Grundlage der vorhandenen Bildinformationen konstruieren. Ein solcher sogenannter indirekter Bias ist nur schwer zu erkennen und noch schwerer zu beheben. Eine Analyse benötigt ein sehr großes, differenziertes Datenset. Um alle Merkmalskombinationen auf herkömmliche Weise auf einen Bias zu testen, müssten tausende neue Bilder angefertigt werden, was in Bezug auf die benötigte Zeit und die Kosten schlichtweg nicht möglich ist.

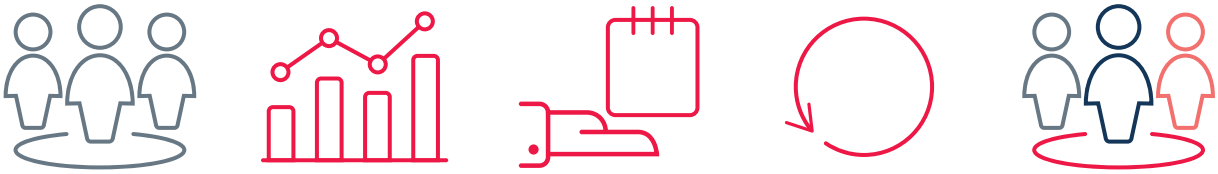
secunet hat sich intensiv mit dem Thema Bias in Bildern und KI-Modellen mit menschlichem Bezug beschäftigt und eine Lösung entwickelt, die nicht nur Verzerrungen in den Daten erkennt, sondern erstmalig auch das KI-Modell auf eben jene Verzerrungen testen kann. Mit dieser Lösung ist es möglich, ein Modell so weiterzuentwickeln, dass ein Bias eliminiert wird. Dazu werden die Trainingsdaten so angepasst, dass alle Merkmale fair verteilt und vorhanden sind und als Konsequenz ein möglicher Bias im Modell mitigiert wird. Das sorgt übrigens nicht nur für faire und diskriminierungsfreie KI-Modelle, sondern erhöht darüber hinaus die Sicherheit und Robustheit der Modelle. Mit zusätzlichen Funktionen wie der Anpassung von Umwelt- und Umgebungsfaktoren können die Limitationen des KI-Modells festgestellt und Lösungsansätze entwickelt werden.

Die Analyse und Lösung des Bias-Problems geschieht dabei in drei Schritten:

1) Die Trainings- und Testdaten werden auf einen Bias in Bezug auf Merkmale wie Alter, Geschlecht und Ethnie analysiert. Damit können bereits frühzeitig Probleme erkannt werden, welche sich später im KI-Modell abbilden würden.

2) Die Lösung von secunet führt einen Test des KI-Modells durch. Dabei generiert sie eine Vielzahl von fotorealistischen künstlichen Identitäten, die sich zum Beispiel in Alter, Geschlecht und Ethnie unterscheiden. Die ursprünglichen Identitäten der Testdaten werden mit den künstlichen Identitäten ausgetauscht, mit der Absicht, die Erkennungsleistung des KI-Modells zu prüfen. Dabei werden beliebige Merkmalskombinationen generiert, schließlich ist auch die tatsächliche menschliche Vielfalt sehr groß. Eine Festlegung auf eine bestimmte Anzahl von Ethnien gibt es nicht, da dies zu einem neuen Bias führen würde. Die maßgeschneiderten Identitäten mit fließenden Übergängen in den Merkmalen bilden somit die gesamte menschliche Vielfalt ab.

3) Wird ein Bias erkannt, können neue Identitäten für die Trainingsdaten erzeugt und das Modell neu trainiert werden. Dieser Prozess wird so oft wiederholt, bis kein Bias mehr nachweisbar ist.



Ausgangslage:
Potentieller Bias

Fairness-
Analyse

Generierung
künstlicher Identitäten

Modell
Re-Training

Resultat:
Faires Modell

Das Verfahren lässt sich einfach und schnell durchführen. Hat ein KI-Modell den Prozess durchlaufen, liegt ein Nachweis dafür vor, dass es fair ist und frei von Diskriminierung. Dies schafft Vertrauen in die KI-Anwendung – aufseiten der Öffentlichkeit, aber auch aufseiten der Betreiber, denn Letztere können nun mit Zuversicht von der Fairness ihres Modells ausgehen.

Darüber hinaus geht es bei der Analyse von KI-Modellen nicht nur um Bias. Weitere wichtige Aspekte, die sich ebenfalls im EU AI Act und auch im BSI AIC4 wiederfinden, sind Robustheit und Sicherheit der Erkennungsleistung. So besteht zum Beispiel die Gefahr, dass eine KI-Anwendung unter bestimmten Witterungsbedingungen oder Lichtverhältnissen relevante Merkmale nicht erkennt, was Sicherheitsrisiken zur Folge hätte. Mit der Forschung und Entwicklung von secunet können verschiedene Umweltfaktoren getestet werden, um so die Grenzen der Erkennungsleistung einer Anwendung aufzuzeigen und mögliche Risiken zu identifizieren.

In der Öffentlichkeit wird viel über die Risiken von KI diskutiert, auch im Zusammenhang mit deren Einsatz für die innere Sicherheit. Eine gründliche und unvoreingenommene Prüfung und Optimierung der relevanten KI-Modelle ist der beste Weg, auf diese Diskussion zu reagieren und die Akzeptanz von KI-Anwendungen zu steigern.

Dominik Lawatsch
dominik.lawatsch@secunet.com

Vernetztes und autonomes Fahren

„Wir brauchen eine öffentliche Diskussion“

Die Automotive-Branche muss gleich mehrere Umbrüche meistern und steht dabei vor einer Vielzahl von Herausforderungen. Eine davon ist die Cybersicherheit. Wie sichert man Systeme ab, die Teil einer vielfältig verflochtenen Infrastruktur sind, einen Lebenszyklus von mehreren Jahrzehnten haben und sich noch dazu – anders als kritische Komponenten in hochsicheren Rechenzentren – potentiell andauernd in „feindlicher“ Umgebung befinden? Vieles lässt sich technisch lösen, aber auch eine herstellerübergreifende, öffentliche Diskussion ist erforderlich, findet der Automotive-Cybersecurity-Experte Manuel Wurm.

Herr Wurm, wo sehen Sie derzeit die größten Herausforderungen auf dem Weg zu einer sicheren Mobilität in der Zukunft?

Der Weg zur einer elektrifizierten, automatisierten und kooperativen Mobilität der Zukunft führt uns von weitestgehend voneinander isolierten, autarken Fahrzeugen zu einem Ökosystem aus vielfältig miteinander verflochtenen Komponenten: automatisierte bzw. autonome Fahrzeuge, Ladeinfrastruktur, Mobilitätsdienstleister, Hersteller, Flottenbetreiber, Telekommunikationsdienstleister und nicht zuletzt die Endkunden. Shared Mobility, das Prinzip der gemeinsam nutzbaren Mobilität, lässt zudem die Bedeutung von Fahrzeugen als Besitz oder gar Statussymbol schrumpfen. Stattdessen wird zukünftig die Mobilität von Personen bzw. der Transport von Gütern im Vordergrund stehen.

Neben all den Vorteilen, die eine derartige Zukunft verspricht, sind auf dem Weg dorthin einige Herausforderungen zu meistern. Die gesamte Automobilindustrie, vor allem die Hersteller und deren Lieferanten, stecken in der Zwickmühle zwischen Zeitdruck und Wettbewerbsfähigkeit auf der einen Seite und neuen gesetzlichen Vorgaben wie etwa UNECE R155/R156[1] auf der anderen Seite – und das auf einem Spielfeld mit zum Teil neuen Mitspielern. Um langfristig die Akzeptanz und das Vertrauen in diese neue Technologie und in diesen neuen Markt zu erhalten, müssen – bezogen auf die Sicherheit – öffentlich und transparent die dafür notwendigen Leitlinien diskutiert und definiert werden. Was ist das gesellschaftlich akzeptierte (Rest-)Risiko für diese neuartige Technologie des vernetzten und automatisierten Fahrens?

Andererseits sind auf technischer Ebene zahlreiche Anforderungen an die Zuverlässigkeit zu erfüllen, um das Vertrauen der Endkunden und letztendlich der gesamten Gesellschaft in die neue Technologie zu stärken und zu erhalten. Dazu zählen die Verfügbarkeit, weil ansonsten finanzielle Ausfälle drohen, die funktionale Sicherheit, weil sonst Gefahr für Leib und Leben besteht und die Security einschließlich Datenschutz zum Schutz vor Cyberangriffen.

> „Was ist das gesellschaftlich akzeptierte (Rest-)Risiko für diese neuartige Technologie des vernetzten und automatisierten Fahrens?“

Bezogen auf die Cybersicherheit lohnt es sich, etwas genauer hinzusehen und ggf. auch den Blickwinkel zu ändern. Ein einheitliches Bild der Bedrohungslage existiert leider nicht. Wer sind die möglichen Angreifer? Welche Ziele verfolgen sie und welche Fähigkeiten und Ressourcen besitzen sie? Vom Standpunkt eines Cyberangreifers aus gesehen stellen vernetzte Fahrzeuge mit ADAS- bzw. AD-Funktionalität, das heißt mit automatisierten bzw. autonomen Fahrfunktionen, ein hochattraktives Ziel dar. Dank ihrer Funkschnittstellen sind sie bequem aus der Ferne erreichbar, zusätzlich können Schwächen in den Backend-Servern Angriffe auf die ganze Flotte ermöglichen, und schließlich werden für das automatisierte Fahren eine Menge teurer und komplexer und für die Fahrzeugindustrie zum Teil neuartiger Komponenten verbaut – inklusive einer mutmaßlich langen Liste potentieller Schwachstellen.

Sie haben ein Fachbuch speziell zum Thema Automotive Cybersecurity veröffentlicht. Was unterscheidet die klassische Cybersicherheit von der Automotive-Cybersicherheit?

Beide Bereiche haben gemeinsam, dass sie für die Absicherung komplexer Rechnersysteme und Netzwerke sorgen. Bisher galt weitestgehend die Behauptung, dass IT-Technologie in der Mehrzahl der Fälle nicht einfach so in Fahrzeuge integrierbar war. Begrenzende Faktoren sind oft die geringeren Ressourcen der Embedded Systeme sowie strengere Anforderungen der Automobilindustrie – etwa an die Temperaturfestigkeit.

Die (klassische) Trennung zwischen IT-Security und Automotive Embedded Security verschwimmt im Automobilbereich allerdings stetig. Wo Fahrzeuge früher noch als isolierte, autarke Systeme begriffen wurden, werden sie zukünftig mit anderen Verkehrsteilnehmern und Verkehrsinfrastrukturkomponenten wie etwa Ampeln kommunizieren. Wo früher ein Netzwerk aus dedizierten Steuergeräten die verschiedenen Steuer- und Regelfunktionen ausführte, werden zukünftig Domänen- oder Zonensteuergeräte mit Hochleistungsrechnern und Softwarekomponenten aus dem „klassischen“ IT- bzw. IoT-Bereich die Rechenaufgaben mehrerer Steuergeräte zusammenfassen und übernehmen. Dank der breitbandigen und flächendeckend verfügbaren Funkverbindung können Algorithmen und Funktionen, beispielsweise die Berechnung der Streckenführung, auch aus dem Fahrzeug in eine Cloud übertragen und dort berechnet werden. Die Security Operation Center, die zumindest alle größeren Unternehmen bereits zur Absicherung ihrer IT-Infrastruktur betreiben, werden zukünftig auf Fahrzeuge als neue Endpoints ausgeweitet werden.

Ein wesentlicher Unterschied, den ich auch in meinem Buch beschreibe, ist der Umstand, dass sich Fahrzeuge potentiell andauernd in feindlicher Umgebung befinden: Angreifer können sich Fahrzeuge und Fahrzeugkomponenten schließlich (legal) beschaffen und gewissermaßen beliebig untersuchen und angreifen. In der IT-Sicherheit schließen wir kritische

[1] Eine Regelung der Wirtschaftskommission für Europa der Vereinten Nationen (UNECE)

Komponenten dagegen in hochsicheren Rechenzentren ein und verhindern somit zumindest die physischen, lokalen Angriffe. Hersteller von mobilen Geräten wie etwa Smartphones sind mit demselben Problem konfrontiert.

Bei der vernetzten Mobilität sind viele Player aktiv – OEMs, Zulieferer, Infrastrukturkomponenten, Versicherungen, öffentliche Stellen, um nur einige zu nennen. Wie kann es gelingen, all diese verschiedenen Teilnehmer sicher zusammenspielen zu lassen?

Das Schaffen kooperativer, intelligenter Transportsysteme und alternativer Mobilitätskonzepte setzt eine bestimmte technologische Transformation voraus, was wiederum zu Veränderungen in der Zulieferkette bzw. in den Geschäftsbeziehungen innerhalb der Automobilbranche führt. An Stelle der etablierten Automobilhersteller mit hierarchischen OEM-Lieferanten-Beziehungen werden zukünftig komplexe Technologie-zentrierte bzw. Geschäftsmodell-zentrierte Ökosysteme, bestehend aus verschiedenen neuen Mitspielern im Mobilitätssektor, eine wichtige oder gar dominierende Rolle spielen. Neue Mitspieler sind unter anderem die Betreiber des öffentlichen Personennahverkehrs, Mobilitätsdienstleister, die über leistungsstarke digitale Plattformen mit zum Teil enormer Reichweite verfügen und Technologie-Lieferanten, die beispielsweise hochauflösendes Kartenmaterial oder LIDAR[2]-Komponenten bereitstellen.

„Im Rahmen einer transparenten Zusammenarbeit auf Augenhöhe, in der alle Partner über dasselbe Wissen und dieselben Kompetenzen verfügen ist die Wahrscheinlichkeit unerkannter Cyberrisiken geringer."

Wie können wir trotz der verschiedensten Interessen innerhalb dieser Ökosysteme dafür sorgen, dass die IT-Sicherheit nicht auf der Strecke bleibt?

Gesetze und Vorschriften können hier helfen, aber meiner Meinung nach nur einen Mindest-Standard definieren und sozusagen die Leitplanken inhaltlich festlegen.

Ein nachhaltiger Weg wäre es, durch vertrauensvolle Zusammenarbeit, etwa durch gemeinsame Entwicklungsplattformen und durch das Schaffen gemeinsamer Standards, Wissen aufzubauen, miteinander auszutauschen und die jeweiligen Lösungsräume anzugleichen. Im Rahmen einer transparenten Zusammenarbeit „auf Augenhöhe", in der alle Partner über dasselbe Wissen und dieselben Kompetenzen verfügen, ist die Wahrscheinlichkeit unerkannter Cyberrisiken geringer. Zumindest was die fachliche Zusammenarbeit im Kontext einer gemeinsamen Cybersecurity-Strategie angeht, sollten Geschäftsbeziehungen und -hierarchien eine untergeordnete Rolle spielen. Letztendlich kann nur eine durchdachte und strukturierte Anwendung von technischen Cybersecurity-Bausteinen zu einem wirksamen Schutz vor Cyberangriffen beitragen.

Fahrzeuge haben einen Lebenszyklus von mehreren Jahrzehnten. Wie geht man am besten mit vagen Zukunftsprognosen um – beispielsweise in Bezug auf Zero-Day-Schwachstellen oder Quantencomputer?

Der lange Lebenszyklus von Fahrzeugen stellt uns tatsächlich vor große Herausforderungen. Rund 15 Jahre – verglichen mit der durchschnittlichen Nutzungsdauer von Smartphones oder PCs ist das eine extrem lange Zeit und gefühlt kommen nur Haushaltsgroßgeräte an diese Zeitspanne heran.

Um direkt auf Ihre beiden Beispiele einzugehen: Gegen Zero-Day-Exploits kann man sich mit endlichen Mitteln vermutlich nicht vollständig schützen, sondern nur vorbereiten und eine Verteidigung aufbauen. Gegen zukünftige Angriffe, die auf Quantencomputern basieren, können wir uns bereits heute schützen oder zumindest darauf vorbereiten: Post-Quanten-Kryptografie, das heißt kryptografische Algorithmen, die vermutlich auch von Quantencomputern nicht in kurzer Zeit entschlüsselt werden können, sollten bereits heute in der Produktentwicklung berücksichtigt werden.

Die Branche wird sich allerdings technologisch und organisatorisch auf längerfristige Supportzeitspannen einstellen müssen, indem erforderliches Personal, Equipment, Werkzeuge und Wissen über den gesamten Zeitraum vorgehalten werden. Im Rahmen der Produktentwicklung sollten Ressourcen reserviert und eine gewisse Flexibilität eingeplant werden, damit ein zukünftiger Austausch von Hardware, das Updaten der Software und insbesondere auch das Anpassen von Krypto-Algorithmen ermöglicht werden. Darüber hinaus sollte bestenfalls bereits in der Entwicklungsphase eine sogenannte „Degraded Functionality" in Erwägung gezogen werden. Das bedeutet, dass beispielsweise die sichere Ausführung bestimmter Funktionen irgendwann nicht mehr gewährleistet werden

[2] „Light Detection and Ranging", eine Methode zur optischen Abstands- und Geschwindigkeitsmessung

kann und deshalb verhindert oder eingeschränkt werden muss. Um alle diese Aufgaben zu stemmen, bedarf es vor allem ausgeklügelter Prozesse sowie personeller und technischer Kapazitäten – bei den Herstellern als auch bei den Lieferanten.

Weil auch hier wieder mehrere verschiedene Parteien betroffen sind, vom Hersteller bis zum Endkunden, sollten die Leitplanken für einen langfristigen Security-Support idealerweise gemeinschaftlich und öffentlich diskutiert und beschlossen werden – und nicht von einzelnen Unternehmen individuell gelöst werden. Folgende Fragen sollten wir uns stellen: Was sind die möglichen Folgen von erfolgreichen Cyberangriffen auf Fahrzeuge und auf ihre digitale Infrastruktur? Zumindest die Größenordnung der möglichen Konsequenzen sollten alle kennen. Was ist das gesellschaftlich akzeptierte Risiko durch Cyberangriffe auf die Fahrzeughersteller und Mobilitätsdienstleister? Wird das verbleibende (Rest-)Risiko von Versicherungen getragen? Wieviel ist (uns) die Security wert? Und wieviel ist der Kunde bereit, dafür zu zahlen? Wie lange sollen Hersteller für die Sicherheit ihrer Produkte gewährleisten und Updates bereitstellen? Wann oder unter welchen Bedingungen können die kostspielige Wartung und Updates vorzeitig beendet werden (End-of-Service vs. End-of-Life)? Wie gehen wir mit Security-Schwachstellen um, die nicht kurzfristig behebbar sind – Fahrzeuge und Mobilitätsdienste stilllegen oder mit eingeschränkter Funktion weiterfahren?

Für die Automobilindustrie sind diese Anforderungen eine Neuerung, weil erforderliche Prozesse erst noch etabliert werden müssen. Erfahrene und branchenübergreifend aufgestellte Dienstleister wie secunet

„Wie gehen andere Branchen mit derartigen Herausforderungen um und sind ihre Erfahrungen auf die Automobilindustrie übertragbar?“

können hier meiner Meinung nach wertvolle Hilfestellung geben. Wie gehen andere Branchen mit derartigen Herausforderungen um und sind ihre Erfahrungen auf die Automobilindustrie übertragbar?

Auch in Deutschland haben wir einen Fachkräftemangel. Sehen Sie im Rahmen Ihrer Dozententätigkeit wachsendes Interesse am Thema IT-Sicherheit?
In den vergangenen Jahren konnten wir glücklicherweise beobachten, dass sowohl mehr und mehr Studiengänge mit Security-Schwerpunkten entstanden sind, als auch dass Security als Themencluster häufiger verschiedene Fachbereiche durchdringt: von Informatik über Elektrotechnik und Mechatronik bis zu Wirtschaftsinformatik und Technologiemanagement.

Um die Neugier für das Thema Security zu wecken, helfen oftmals einfache Vorführungen, „Live-Hacks“, die den Studenten demonstrieren, wie niederschwellig der Zugang zum „Hacking“ sein kann. Dank der Verfügbarkeit kostengünstiger Hardware und Software wird man heute mit einem Budget von weniger als 100 Euro technisch in die Lage versetzt, ein breites Spektrum von Angriffen auf Fahrzeuge durchzuführen. Anleitungen, How-To-Videos und Software sind meist frei verfügbar und leicht zu finden.

Manuel Wurm

Manuel Wurm ist in der Automotive-Branche als Forschungs- und Entwicklungsingenieur tätig. Seit 2012 ist er Dozent an der DHBW Ravensburg und seit 2019 auch an der Fachhochschule Vorarlberg in Dornbirn (Österreich). Sein Buch „Automotive Cybersecurity: Security-Bausteine für Automotive Embedded Systeme“ erschien im Jahr 2022 bei Springer Vieweg und ist unter anderem im Online-Buchhandel erhältlich.

© Dieter Seibel, Wangen

Cybersecurity-Gesetze für Industrieunternehmen

Der Weg aus dem Dschungel der EU-Cyberregulierung

Cyber Resilience Act, NIS-2 und die CER-Richtlinie: Die Cybersecurity-Gesetzeslage für Industrieunternehmen in Europa ist vielfältig und unübersichtlich. Doch die Umsetzung der unterschiedlichen regulatorischen Anforderungen kann dabei helfen, Cyberangriffe erfolgreich abzuwehren. Das ist auch dringend notwendig, denn die Zahl der Cyberangriffe nimmt zu. Laut der techconsult-Studie „Angriffserkennung in Unternehmen Kritischer Infrastrukturen" von Anfang 2023 schätzen 79 Prozent der Unternehmen die aktuelle Bedrohungslage als wachsend bis stark wachsend ein. Doch wen betreffen die Regulierungen? Welche Pflichten entstehen daraus? Und welche Fristen müssen Industrieunternehmen beachten? Hier ein Überblick der wichtigsten Cybersecurity-Gesetze in Europa.

1. Directive on Security of Network and Information Systems (NIS-2 Richtlinie)

Die NIS-2 Richtlinie ist ein wichtiger Teil der EU-Digitalstrategie „Gestaltung der digitalen Zukunft Europas" und die Weiterentwicklung der bereits 2016 erlassenen NIS Richtlinie. Ziel ist es, ein hohes Cybersicherheitsniveau auf europäischer Ebene sicherzustellen und damit den Binnenmarkt zu stärken. Die Richtlinie ist am 16. Januar 2023 in Kraft getreten. Die EU-Mitgliedstaaten haben bis zum 17. Oktober 2024 Zeit, die Bestimmungen in nationale Gesetzgebung zu überführen.

Betroffene Wirtschaftszweige sind in zwei Kategorien unterteilt: essential/wesentlich – also Sektoren mit hoher Kritikalität – und important/wichtig – weitere kritische Sektoren. Unter erstere fallen beispielsweise Energie, Transport und Verkehr, Finanzmärkte, der Gesundheitssektor, digitale Infrastrukturen sowie die öffentliche Verwaltung. Weitere kritische Sektoren sind unter anderem Post- und Kurierdienstleistungen, produzierendes Gewerbe, Chemie sowie

die Fertigung von Medizingeräten, elektronischen Geräten, Maschinen und Transportmitteln. Welche Unternehmen innerhalb der definierten Sektoren genau betroffen sind, wird durch die jeweilige nationale Gesetzgebung festgelegt.

Für Industrieunternehmen bringt NIS-2 neue Spielregeln und damit neue Aufgaben. So müssen sich Firmen registrieren und Cybersicherheitsvorfälle nach fest definierten Vorgaben in einem mehrstufigen Prozess an die zuständigen Behörden melden.

Unternehmen müssen zudem ein aktives Risikomanagement einführen und sich an Standards beispielsweise für Netzwerk- und Systemsicherheit, Vorfallbehandlung, Krisenmanagement sowie zu sicheren Lieferketten und dem Asset Management halten. Schutzmechanismen und eingesetzte Technologien müssen dem Stand der Technik entsprechen. Eine Zertifizierungspflicht zur Darstellung der Compliance kann durch die Nationalstaaten zusätzlich gefordert und eingeführt werden.

National ist geplant, NIS-2 durch das NIS-2-Umsetzungs- und Cybersicherheitsstärkungsgesetz (NIS2UmsuCG) in nationales Recht zu überführen. Es handelt sich erneut um ein Artikelgesetz, welches viele bestehende Gesetze gemäß der Richtlinie anpasst. KRITIS-Betreiber in Deutschland haben in Folge des IT-Sicherheitsgesetzes bereits ein solides Fundament aufgebaut. So sind zum Beispiel Unternehmen, die ein Information Security Management System (ISMS) und die nötige vertrauenswürdige Cybersicherheitstechnologie implementiert haben, gut aufgestellt und müssen mit nur geringen Anpassungen rechnen.

2. EU Cyber Resilience Act – Cybersicherheit für vernetzte Produkte

Der Cyber Resilience Act (CRA) der EU ist ein Gesetzentwurf mit dem Ziel, Endverbraucher und Unternehmen vor Produkten zu schützen, welche Cybersicherheit nur unzureichend berücksichtigen. Zu diesem Zweck soll das Gesetz Anforderungen an Produkte mit digitalen Elementen hinsichtlich Entwicklung, Ausgestaltung und Produktion definieren und damit Cybersicherheit im gesamten Lebenszyklus sichern – so zum Beispiel auch die Bereitstellung von Softwareupdates. Das Sicherheitsniveau von vernetzten Endprodukten soll erhöht werden, um Cyberkriminalität vorzubeugen. Das Gesetz wird voraussichtlich 2023 in Kraft treten. Danach haben die Betroffenen zwölf bis 24 Monate Zeit für die Umsetzung der neuen Anforderungen.

Von den Vorschriften betroffen sind viele Hersteller von Hard- und Softwareprodukten. Die Anforderungen werden je nach möglicher Auswirkung unterschieden. Für Produkte, die größere wirtschaftliche Bereiche betreffen, wie IoT- und Mobilfunkgeräte oder Betriebssysteme, werden strengere Vorschriften erwartet. So soll die Cybersicherheit bereits im Produktionsprozess bzw. bei der Konfiguration berücksichtigt werden („Security by Design and Default“) – beginnend mit der Planung eines Produkts bis in die Betriebsphase und einige Jahre nach dem Produktverkauf (bis zu fünf Jahre). Zusätzlich müssen Hersteller ausführliche Dokumentation führen. Das Bereitstellen von Softwareupdates bzw. -patches und die aktive Kommunikation zu Sicherheitslücken und deren Fehlerbehebung ist ein weiterer wesentlicher Baustein der Regulierung. Des Weiteren müssen für betroffene Produkte klare und verständliche Bedienungs- bzw. Betriebsanleitungen zur Verfügung gestellt werden.

3. Directive on the resilience of critical entities

Die EU-Richtlinie über die Resilienz kritischer Einrichtungen (CER-Richtlinie) hat das Ziel, die physische Widerstandsfähigkeit kritischer Einrichtungen zu stärken, und soll somit insbesondere hybriden Bedrohungen entgegenwirken. Die CER-Richtlinie ersetzt die alte Richtlinie 2008/114/EC und weitet den Anwendungsbereich aus. Durch diese neuen Vorschriften werden die EU-Mitgliedstaaten zur Identifikation von kritischen Einrichtungen und Stärkung von deren Widerstandsfähigkeit verpflichtet. Die CER-Richtlinie ist am 16. Januar 2023 in Kraft getreten. Die EU-Mitgliedstaaten haben bis zum 17. Oktober 2024 Zeit, die Bestimmungen in nationale Gesetzgebung zu überführen.

Betroffene Wirtschaftszweige sind gemäß der Richtlinie in die Kategorien wesentlich und wichtig unterteilt. Insgesamt elf Sektoren gehören zum Geltungsbereich, der sich teilweise mit der NIS-2 Richtlinie überschneidet: Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheit, Trinkwasser, Abwasser, digitale Infrastruktur, öffentliche Verwaltung, Weltraum sowie Produktion, Verarbeitung und Vertrieb von Lebensmitteln.

Unternehmen müssen sowohl organisatorische als auch technische Sicherheitsmaßnahmen umsetzen. Dazu zählt ein funktionsfähiges Risikomanagement, um Betriebsunterbrechungen zu verhindern. Ein Business Continuity Management System (BCMS) kann hier eine geeignete Maßnahme darstellen. Zudem sollen Unternehmen in der Lage sein, adäquat auf Sicherheitsvorfälle zu reagieren und dementsprechend einen Plan zur Vorfallbehandlung (Incident Management) zu definieren. Sicherheitsvorfälle sollen an die zuständigen Aufsichtsbehörden gemeldet werden. Diese können eigene Inspektionen und Audits durchführen und die Implementierung von angemessenen Maßnahmen einfordern.

Step by step zu mehr Sicherheit – das können Unternehmen jetzt tun

In fünf Schritten können Industrieunternehmen sich auf die Regulierungen vorbereiten:

1) Betroffenheit prüfen (Produkthersteller, Betreiber, Integratoren)

2) Anforderungen prüfen

3) Meldeprozesse vorbereiten bzw. vorhandene Umsetzungen hierzu anpassen

4) Sicherheitskonzepte, Informationssicherheitsmanagement (zum Beispiel auf Basis ISO/IEC 27001 bzw. IEC 62443) inkl. Business Continuity Management etablieren

5) Risikomanagement im definierten Geltungsbereich umsetzen

Ob CRA, NIS-2 oder die CER-Richtlinie: Halten sich Unternehmen nicht an die Vorschriften, können die EU-Staaten Bußgelder verhängen. Diese betragen zum Beispiel beim CRA bis zu 15 Mio. Euro bzw. 2,5 Prozent des Jahresumsatzes. Umso wichtiger ist eine strukturierte und ganzheitliche (Cyber-) Security-Strategie. Neben technischen Maßnahmen wie der Absicherung der Netzwerke und Geräte zählt dazu auch ein Blick auf die Absicherung der Unternehmensprozesse und die Sensibilisierung für das Thema bei den Mitarbeitenden.

Alexander Schlensog
alexander.schlensog@secunet.com

Steffen Heyde
steffen.heyde@secunet.com

Informationssicherheitsmanagement

Das Reifegradmodell: ISMS zu Ende gedacht

Autor Gunter Pilger ist bei secunet unter anderem IT-Security Beauftragter (TÜV), Grundschutz Praktiker (BSI) und Datenschutzbeauftragter (TÜV) und auf Informationssicherheit spezialisiert.

Aktuell endet bei den meisten Behörden und Unternehmen der Horizont der Informationssicherheit, nachdem ein Informationssicherheitsmanagementsystem (ISMS) eingeführt ist. Zwar leben viele ein ISMS aktiv, sei es durch regelmäßige (interne) Audits, Ableitung von Maßnahmen und Umsetzung dieser Maßnahmen, jedoch fehlt in vielen Fällen ein systematischer Prozess, der Maßnahmen nachvollziehbar abbildet und den aktuellen Zustand eines ISMS aggregiert darstellt. An dieser Stelle setzt das sogenannte Reifegradmodell (RGM) an. Es hilft auch dabei, den Erfordernissen der ISO/IEC 27001 (explizit: ISO/IEC 27004) und des BSI Grundschutzes[1] gerecht zu werden.

Ziel der Einführung und später der Anwendung eines Reifegradmodells ist es, die Qualität und Leistungsfähigkeit des ISMS festzustellen und zu erhöhen (vgl. Abb. 1). Durch regelmäßige Auswertungen kann mithilfe des RGM überprüft werden, welche (Teil-) Prozesse noch nicht optimal gesteuert werden. An Stellen, an denen der ermittelte Reifegrad niedrig ist, besteht Handlungsbedarf.

RGM können dabei unterstützen, Priorisierungen für die Weiterentwicklung und Verbesserung eines ISMS zu setzen. Durch die Anwendung eines RGM soll ein umfassender Blick auf die Effizienz des Informationssicherheitsprozesses erlangt werden. Hierzu wird das ISMS über längere Zeit analysiert, um die Effizienz des ISMS-Prozesses zu messen, in regelmäßigen Abständen zu überprüfen und bei Bedarf Korrekturmaßnahmen zur Verbesserung zu ergreifen.

Vorgehensweise zur erfolgreichen Implementierung eines RGM

Es bietet sich an, das RGM zunächst auf einen eingeschränkten Informationsverbund anzuwenden und danach schrittweise in die Organisation auszurollen und den Geltungsbereich dadurch zu vergrößern.

Bevor der RGM-Prozess gestartet wird, muss sichergestellt sein, dass Sicherheitsziele im Detail definiert sind. Dies ist von großer Bedeutung, weil nur dadurch gewährleistet werden kann, dass Kennzahlen (KPI[2]) abgeleitet und am Ende wiederum an den

[1] ISMS.1.A11, ORP.3.A8, OPS.1.1.3.A13, DER.4.A15

[2] Key Performance Indicator

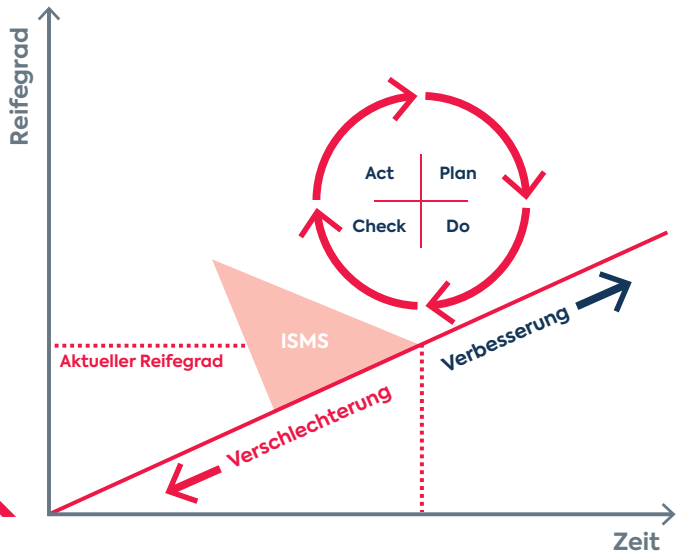


Abb. 1: Reifegrad und kontinuierliche Verbesserung

ISMS
Ein ISMS bildet durch festgelegte Regeln und Methoden den Rahmen, mit welchem die Informationssicherheit einer Organisation gewährleistet werden kann. secunet unterstützt Unternehmen beim Aufbau eines ISMS nach dem IT-Grundschutz des Bundesamts für Sicherheit in der Informationstechnik (BSI) sowie nach ISO 27001.

Reifegradmodell (RGM)
Ein RGM dient der Bewertung und Verbesserung von ISMS-Prozessen. Ebenfalls hilft ein RGM bei der Beobachtung von Entwicklungstrends.

Nutzen eines RGM
Das RGM kann zur Optimierung und systematischen Steuerung von Prozessen verwendet werden.

Sicherheitszielen ausgerichtet werden können. Dies setzt voraus, dass die Ziele verständlich definiert und messbar sind und neben der klaren Verbindung zu den Zielobjekten auch ein Zusammenhang bzw. eine Ursache-Wirkungs-Beziehung hergestellt werden kann, ähnlich wie bei einer Balanced Scorecard. Ein Beispiel: Bei einer hohen Schulungsquote wird davon ausgegangen, dass Sicherheitslücken schneller erkannt und behoben werden. Dies führt zu einer höheren Kundenzufriedenheit und einer besseren Reputation. Bei einem definierten strategischen Ziel „höhere Reputation“ wäre somit eine Kausalität zwischen Ursache und Wirkung hergestellt.

Inhalte eines RGM

Nach der Festlegung der Vorgehensweise zur Implementierung gilt es im Folgenden, die Reifegradstufen festzulegen (vgl. Abb. 2). Hierbei wird beispielsweise auch konkretisiert, ab welcher Reifegradstufe die Einführung von Kennzahlen angestrebt wird.

Es ist zu empfehlen, in mehreren Workshops für die Organisation passende KPI zu erarbeiten und auf Basis der festgelegten Themenbereiche abzuleiten. Alle Beteiligten sollten von Anfang an bei der Definition der Kennzahlen eingebunden sein und mitgenommen werden, damit sie sich mit den Kennzahlen identifizieren können. KPI können in einem Kennzahlensteckbrief dargestellt werden, mit Detailangaben dazu, wie sie zu ermitteln und zu bewerten sind.

Abb. 2: Vorgehensweise bei der Implementierung

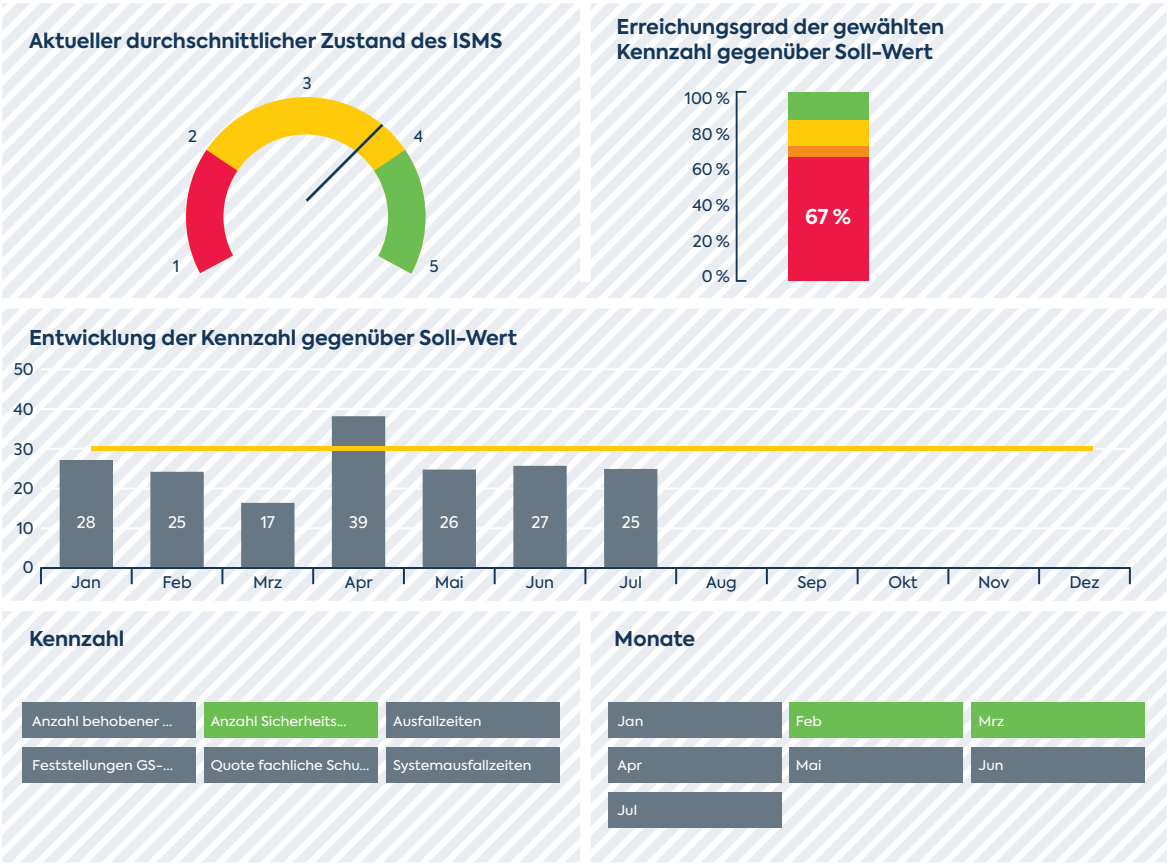


Abb. 3: Dynamisches Dashboard

Die KPI spiegeln nur dann die Realität wieder, wenn sie unter kontinuierlicher Beobachtung und Kontrolle stehen und qualitativ bzw. quantitativ erfasst werden, um zu sehen, wie sich Maßnahmen tatsächlich ausgewirkt haben.

Es ist das erklärte Ziel, KPI möglichst effizient zu erheben und zu ermitteln. Realisiert wird dies, indem sie aus bestehenden Systemen und Datenbeständen weitestgehend automatisiert abgeleitet werden. Die ermittelten Kennzahlen und deren Wert sollten außerdem wieder in den übergeordneten Risikomanagementprozess zur kontinuierlichen Verbesserung zurückfließen. Auf dieser Basis sollen die für die Reifegradmessung mit KPI erforderlichen Prozesse und das Unternehmen bzw. die Behörde ebenfalls der kontinuierlichen Verbesserung unterliegen.

Aus den Werten der KPI wird auch ein Gesamtergebnis ermittelt, anhand dessen sich beurteilen lässt, ob eine Verbesserung oder Verschlechterung des gesamten RGM stattgefunden hat.

Darstellung der Kennzahlen (KPI)

Es bietet sich an, einzelne KPI in einem Dashboard darzustellen (vgl. Abb. 3), damit diese zur Steuerung übersichtlich und nachvollziehbar bleiben sowie der Organisationsleitung in einem monatlichen Report einen Grobüberblick über den aktuellen Stand des ISMS geben.

Die KPI werden für den Management-Bericht in unterschiedlichen Diagrammtypen dargestellt, um schnell einen aussagekräftigen Überblick zu erlangen. Zur Darstellung können sowohl einzelne KPI als auch die Betrachtungszeiträume als Aggregation der KPI über einen bestimmten Zeitraum hinweg ausgewählt werden.

Fazit

Ein Reifegradmodell wird immer häufiger explizit gefordert und auch der Nutzen sowohl für Unternehmen als auch Behörden wird immer größer. Die Mitarbeitenden beschäftigen sich mit Prozessen, diese werden dadurch verständlich und greifbar und KPI messen und steuern die Prozesse. Die KPI können damit wie bei einer Balanced Scorecard für Prozessoptimierungen verwendet werden und dienen zugleich dem kontinuierliche Verbesserungsprozess, der sowohl beim BSI Grundschutz als auch zum Beispiel im Rahmen der ISO/IEC 27001 von Auditoren überprüft wird. secunet hat bereits einige RGM erfolgreich bei Kunden eingeführt und kann damit sowohl Behörden als auch Unternehmen bei Bedarf qualifiziert unterstützen.

Gunter Pilger
gunter.pilger@secunet.com

Gesundheitswesen

Beim TI-Zugang haben Leistungserbringer die Wahl

Der secunet konnektor sorgt für eine sichere Anbindung von Arztpraxen, Krankenhäusern und anderen medizinischen Leistungserbringern an die Telematikinfrastruktur (TI), die Datenautobahn des deutschen Gesundheitswesens. Die Konnektoren enthalten Smartcards (gSMC-K) mit Zertifikaten, die gemäß den Sicherheitsvorgaben in der TI nach fünf Jahren ablaufen. Danach muss ein neuer Konnektor verwendet werden, der mit einer gSMC-K mit aktuellem Schlüsselmaterial ausgestattet ist. Die ersten Konnektoren von secunet für den Online-Produktivbetrieb wurden Ende November 2018 produziert. Somit laufen deren Zertifikate bis Ende 2023 ab.

Neben der Option eines Konnektor-Austauschs bietet secunet Leistungserbringern nun ein Softwareupdate zur Laufzeitverlängerung der secunet Konnektoren an. Dieses ermöglicht ab August 2023 für alle secunet Konnektoren, die vor dem 1.1.2021 ausgestellte Zertifikate enthalten, eine Verlängerung bis 31.12.2025 – unabhängig davon, ob der Konnektor mit ECC- oder RSA-Schlüsseln eingerichtet ist. Für Leistungserbringer ändert sich nichts am Setup oder Tagesablauf, sie erhalten das Update bei ihrem Vertragspartner.

„Mit der Laufzeitverlängerung bieten wir Nutzer*innen des secunet Konnektors neben dem Austausch der Hardware eine weitere schnelle und unkomplizierte Alternative und verschaffen ihnen Zeit für eine wohldurchdachte Entscheidung, welcher Weg in die TI für ihr Anforderungsprofil zukünftig der beste ist“, so Markus Linnemann, Vice President Division eHealth, secunet.

Neben dem Konnektor vor Ort sind bereits heute erste „TI as a Service“-Angebote auf Basis zentral betriebener Einbox- und Rechenzentrumskonnektoren verfügbar. Mit dem TI-Gateway und dem Highspeedkonnektor bereitet secunet parallel die nächste Evolutionsstufe der „TI as a Service“-Angebote vor. „Die TI 2.0 stellt neue Modelle in den Fokus, die ohne lokale physische Zugangspunkte auskommen“, so Linnemann. „Mit dem Highspeedkonnektor bietet secunet die technische Basis dafür.“

Leistungserbringer werden also künftig in der Lage sein, ihre favorisierte TI-Anbindung – Einboxkonnektor, Highspeedkonnektor oder TI as a Service – abhängig von ihren jeweils individuellen Anforderungen auszuwählen.

Der secunet Highspeedkonnektor, der sich derzeit im Zulassungsprozess befindet, wird noch im Jahr 2023 entscheidende Vorteile für Krankenhäuser und „TI as a service“-Anbieter bieten. Er kann zentral betrieben werden und bedient Anforderungen großer IT-Netzwerke und Gesundheitseinrichtungen. Speziell für „TI as a Service“-Anbieter ist er multimandantenfähig.

Arztpraxen und andere medizinische Leistungserbringer benötigen einen Zugang zur Telematikinfrastruktur (TI).

Die Lösung sorgt für maximale Performance, einfach zu skalierende Last sowie eine hohe Ausfallsicherheit des TI-Zugangs.

Auf dem Weg in die TI 2.0 steigt die Wahlfreiheit der Leistungserbringer. Die Qual der Wahl lohnt sich, da sich der individuelle Bedarf künftig besser berücksichtigen lässt.

Aktuelle Informationen zum TI-Zugang und anderen Themen rund um die Digitalisierung des Gesundheitswesens bietet der secunet eHealth Newsletter. Hier geht es zur Anmeldung:

https://www.secunet.com/anmeldung-ehealth-newsletter

Hilfe bei IT-Sicherheitsvorfällen

Cyberangriff – was nun?

Als deutschlandweit erster IT-Sicherheitsdienstleister ist secunet beim Bundesamt für Sicherheit in der Informationstechnik (BSI) für den Geltungsbereich „Vorfallbearbeitung“ gelistet und gleichzeitig auch erster registrierter IT-Sicherheitsdienstleister des Cyber-Sicherheitsnetzwerks (CSN). Das CSN ist ein freiwilliger Zusammenschluss qualifizierter Experten für eine IT-Vorfallbearbeitung. Die zertifizierten Cybersicherheits-Dienstleister sollen Unternehmen dabei unterstützen, schnell auf Sicherheitsvorfälle zu reagieren und diese erfolgreich abzuwehren.

Die secunet Prüfstelle bedient bereits seit vielen Jahren die Bereiche Konformität mit Technischen Richtlinien, Informationssicherheits-Managementsysteme (ISMS) und Penetrationstests und unterstützt so bei der Gefahrenabwehr. Das neue Gebiet erweitert dieses Portfolio nun um verschiedene Dienstleistungen im Rahmen einer schrittweisen Bekämpfung von Sicherheitsvorfällen, die von einem Team BSI-zertifizierter Vorfallexperten durchgeführt werden.

Konkret sind dies:

- Analyse von komplexen IT-Sicherheitsvorfällen, insbesondere vor Ort
- Zügige Eindämmung des Schadensausmaßes eines größeren IT-Sicherheitsvorfalls
- Ermittlung der Ursachen von komplexen Angriffen
- Wiederherstellung verschiedener betroffener Systeme nach einem IT-Sicherheitsvorfall

„Unternehmen sind häufig mit der Bewältigung von IT-Sicherheitsvorfällen überfordert. Insbesondere in komplexen Fällen, die eine starke fachliche Expertise und Erfahrung in der Vorfallanalyse und -behandlung erfordern und personelle Kapazitäten beanspruchen, gelangt die IT-Abteilung schnell an ihre Belastungsgrenze. Ein zertifizierter IT-Sicherheitsdienstleister kann hier helfen“, erklärt Holger Funke, Director Business Development, dem die Leitung der Prüfstelle obliegt.

Holger Funke
holger.funke@secunet.com

secunet ist das erste BSI-zertifizierte Unternehmen für Vorfallbearbeitung.

Social Days

Gemeinsam Verantwortung übernehmen

secunet ist Deutschlands führendes Cybersecurity-Unternehmen und steht für den bestmöglichen Schutz digitaler Infrastrukturen, Daten und Anwendungen. Doch für was steht secunet darüber hinaus? Welche Werte vertritt secunet als Unternehmen? Was macht secunet aus? Wer könnte diese Fragen besser beantworten als die Treiber des Unternehmenserfolgs: die secunet Mitarbeiter*innen. Gemeinsam haben sie die Unternehmenswerte formuliert. In diesem Zusammenhang lautet eine der wesentlichen Aussagen: Wir übernehmen gemeinsam Verantwortung. Und zwar aktiv. Damit diese Aussage – auch neben dem Business – keine theoretische Absichtserklärung bleibt, engagiert sich secunet in Form der neu etablierten Social Days. secunet unterstützt soziale Projekte im Bereich der Kinder- und Jugendarbeit finanziell und mit dem Engagement der Mitarbeitenden. Los ging es an den großen Standorten in Berlin, Dresden, Essen und München. Über 100 Mitarbeitende beteiligten sich an Gartenarbeiten, der Verschönerung von Außengeländen, Museumsbesuchen oder Upcycling-Aktionen mit Grundschulklassen. „Ein toller Tag, der nicht nur den Kindern Spaß gemacht hat. Neben dem sozialen Engagement konnten wir neue Kolleg*innen kennenlernen, erfolgreich im Team arbeiten und gemeinsam etwas Gutes tun. Beim nächsten Social Day sind wir auf jeden Fall wieder dabei“, so das Resümee einer Teilnehmerin. „Ein großer Dank gilt allen secunet Mitarbeiterinnen und Mitarbeitern, die dieses Jahr mitgemacht haben und unsere Werte aktiv gemeinsam im Team leben. Wir freuen uns auf die nächsten Social Days“, sagt Axel Deininger, CEO von secunet.

Termine – August bis Dezember 2023

23. August 2023
Polizeitag Düsseldorf | Düsseldorf

20. bis 21. September 2023
PITS Public IT Security | Berlin

25. bis 26. September 2023
AUTOMA+ | Zürich, Schweiz

2. bis 4. Oktober 2023
IKT Sicherheitskonferenz | Linz, Österreich

10. bis 12. Oktober 2023
it-sa | Nürnberg

10. bis 12. Oktober 2023
JAPCC | Essen

11. bis 12. Oktober 2023
LEA DER | Prag, Tschechien

18. bis 20. Oktober 2023
Intergraf | Bilbao, Spanien

19. Oktober 2023
Polizeitag Dresden | Dresden

14. bis 16. November 2023
Space Tech Expo | Bremen

14. bis 17. November 2023
Milipol | Paris, Frankreich

29. bis 30. November 2023
Berliner Sicherheitskonferenz | Berlin

6. Dezember 2023
Polizeitag München | München

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. 3, 5, 8, 10, 11, 13, 16, 17, 26, 27, 30: secunet
S. 2 (oben), 6, 22, 23, 28: Getty Images
S. 2 (unten), 18, 29: Adobe Stock
S. 12: iStock
S. 21: Dieter Seibel, Wangen

Als langjähriger IT-Sicherheitspartner der Bundesrepublik Deutschland gestalten wir schon heute souveräne Cloud-Lösungen ganz nach Ihren Bedürfnissen – on-premise, public oder auch kombiniert als flexible Hybrid Cloud.

secunet.com **protecting digital infrastructures**

secunet