

Technische Systeme werden intelligent

Prof. Dr. Sabina Jeschke
über technologische Führung,
offene Modelle und die Frage, ob
Europa sich selbst im Weg steht

Zertifizierungsdschungel Cloud

Was sagen die verschiedenen Nachweise aus?

Hilfe beim Kampf gegen Deepfakes

Technologie erkennt KI-generierte Inhalte

National

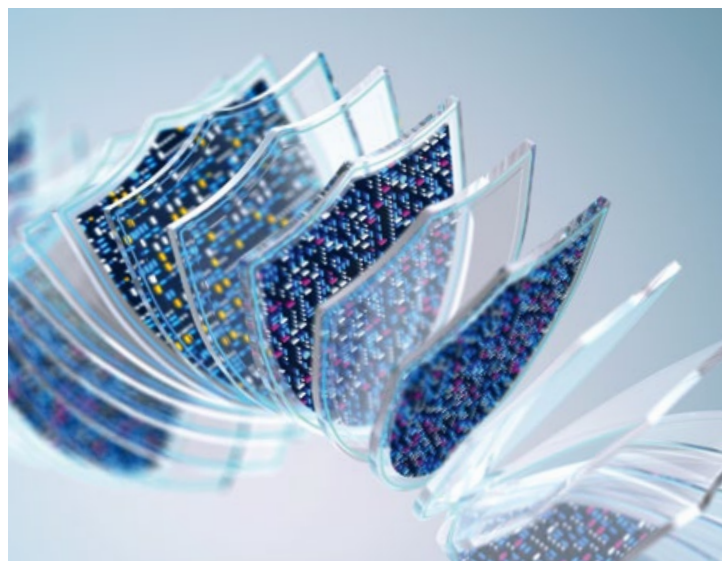
- 4 Compliance:
Zertifizierungsdschungel Cloud
- 7 Hochsichere Cloud: Verschlusssachen
in der Cloud „as a Service“
- 8 Datenintegration und -analyse bei
Polizei- und Sicherheitsbehörden:
Massendatenanalyse geht auch
„Made in Germany“

Künstliche Intelligenz

- 10 KI-Revolution: „Technische Systeme
werden intelligent“
- 18 Cybersicherheit im beginnenden
KI-Zeitalter: Zurück auf Los?
- 26 Erkennung KI-generierter Inhalte:
Hilfe beim Kampf gegen Deepfakes

International

- 30 Edge-Cloud-Infrastruktur 8ra:
Europas digitale Souveränität beginnt
am Netzwerkrand



4

Zertifizierungsdschungel Cloud:
Was sagen die verschiedenen Nachweise aus?

Perspektive

- 33 Sichere IT-Infrastrukturen vs. digitaler
Fortschritt? Ohne Cloud keine digitale
Souveränität

Richtlinien & Standards

- 37 Standardisierung von IPsec:
Sicherheit für das Internet von
heute und morgen

Kurz notiert

- 40 Social Days 2026:
Gemeinsam für den guten Zweck

Service

- 41 Impressum



26

Hilfe beim Kampf gegen Deepfakes:
Technologie erkennt KI-generierte Inhalte

Liebe Leserinnen und Leser,

von dieser Seite lächelt Ihnen heute ein neues, aber vielleicht auch schon etwas vertrautes Gesicht entgegen. Nach über einem Jahr als CEO bei secunet kommt immer wieder Neues auf mich zu. Zum Beispiel darf ich zum ersten Mal dieses Heft eröffnen. Und dabei kann ich auf ein bewegtes Jahr für die Cybersecurity-Branche blicken.

Bei all dem, was gerade los ist – wir beobachten einen Dreiklang aus veränderten makroökonomischen, technologischen und regulatorischen Rahmenbedingungen – hat ein Technologiethema mit Abstand die höchste Stufe auf dem Siegertreppchen der öffentlichen Aufmerksamkeit ergattert: Künstliche Intelligenz.

Wer sich heute mit dem Thema Cybersecurity auseinandersetzt, kommt um KI nicht mehr herum. Das dürfte Sie, liebe Leserinnen und Leser, wenig überraschen. Was uns alle jedoch vermutlich immer wieder überrascht, ist die Geschwindigkeit, die sich hier aufgebaut hat. KI-Agenten brechen aus Testumgebungen aus, greifen Plattformen an und schreiben Phishing-Mails. Um nur einige Beispiele zu nennen.

KI ist eine durchdringende Technologie, oder wie KI-Expertin Prof. Dr. Sabina Jeschke es beschreibt: „KI ist eine industrielle Revolution“. Im exklusiven secuvew Interview erklärt die frühere Wissenschaftlerin und Bahn-Vorständin, die heute Aufsichtsrätin und CEO des KI Park e.V. ist, wieso sie das so sieht. Zudem spricht sie über Europas verlorene technologische Führungsposition und neue Wege zu digitaler Souveränität.

Apropos Souveränität: Die Dynamik rund um KI zeigt sich nicht nur bei der Frage, wer technologisch die Nase vorn hat. Sie verändert auch das Spielfeld der Cybersecurity. KI demokratisiert die Methoden der Angreifer, stärkt aber auch die Verteidiger. Mit welchen Veränderungen müssen wir rechnen und wer hat die besseren Karten in diesem Katz-und-Maus-Spiel? secunet CTO Dr. Kai Martius teilt seine Gedanken dazu in der vorliegenden Ausgabe und erklärt, warum Secure-by-Design wichtiger wird denn je.



Marc-Julian Siewert,
CEO bei secunet

Zudem wird es darauf ankommen, Kräfte zu bündeln und gleichzeitig die Kontrolle zu behalten. Als secunet stehen wir für digitale Souveränität. Sie ist ein enorm wichtiges Ziel, insbesondere mit Blick auf die aktuelle geopolitische Situation. Aber sie darf nicht mit Autarkie verwechselt werden. Deshalb bauen wir mit starken Technologiepartnern, zu denen auch außer-europäische, global führende Akteure wie NVIDIA und Cloudflare gehören, zukunftsfähige Ökosysteme. Bei Themen wie Massendatenanalyse oder der Verschlusssachen-Cloud „as a Service“ setzten wir hingegen auf Lösungen komplett „made in Germany“. Auch um diese Themen geht es in diesem Heft – und noch um einige mehr.

Ich wünsche Ihnen viel Spaß beim Lesen!

Ihr Marc-Julian Siewert

Compliance

Zertifizierungs- dschungel Cloud

Digitale Souveränität entscheidet sich heute insbesondere in der Cloud. Unternehmen, Behörden und regulierte Organisationen wollen und müssen Cloud-Dienste nutzen, ohne die Kontrolle über ihre Daten und Prozesse zu verlieren.

Zertifizierungen können dabei helfen, aber auch verwirren. ISO 27001, ISO 27017, ISO 27018, IT-Grundschutz, C5 Typ 1 und Typ 2: Wer eine Cloud-Lösung beschaffen, auditieren oder intern freigeben muss, steht schnell vor der Frage: Was davon ist für uns relevant? Und was sagt der jeweilige Nachweis tatsächlich aus?

Ende 2025 hat die Public Cloud der secunet-Tochter SysEleven das C5-Testat Typ 2 des Bundesamts für Sicherheit in der Informationstechnik (BSI) erhalten. Im Gegensatz zum Testat Typ 1, das bestätigt, dass ein umfangreicher Katalog von Sicherheitsmechanismen zu einem bestimmten Zeitpunkt angewendet wird, betrachtet Typ 2 rückblickend über einen definierten Prüfzeitraum, ob diese Maßnahmen im laufenden Betrieb tatsächlich wirksam umgesetzt wurden. Es geht also nicht nur um den Status quo, sondern um die gelebte Praxis: Typ 1 zeigt, dass Sicherheitsmaßnahmen vorgesehen sind. Typ 2 zeigt, dass sie ihre Wirksamkeit im Betrieb bereits bewiesen haben.

Dies schafft für Organisationen mit hohen Sicherheitsanforderungen Transparenz, Vergleichbarkeit und eine belastbare Entscheidungsgrundlage. Oft sind die Testate auch Teil konkreter regulatorischer Vorgaben. Im Gesundheitswesen etwa regelt §393 SGB V den Cloud-Einsatz für die Verarbeitung von Gesundheits- und Sozialdaten, seit 1. Juli 2025 ist hier ein Typ-2-Testat vorgesehen. Doch auch öffentliche Auftraggeber, KRITIS-nahe Organisationen, Finanzunternehmen, Versicherungen und andere regulierte Branchen müssen zunehmend nachweisen, dass sie Risiken in ihrer digitalen Lieferkette beherrschen. Testate sind meist nicht die ganze Lösung, sondern ein einzelner Bestandteil eines umfangreichen Kataloges an Sicherheitsanforderungen, die Cloud-Lösungen in kritischen Kontexten erfüllen sollten.

Mehr als ein einzelnes Siegel

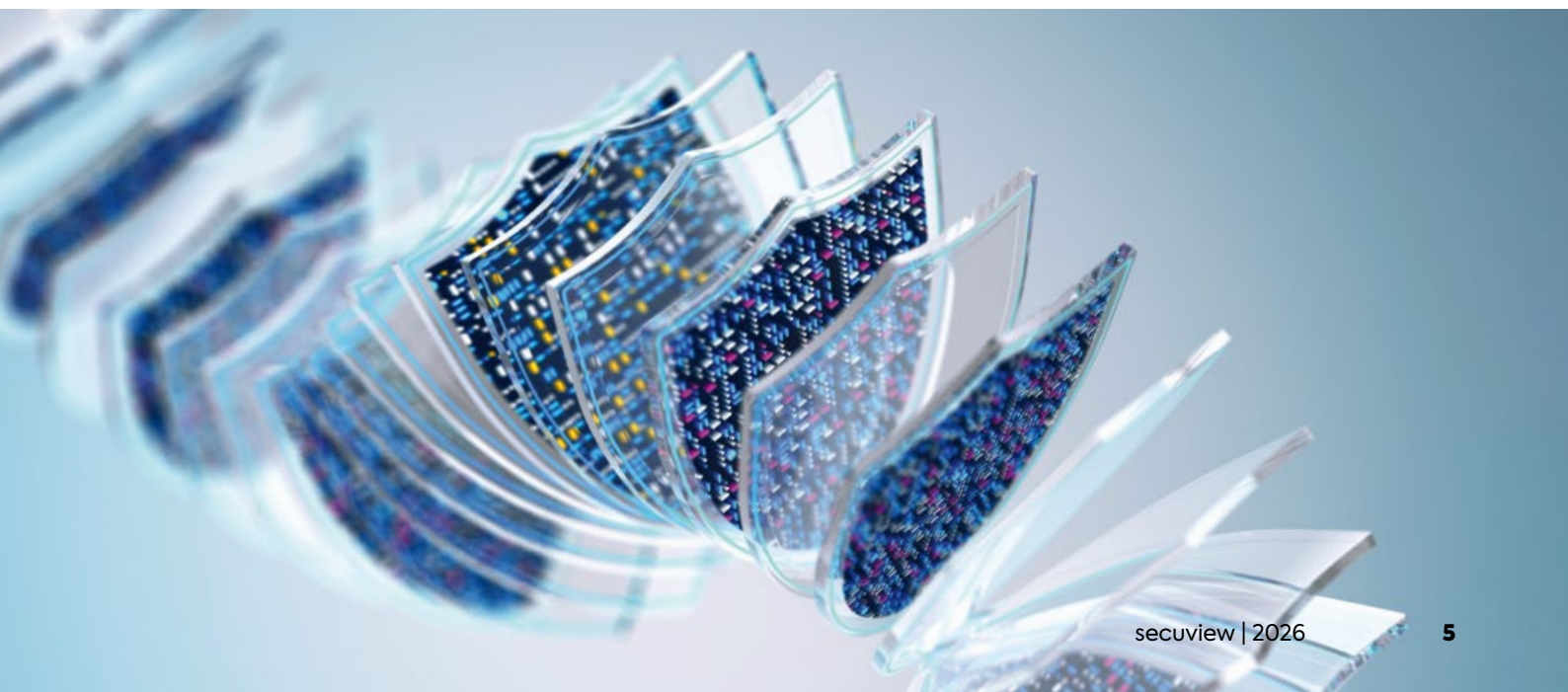
Cloud-Sicherheit lässt sich nicht einfach durch ein Anbieter-Logo auf der Website belegen. Sie entsteht durch Prozesse, Verantwortlichkeiten, technische Schutzmaßnahmen, aktuelle Nachweise und ein klares Verständnis darüber, wer in der Lieferkette wofür verantwortlich ist. Gerade im Cloud-Umfeld ist diese geteilte Verantwortung zentral: Der Anbieter stellt Infrastruktur, Plattformdienste oder Managed Services bereit, während der Kunde entscheidet, welche Daten verarbeitet werden, wie Anwendungen konfiguriert sind und welche nutzerabhängigen Sicherheitsmaßnahmen zusätzlich umgesetzt werden müssen.

Genau deshalb reicht es nicht, Zertifizierungen und Testate nur als „erfüllt“ oder „nicht erfüllt“ zu betrachten. Sie beantworten unterschiedliche Fragen. Eine ISO-27001-Zertifizierung sagt vor allem etwas darüber aus, ob ein Informationssicherheitsmanagementsystem wirksam aufgebaut und betrieben wird. Der BSI-IT-Grundschutz prüft Sicherheitsanforderungen innerhalb eines definierten Informationsverbunds sehr strukturiert anhand konkreter Bausteine. C5 wiederum richtet den Blick stärker auf die Schnittstelle zwischen Cloud-Anbieter und Cloud-Kunde und auf die tatsächliche Umsetzung im Alltag. Das BSI beschreibt C5 als Kriterienkatalog, der Mindestanforderungen an sicheres Cloud Computing spezifiziert. Gemeinsam bilden diese Nachweise Bausteine eines Sicherheits- und Compliance-Gesamtbildes. Sie helfen, Risiken sichtbar zu machen, Zuständigkeiten zu klären und Sicherheitslücken zu schließen, bevor sie zum Problem werden.

ISO 27001 & IT-Grundschutz: Managementsystem und Transparenz

Die ISO/IEC 27001 ist einer der bekanntesten Standards für Informationssicherheitsmanagementsysteme (ISMS). Sie definiert klare Anforderungen und unterstützt Organisationen dabei, Informationssicherheit systematisch aufzubauen, zu betreiben, zu überwachen und kontinuierlich zu verbessern. Die Norm betrachtet dabei nicht ein einzelnes Produkt, sondern die Struktur, über die Risiken, Vertraulichkeit, Integrität und Verfügbarkeit gesteuert werden. Das ist ein wichtiger Unterschied. Eine ISO-27001-Zertifizierung bedeutet nicht, dass jeder einzelne Dienst automatisch sicher ist. Sie bedeutet vielmehr: Eine Organisation hat ein System etabliert, um Informationssicherheitsrisiken zu identifizieren, Maßnahmen abzuleiten, Verantwortlichkeiten zu regeln und Verbesserungen anzustoßen. Für Cloud-Anbieter ist das eine wichtige Grundlage, aber eben noch nicht die ganze Antwort.

Ergänzend kommen im Cloud-Kontext häufig weitere ISO-Leitlinien ins Spiel. ISO/IEC 27017 gibt zusätzliche Leitlinien für Informationssicherheitsmaßnahmen bei der Bereitstellung und Nutzung von Cloud-Diensten sowohl für Cloud-Service-Provider als auch für Cloud-Kunden. ISO/IEC 27018 hingegen bezieht sich auf Schutzmaßnahmen für personenbezogene Daten in Public Clouds, wenn der Cloud-Anbieter als Auftragsverarbeiter handelt. Zusammen ergeben diese Standards ein starkes Fundament für Cloud-Sicherheit und Datenschutz, mit dem ISMS als organisatorischem Kern.



Der BSI-IT-Grundschutz verfolgt eine andere Logik. Auch hier spielt ein ISMS eine zentrale Rolle. Gleichzeitig geht der Grundschutz jedoch stärker in die konkrete Ausgestaltung eines definierten Informationsverbunds hinein. Dabei werden Assets, Prozesse, Systeme, Anwendungen, Räume, Netze und organisatorische Rahmenbedingungen anhand strukturierter Bausteine betrachtet. Wie auch beim ISO-Standard werden Prüfungen dabei stichprobenartig durchgeführt.

C5: Der Blick in die Praxis

Der C5-Kriterienkatalog setzt genau an dieser Stelle an. Er richtet sich an Cloud-Anbieter, -Prüfer und Cloud-Kunden und fragt ganz konkret: Welche Anforderungen muss ein Cloud-Service erfüllen, damit Kunden den Dienst sicher, transparent und nachvollziehbar nutzen können?

Damit ist ein C5-Testat in der Praxis besonders relevant für Organisationen, die Cloud-Dienste beschaffen oder gegenüber Revision, Datenschutz, Aufsicht oder Auftraggebern bewerten müssen. Es betrachtet unter anderem Themen wie Sicherheitsorganisation, Zugriffskontrolle, Kryptografie, Betriebssicherheit, Logging, Monitoring, Incident Management, physische Sicherheit, Lieferantensteuerung und Transparenzpflichten. Damit kann es den Auditaufwand deutlich verringern, weil zentrale Informationen tiefgehend geprüft wurden und strukturiert sowie nachvollziehbar vorliegen. Das bietet konkreten praktischen Mehrwert:

1. Das Testat erleichtert die Beschaffung und Lieferantenbewertung. Kunden müssen nicht bei null anfangen, sondern können auf einen strukturierten Prüfbericht zu verschiedenen Services zurückgreifen.
2. Es unterstützt interne Compliance- und Revisionsprozesse gerade für größere Organisationen, die regelmäßig nachweisen müssen, dass ihre Dienstleister angemessen gesteuert werden.
3. C5 schafft Transparenz über Verantwortlichkeiten. Das ist wichtig, weil Cloud-Sicherheit immer auch gemeinsame Verantwortung von Anbieter und Kunde ist.
4. Ein Typ-2-Testat stärkt das Vertrauen in den laufenden Betrieb. Es belegt nicht nur, dass Maßnahmen beschrieben sind, sondern dass ihre Wirksamkeit über Zeit betrachtet wurde.

Compliance ist kein Selbstzweck

Das BSI hat im April 2026 den neuen C5:2026 veröffentlicht, der den bestehenden Kriterienkatalog weiterentwickelt und an aktuelle technologische, regulatorische und sicherheitsrelevante Anforderungen angepasst hat. Das zeigt: Compliance ist ein kontinuierlicher Prozess. Sicherheitsnachweise müssen nicht einmalig erbracht, sondern regelmäßig geprüft, eingeordnet und aktualisiert werden. Aus diesem Grund sind Zertifikate, Testate und ISO-Standards kein Selbstzweck. Sie schaffen Vergleichbarkeit in einem Markt, der für viele Kunden schwer durchschaubar ist. Sie übersetzen Sicherheitsversprechen in überprüfbare Nachweise. Und sie helfen dabei, Cloud-Nutzung nicht als Black Box zu verstehen, sondern als kontrollierbare, auditierbare und souveräne Betriebsentscheidung.

Für die von SysEleven betriebene Public Cloud, die zum secunet cloud Portfolio gehört, ist das C5-Typ-2-Testat deshalb ein wichtiger Nachweis. Es zeigt, dass Sicherheit nicht nur konzipiert, sondern im laufenden Betrieb wirksam umgesetzt wurde. Für Kunden mit hohen Anforderungen an Compliance, Datenschutz und digitale Souveränität ist genau das entscheidend.



Benjamin Böhl
b.boehl@sys eleven.de



Hochsichere Cloud

Verschlusssachen in der Cloud „as a Service“

Cloud-Technologie für Verschlusssachen (VS) ohne eigenes Rechenzentrum: Mit SINA Cloud as a Service stellt secunet die erste VS-fähige Cloud als Infrastructure as a Service (IaaS) bereit.

Behörden, Verteidigung und innere Sicherheit arbeiten täglich mit Informationen, die strengen Schutzanforderungen unterliegen. Wer Verschlusssachen digital verarbeitet, muss jedoch IT-Sicherheitsprodukte mit Einsatzernlaubnis oder Zulassung verwenden, zahlreiche Standards einhalten und einen aufwändigen Freigabeprozess durchlaufen. Eine eigene VS-fähige Cloud verschärft die Lage: Hochsicherheits-Rechenzentren erfordern spezialisiertes Personal, einen Betrieb rund um die Uhr und die laufende Anpassung an neue Vorgaben.

Betrieb aus einer Hand

Hier setzt SINA Cloud as a Service an. Die Infrastruktur wird in zertifizierten Hochsicherheits-Rechenzentren von secunet in Deutschland gehostet. secunet übernimmt Betrieb, Updates und Lifecycle-Management und ist auch bei neuen Vorgaben compliant. Der Zugriff auf die Cloud erfolgt über zugelassene IT-Sicherheitsprodukte und SINA-gesicherte Endgeräte. Die Aufgabenteilung ist klar: secunet verantwortet alles vom Rechenzentrum bis zum Zugang, Kunden konzentrieren sich auf ihre Anwendungen.

SINA Cloud as a Service basiert auf IT-Sicherheitsprodukten mit Einsatzernlaubnis des Bundesamts für Sicherheit in der Informationstechnik (BSI) für Verschlusssachen auf der Stufe VS-NfD. Dies ermöglicht eine schnelle und einfache VS-Freigabe. Zudem gewährt die Lösung Vorteile durch ausgelagerten Betrieb und Skalierbarkeit. Der Betrieb ist nach IT-Grundschutz zertifiziert, ISO-27001- und DSGVO-konform. Da die IT-Sicherheit bereits im Produkt integriert ist, vereinfacht sich der Weg zur VS-Freigabe. Eine Bundesbehörde nutzt den Service bereits.

Sicherheit als Fundament

Technisch basiert SINA Cloud auf einer Architektur, die Sicherheitsfunktionen strukturell vom Cloud-Betrieb trennt. Ein Security-Layer aus Komponenten mit BSI-Einsatzernlaubnis oder Zulassung bildet das Fundament. Darüber arbeitet ein Orchestrierungslayer mit Open-Source-Technologien wie OpenStack, Kubernetes und Yaook. So lässt sich der Funktionsumfang laufend erweitern, ohne die Einsatzernlaubnis oder Zulassung zu gefährden. Kryptografische Mandantentrennung erlaubt es, Daten mehrerer Kunden strikt getrennt auf einer gemeinsamen VS-konformen Infrastruktur zu verarbeiten. Ressourcen lassen sich bei steigenden Workloads flexibel skalieren.

Typische Einsatzszenarien sind Kollaborations- und Office-Anwendungen wie beispielsweise Nextcloud, die Behörden im VS-NfD-Kontext nutzen möchten. Bei Planung und Umsetzung begleiten die Expertinnen und Experten von secunet die Kunden.

Teil von secunet cloud

SINA Cloud as a Service ist Teil von secunet cloud, der Dachmarke für die Cloud-Lösungen von secunet. Für Behörden mit eigener VS-Infrastruktur ist SINA Cloud als On-Premises-Lösung verfügbar, wodurch Verschlusssachen bis GEHEIM verarbeitet werden können.



Datenintegration und -analyse bei Polizei- und Sicherheitsbehörden

Massendaten-analyse geht auch „Made in Germany“

Die beiden IT-Unternehmen secunet und INNOSYSTEMEC haben für deutsche Polizei- und Sicherheitsbehörden den sicheren Betrieb einer leistungsfähigen Datenintegrations- und -analyseplattform auf Basis einer souveränen Cloud realisiert. Das gemeinsame Angebot SCOPE × SINA Cloud wird vollständig in Deutschland entwickelt, unterliegt dem nationalen Rechtsrahmen und erfüllt die zentralen Anforderungen von Polizei- und Sicherheitsbehörden.

Deutsche Polizeien müssen wachsende Datenmengen aus unterschiedlichen Quellsystemen schnell, rechtmäßig und sicher zusammenführen, durchsuchen und analysieren können. Gleichzeitig ist die bestehende Systemlandschaft häufig fragmentiert und nur begrenzt interoperabel. Somit steigt der Bedarf an einer Lösung, die Leistungsfähigkeit, Sicherheit und digitale Souveränität in einem Angebot zusammenführt. Mit SCOPE × SINA Cloud entstand ein zuverlässiges Werkzeug für die sichere Verarbeitung, Zusammenführung und Auswertung sensibler Daten und Informationen in Verschlusssachen-Umgebungen im täglichen Einsatz.

„Das gemeinsame Angebot von secunet und INNOSYSTEMEC ist technologisch und organisatorisch belastbar und leistungsfähig“, sagt Marc-Julian Siewert, CEO von secunet. „Und es ist ausdrücklich als nationale Lösung konzipiert: Entwicklung, Betrieb und Support erfolgen in Deutschland. Für Polizei- und Sicherheitsbehörden bedeutet dies mehr Kontrolle über Daten, Prozesse und Technologien – ganz ohne bedenkliche Abhängigkeiten.“

„secunet und INNOSYSTEMEC stärken mit dieser gemeinsamen deutschen Lösung die nationale digitale Souveränität im Sicherheitsbereich und bieten eine sofort verfügbare, cloudbasierte Datenanalyseplattform an“, sagt Stefan Günzel, CEO von INNOSYSTEMEC.



Stefan Günzel (links) und Marc-Julian Siewert



Leistungsfähig, skalierbar und datenschutzkonform

Die SINA Cloud von secunet vereint modernste Sicherheitsmechanismen mit Open-Source-Technologien wie Kubernetes und OpenStack zu einem hoch-sicheren Cloud-Stack, der für die besonderen Anforderungen der Sicherheitsbehörden On-Premises im staatlichen Rechenzentrum betrieben werden kann.

Das skalierbare Produkt SCOPE von INNOSYSTEMEC zur Integration, Analyse und Visualisierung großer Datenmengen erfüllt die zentralen Analyseanforderungen der Polizeien auf höchstem Niveau, verbessert die Verfügbarkeit polizeilicher Informationen und bleibt dank offener, modularer Architektur flexibel für künftige Anforderungen und technologische Entwicklungen.

Die Gesamtlösung SCOPE × SINA Cloud erfüllt einen zentralen operativen Bedarf der Polizeien: Informationen schneller verfügbar zu machen und für

Entscheidungen nutzbar aufzubereiten. Dabei ist die Gesamtarchitektur skalierbar angelegt, sodass die Gesamtlösung von einer potenziell unbeschränkten Anzahl von Anwendern und verschiedenen deutschen Polizeien genutzt werden kann.

Zugleich stärkt die Lösung den Datenschutz durch Technik. Die besondere Sensitivität von Analysen in sicherheitsrelevanten Umgebungen wird von Beginn an berücksichtigt. Technische Schutzmechanismen, klare Rollen- und Berechtigungskonzepte, Protokollierung sowie hohe Transparenz in der Nutzung verhindern Missbrauch wirksam und stärken somit das Vertrauen in die rechtssichere Verarbeitung sensibler Informationen.

Die Gesamtlösung SCOPE × SINA Cloud steht ab sofort bereit und kann von interessierten Polizeien unmittelbar für die sichere, leistungsfähige und digital souveräne Integration und Analyse polizeilicher Daten genutzt werden.

KI-Revolution

„Technische Systeme werden intelligent“

Sabina Jeschke verbindet Wissenschaft und Wirtschaft: Die Physikerin war Professorin an der RWTH Aachen und Vorständin der Deutschen Bahn; heute ist sie Aufsichtsrätin und CEO des KI Park e.V. Im Interview mit secuvie spricht sie über KI als industrielle Revolution, Europas verlorene technologische Führungsposition und neue Wege zu digitaler Souveränität.

Erinnern Sie sich an den Moment, in dem Ihnen klar wurde, dass KI weit mehr sein würde als ein weiteres Digitalisierungsthema?

Es war kein Moment, es waren einige Monate um 2012, während meiner Zeit als Professorin in Aachen. Zwei Ereignisse fielen fast zusammen: Das Google Car fuhr selbstständig durch eine amerikanische Kleinstadt, IBM Watson gewann Jeopardy. Bis dahin hatte KI im Labor gelebt – Deep Blue spielte Schach, feste Regeln, vollständige Information, keine Überraschungen. Und plötzlich fährt ein Fahrzeug durch eine ganz normale Kleinstadt, in der jederzeit ein Kind auf die Straße springen kann.

Das war der Kipppunkt: Technische Intelligenzen können sich in der Komplexität des menschlichen Alltags bewegen. Verkürzt man die erste industrielle Revolution auf ein Wort, dann wäre das „Dampfmaschine“. Verkürzt man die vierte auf ein Wort, wäre das „KI“. Und ausformuliert lautet der Satz: Technische Systeme werden intelligent. Das ist keine weitere Stufe der Digitalisierung, sondern eine andere Kategorie.

Im öffentlichen Diskurs wird KI auf Chatbots und Produktivitätsgewinne reduziert. Wo sehen Sie die größten Missverständnisse?

Viele sind bei dem Bild stehen geblieben, das 2022 entstanden ist. Ich unterscheide drei Phasen. Phase eins, 2022/23: kleine, konkrete Fragen. Übersetz mir diesen Text. Mal mir ein Bild im Stil von van Gogh, aber ohne Sonnenblume. Im Grunde eine bessere Suchmaschine.

Phase zwei, ab 2024: KI als Mitarbeiter – oder zumindest als Teil eines Mitarbeiters. „Hier sind die Interviewfragen, mach mir einen Antwortentwurf, du kennst mich ja.“ Genau das hätte ich als Vorständin früher meinem Assistenten gegeben.

Phase drei, heute: KI als Betriebssystem. Der Vergleich dafür kommt aus Ihrer Welt. Mein Rechner ist nicht deshalb sicher, weil ich kontrolliere, ob der Virens Scanner läuft, sondern weil im Hintergrund permanent Prozesse mitlaufen, die das System selbst überwachen. Sie arbeiten mit Mustererkennung: Wenn nachts um drei ungewöhnliche Datenbankzugriffe stattfinden, wenn Sende- und Empfangsvorgänge aus dem gewohnten Rahmen fallen, schlagen Anomaliedetektoren an – und dann greift das System ein, bevor ich überhaupt etwas bemerke.

In dieselbe Richtung entwickelt sich KI: ein System, das mitläuft, in meine Mailbox schaut und sagt: „Du hast um elf ein Gespräch, du bist nicht vorbereitet, hier ist bereits ein Entwurf.“ Wer heute über Produktivitätsgewinne beim Textschreiben diskutiert, diskutiert noch Phase eins.

Welche drei Fragen sollte sich ein mittelständisches Unternehmen stellen, bevor es KI flächendeckend einführt?

Erstens: Was ist unsere KI-Gesamtstrategie? Ich erlebe überall Leuchttürme – hier wird etwas ausprobiert, dort etwas aufgesetzt. Das ist gut, aber es ersetzt keine Antwort darauf, wo wir in drei bis fünf Jahren stehen wollen. Stattdessen wird diskutiert, ob ChatGPT gerade besser ist als Claude oder umgekehrt und ob die chinesischen Modelle inzwischen aufgeholt haben. Solche Diskussionen greifen viel zu kurz.

Zweitens: Wie verändert sich das Geschäftsmodell entlang des Kernprodukts? Nicht in HR, nicht im Support – im Kern. Wenn ich heute Autos baue: Baue ich in fünf Jahren immer noch Autos? Oder verkaufe ich gar keine Fahrzeuge mehr, sondern betreibe Flotten und verkaufe garantierte Verfügbarkeit von Mobilität, weil die Wertschöpfung dann in Disposition, Daten und Vorhersage liegt und nicht mehr im Blech? Ich habe Möglichkeiten, die ich vorher nicht hatte, und Wettbewerber, die es vorher nicht gab.

Drittens: Wie entsteht Kompetenz in der Organisation? Nicht dadurch, dass die Geschäftsführung 42 Schulungsmodule einkauft, sondern dadurch, dass die Mitarbeitenden selbst akzeptieren, dass sie sich

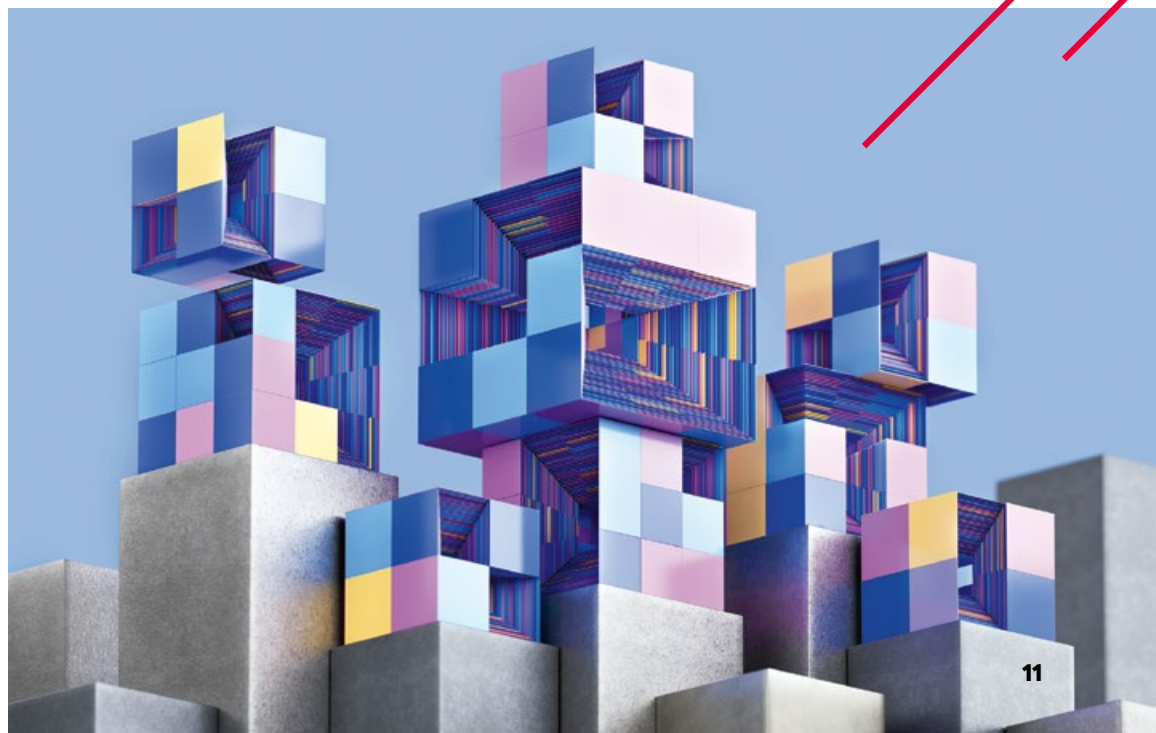
weiterentwickeln müssen. Man kann sich nicht in den Bus setzen und darauf warten, dass der einen zur Kompetenz fährt. Man muss sein Fahrrad herausholen, die Kette ölen und den Berg selbst hochfahren.

Und es braucht jemanden, der den Hut aufhat – nicht zwingend unter der Bezeichnung Chief AI Officer, aber in dieser Rolle: auf Vorstandsebene oder unmittelbar darunter, mit dem Mandat, die verstreuten Initiativen über die Gesamtorganisation hinweg zu bündeln. Das ist dieselbe Debatte, die wir vor einigen Jahren über den Chief Digital Officer geführt haben. Was hat man denn geglaubt, wie es sonst gehen soll – dass die Dinge von allein konvergieren, obwohl niemand sie zusammenführt?

Es entstehen viele Pilotprojekte, aber vergleichsweise wenige Anwendungen gehen in den produktiven Betrieb. Woran scheitert der Übergang?

An zwei Punkten, und der zweite liegt tiefer. Erstens entstehen frühe KI-Projekte oft aus einem kleinen verschworenen Team heraus, einem gallischen Dorf. Sie stärken das Selbstbewusstsein der Organisation. Aber es sind Inseln, denen Brücken und Fährverbindungen fehlen. Sie setzen auf Technologien, die zwei Jahre später keine Rolle mehr spielen, lassen sich nicht in die Gesamtarchitektur integrieren und sterben irgendwann – auch wenn sie fachlich gut waren.

Zweitens, und das wird kaum diskutiert: Die Generationszeit von KI beträgt sechs Monate. (Nur zum Vergleich: Beim Verbrennerauto sind es sechs Jahre). Wenn wir heute sagen, wenige KI-Anwendungen schafften es in den Betrieb, schauen



„Vertrauen entsteht durch das Experiment, einen anderen Weg gibt es nicht.“

Prof. Dr. Sabina Jeschke,
Aufsichtsrätin und CEO des KI Park e.V.

wir auf etwas, das vor zwei Jahren konzipiert und vor einem Jahr evaluiert wurde – sonst könnten wir es gar nicht beurteilen. Wir beurteilen also eine KI, die im Kindergarten war, während die heutige Abitur macht.

Compliance und Governance sind übrigens nicht das Problem des Übergangs, sie sind der Showstopper davor. Jedem Pilotprojekt, das überhaupt existiert, muss man beinahe gratulieren: Entweder wurde die Compliance ausgedribbelt – oder sie wurde schlicht nicht gefragt.

KI-Agenten bereiten Entscheidungen zunehmend vor oder treffen sie mit. Wo verläuft die Grenze zwischen Assistenz und Delegation?

Das ist keine harte Grenze, sie verschiebt sich mit der Leistungsfähigkeit der Systeme. Stellen Sie einem LLM dieselbe substanzielle Frage heute und vor drei Jahren: Die Halluzinationsquote ist massiv gefallen. Vor drei Jahren war das eher ein Brainstorming – „mal sehen, was ChatGPT dazu sagt“. Heute delegiere ich das Anschreiben an einen Geschäftspartner vollständig. Themenabhängig bleibt es unterschiedlich: Wo mache ich Urlaub in Thailand, und buch mir das Hotel gleich mit – das kann ich abgeben. Soll ich meinen Job kündigen – da delegiere ich nicht.

Mein Vater war Techniker und besetzte im Kernkraftwerksbau die Position eines Ingenieurs. Als die ersten Taschenrechner erschwinglich wurden, saß er mit dem Rechenschieber daneben und rechnete nach, weil er dem Gerät nicht glaubte. Zwei Jahre lang musste der Taschenrechner beweisen, dass er rechnen

kann. Dann wurde aus Assistenz Delegation. Heute würde niemand ein Ingenieurbüro beauftragen, das die Statik eines Hauses mit Stift und Papier rechnet statt mit soliden numerischen Verfahren.

Im Grunde ist die Frage falsch gestellt. Aber sie ist gut, weil man an ihr sieht, wo die Grenzen des eigenen Denkens liegen, sobald man akzeptiert, dass man es mit einer nicht-biologischen, aber intelligenten Entität zu tun hat.

Vertrauen gilt als zentraler Erfolgsfaktor für KI. Wodurch entsteht es?

Vertrauen entsteht durch das Experiment; einen anderen Weg gibt es nicht. Die Technikgeschichte kennt viele Beispiele dafür, die Eisenbahn ist eines: Im 19. Jahrhundert wurde ernsthaft medizinisch darüber gestritten, ob der menschliche Organismus diese Geschwindigkeiten und Erschütterungen überhaupt verträgt: Es gab eine ausgewachsene Debatte über die sogenannte Eisenbahnkrankheit, und der Chirurg John Eric Erichsen beschrieb in den 1860er-Jahren mit dem railway spine ein Nervenleiden, das er auf das Reisen mit der Bahn zurückführte. Widerlegt wurden diese Sorgen nicht durch Gutachten, sondern dadurch, dass man mit der Bahn fuhr.

Und hätten wir das Automobil vor hundert Jahren so reguliert, wie wir heute KI regulieren, hätten wir vorher wissen müssen, dass es Führerschein, Verkehrszeichen, Sicherheitsgurt und Airbag braucht. Damals wusste niemand, was ein Airbag ist. Offensichtlich funktioniert es doch so: Man führt eine Technologie ein,

obwohl man ihr nicht vollständig traut, gewinnt Vertrauen, weil sie im eigenen Gebrauch funktioniert – und stellt dort ein Verkehrsschild auf, wo sie es nicht tut. Man reguliert nach, an den Stellen, an denen die Risiken tatsächlich auftreten.

Deepfakes, synthetische Identitäten, automatisiertes Social Engineering: Welche Folgen hat der Vertrauensverlust in digitale Informationen?

Fälschung und Manipulation sind nichts Neues, und die gesellschaftliche Antwort darauf kam historisch fast immer nachlaufend. Der Buchdruck machte religiöse Texte, politische Pamphlete und Bibelübersetzungen plötzlich massenhaft vervielfältigbar. Fürsten, Reformatoren und Kirchen nutzten das neue Medium, um ihre jeweilige Lesart zu verbreiten; die Gegenreaktion bestand in Druckprivilegien, Zensur und Verboten. Beim Internet war die Befürchtung ähnlich: In Wikipedia könne jeder seinen Unsinn hineinschreiben. Das kann grundsätzlich tatsächlich passieren – nur ist es dann potenziell tagesaktueller und ebenso schnell korrigierbarer Unsinn. In der letzten gedruckten Brockhaus-Ausgabe konnte dagegen noch nicht stehen, was Deep Learning in seiner heutigen Bedeutung ist. Diese Enzyklopädien waren in Sorgfalt und redaktioneller Qualität kaum zu überbieten. Sie konnten aber immer nur den Wissensstand ihres Redaktionsschlusses abbilden.



Hier hat generative KI die Rolle künstlicher Intelligenz als persönlicher Assistent bildlich dargestellt.

Jede neue Medientechnologie zerstört damit zunächst einen Teil der bisherigen Vertrauensordnung. Wenn Herkunft, Autorität und Echtheit nicht mehr selbstverständlich erkennbar sind, müssen neue Verfahren entstehen, die Seriosität anders begründen: durch nachvollziehbare Quellen, institutionelle

Verantwortung, redaktionelle Kontrolle oder – in der Wissenschaft – durch Peer Review. Solche Mechanismen entstehen jedoch fast immer erst, nachdem das neue Medium die alten Gewissheiten bereits erschüttert hat.

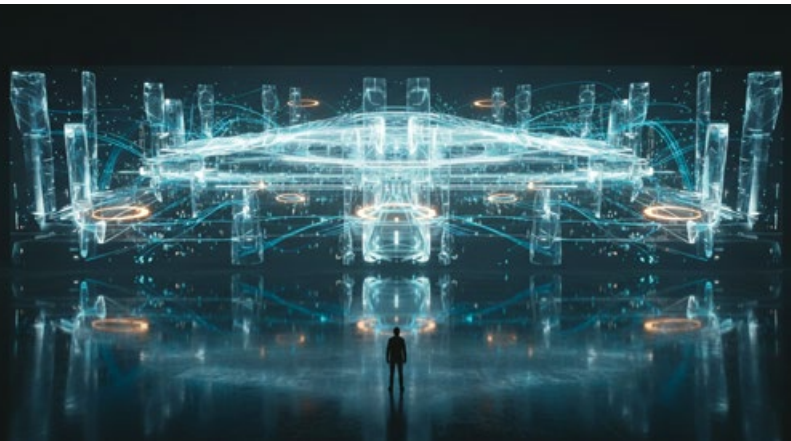
Die These, wir könnten Deepfakes so regulieren, dass sie nicht mehr passieren, halte ich keine Sekunde für plausibel. Was hilft, ist Urteilskompetenz. Noch nie hatte ein so großer Anteil der Bevölkerung über so viele Jahre Zugang zu Schule, beruflicher Qualifikation, Hochschulbildung und frei verfügbarem Wissen. Wir sind die bestgebildete Gesellschaft, die es je gab. Und wir lassen Sechzehnjährige wählen. Dann müssen wir uns auch zutrauen, dass Menschen Plausibles von Unplausiblem trennen. Die Schule muss die Gesellschaft anbieten; lernen muss ich selbst.

Ist der europäische AI Act eher ein Innovationshemmnis oder die Voraussetzung dafür, dass KI langfristig Akzeptanz findet?

Ein regulatorischer Rahmen ist sinnvoll. Der AI Act in dieser Form ist es nicht.

Sein konzeptionelles Fundament wurde im April 2021 gelegt. Ende 2022 erschien ChatGPT; Anfang 2023 wurde sichtbar, dass generative KI nicht nur eine weitere Anwendung, sondern ein technologischer Paradigmenwechsel war. Trotzdem wurde im Dezember 2023 ein Regelwerk politisch beschlossen, dessen Grundarchitektur aus der Welt vor ChatGPT stammte. Generative KI ließ sich nun nur noch nachträglich in diese Architektur einbauen. Genau darin zeigt sich das Problem: Ein Gesetzgebungsverfahren, das fast drei Jahre benötigt, kann eine Technologie mit Entwicklungszyklen von wenigen Monaten nicht angemessen erfassen. Richtig wäre gewesen zu sagen: Gute Idee, wichtige Vorarbeit – aber die technologische Grundlage hat sich verändert, also setzen wir neu an. Verloren hätte man wenig. Die Beteiligten waren klug und eingearbeitet, das Netzwerk stand, und die richtigen Fragen waren gestellt.

Bei dieser hohen Dynamik der KI ist ein Risiko, das ich heute identifiziere, morgen vielleicht keines mehr – und das entscheidende sehe ich heute noch gar nicht. Man sollte sich außerdem fragen, warum die technologisch führenden Regionen der Welt überwiegend darauf verzichten, der gesamten Technologie vorab ein umfassendes horizontales Regelwerk überzustülpen. Die Antwort ist: Wer so vorgeht, sitzt nicht im Driver's Seat. Und wer nicht im Driver's Seat sitzt, bestimmt die Richtung nicht.



Fragt man KI im Jahr 2026, wie sie sich die Kommunikation mit Menschen vorstellt, erhält man ein Bild wie dieses. Künftig könnten realistische virtuelle Räume genutzt werden, um Arbeitsergebnisse einer KI zu beurteilen.

Umgekehrt wäre es richtig: erst die technologische Führung zurückgewinnen, dann den Rahmen schrittweise entwickeln – wie beim Automobil, mit klarem Ziel, am liebsten null Verkehrstote. Aber nicht vorher so tun, als wüsste man, wo die Risiken liegen.

Wenn Regulierung nicht der Weg zu technologischer Souveränität ist – was dann?

Dass unsere Daten in die USA fließen – oder nach China, da kann man inzwischen wählen –, liegt allein daran, dass wir uns diesen Technologien nicht rechtzeitig geöffnet und deshalb keine eigenen, souveränen Lösungen aufgebaut haben, auf die wir heute zurückgreifen könnten. Das ist natürlich eine Rückschaubetrachtung auf vergossene Milch, die sich nicht mehr zurück in die Flasche bringen lässt. Umso schneller müssen wir auf den Vordersitz, statt weiter wie ein Wackeldackel auf der Hutablage mitzufahren.

Und es gibt eine neue Chance, etwas kontraintuitiv: die offenen chinesischen Modelle. Mich erinnert das gerade ein bisschen an den alten „Linux gegen Windows“ Streit – und natürlich steht auch bei den offenen Modellen ein Geschäftsmodell dahinter: Wer Qwen nimmt, soll die Alibaba Cloud nehmen – und hat dann sein Problem statt in den USA in China. Aber ich muss das nicht tun. So, wie ich früher meine eigene Linux-Distribution betreiben konnte, ohne Suse oder Red Hat zu kaufen, kann ich diese Modelle wirklich lokal hosten, entkoppelt von der Infrastruktur des Anbieters. Das ist ein Stück weit Insourcing: wieder mit eigenen Leuten, dafür vollständig in der Kontrolle.

Ich diskutiere das gerade mit einer der großen deutschen Universitäten für deren Verwaltung. Da geht es nicht um echtzeitfähige Prozesse wie etwa in einer Bank, sondern um Personalverwaltung, Einschreibungen, Prüfungsverfahren, saubere Belege. Wenn das offene Modell bei solchen Anwendungen der absoluten technologischen Spitze einige Wochen oder Monate hinterherläuft, ist das völlig unerheblich – dafür habe ich volle Autonomie.

Was DeepSeek im Januar 2025 vorgeführt hat, ist im Übrigen kein Voodoo, sondern schlicht eine hervorragende ingenieurstechische Leistung, zu der man den Chinesen nur gratulieren kann – erbracht mit einem Bruchteil des Geldes, der Trainingszeit und der Entwicklungszeit, die für die großen amerikanischen Modelle aufgewendet wurden. Und genau das ist der Punkt: Diese Leistung hängt nicht an gigantischen Finanzinvestments und nicht daran, dass ein Konzern wie Microsoft oder Amazon dahintersteht. Ein gut ausgestattetes Forscherteam in Deutschland oder Europa hätte das ebenso leisten können.

KI verändert auch die digitale Bedrohungslandschaft. Welche Entwicklungen beobachten Sie besonders aufmerksam?

Ich sehe drei Schichten. Die klassische Kriegsebene: intelligente Drohnen, autonome Systeme. Darunter die hybride Kriegsführung: Desinformation, Cyberoperationen, Beeinflussung.

Und dann die individuelle Ebene, der bislang viel zu wenig Gewicht beigemessen wird. In der Cybersecurity gibt es dafür den Begriff *harvest now, decrypt later*. Daten werden heute abgegriffen und gespeichert, obwohl sie verschlüsselt und damit im Moment wertlos sind – in der Erwartung, dass leistungsfähige Quantenrechner sie in zehn oder fünfzehn Jahren entschlüsseln können. Das verändert die Zeitachse von Angreifbarkeit grundlegend.

Denken Sie das zu Ende. Jemand ist heute politisch, wirtschaftlich und gesellschaftlich völlig unbedeutend und hinterlässt Spuren, für die sich niemand interessiert. Zwei Jahrzehnte später steht dieselbe Person an der Spitze eines Unternehmens, einer Behörde oder einer Partei – und plötzlich ist Material verwertbar, das zum Zeitpunkt seiner Entstehung als sicher galt. Im besten der schlechten Fälle erkennt die betroffene Person die Gefahr und zieht sich aus ihrer Position zurück. Im schlechtesten bleibt sie – und wird erpressbar. Dann ist nicht mehr sie das eigentliche Ziel, sondern die Institution, für die sie steht.

Das halte ich für die gefährlichste Entwicklung in diesem Feld, gerade weil sie erst mit großer Verzögerung sichtbar wird und deshalb heute niemanden alarmiert. Und genau deshalb sollte jetzt niemand auf die Idee kommen, Quantum Computing regulieren zu wollen. Das Ergebnis wäre, dass wir die Technologie auch nicht verstehen – und diejenigen, die es gegen uns einsetzen, sehr wohl.

Umgekehrt eröffnet KI neue Möglichkeiten für die Cyberabwehr. Wo liegt das größte Potenzial?

KI verschiebt die Abwehr zeitlich nach vorn. In der ältesten Logik erkannte man den Angriff erst, als die Bombe einschlug. Der nächste Entwicklungsschritt bestand darin, die Flugbahn eines Geschosses zu erkennen und es noch in der Luft abzufangen – der Iron Dome zeigt dieses Prinzip eindrucksvoll. Künftig geht es darum, noch früher anzusetzen: etwa ungewöhnliche Beschaffungsmuster bei Chemikalien, Bauteilen oder anderen Dual-Use-Gütern zu erkennen, bevor daraus überhaupt eine konkrete Waffe oder ein Anschlagplan entsteht. Voraussetzung dafür sind technologische Führungsfähigkeit und Datenfusion – in Kürze, das Geschäftsmodell von Palantir.

Der Attentäter vom Berliner Weihnachtsmarkt 2016 war den Behörden bereits bekannt; das Problem war weniger das völlige Fehlen von Informationen als ihre

Bewertung, Zusammenführung und konsequente Nutzung. KI hätte aus verstreuten Kontakten, Bewegungen und Warnhinweisen womöglich früher ein Gesamtbild erzeugen können – bevor Amri einen LKW kaperte und ihn als Waffe gegen den Weihnachtsmarkt einsetzte.

Der Preis ist eine stärkere Beobachtung des Individuums. Ich bin Halbschwedin. In Schweden bekommt man bei der Geburt eine Personnummer, die einen das ganze Leben begleitet – Handyvertrag, Kindergarten, Zahnarzt; sie ist beinahe wichtiger als der Name. Fragen Sie dagegen Deutsche, ob Schweden ein Land sei, das seine Bürger stark überwacht, dann ernten Sie Kopfschütteln: „Schweden? Das ist doch Bullerbü.“ Genau so denken wir hier über dieses Land – Astrid Lindgren, rote Holzhäuser, Mittsommer. Eine freundliche Verklärung, die mit der tatsächlichen Datenlage des schwedischen Staates wenig zu tun hat. Die Zuschreibung ist also eine völlig andere, obwohl die Beobachtungstiefe dort erheblich größer ist als bei uns. Jeder Schritt der Menschheitsentwicklung hat zu mehr Transparenz geführt und im Großen und Ganzen mehr genutzt als geschadet. Mir ist trotzdem klar, dass solche Modelle kippen können.

Und ganz nüchtern: Die Menschen in Deutschland vertrauen ihrem Staat gerade nicht grenzenlos. Wenn Sie eine europäische Palantir-Alternative bauen, die

„Umso schneller müssen wir auf den Vordersitz, statt weiter wie ein Wackeldackel auf der Hutablage mitzufahren.“

Prof. Dr. Sabina Jeschke,
Aufsichtsrätin und CEO des KI Park e.V.

„Wir werden künftig in hybriden Teams aus Menschen und technischen Intelligenzen arbeiten.“

Prof. Dr. Sabina Jeschke,
Aufsichtsrätin und CEO des KI Park e.V.

technologisch mithält – hervorragend, und lassen Sie sich davon nicht abschrecken.¹ Trotzdem wird ein erheblicher Teil der deutschen Wählerschaft fragen, wie viel Transparenz er dem eigenen Staat zugestehen will. Und das ist im Kern keine technische Frage, sondern eine Vertrauensfrage: Wie viel Vertrauen bringe ich einer Institution entgegen, die Daten über mich zusammenführt, und worauf gründet dieses Vertrauen? Solange es fehlt, hilft auch die beste europäische Lösung nicht. Diese Frage wird neu ausgehandelt werden müssen – und sie ist von der Souveränitätsfrage strikt zu trennen. Das sind zwei Paar Schuhe.

Welche Formen der Zusammenarbeit von Mensch und KI halten Sie langfristig für erfolgversprechend – und auf welche menschlichen Fähigkeiten kommt es an?

Wir werden diese Systeme weiter in Richtung Menschenähnlichkeit entwickeln, weil wir Intelligenz nur aus unserer eigenen, menschlichen Perspektive entwerfen können. Ein System gezielt in Richtung einer „Marsmenschintelligenz“ zu entwickeln, ist uns gar nicht möglich, weil wir nicht wissen, wie eine solche Intelligenz beschaffen wäre. Bei humanoiden Robotern kommt reiner Pragmatismus hinzu: Ich will, dass er meine Küche aufräumt, also gebe ich ihm Hände mit fünf Fingern und ungefähr menschliche Proportionen – sonst muss ich andere Griffe an die Schränke schrauben.

Wir werden künftig in hybriden Teams aus Menschen und technischen Intelligenzen arbeiten. Das kennen wir längst, bisher nur biologisch: Der Drogenfahnder und sein Hund bilden ein hybrides Team über

Artengrenzen hinweg, ebenso der Blinde mit seinem Blindenhund. Neu ist, dass das Trüffelschwein jetzt robotisch sein kann – dann braucht es nachts keine Pause und riecht womöglich besser. Die Menschenähnlichkeit der Intelligenz ist dabei ein Erfolgsfaktor: Damit kann ich schneller und sicherer kommunizieren als mit einem System, dessen Intelligenz mir nicht zugänglich ist.

Bei den menschlichen Fähigkeiten in Ihrer Frage wäre ich außerdem vorsichtig mit zeitlich-stabilen Antworten. Jede solche Antwort unterstellt, dass der Differenzvektor zwischen menschlichem und technischem Können bleibt. Vor einigen Jahren hieß es: Macht etwas mit sozialen Skills, die Betreuung von Menschen durch Menschen bleibt uns. Heute empfinden es sehr viele Menschen als ausgesprochen angenehm, sich einem Berater oder Therapeuten anzuvertrauen, der eine künstliche Intelligenz ist – weil sie ihm Dinge sagen, die sie einem Menschen gegenüber nicht aussprechen würden.

Was wird derzeit überschätzt, was unterschätzt?

Überschätzt wird der Blick auf die Modelle selbst. Sie können das genialste LLM haben – wenn Sie kein High-Performance Computing (HPC) haben, auf dem es gerechnet wird, hilft die Verbesserung des Algorithmus überhaupt nichts. Und wenn Sie ein hoch echtzeitfähiges Problem haben, aber kein 5G, kein 6G und keine redundante Schicht über Satellitenkommunikation, nützt es Ihnen nicht, dass der Algorithmus es theoretisch hätte lösen können. Unterschätzt werden deshalb erstens Rechenleistung – HPC und perspektivisch Quantum – und zweitens Konnektivität samt Satelliten und Redundanzen.

¹ secunet bietet gemeinsam mit dem Partner INNOSYTEC die sichere und souveräne Datenintegrations- und Analyseplattform SCOPE x SINA Cloud an.

Und drittens, am stärksten unterschätzt: virtuelle Welten und Simulationstechniken. Seit der Meta-verse-Hype abgeklungen ist, steht das Thema kaum noch im öffentlichen Rampenlicht – obwohl in Forschung und Industrie intensiv daran weitergearbeitet wird. Dabei stellt sich eine sehr praktische Frage: Wenn ich eine KI bitte, eine Sicherheitsplanung für den Flughafen Berlin bei doppeltem Passagieraufkommen zu machen – wie beurteile ich eigentlich die Antwort? Dafür brauche ich virtuelle Räume, die ich gemeinsam mit der KI begehen kann. Virtuelle Welten sind das Kommunikationsinterface zwischen technischer und biologischer Intelligenz.

Und dieses Interview – ist es mit künstlicher Intelligenz entstanden?

Selbstverständlich. Ausgangspunkt war ein strukturiertes Interview, das mit mir geführt und anschließend transkribiert wurde. Auf dieser Grundlage habe ich den Text mit Unterstützung mehrerer KI-Systeme entwickelt: recherchiert, strukturiert, verdichtet, sprachlich geschärft, auf Widersprüche geprüft und mehrfach redigiert. Die Gedanken, Thesen und Bewertungen sind meine. KI war dabei weder Ghostwriter noch Orakel, sondern ein außerordentlich leistungsfähiges Arbeitsinstrument. Ich schulde den Lesern nicht den umständlichsten Entstehungsprozess, sondern den bestmöglichen Text. Dabei auf die besten verfügbaren Werkzeuge zu verzichten – das hielte ich eher für eine Beleidigung ihrer Zeit und ihrer Intelligenz.

Dass Politiker seit Jahrzehnten Reden vortragen, die von Referenten und Assistenten vorbereitet wurden, wurde stets akzeptiert. Sobald eine künstliche Intelligenz beteiligt ist, wird daraus plötzlich eine Debatte über die Reinheit der Autorschaft. Das ist weniger Sorge um die Autorschaft als eine Abwehrreaktion auf die vierte narzisstische Kränkung: Nun sind nicht einmal Denken und Sprache noch ausschließlich menschliches Hoheitsgebiet. Entscheidend ist nicht, ob ein Text mit Stift, Textverarbeitung, menschlicher Unterstützung oder künstlicher Intelligenz entstanden ist. Entscheidend ist, wer ihn verantwortet. Für diesen Text gilt deshalb ganz einfach: Ich stehe mit meinem Namen dafür ein – für jeden Gedanken, jede Aussage und jeden Satz.



Prof. Dr. Sabina Jeschke,
Aufsichtsrätin und CEO des KI Park e.V.

Cybersicherheit im beginnenden KI-Zeitalter

Zurück auf Los?

Ein Kommentar von Dr. Kai Martius, CTO von secunet

Bei secunet sind wir, und auch ich ganz persönlich, seit jeher überzeugte Verfechter von „Secure-by-Design“-Systemarchitekturen. Was mich dabei immer wieder beschäftigt und antreibt, ist die Tatsache, dass wir theoretisch seit etwa 50 Jahren wissen, wie man sichere Computersysteme baut: kleine, robuste und überprüfbare Komponenten, Hardware-Roots-of-Trust, Integritätsmechanismen mit Attestierung, starke Isolation, Unumgebarkeit von Sicherheitsrichtlinien und vieles mehr. Und dennoch zwingen Budgets, Time-to-Market, Benutzerfreundlichkeit, Effizienz, wie auch immer man es nennen möchte, die IT-Branche jeden Tag zu Kompromissen im Systemdesign.

Wie also können wir es besser machen? Die allgemeine Cybersicherheitslage verbessert sich jedenfalls nicht spürbar. Zugegeben: Im Vergleich zum PC-Ökosystem der frühen 2000er Jahre sehen wir Fortschritte (wobei dieses damals deutlich schlechter war als die Mainframe-Ära davor). Hyperscaler haben massiv in Plattform-Sicherheit

investiert, weil ihr Geschäftsmodell davon abhängt. Mobile Plattformen skalieren beeindruckend, ohne dass wir flächendeckend katastrophale Angriffe erleben. Microsoft hat mit „Virtualization Based Security“ (VBS) und Hyper-V mehr strukturelle Sicherheit in den Windows-Kernel gebracht. Und trotzdem leben wir weiterhin im Paradigma des „Assume Breach“: Wir gehen vorsichtshalber davon aus, dass Angreifer bereits in die Infrastruktur eingedrungen sind. Wir patchen, so gut wir können. Wir erleben spektakuläre Fehlschläge wie das CrowdStrike-Update, verlorene Schlüssel und eine stetig steigende Zahl von Schwachstellen. Unsere Architekturen leiden unter sehr grundlegenden Problemen, wie etwa den Eigenschaften der Von-Neumann-Architektur, in der Daten und Code nicht unterschieden werden, so dass der Großteil der Angriffsszenarien überhaupt erst möglich wird. Oder den immer komplexeren Software-Stacks, deren Abhängigkeiten kaum noch jemand überblickt. Und von solchen Problemen gibt es noch etliche mehr.

Dr. Kai Martius,
CTO von secunet



Die heutige Debatte hat sich zudem teilweise in Richtung Souveränität und Abhängigkeiten verschoben. Diese sind nicht per se ein Sicherheitsproblem, beides existiert vielmehr unabhängig voneinander. Doch Vertrauenswürdigkeit ist der gemeinsame Nenner von Sicherheit und Souveränität. Eben hier versagen viele Plattformen zunehmend, sowohl die Infrastruktur der Hyperscaler als auch SaaS-Angebote von ServiceNow bis Salesforce. Und das nicht nur aus technischen, sondern auch aus politischen Gründen: Der CLOUD Act ist hier ein naheliegendes Beispiel. Deshalb sind wir weiterhin überzeugt, dass stärkere Sicherheitsarchitekturen nötig sind – sowohl für einzelne Produkte als auch für ganze IT-Systeme. Dafür treiben wir drei zentrale Prinzipien voran:

1. Open Source und offene Standards

Dieser Punkt ist entscheidend, um Vertrauen aufzubauen. Er ermöglicht Einblicke in die Sicherheitsmechanismen und fördert ein breites, widerstandsfähiges Ökosystem.

2. Ein Secure Software Development Lifecycle (SSDLC)

Reproduzierbare Prozesse, rigorose Tests, CVE-Management sowie Transparenz bei SBoM (Software Bill of Materials) und CBoM (Cryptographic Bill of Materials) sind das Schmiermittel, um Entwicklungs- und Zertifizierungszyklen zu verkürzen. Sie ersetzen keine sichere Produktarchitektur, verschieben den Fokus aber von manuellen Tests und Dokumentation hin zu prozessintegrierten Nachweisen. Gleichzeitig müssen Produkte im Feld einfach und dennoch vertrauenswürdig patchbar sein.

3. Formale Verifikation

Wir gehen noch einen Schritt weiter mit unserer komponentenbasierten Architektur, die formale Verifikation ermöglicht. Das ist ein neues Niveau von Secure-by-Design, bedeutet derzeit aber auch enormen Implementierungs- und Zertifizierungsaufwand. Das Konzept geht weit über DevSecOps (Development, Security and Operations) hinaus. Gleichzeitig ist der Ansatz bereits darauf vorbereitet, KI zur Unterstützung bei der Erzeugung formaler Beweise einzusetzen.

Was hat KI mit alledem zu tun?

Zunächst einmal: Die Fortschritte bei Modellfähigkeiten, generativer KI und der daraus entstehenden Innovationsspirale – sprich Automatisierung – sind beeindruckend. Ihre nächste Evolutionsstufe heißt Agentic AI. Im Grunde haben wir das Wissen der Welt angesammelt und daraus ein System geschaffen, das sich ständig selbst mit neuem Input versorgt. Marc Andreessen formulierte es so:

„AI transfers sand into thoughts“, also KI macht aus Sand Gedanken.

Ob das philosophisch oder ethisch tatsächlich Gedanken sind, möchte ich hier offenlassen. Technisch betrachtet haben wir jedoch ein ultimatives kybernetisches System geschaffen, das wie eine Art unendliche Rückkopplungsschleife wirkt. Als Computerprogramm betrachtet, verändert sich grundlegend, wie Programm und Daten miteinander verschmelzen: Daten werden zu Programmcode. Nicht durch einen erfolgreichen Hack oder eine ausgenutzte Schwachstelle, sondern systemisch. Und weil diese Daten – also der Programmcode – probabilistisch erzeugt werden, wird dieser stochastisch.

Das ist ein völlig neues Paradigma, oder? Es gibt keine statische Anwendung mehr, die gegen ein Sicherheitsmodell geprüft werden kann. Es gibt keine Programmiersprache mehr, weder das alte, unsichere C noch das modernere, sicherere Rust. Also gibt es keine Sicherheit mehr ... Moment.

Das geht – für den Moment – zu weit. Wir sollten einen Schritt zurücktreten und vorn anfangen: Schauen wir, wo wir beim Einsatz von KI – für gute wie schlechte Zwecke – in der Cybersicherheit stehen.

Automatisiertes Hacking

Bis letztes Jahr (2025) brauchte man noch ein erfahrenes Team von Hackern, die wussten, wo sie mit der Suche nach Schwachstellen beginnen mussten. Social Engineering war häufig der erste Schritt, über Phishing Schadsoftware einzuschleusen. Port-scans machten offen erreichbare Dienste sichtbar. System-Fingerprints verrieten ungepatchte Softwarestände. Und dann begann die Reise durch den Datenschlingel mit dem Ziel, unbemerkte Hintertüren zu installieren, Daten und Infrastruktur zu sabotieren oder Lösegeld zu erpressen. Werkzeugkästen und sogar „gemietete Hacker“ existieren als Teil organisierter Kriminalität bereits seit Langem.

Dafür nutzen sie größtenteils bereits bekannte Schwachstellen aus. Doch glücklicherweise für die Angreifer, und unglücklicherweise für alle anderen, gibt es davon im Feld unzählige, weil Patch-Management in produktiven Umgebungen oft schwierig zu organisieren ist. Dazu gehören Systemtests, Ausfallplanung und vieles mehr. Wir werden vermutlich einen massiven Anstieg automatisierter Angriffe auf ungepatchte Systeme erleben. Und wir werden auf die harte Tour lernen, dass die Qualität der Software, die unsere Branche heute produziert, kein Fundament ist, auf dem wir weiterbauen sollten. Wir fordern deshalb seit jeher, auf Secure-by-Design zu setzen statt auf eine Kultur aus „Assume Breach“ und ständigem Patchen. Man möchte fast sagen: Wir haben es euch ja gesagt.

„Wir werden vermutlich einen massiven Anstieg automatisierter Angriffe auf ungepatchte Systeme erleben.“

Dann der Paradigmenwechsel: Im Jahr 2025 wurde generative KI leistungsfähig genug, um diese Fähigkeiten zu demokratisieren. Es ist unklar, wie wirksam Sicherheitsbarrieren verhindern können, dass LLMs entsprechendes Wissen preisgeben. Schließlich wurden diese Modelle mit genau diesem Wissen trainiert, gespeist aus wissenschaftlichen Arbeiten, CVE-Datenbanken und anderen öffentlichen Quellen. Mit den richtigen Prompts und ausreichend Feedback können AI Agents heute nahezu autonom in verwundbare Systeme eindringen, ohne dass dafür hochqualifizierte Hacker nötig wären.

KI-gestützte Schwachstellenanalyse

Hier beginnt gerade etwas wirklich Interessantes. Denn es gibt Schwachstellen, die ganz bewusst geheim gehalten werden. Angriffsvektoren werden auf dem Schwarzmarkt gehandelt, von Staaten für Cyberoperationen genutzt, von Herstellern zurückgehalten, weil noch kein Patch existiert, oder schlichtweg ignoriert. Hinzu kommen die „Unknown Unknowns“, also Schwachstellen, die bisher tatsächlich noch niemand entdeckt hat. Das sind alles offene Türen, die im Verborgenen existieren und derzeit nicht geschlossen werden können, weil es noch keine Lösung gibt.

Einerseits bin ich kein Freund von „Security by Obscurity“, deshalb geben wir uns im Security Engineering größte Mühe: mehrere Verteidigungslinien, Minimierung der Angriffsfläche und sogar der Einsatz formaler Methoden zum Nachweis der Korrektheit. Außerdem waren die Waffen im Wettlauf von der Erkennung bis zur Behebung, insbesondere in Bezug auf die „Unknown Unknowns“, mit denen wir seit jeher leben, bislang ziemlich gleich verteilt. Bis jetzt.

Im März und April 2026 sahen wir erstmals Modelle, die offenbar außergewöhnlich gut darin sind, neue Schwachstellen zu finden und direkt passende Exploits zu schreiben. Anthropic bewirbt beispielsweise ein Modell namens „Mythos“, hielt es aber gleichzeitig zurück, um die Welt „nicht zu gefährden.“ Das wirft Fragen auf: Handelt es sich um einen echten Sprung in den Modellfähigkeiten oder nur um Marketing? Entwertet sich Wissen gegenüber dem Besitz der leistungsfähigsten Modelle? Müssen die

„Guten“ künftig im Dunkeln tappen? Die Realität liegt vermutlich irgendwo dazwischen. Schon heute sind frei verfügbare Open-Weight-Modelle bemerkenswert leistungsfähig. Einige sind besser im Finden von Schwachstellen, andere besser im Schreiben von Exploits. Der Punkt ist: Auch ohne „Mythos“ liegen bereits extrem mächtige Werkzeuge auf dem Tisch.

Optimistisch betrachtet kann das zu deutlich besserer Software führen, weil solche Systeme (auch automatisiert) in QA-Prozesse integriert werden können. Pessimistisch betrachtet existiert draußen jedoch eine gewaltige Menge schlechter Software, und das auch in kritischen Systemen. Genau deshalb könnten diese Fähigkeiten ebenso zu verheerenden Angriffen führen. Vor diesem Hintergrund halte ich den beschriebenen Umgang von Anthropic für nachvollziehbar verantwortungsvoll. Zugleich sollten die „Guten“ unverzüglich damit beginnen, diese Techniken einzusetzen, um die Softwarequalität zu verbessern und das Patchen so einfach wie möglich zu machen.

All dies bestätigt in meinen Augen, dass Secure-by-Design unerlässlich ist, um Angriffsflächen zu minimieren und den Schaden im Falle ausnutzbarer Schwachstellen zu begrenzen. Es untermauert unsere drei oben dargelegten Grundprinzipien.

In diesem Zusammenhang noch eine Anmerkung zu Open Source Software (OSS): Die Gegner von OSS werden sich in ihren Argumenten durchaus bestätigt sehen: Jetzt kann jeder blitzschnell Schwachstellen in der frei verfügbaren OSS finden, und das macht OSS von Grund auf weniger sicher. Ist das so? Das Gegenargument bleibt ebenfalls wahr: Wir müssten darauf warten, dass Unternehmen (die vielleicht gar nicht mehr existieren) sich darum kümmern, dass fähige Modelle veröffentlicht werden oder jemand einfach genug Geld bezahlen kann, um Zugang zu Funktionen zu erhalten, welche die eigenen Produkte sicher machen. Das entspricht nicht unserem Verständnis von Souveränität.

Agentische KI

Aus Sicht eines Angreifers stellt agentische KI lediglich eine weitere Stufe der Automatisierung und Demokratisierung von Hacking-Fähigkeiten dar, da sie noch weniger Interaktion durch geschultes Personal erfordert. Das Wissen und die Fähigkeiten liegen in den KI-Modellen. Im Hinblick auf die Angriffsfähigkeiten ist dies eine evolutionäre Entwicklung. Die eigentliche Revolution ist mit den Modellfähigkeiten bereits da.



Aus Sicht der Entwickler befinden wir uns jedoch wahrscheinlich inmitten einer Revolution. Die Codegenerierung ist schneller denn je. Vibe-Coding – bei dem die KI allein auf Basis eines Prompts selbstständig Code entwickelt – gibt es bereits, allerdings noch mit einer enormen Fehlerquote. Es wird also zunächst einmal spannend sein zu sehen, ob wir durch die Kombination von Codegenerierung und Fehlertests in einer automatisierten Pipeline zeitnah UND schnell fehlerfreien Code erhalten. Da sind viele offene Fragen: Wer erhält (zu welchen Kosten) Zugang zu den leistungsfähigsten Modellen? Welche Hardware-Ressourcen werden benötigt, und wie effizient lassen sich diese Code-Analysefunktionen in automatisierte Pipelines integrieren? Welche Art von Fehlern wird die KI selbst verursachen, also neue „Unknown Unknowns“? Woran lässt sich hier die Vertrauenswürdigkeit messen, wenn wir sowohl die Codegenerierung als auch die Sicherheitstests an Agenten delegieren?

Geht man noch einen Schritt weiter, wird die Programmlogik zu einer verborgenen Ebene in einer agentenbasierten KI, die von einem Agenten im Laufe der Aufgabenbewältigung spontan als stochastisches, vergängliches Artefakt generiert wird. Wie kann dieser vergängliche Code sicher und vertrauenswürdig sein? Was IST in diesem Zusammenhang wirklich sicher und vertrauenswürdig? Und schließlich: Braucht es noch all unsere Kernkompetenzen einer sicheren Softwareentwicklung, eines sicheren Lebenszyklus, von Open Source, Sicherheitsbewertung ...? Viele wichtige Fragen. Versuchen wir, einen strukturierten Blick darauf zu werfen, was sich in den Tiefen der Software verändert und was gleich bleibt ...

Anders, aber doch gleich?

Das neue KI-Paradigma wird wahrscheinlich zunächst für die Geschäftslogik gelten. Diese ist eigentlich der einzige Grund, warum Computer existieren: Sie müssen reale Probleme lösen, alles andere sind unterstützende Funktionen dafür.

Diese unterstützenden Funktionen sind jedoch unverzichtbar. Es geht um die Infrastruktur zur Kommunikation, Speicherung und Verarbeitung von Daten, also Netzwerk, Datenspeicher und Rechenleistung. Und daran ändert sich auch mit agentischer KI nichts. Auf der unteren Ebene haben wir nach wie vor schnelle Prozessoren und Coprozessoren, große SSDs und superschnelle Netzwerke. Für jede Aufgabe werden Daten generiert, übertragen, verarbeitet und gespeichert. Das Volumen steigt, die Geschwindigkeit ebenso. Und wir haben im letzten Jahrzehnt mit der Cloud-Technologie eine stark skalierbare Infrastrukturschicht aufgebaut. Nicht unbedingt bewusst als Voraussetzung für agentische KI, aber heute wird sie genau dadurch ermöglicht.

Diese Infrastrukturen sind sowohl in funktionaler als auch in sicherheitstechnischer Hinsicht unverzichtbar. Die Cloud-Ebene spielt eine zentrale Rolle bei der Durchsetzung grundlegender Sicherheitsrichtlinien: Sie verhindert unbefugten Datenzugriff durch Isolation (Virtualisierung, Container, virtuelle Netzwerkebenen). Das alles ist über mehrfach verschachtelte Steuerungsebenen darauf ausgelegt, die Dynamik des Cloud Computing zu ermöglichen. Agentische KI bildet eine weitere Automatisierungsebene darüber, nutzt jedoch diese bestehende Infrastruktur.

Was bedeutet das nun? Zuerst: Die Integrität der Infrastruktur ist von größter Bedeutung. Wir brauchen mehr denn je eine funktionierende, robuste und sichere Infrastruktur. Dabei geht es nicht um KI, sondern um klassische Computersicherheit. KI kann dazu beitragen, diese zu erhöhen, Fehler aufzuspüren und sogar zu verhindern. Unsere Grundprinzipien für sicheres Software-Design sind hier unverzichtbar und essentiell. Erst recht, wenn es um sensible oder geheime Informationen geht, wird es umso wichtiger sein, ein gewisses Maß an Souveränität über die Infrastrukturen und deren Vertrauenswürdigkeit für Akteure und Daten zu gewährleisten.

Auf der Infrastrukturebene verfügt secunet über diese Fähigkeiten bereits. Wir haben eine Grundlage aus hardwarebasierten Trennungsfunktionen für Speicher und Netzwerk geschaffen. Wir verfügen über Betriebssysteme wie den Muen-Separation Kernel¹ und einen Rust-basierten Hypervisor wie Cloud-HV. Darüber hinaus bieten wir Open-Source-Stacks zur Verwaltung offener Modelle und deren Nutzung (MLOps) in unserer Cloud an. Somit können wir bereits eine, wenn auch noch recht grobmaschige, „Hülle“ um die Agenten herum bereitstellen, um sie unter Kontrolle zu halten.

Diese Hülle ist jedoch zu statisch, um das volle Potenzial der agentischen KI auszuschöpfen. Ausgehend von einer geschlossenen Umgebung benötigen wir kontrollierte Verbindungen nach draußen, also in einen öffentlichen oder externen Raum von Agenten und Daten. Und damit einhergehend viel mehr Dynamik bei der Definition und Konfiguration von Sicherheitsrichtlinien rund um und zwischen Gruppen von Agenten. Zero-Trust-Konzepte scheinen sich hier grundsätzlich gut anwenden zu lassen. Ich habe bislang jedoch in keinem bestehenden Produkt einen Automatisierungsgrad bei der übergreifenden horizontalen und vertikalen Richtlinienverwaltung und -steuerung gesehen, der in der Lage wäre, eine ganze Flotte von Agenten zu steuern.

Das führt zu der Frage, ob und wie agentische KI unser Konzept von Sicherheit grundlegend verändern wird.

Welche fundamentalen Veränderungen stehen an?

Große Sprachmodelle (LLMs) werden bei der Codegenerierung immer leistungsfähiger. Derzeit werden sie vor allem von menschlichen Programmierern genutzt, um die Effizienz in der herkömmlichen Softwareentwicklung zu steigern und, hoffentlich, die Qualität zu verbessern. Was Sicherheitslücken angeht, könnte die Qualität deutlich steigen, wenn KI-basierte Analysefunktionen in die Entwicklungspipelines integriert werden.

Aber warum sollte ein menschlicher Programmierer die Kundenanforderungen weiterhin in einen Prompt zur Codegenerierung übersetzen? Das könnte der Kunde doch eigentlich auch selbst tun. Und selbst die Aufforderung, Code zu schreiben, kann von einem Agenten gegeben werden, der wiederum von einem anderen Agenten gestartet wird, um letztlich eine Benutzeraufgabe zu erfüllen. Wir werden

¹ <https://muen.sk/>

„Aber warum sollte ein menschlicher Programmierer die Kundenanforderungen in einen Prompt zur Codegenerierung übersetzen? Das könnte der Kunde auch selbst tun, oder ein Agent, der von einem anderen Agenten gestartet wird.“

also wahrscheinlich viel weniger Anwendungsprogrammierung im herkömmlichen Sinne sehen, dafür aber viel mehr Aufgabenbeschreibungen durch Endnutzer, die wiederum von LLMs in kurzlebigen Code umgesetzt werden.

Und was ist dann mit der Sicherheit? Werden Sicherheitslücken im Code überhaupt noch ein Problem sein? Möglicherweise sind sie das bald nicht mehr, entweder durch die Integration von Schwachstellenprüfungen direkt in die Programmierfähigkeiten des Agenten oder aufgrund der kurzen Lebensdauer des eigentlichen Programms (oder beides). Andererseits haben wir gelernt, dass die Codegenerierung bei der Verwendung von LLMs ein stochastischer Prozess ist. Wir können die Korrektheit nicht standardmäßig garantieren (genauso wenig wie bei menschlichen Programmierern). Deshalb wurden formale Methoden entwickelt, um nachweisen zu können, dass ein Programmierer eine bestimmte Anforderung formal korrekt umgesetzt hat. Diese Methoden lassen sich heutzutage jedoch nicht über sehr kleine Softwarekomponenten hinaus skalieren. Das ist übrigens auch der Grund, warum wir eine komponentenbasierte Architektur entwickeln. Es gibt jedenfalls Anzeichen

dafür, dass formale Methoden mit den Fähigkeiten von LLMs viel besser skalieren. Es scheint, als könnten wir mit ihnen nicht nur den Code selbst generieren, sondern sie sogar dazu bringen, formale Beweise für die Erfüllung von Anforderungen zu erstellen. Das allein wäre schon eine wirklich gute Nachricht für „Secure-by-Design“-Software, und das weit über automatisierte Schwachstellenprüfungen hinaus!

Aber: Das eigentliche Problem verlagert sich nur. Schon heute besteht die größte Herausforderung darin, die Anforderungen der Nutzer zu verstehen und sie in Code zu übersetzen. Denn hier passiert die Magie: Wenn man es richtig macht, wenn man gar die aktuellen und zukünftigen Wünsche einer breiten Nutzergemeinschaft vorhersagen kann, wird das Produkt ein großer Erfolg. Es wird jedoch noch schwieriger, wenn „Sicherheit“ zu diesen Anforderungen hinzukommt. Was bedeutet „sicher“ für den Nutzer, für den Betreiber, für Daten, die von irgendwoher stammen? Was ist nur eine kontextbezogene Richtlinie, was ist eine konkrete Sicherheitsfunktion? Das ist der wirklich schwierige Teil des Security Engineering und der Schlüssel zur Entwicklung wirklich sicherer Produkte.

Ich glaube, wir können von einem Nutzer, selbst in einer agentischen Welt, nicht erwarten, dass er seine Sicherheitsanforderungen so korrekt und umfassend formuliert, dass dies immer zum richtigen Ergebnis führt. Sicherheit ist dynamisch und vielschichtig und bildet sich auf Funktionen und Richtlinien auf verschiedenen Ebenen des Tech-Stacks ab. Tatsächlich gilt dies bereits für die heutige Funktionsweise von IT-Systemen: von den Kundenanforderungen über die Anwendungen bis hin zur Infrastruktur, auf der diese Anwendungen laufen. Der Unterschied ist: Heute ist

das System viel statischer. Wenn Agenten hingegen „Schreibzugriff auf die reale Welt“ haben und durchdrehen, ist es vorbei (abhängig davon, wie gut die vorhandenen Sicherheitsvorkehrungen halten).

Im Kern ändern sich also die Fähigkeiten, die Geschwindigkeit, die Benutzererfahrung, aber auch das Schadenspotenzial dramatisch. Die grundlegenden Probleme und ihre Lösungsmöglichkeiten ändern sich jedoch kaum. Sie verlagern sich lediglich auf eine andere Ebene.



Wie geht es nun weiter?

1. Die Sicherheit der Infrastruktur bleibt von größter Bedeutung.

Sie bildet die grundlegende Ebene, ist eher statisch und zum Teil physisch. Agentische KI wird hier kein Game Changer sein, aber wir müssen KI-Fähigkeiten nutzen, um die Infrastruktur noch sicherer zu machen und unsere bestehenden Methoden zu optimieren: Erkennung und Prävention von Schwachstellen, Korrektheit und Integrität, formale Methoden. Und natürlich die integrierte, „klassische“ Datensicherheit: Vertraulichkeit, Authentizität, Integrität und Resilienz.

2. Die Begrenzung des Aktionsbereichs eines Agenten bleibt ein sinnvoller Ausgangspunkt.

Es geht darum, den „Explosionsradius“, also das Ausmaß des Schadens, falls etwas schiefgeht, möglichst gering zu halten. Auch dafür verfügen wir über die Bausteine: Virtualisierung, Modularisierung und Trennung von Sicherheitsfunktionen, gute Credential-Vaults, kurzlebige Zugriffstoken usw. Die Herausforderung besteht darin, diese Ebene mit einem übergeordneten Richtlinienmanagement zu verknüpfen, da Agenten viel dynamischer kommen und gehen.

3. Datensicherheit wird noch wichtiger.

Alle Daten für agentische Arbeit müssen so detailliert gekennzeichnet und gesichert werden, wie es die spätere Zugriffskontrolle erfordert, sei es auf Dateisystemebene, in Buckets eines Cloud-Speichers oder in einer Datenbank. Zugriffskontrollschichten gibt es bereits. Das gilt auch für Daten, also Wissen in einem selbsttrainierten oder RAG-basierten LLM. Öffentliche Daten müssen dagegen nicht auf dieselbe Weise im Sinne einer Zugriffskontrolle gesichert werden. Vielmehr braucht es definierte Gateways zu diesen Datenquellen, um das Durchsickern sensibler Daten zu verhindern. Entscheidend ist hier die Zugriffskontrollschicht. Da Datenquellen sehr vielfältig sind und sich die Verwaltung von Anmeldedaten sowie technischer Zugriff, etwa APIs oder Datei-Handles stark unterscheiden, könnte es sinnvoll sein, dies unter eine andere Art von API zu stellen. Zumindest gilt: Dieser „Policy Enforcement Point“ ist entscheidend, um Datensicherheit auch bei nicht vertrauenswürdigen Agenten zu gewährleisten. Deshalb sollte man sich gerade hier an unsere Grundprinzipien halten, um ihn sicher und korrekt zu implementieren. Das Gleiche gilt für das Datengateway zur öffentlichen Welt.

4. Richtlinienverwaltung wird wahrscheinlich der schwierigste Teil.

Sie reicht von der Nutzerabsicht über die Zugriffsrichtlinien der Dateneigentümer bis hin zu beliebigen Regeln auf verschiedenen Ebenen des Stacks, mit unterschiedlichen Sprachen, Credential-Systemen und technischen Abstraktionen. Bausteine sind vorhanden, wenn auch in unterschiedlicher Qualität. Die kombinatorische Komplexität scheint jedoch enorm zu werden. Vielleicht kann KI auch hier helfen.

5. Sicherheit und Vertrauenswürdigkeit der Agenten sowie der KI selbst werden zentral.

Letztendlich brauchen wir von vornherein vertrauenswürdige und fehlerfreie Agenten, da die Komplexität sonst nicht bewältigt werden kann. Lässt sich dies auch mit formalen Methoden erreichen? Ideen dazu gibt es bereits.

6. Aber was heißt „vertrauenswürdige“ KI?

Derzeit laufen zahlreiche Initiativen zur Entwicklung souveräner Basismodelle in Europa und anderswo, die auf bekannten und „sauberen“ Daten beruhen. Auch im Kontext Anti-Bias-Forschung und Ähnlichem passiert viel. Uns fehlen jedoch nach wie vor Maßstäbe, um Open-Weight-Modelle im Feld, also in der Praxis, im Hinblick auf „vertrauenswürdige Verhalten“ zu verstehen und zu bewerten. Ehrlich gesagt habe ich ein Problem mit einer eindeutigen Definition von „Vertrauenswürdigkeit“ für KI-Modelle, da diese probabilistischer Natur sind. Okay, vielleicht beginnen wir einfach mit einer Definition von Vertrauenswürdigkeit für Trainingsdaten.

Insgesamt scheint es einerseits ein langer Weg und eine große Herausforderung zu sein, ein System zu entwerfen und aufzubauen, das eine sichere und leistungsfähige Plattform für agentische KI bietet. Andererseits wirkt genau das vielversprechend, weil ein solches System bislang niemand wirklich hat. Und ist das nicht die Art von Herausforderung, die ein Cybersecurity-Unternehmen reizen sollte? Wir bei secunet nehmen sie jedenfalls gern an.

Erkennung KI-generierter Inhalte

Hilfe beim Kampf gegen Deepfakes

Lange Zeit galt die Manipulation von Bildern oder Videos als aufwendig und vergleichsweise leicht nachvollziehbar. Heute stehen leistungsfähige KI-Werkzeuge nahezu jedem zur Verfügung.

Deepfakes können Gesichter austauschen, Stimmen imitieren oder vollständig synthetische Szenen erzeugen, deren künstlicher Ursprung für menschliche Betrachter kaum noch erkennbar ist. Hier kommen digitale Erkennungssysteme ins Spiel. Eine Detektionslösung, die secunet gemeinsam mit der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) entwickelt hat, bietet den Deepfake-Generatoren die Stirn.

Gefälschte Videoanrufe vermeintlicher Vorgesetzter, manipulierte Aufnahmen politischer Persönlichkeiten oder KI-generierte Dokumente verdeutlichen, dass Deepfakes längst keine theoretische Bedrohung mehr sind. Sie sind Bestandteil der digitalen Realität geworden. Und das Vertrauen in die Echtheit digitaler Informationen schwindet. Diese Entwicklung ist insbesondere aus sozialen Netzwerken und dem öffentlichen Diskurs bekannt. Doch auch Behörden, Unternehmen und Betreiber kritischer Infrastrukturen treffen täglich Entscheidungen auf Grundlage digitaler Informationen. Ermittlungsbehörden werten Bilder und Videos aus, Unternehmen und Politik schützen sich vor Identitätsbetrug und Desinformationskampagnen, Plattformbetreiber und Journalisten müssen manipulierte Inhalte erkennen und einordnen.

Mit jeder Verbesserung generativer KI wächst deshalb die Bedeutung einer grundlegenden Frage: Ist ein digitaler Inhalt authentisch oder künstlich erzeugt? Deepfake-Detection-Systeme können dabei helfen, diese Frage zu beantworten.

Digitale Authentizität wird zur kritischen Sicherheitsfrage

Die zunehmende Verbreitung synthetischer Medien verändert den Stellenwert digitaler Authentizität grundlegend. Dass Inhalte plausibel erscheinen, reicht nicht länger aus. Ihre Echtheit muss technisch überprüfbar werden. Für Sicherheitsbehörden gewinnt diese Entwicklung besondere Relevanz. Bilder und Videos dienen regelmäßig als Beweismittel in Ermittlungsverfahren. Gleichzeitig entstehen neue Kriminalitätsformen. Synthetische Stimmen ermöglichen Varianten des sogenannten „CEO-Frauds“ oder des „Enkeltricks“, während manipulierte Bilder und



KI analysiert Bilder oder Videos realer Personen und kann dann auf dieser Basis vollständig synthetische Szenen erzeugen.

Dokumente Ermittlungen erschweren, falsche Spuren erzeugen oder die Authentizität echter Beweismittel infrage stellen.

Besonders deutlich zeigt sich diese Entwicklung im Bereich KI-generierter Darstellungen sexuellen Missbrauchs von Kindern. Internationale Ermittlungen belegen, dass vollständig synthetische Inhalte inzwischen arbeitsteilig erstellt, verbreitet und kommerzialisiert werden. Für Ermittlungsbehörden bedeutet dies nicht nur erheblich größere Datenmengen, sondern auch die Herausforderung, authentisches Material von künstlich erzeugten Inhalten zuverlässig unterscheiden zu können. Dadurch steigt die Belastung der Ermittlerinnen und Ermittler, die solche potenziell traumatisierenden

Inhalte sichten müssen. Automatisierte Assistenzsysteme können dazu beitragen, große Datenbestände vorzustrukturieren und menschliche Expertise gezielt dort einzusetzen, wo sie tatsächlich erforderlich ist.

Und auch außerhalb der Strafverfolgung wächst der Bedarf. Unternehmen sehen sich mit Identitätsdiebstahl, Reputationsangriffen oder manipulierten Kommunikationsinhalten konfrontiert. Für Medienhäuser stellt sich die Frage nach der Verifizierung journalistischer Quellen. Plattformbetreiber wiederum müssen Transparenz schaffen, ohne legitime Inhalte unnötig einzuschränken. Digitale Authentizität entwickelt sich damit zunehmend zu einer Grundvoraussetzung für vertrauenswürdige digitale Prozesse.

„Neben forensischen Analyseverfahren gewinnen Verfahren zur Herkunftssicherung digitaler Inhalte an Bedeutung.“

Ein Wettrennen zwischen Erzeugung und Erkennung

Als Ergebnis dieser rasanten Entwicklung hat sich ein technologisches Wettrennen zwischen Deepfake-Generatoren und Detektionsverfahren etabliert. Jede neue Generation leistungsfähiger Modelle verbessert die Qualität synthetischer Inhalte und stellt bestehende Erkennungsverfahren vor neue Herausforderungen. Viele heute verfügbare Detektoren basieren derweil auf einem vergleichsweise einfachen Prinzip. Sie werden mit Inhalten trainiert, die von bekannten KI-Modellen erzeugt wurden, und lernen, charakteristische Muster, sogenannte „Artefakte“ dieser Generatoren zu erkennen. Solange dieselben Modelle verwendet werden, liefern solche Verfahren häufig gute Ergebnisse. Erscheinen jedoch neue Generatoren oder verändern bestehende Modelle ihre internen Strukturen, verlieren diese Erkennungsmerkmale schnell an Aussagekraft.

Gerade diese eingeschränkte Generalisierbarkeit gehört zu den größten Herausforderungen moderner Deepfake-Erkennung. In der Praxis müssen Behörden oder Unternehmen Inhalte bewerten, deren Ursprung zunächst unbekannt ist. Deshalb verfolgen Forschung und Standardisierung zunehmend hybride Ansätze. Neben forensischen Analyseverfahren gewinnen Verfahren zur Herkunftssicherung digitaler Inhalte an Bedeutung. Kryptografische Signaturen sowie manipulationssichere Herkunftsnachweise können künftig zusätzliche Informationen darüber liefern, wann und wie digitale Inhalte entstanden sind. Deepfake-Erkennung ist ein zentraler Baustein davon.

Deepfake-Erkennung braucht mehr als ein Erkennungsverfahren

Vor diesem Hintergrund hat secunet gemeinsam mit der Friedrich-Alexander-Universität Erlangen-Nürnberg (FAU) ein Deepfake-Detection-System entwickelt, das auf eine möglichst hohe Generalisierbarkeit ausgelegt ist. Gefördert wurde das Projekt von SPRIND – Bundesagentur für Sprunginnovationen. Im Mittelpunkt steht die Fähigkeit, KI-generierte Bilder auch dann zu identifizieren, wenn der zugrunde liegende Generator während der Entwicklung des Systems nicht bekannt war.

Die Lösung kombiniert dazu mehrere komplementäre Erkennungsverfahren innerhalb einer mehrstufigen Architektur. Anstatt ausschließlich charakteristische Artefakte einzelner Generatoren auszuwerten, berücksichtigt die Zero Shot Detection nur allgemeine Merkmale echter Bilddaten. Dadurch bleibt die Erkennung auch dann belastbar, wenn neue Modelle oder bislang unbekannte Fälschungsmethoden auftreten. Ergänzend kann sich das System durch eine Few-Shot-Komponente auf der Grundlage von weniger als 100 geeigneten Beispielbildern an neue Manipulationsmuster oder spezifische Einsatzszenarien anpassen. Dadurch können Organisationen auf veränderte Bedrohungslagen reagieren, ohne spezialisiertes Personal einsetzen zu müssen und ohne umfangreiche neue Trainingsdatensätze aufzubauen. Dieser Ansatz verbindet wissenschaftliche Forschung mit den Anforderungen sicherheitskritischer Einsatzumgebungen, in denen neue Angriffsmethoden häufig schneller entstehen als umfassende Referenzdatensätze.

Wichtig dabei ist, dass die eigentliche Entscheidung über die Authentizität eines Inhalts stets beim Menschen verbleibt. Das Deepfake Detection System versteht sich als Assistenzsystem. Es unterstützt Fachanwenderinnen und Fachanwender bei der automatisierten Voranalyse großer Datenbestände, priorisiert auffällige Inhalte und stellt zusätzliche Kontextinformationen bereit, die eine fundierte Bewertung erleichtern. Kriminalistische oder forensische Expertise wird dadurch nicht ersetzt, sondern gezielt unterstützt.

Flexible Integration in bestehende Sicherheitsarchitekturen

Technische Leistungsfähigkeit allein genügt in hochregulierten Umgebungen jedoch nicht. Neue Lösungen müssen sich in bestehende Prozesse integrieren lassen und regulatorische Anforderungen erfüllen, um in sicherheitskritischen Umgebungen laufen zu können. Das secunet Deepfake Detection System wurde deshalb als Cloud-native Lösung entwickelt und kann sowohl als Cloud-Service als auch vollständig On-Premises betrieben werden. Die Integration in bestehende digitale Infrastrukturen ermöglicht den Einsatz sowohl für die automatisierte Analyse großer Bildbestände als auch in besonders geschützten Betriebsumgebungen mit hohen Anforderungen an Datenschutz und Informationssicherheit.

Für Organisationen mit sensiblen Datenbeständen besteht darüber hinaus die Möglichkeit, das System direkt innerhalb der eigenen Infrastruktur auf spezifische Anwendungsfälle zu optimieren. Sämtliche Trainings- und Bilddaten verbleiben dabei vollständig

unter der Kontrolle der jeweiligen Organisation. Die Datenhoheit bleibt jederzeit erhalten. Gleichzeitig sind Anforderungen aus Datenschutz, Informationssicherheit und dem europäischen KI-Regulierungsrahmen integriert und von Anfang an mitgedacht.

Vertrauen braucht überprüfbare Technologien und einen transparenten Rahmen

Gemeinsam mit Behörden und weiteren Bedarfsträgern arbeitet secunet daran, das Deepfake Detection System im Rahmen von Pilotierungs- und Evaluierungsprojekten unter realen Einsatzbedingungen weiterzuentwickeln. Dazu zählen unter anderem gemeinsame Projekte mit der Polizei.

Entscheidend wird sein, technische Innovation, regulatorische Anforderungen und praktische Einsatzfähigkeit miteinander zu verbinden. Dazu gehören leistungsfähige Erkennungsverfahren ebenso wie transparente Prozesse, nachvollziehbare Herkunftsnachweise und sichere Infrastrukturen. Denn die Frage, ob Inhalte echt oder manipuliert sind, hat sich in den letzten Jahren von einer Einzelfallentscheidung zu einer dauerhaften Aufgabe moderner Sicherheitsarchitekturen entwickelt.

Parallel zur technologischen Entwicklung entstehen deshalb neue regulatorische Rahmenbedingungen, die Transparenz schaffen. So setzt der EU AI Act einen rechtlichen Rahmen, in dem KI-basierte Anwendungen entwickelt werden können. Dennoch wird es weiterhin Inhalte geben, die sich nicht an die Vorschriften halten. Genau da setzt die Deepfake Detection an.



Edge-Cloud-Infrastruktur 8ra

Europas digitale Souveränität beginnt am Netzwerkrand

Von Torsten Redlich, Global Head of Edge Unit bei secunet

Wird die Frage nach digitaler Souveränität in Europa gestellt, richtet sich der Blick zunächst oft auf das Rechenzentrum.

Genauso wichtig ist es aber, dorthin zu schauen, wo Daten entstehen, wo Maschinen, Anlagen und

Sensoren in Echtzeit reagieren und kritische

Prozesse auch dann weiterlaufen müssen,

wenn Gefährdungslagen auftreten oder

zentrale Ressourcen ausfallen. Genau des-

halb rückt der Netzwerkrand, die Edge,

strategisch immer mehr in den Mittelpunkt. Mit der 8ra-Initiative (gesprochen „Oora“)

arbeitet Europa an dem Aufbau einer offenen, interoperablen und souveränen digitalen

Infrastruktur für den gesamten Kontinent. Mehr als 120 Partner aus zwölf EU-Mitglied-

staaten treiben dieses Multi-Provider-Cloud-

Edge-Kontinuum inzwischen voran. 2026

hat sich das Ökosystem zudem für weitere

Unternehmen und Partner geöffnet, und

das weit über den Rahmen des ursprüng-

lichen IPCEI-CIS-Projekts, aus dem 8ra

hervorging, hinaus.

Der strategische Hintergrund ist klar: Europa will digitale Infrastrukturen schaffen, die nicht nur leistungsfähig, sondern auch kontrollierbar, auditierbar und unter europäischen rechtlichen und operativen Bedingungen steuerbar sind. Das Ziel: Technologische Abhängigkeiten reduzieren, Wahlfreiheit erhöhen und digitale Infrastrukturen belastbarer machen. 8ra beschreibt digitale Souveränität deshalb als eine klar überprüfbare Fähigkeit in vier Dimensionen: Daten-, Technologie-, Betriebs- und Rechtssouveränität. Dahinter steht der sehr praktische Anspruch, dass Workloads zwischen Anbietern und Standorten verschiebbar bleiben, Datenflüsse transparent gesteuert werden können und Dienste auch bei Anbieterwechseln, Störungen oder Krisen funktionsfähig und beherrschbar bleiben.

Edge und Cloud gehören zusammen

Die eigentliche Stärke von 8ra liegt darin, Cloud und Edge Computing nicht länger als zwei getrennte Welten zu behandeln. In vielen industriellen und öffentlichen Szenarien reicht ein rein zentrales Cloud-Modell nicht aus. Latenzen sind zu hoch, Datenmengen zu groß, regulatorische Anforderungen zu streng und Ausfallszenarien zu kritisch. 8ra setzt daher auf ein verteiltes Kontinuum, in dem Rechenleistung und Dienste dort bereitgestellt werden, wo sie fachlich und technisch am sinnvollsten sind. Das können zentrale Clouds, regionale Infrastrukturen oder der direkte Netzwerkrand, die „Edge“, sein.





Das erhöht Performance und Resilienz, reduziert strukturelle Lock-in-Risiken und schafft die Grundlage für Anwendungen wie industrielle Echtzeitverarbeitung, Edge AI oder föderierte Datenräume.

Dabei werden nicht zuletzt auch zentrale Marktprobleme Europas adressiert. Anders als die USA oder China kämpft Europa mit zersplitterten Anbieterlandschaften und mangelnder Interoperabilität vieler Lösungen. Die daraus resultierende hohe Abhängigkeit von dominanten Plattformen aus Übersee verschärfte dieses Problem nur weiter und sorgte dafür, dass kleine und mittlere Anbieter sich nur schwer in ein belastbares Ökosystem einbinden lassen.

Mehr als ein Architekturkonzept

Diese Herausforderungen machen die 8ra-Architektur zu mehr als einem technischen Ideal. Sie ist ein industriepolitisches Programm, um einen technologischen Raum zu schaffen, der über einzelne Lösungen hinaus Wirkung entfaltet. Beim 8ra Annual Summit 2026 in Rotterdam stand deshalb nicht mehr allein die reine Grundlagenarbeit im Vordergrund, sondern die nächste Phase: Umsetzung, Skalierung und Marktintegration. Europa diskutiert 8ra inzwischen weit über den Forschungsgedanken hinaus als infrastrukturelle Antwort auf die Frage, wie sich digitale Handlungsfähigkeit in Cloud-, Edge- und künftig auch KI-Umgebungen praktisch organisieren lässt.

Genau an dieser Stelle bringt secunet seine fast 30 Jahre Cybersicherheitserfahrung in die 8ra-Initiative ein. Der Beitrag von secunet zielt darauf ab, Edge-to-Cloud-Infrastrukturen nicht nur funktionsfähig, sondern hochsicher und betrieblich beherrschbar zu machen. Bereits zum Projektstart begann das Projekt **secunet edge cloud**, um gemeinsam mit Partnern hochsichere, sich automatisch vernetzende Edge-Cloud-Infrastrukturmodule zu entwickeln, die auch in kritischen Infrastrukturen eingesetzt werden können. Das technologische Fundament dafür ist nun gelegt.

8ra Annual Summit 2026 in Rotterdam



secunet edge cloud: Sicherheit und Rechenleistung am Netzwerkrand

Einer der ersten Schwerpunkte von secunet edge cloud lag auf **Hochsicherheitsmodulen für Cloud-Infrastrukturen**, insbesondere für Szenarien mit hohen regulatorischen Anforderungen. Mandantentrennung, Vertrauensanker, kryptografische Schutzmechanismen sowie abgesicherte Orchestrierungs- und Betriebsprozesse sind dabei Teil des architektonischen Fundaments. Dieses Fundament basiert auf wiederverwendbaren Sicherheitsbausteinen. Sicherheit wird also nicht nachträglich auf eine Plattform aufgesetzt, sondern über Prinzipien wie Design-by-Compliance und Security-by-Default von Beginn an mitgedacht. Denn gerade in einem Multi-Provider-Umfeld gilt: Wer föderierte Infrastrukturen schaffen will, braucht gemeinsame Sicherheitsprinzipien, standardisierte Schnittstellen und überprüfbare Baselines.

Ebenso wichtig jedoch ist die zweite Seite des Projekts: die Edge selbst. Hierzu wurde eine **modulare Edge-Node-Plattform** entwickelt, die Rechenleistung, Sicherheitsfunktionen und Plattformdienste direkt „an den Netzwerkrand bringt“, also dorthin, wo Maschinen, Geräte und Gateways arbeiten. Robuste, sichere Edge-Architekturen ermöglichen die lokale Datenverarbeitung auch bei eingeschränkter Konnektivität, in verteilten Betriebsmodellen und unter hohen Anforderungen an Verfügbarkeit, Datenschutz und Echtzeitfähigkeit. Der Ansatz macht es zudem

möglich, Anwendungen wie Edge AI, Sicherheitsfunktionen oder industrielle Services nahe am Entstehungsort der Daten zu betreiben.

Doch diese Komponenten allein reichen nicht aus, wenn Entwicklungs- und Betriebsprozesse nicht ebenso schnell und sicher mitskalieren. Deshalb hat secunet im Projekt eine **Internal Developer Platform (IDP)** aufgebaut, die DevSecOps-Prinzipien, standardisierte Toolchains, definierte Schnittstellen und Plattform-Services zusammenführt. Dieser Hebel ist vor allem strategisch, denn Entwicklungs-, Betriebs- und Sicherheitsanforderungen werden so nicht in separaten „Silos“ behandelt, sondern auf einer gemeinsamen Basis beschleunigt und über Produkt- und Projektgrenzen hinweg vereinheitlicht. Das schafft die Voraussetzungen dafür, neue Edge- und Cloud-Funktionen schnell in die Praxis zu überführen und die Zusammenarbeit mit Partnern in einem heterogenen europäischen Ökosystem zu erleichtern.

Von der Referenzarchitektur in die Anwendung

Die 8ra-Initiative bewegt sich derzeit sichtbar von der Architektur- und Referenzebene in Richtung praktischer Nutzung. Nach dem Aufbau der technologischen Grundlagen rückt dabei nun die Überführung in marktfähige Edge-to-Cloud-Szenarien stärker in den Vordergrund. secunet hat dafür bereits den organisatorischen Rahmen geschaffen. In Kooperation mit Partnern werden daraus belastbare Managed-Cloud- und Edge-Architekturen entstehen, die souveräne Rechenzentren, hybride Infrastrukturen sowie Maschinen, Geräte und kritische Netzsegmente in ein integrierbares, mandantenfähiges und betrieblich beherrschbares Gesamtsystem gießen. Die Bandbreite reicht von der sicheren Digitalisierung bestehender Anlagen über die Anbindung verteilter Standorte bis hin zur Interoperabilität zwischen modernen Plattformen und Legacy-Systemen, Edge-Security-Lösungen und lokaler KI-Verarbeitung.

8ra macht damit sichtbar, was digitale Souveränität in Europa praktisch bedeutet: nicht Abschottung, sondern kontrollierbare Offenheit. Kein einzelner Anbieter, sondern ein interoperables Ökosystem. Und nicht nur Architekturprinzipien, sondern reale Betriebsfähigkeit. Die Initiative schafft einen europäischen Handlungsraum, in dem digitale Infrastruktur offen, sicher und unabhängig genug wird, um langfristig tragfähig zu sein.



Torsten Redlich
Global Head of Edge Unit bei secunet



Sichere IT-Infrastrukturen vs. digitaler Fortschritt?

Ohne Cloud keine digitale Souveränität

Von Markus Linnemann, Vice President Critical Infrastructures bei secunet

Ob elektronische Patientenakte, E-Rezept, KI-gestützte Diagnostik oder datenbasierte Forschung: Die Digitalisierung des Gesundheitswesens entscheidet sich nicht allein an einzelnen Anwendungen. Entscheidend ist die Infrastruktur dahinter. Sie muss hochsensible Daten schützen, regulatorische Anforderungen erfüllen, zuverlässig verfügbar sein und zugleich so nutzerfreundlich funktionieren, dass digitale Prozesse im Versorgungsalltag tatsächlich ankommen. Cloud-Technologie verspricht diese Effizienz und kann mittlerweile auch das dafür notwendige Sicherheitsniveau liefern. Das macht sie zu einer Grundvoraussetzung sowohl für die digitale Souveränität als auch für den digitalen Fortschritt in Deutschland und Europa.

Lange Zeit wurde IT-Sicherheit im Rahmen von Digitalisierungsprozessen vor allem als Bremse wahrgenommen. Diese Sichtweise ist nicht nur überholt, sondern hat sich faktisch ins Gegenteil verkehrt: Heute ist IT-Sicherheit ein Enabler für Digitalisierung. Denn je stärker kritische Prozesse, personenbezogene Daten und versorgungsrelevante Systeme digitalisiert werden, desto wichtiger wird das Vertrauen in die technische Grundlage. Ohne Sicherheit keine Akzeptanz. Und ohne Akzeptanz keine skalierbare Digitalisierung.

Eine robuste Infrastruktur ist die Basis

Diese Entwicklung zeigt sich besonders deutlich in den aktuellen Regulierungsmaßstäben, die auf EU-Ebene angelegt werden. So verpflichtet etwa die NIS-2-Richtlinie betroffene Unternehmen dazu,

geeignete, verhältnismäßige und wirksame technische und organisatorische Maßnahmen zu ergreifen und diese zu dokumentieren. Das KRITIS-Dachgesetz ist am 17. März 2026 in Kraft getreten und stärkt ergänzend die digitale wie auch physische Resilienz kritischer Anlagen. Für Unternehmen und Einrichtungen bedeutet das, dass Informationssicherheit nicht länger eine rein operative Aufgabe der IT sein kann. Sie wird Bestandteil der Unternehmensführung.

Wer heute digitale Dienste betreibt, muss über die reine Absicherung der Systeme hinaus Verantwortlichkeiten klären, Risiken bewerten, Nachweise führen und die eigene Infrastruktur so gestalten, dass sie auch unter Druck funktioniert. Der wichtigste Rat lautet deshalb: Begonnen werden sollte nicht mit schnellen Einzelmaßnahmen, sondern zunächst mit einer strukturierten Bestandsaufnahme:

- Wie ist die Informationssicherheit aktuell aufgestellt?
- Welche Anforderungen werden bereits erfüllt?
- Wo bestehen Lücken?
- Welche Systeme sind besonders kritisch?

Daraus entsteht ein Umsetzungsplan, der Prioritäten setzt und Investitionen sinnvoll lenkt. Gerade in regulierten Branchen wie dem Gesundheitswesen, der Energieversorgung oder dem öffentlichen Sektor ist eine robuste IT-Infrastruktur die Voraussetzung, um nicht nur heutige, sondern auch künftige Anforderungen sicher und effizient zu bewältigen und Innovationen umzusetzen.

Datenschutz ist kein Gegenspieler der Innovation

Gerade der Datenschutz wird in Deutschland oft als reines Hemmnis diskutiert. Diese Debatte greift deutlich zu kurz. Es gibt nicht „den einen Datenschutz“ und erst recht nicht „das eine Sicherheitsniveau“. Entscheidend ist immer der konkrete Schutzbedarf. Für europäische Unternehmen und öffentliche Einrichtungen ergibt sich daraus ein ganz konkreter Anspruch. Wer sensible Daten verarbeitet, muss wissen, welchem Recht der Anbieter unterliegt, welche Zugriffsmöglichkeiten bestehen und wie die Kontrolle technisch sowie organisatorisch abgesichert wird. Kurz: Gesundheitsdaten, Forschungsdaten, Verwaltungsdaten und industrielle Prozessdaten haben unterschiedliche Anforderungen. Die technische Architektur muss darauf abgestimmt sein und die richtige Balance zwischen Schutz, Nutzbarkeit und Innovationsmöglichkeit schaffen.



„Die Zukunft des Gesundheitswesens wird digital sein. Erfolgreich ist sie nur dann, wenn sie auf sicheren, souveränen und vertrauenswürdigen Infrastrukturen aufbaut.“

Digitale Souveränität heißt Kontrolle, nicht Abschottung

Das führt über kurz oder lang zum Grundgedanken digitaler Souveränität, denn im Kern geht es auch hier um Kontrolle: Welche Daten möchte eine Organisation wie schützen? Wer betreibt die Infrastruktur? Wer kann auf Daten zugreifen? Wie transparent sind Technologien und Prozesse? Und wie frei ist die Organisation, Anbieter zu wechseln, ohne in Abhängigkeit zu geraten?

Digitale Souveränität bedeutet nicht, alles selbst zu bauen oder internationale Zusammenarbeit auszuschließen. Sie bedeutet, handlungsfähig zu bleiben. Dazu gehören offene Standards, Interoperabilität, überprüfbare Sicherheitsmechanismen und die Möglichkeit, kritische Prozesse unter europäischen rechtlichen und operativen Bedingungen zu betreiben. Gerade Regierungen, Behörden, KRITIS-Unternehmen und Einrichtungen des Gesundheitswesens sollten deshalb Anbieter wählen, die für Zuverlässigkeit, Stabilität, Zertifizierungen und die Einhaltung europäischer Datenschutz- und Sicherheitsstandards stehen. Digitale Souveränität entsteht durch eine nachprüfbar Architektur und bewusst getroffene Entscheidungen.

Die sichere Cloud ist der größte Innovationstreiber

Ohne Cloud keine digitale Souveränität. Das mag zunächst paradox klingen, denn Cloud-Technologie wird aufgrund bestehender Abhängigkeiten von US-Anbietern häufig mit Abhängigkeit verbunden. Tatsächlich aber kommt es vor allem auf das Modell an. Ähnlich wie beim Datenschutz gibt es nicht „die eine Cloud“. Private, Public, Hybrid, Multi-Cloud oder On-Premises-Modelle bieten unterschiedliche Freiheitsgrade, Schutzmechanismen und Betriebsformen. Entscheidend ist, dass Organisationen ihr Schutzniveau kennen und die passende Infrastruktur wählen.

Für das Gesundheitswesen ist das beispielsweise besonders relevant. Medizinische Daten müssen besonders geschützt werden, zugleich braucht Forschung umfangreich verfügbare, strukturierte und oftmals anonymisierte oder pseudonymisierte Datenbestände. Digitale Anwendungen wie das E-Rezept oder die elektronische Patientenakte zeigen, wie stark Versorgung künftig von sicheren Infrastrukturen abhängt. Das E-Rezept ist nach Angaben der gematik inzwischen Standard für verschreibungspflichtige Arzneimittel; die „ePA für alle“ bündelt relevante Gesundheitsdaten und soll Behandlungen passgenauer machen.

All dies macht die sichere Cloudifizierung lokaler Datenbanken zu einem der größten Treiber medizinischer Innovation, denn Bedarf wie auch Chancen sind riesig: Ein Jahr nach Einführung der „ePA für alle“ meldete die gematik mehr als 100 Millionen hinterlegte Dokumente und bis zu 93.000 Arzt- und Zahnarztpraxen, die wöchentlich auf die ePA ihrer Patientinnen und Patienten zugreifen. Solche Datenmengen lassen sich nicht mit Insellösungen beherrschen. Sie benötigen skalierbare, sichere und nachvollziehbare Cloud- und Plattformarchitekturen.

Digitalisierung braucht Vertrauen und muss einfach sein

Die entscheidende Herausforderung liegt deshalb im Zusammenspiel des gesamten IT-Ökosystems. Digitalisierung im Gesundheitswesen funktioniert nur, wenn viele Akteure zusammenspielen: Leistungserbringer, Krankenkassen, Industrie, Forschung, Plattformanbieter, Regulatoren und Sicherheitsdienstleister. Bei aller technologischen Komplexität darf dabei jedoch nicht aus dem Blick geraten, dass digitale Systeme nur genutzt werden, wenn sie im Alltag funktionieren. Sicherheit muss deshalb smart und nutzerfreundlich integriert sein. Sie darf nicht gegen Effizienz ausgespielt werden, sondern muss Prozesse einfacher, verlässlicher und robuster machen. Das gilt für Ärztinnen und Ärzte ebenso wie für Patientinnen und Patienten, Pflegekräfte, Verwaltungsmitarbeitende oder IT-Teams.

Cloud und KI werden dabei in den kommenden Jahren eine zentrale Rolle spielen: bei der strukturierten Auswertung großer Datenmengen, bei intelligenter Suche, bei automatisierter Dokumentation, bei Entscheidungsunterstützung oder in der Diagnostik. All diese Anwendungen können dazu beitragen, die Versorgung zu verbessern, Forschung zu beschleunigen und Fachkräfte zu entlasten. Sie setzen jedoch voraus, dass die Datenbasis vertrauenswürdig ist und die Infrastruktur den Schutzbedarf erfüllt.

Als Anbieter für IT-Sicherheit und Digitalisierung in hochregulierten Umfeldern unterstützt secunet die digitale Transformation im Gesundheitswesen unter anderem in den Bereichen Telematikinfrastruktur, Telemedizin, Medizintechnik und cloudbasierte Gesundheitsplattformen. Für Organisationen mit regulatorischen Anforderungen bietet secunet zudem sichere Cloud-Lösungen „Made in Germany“, von Public-, Private-, Hybrid- und Multi-Cloud-Modellen bis hin zu On-Premises-Szenarien.

Souveräne Cloud ist kein Selbstzweck

Digitale Souveränität ist keine abstrakte politische Formel. Sie zeigt sich ganz konkret in der Frage, ob eine Organisation ihre Daten kontrollieren, ihre Systeme verlässlich betreiben, Anbieter frei wählen und dabei Innovationen wirksam etablieren kann. Gerade im Gesundheitswesen entscheidet diese Fähigkeit darüber, ob Digitalisierung Vertrauen schafft oder neue Abhängigkeiten entstehen lässt.

Cloud-Technologie ist dabei kein Sicherheitsproblem, sondern Innovationstreiber. Sie ist es, die Skalierung, Vernetzung, KI-Integration und datengetriebene Versorgung überhaupt erst möglich macht. Oder anders gesagt: Die Zukunft des Gesundheitswesens wird digital sein. Erfolgreich ist sie nur dann, wenn sie auf sicheren, souveränen und vertrauenswürdigen Infrastrukturen aufbaut.



Markus Linnemann
Vice President Critical Infrastructures
bei secunet

Standardisierung von IPsec

Sicherheit für das Internet von heute und morgen

Von Steffen Klassert, secunet Security Networks AG

Verschlüsselung bildet den Kern der Internetsicherheit, und eine zentrale Technologie dafür ist IPsec. Die Protokollsuite muss kontinuierlich angepasst werden, um neuen Herausforderungen wie leistungsfähigen Quantencomputern standhalten zu können. secunet beteiligt sich aktiv an dieser Weiterentwicklung.

Das Internet hat sich seit den 1990er-Jahren grundlegend verändert. Netzwerke sind schneller geworden, Rechenleistung wird zunehmend parallel verarbeitet, Cloud-Architekturen haben neue Kommunikationswege geschaffen und Anwendungen wie Künstliche Intelligenz stellen hohe Anforderungen an Geschwindigkeit und Skalierbarkeit. Gleichzeitig bleiben die grundlegenden Anforderungen an die Sicherheit digitaler Kommunikation bestehen: Daten müssen vertraulich übertragen, Kommunikationspartner authentifiziert und Verbindungen gegen Manipulation geschützt werden.

Eine zentrale Rolle spielt dabei IPsec. Hierbei handelt es sich um eine Protokollsuite, also eine Sammlung von Netzwerkprotokollen für sichere und verschlüsselte Kommunikation, die es ermöglicht, Daten auf der Netzwerkebene kryptografisch abzusichern. Sie ist Bestandteil zahlreicher Sicherheitslösungen und wurde seit der ersten Standardisierung kontinuierlich an neue technische Anforderungen angepasst. Diese Anpassung obliegt der internationalen Internet Engineering Task Force (IETF).

secunet beteiligt sich in diesem Umfeld an maßgeblichen Open-Source-Projekten wie der IPsec-Implementierung im Linux-Kernel und der millionenfach verbreiteten Software strongSwan, mit der sich IPsec-gesicherte Virtual Private Networks (VPNs) aufbauen lassen. Zudem arbeitet secunet an der Standardisierung innerhalb der Internet Engineering Task Force (IETF) mit.



Vom sicheren Internet zur Protokollsuite für moderne Netze

Während bei IPsec zunächst die sichere Kommunikation über das entstehende Internet im Mittelpunkt stand, geht es heute zunehmend um hochperformante Netzwerke, neue Rechnerarchitekturen und die Vorbereitung auf eine Welt mit leistungsfähigen Quantencomputern. Die für eine stetige Weiterentwicklung notwendige Standardisierung von IPsec begann entsprechend bereits Mitte der 90er-Jahre. Die Protokollsuite besteht vereinfacht aus zwei Bereichen: der Controlplane und der Dataplane.

Die Controlplane übernimmt unter anderem die sichere Aushandlung kryptografischer Schlüssel. Dafür wurde 1998 mit Internet Key Exchange (IKEv1) ein entsprechendes Protokoll standardisiert. In der Dataplane werden dann die zuvor ausgehandelten Schlüssel verwendet, um Nutzdaten zu verschlüsseln und zu authentifizieren. Neben dem Authentication Header (AH) wurde dafür das Encapsulating Security Payload (ESP) entwickelt. Während AH ausschließlich eine Authentifizierung ermöglicht und beispielsweise in Fällen wie der Network Address Translation (NAT) an Grenzen stößt, bietet ESP sowohl Authentifizierung als auch Verschlüsselung und lässt sich auch in komplexeren Netzwerkkombinationen einsetzen. ESP hat sich deshalb als das heute maßgebliche Sicherheitsprotokoll innerhalb von IPsec etabliert.

Mit der zunehmenden Verbreitung und Komplexität großer Netzwerke zeigten sich jedoch neue Anforderungen. Während ESP den Anforderungen noch gerecht blieb, kritisierten Betreiber großer

Infrastrukturen unter anderem die Komplexität von IKEv1. 2005 wurde deshalb mit IKEv2 eine umfassende Weiterentwicklung standardisiert. Die grundlegende Architektur von IPsec blieb dabei erhalten, der Prozess jedoch ist ein fortlaufender: Mit zunehmender Veränderung der Netzwerktechnik mussten weitere Teile der Protokollsuite angepasst werden.

Schutz vor Quantencomputern

Eine wesentliche Erweiterung betrifft etwa die Bedrohung durch leistungsfähige Quantencomputer. Seit 2017 arbeitet die IETF deshalb daran, IPsec für Post-Quanten-Kryptografie (PQC) zu ertüchtigen. Hintergrund ist unter anderem das Angriffsszenario „Store now, decrypt later“. Dabei können Angreifer verschlüsselte Kommunikation bereits heute aufzeichnen und speichern, um sie zu einem späteren Zeitpunkt mit leistungsfähiger Quantencomputertechnologie zu entschlüsseln. Ein langfristig sicherer Kommunikationsweg muss daher bereits heute auf diese Entwicklung vorbereitet werden.

Für die symmetrischen Kryptoverfahren der ESP-Dataplane genügt dafür grundsätzlich eine Anpassung der Schlüssellänge. Anders stellt sich die Situation beim asymmetrischen Schlüsselaustausch in der Controlplane dar. Hier werden neue kryptografische Verfahren benötigt. Die IETF spezifiziert hierfür unter anderem Erweiterungen des IKE-Protokolls, die zusätzliche Verfahren für den Schlüsselaustausch ermöglichen. Dazu gehören auch hybride Ansätze, bei denen klassische und quantensichere Verfahren kombiniert werden. secunet treibt das Thema PQC seit Langem voran, so auch bei der Spezifizierung eines hybriden Verfahrens auf Basis des vom BSI empfohlenen PQC-Verfahrens FrodoKEM.

Wenn Netzwerke schneller werden

Während die Post-Quanten-Erweiterungen vor allem die kryptografische Grundlage betreffen, entstanden Anfang der 2010er-Jahre auch neue Herausforderungen auf der Dataplane-Seite. Der Grund dafür liegt in der Entwicklung moderner Computerarchitekturen. ESP wurde ursprünglich für Systeme entwickelt, bei denen ein einzelner Prozessor den Netzwerkdatenpfad verarbeitet. Moderne Systeme setzen dagegen zunehmend auf viele Prozessorkerne, die Aufgaben parallel bearbeiten und priorisieren. Das gilt für Autonomes Fahren, KI-Anwendungen, aber auch normale Videostreams im Wohnzimmer. Gleichzeitig steigen die Geschwindigkeiten von Netzwerken weiter, während sich die Taktfrequenzen von CPUs bereits seit Jahren weniger stark erhöhen.

Für die Verarbeitung großer Datenmengen bedeutet das: Die Netzwerkkommunikation muss stärker parallelisiert werden. Erste Versuche, diese Herausforderung ausschließlich durch Anpassungen bestehender Implementierungen zu lösen, zeigten, dass dafür teilweise Änderungen am Protokoll selbst erforderlich sind. IPsec ESP ist zum Flaschenhals für Netzwerk-Performance geworden.

Mit EESP für moderne Netzwerkarchitekturen

Gemeinsam mit der TU Ilmenau begann secunet deshalb, die bestehenden Herausforderungen systematisch zu untersuchen. Im Februar 2023 wurde dazu ein erster Vorschlag in der IETF veröffentlicht. Eine Lösung für das Multicore-Problem wurde 2024 unter maßgeblicher Mitarbeit von secunet als RFC 9611 standardisiert. Damit können über IKEv2 dedizierte Sicherheitsbeziehungen für einzelne CPUs beziehungsweise Prozessorkerne ausgehandelt werden.

Für andere Anwendungsszenarien reicht dieser Ansatz jedoch nicht aus. Im modernen Rechenzentrum oder Telekommunikationsnetz wäre die Suche nach der jeweils passenden Sicherheitsbeziehung so unnötig komplex. Hier setzt das von secunet im Oktober 2024 vorgeschlagene Enhanced Encapsulating Security Payload (EESP) an. Das neue Sicherheitsprotokoll wurde im Mai 2025 von der IETF-IPsecME-Arbeitsgruppe als Arbeitsgruppendokument angenommen. EESP ist speziell auf moderne Netzwerkarchitekturen ausgelegt und soll Anwendungsfälle adressieren, bei denen ESP an technische Grenzen stößt.

„Store now, decrypt later“

ESP und EESP können dabei parallel eingesetzt werden. Unternehmen und Betreiber erhalten damit die Möglichkeit, abhängig von ihren jeweiligen Anforderungen das passende Sicherheitsprotokoll einzusetzen. Ein fertiger EESP-Standard wird derzeit für 2027 erwartet.

Offene Standards als Grundlage für sichere Netzwerke

Neue Rechnerarchitekturen, steigende Übertragungsgeschwindigkeiten und neue kryptografische Bedrohungen: Die Entwicklung von IPsec zeigt, dass Netzwerksicherheit eng mit der technischen Entwicklung der Netzwerke selbst verbunden ist. Das verändert die Anforderungen an Sicherheitsprotokolle kontinuierlich. Standardisierung schafft dabei die Grundlage dafür, dass Sicherheitsmechanismen nicht isoliert für einzelne Produkte entwickelt werden, sondern in unterschiedlichen Systemen und Infrastrukturen eingesetzt werden können. Mit seiner Arbeit in der IETF und Open Source-Implementierungsmöglichkeiten trägt secunet dazu bei, diese Entwicklung technisch mitzugestalten.

Social Days 2026

Gemeinsam für den guten Zweck

Vier Jahre secunet Social Days, in diesem Jahr in elf Projekten an sechs Standorten – und immer wieder gibt es Momente, die besonders hängen bleiben.



Für die AWO Kita Schlängelbachweg in Pirna entsteht eine neue Spielhütte ...

Zum Hands-on-Projekt in der AWO Kita Schlängelbachweg in Pirna hat sich für den sogenannten „Dresden-Move“ ein großes, eingespieltes Team gefunden: Handwerkliches Geschick bündelt sich in diesem Team so sehr, dass Jahr für Jahr selbst umfangreiche und anspruchsvolle Aufgaben an einem Tag gelingen. So sind auch in diesem Jahr ein barrierefreies Hochbeet, eine neue Spielhütte und ein frisch gestrichener Gerätecarport in der Kita entstanden – trotz zwischenzeitlich kräftiger Regenschauer. Die Kita bedankte sich später: Die Spielhütte sei „sofort begeistert in Beschlag genommen“ worden.

... und ein barrierefreies Hochbeet.



In den Ausflugsprojekten stellten Mitarbeitende von secunet ganz andere Stärken unter Beweis – beobachten, hinhören, begleiten, ermutigen: Im SEA LIFE Hannover durften Kinder große Insekten auf die Hand nehmen. Das trauten sich nicht alle Kinder im ersten Anlauf, aber letztlich gewann die Neugier. Im Legoland Oberhausen erlebten Kinder mit besonderem Förderbedarf einen Tag, der im Alltag sonst nicht vorkommt – die gesamte Gruppe schickte später selbst gestaltete Dankeskarten an ihre Patinnen und Paten. Beim Berliner Ausflug erzählte eine Erzieherin von einem Jungen, der bislang nur einen Weg kannte: vom Hochhaus in die Kita und wieder zurück. Und im Dresdner Karl-May-Museum blieb ein Satz besonders in Erinnerung: „Bester Ausflug in meinem Leben“, sagte ein Junge nach dem Goldwaschen.

Wie viel dieser Einsatz zurückgibt, brachte Marc-Julian Siewert auf den Punkt, der die Social Days in diesem Jahr zum ersten Mal miterlebte – er ist seit Juli 2025 CEO von secunet. Bei seinem Einsatz in München sagte er: „Ich lerne eine ganz andere Seite von secunet kennen.“ Es sei ein Tag, an dem man mit den Kindern in ihrem Garten Dinge erneuere, verschönere und „wirklich handwerklich“ arbeite – „ich bin total beeindruckt von den Kindern, von den Erziehern. Es macht großen Spaß und dieser Tag bedeutet uns sehr viel bei secunet.“



Im SEA LIFE Hannover durften Kinder große Insekten auf die Hand nehmen.

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

Sophie Huppert und Annica Lill, lessislovable.de

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

Urheberrecht

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

Bildnachweis

Titel / S. 17: Prof. Dr. Sabina Jeschke
S. 2 (oben) / 5, 6 / 7, 21, 24, 38: iStock
S. 2 (unten) / 27, 11, 31 (oben), 33, 34: Getty Images
S. 3, 8, 9, 18, 32, 36, 40, 41: secunet
S. 13, 14: KI-generiert
S. 29: Alamy
S. 31 (unten): Europäische Kommission



***Irgendwer muss nachts
um drei rangehen, wenn
im Rechenzentrum was
ausfällt.***



KI-generiert

***Das Problem:
Sie sind Irgendwer.***

SINA Cloud als Service.

Die Cloud-Lösung für Verschlusssachen.

secunet cloud