2024 /// WWW.DIGITALBUSINESS-CLOUD.DE

D, A, CH: 11,50 | weitere EU-Länder: 13,70 | ISSN 2510-344X

DIGITAL BUSINESS CLOUD

EXPERTENMAGAZIN FÜR DIGITALE TRANSFORMATION

Eine Publikation der WIN Verlag GmbH & Co. KG |

SONDERHEFT SECURITY

KÜNSTLICHE INTELLIGENZ

DAS NEUE YIN UND YANG DER CYBERSECURITY?

TOP-THEMA:
FRAUEN IN DER IT-SECURITY

Plädoyer für eine diverse Cyber Security-Welt:
Frauen sind noch immer unterrepräsentiert. Um die Herausforderungen der digitalen Zukunft zu meistern, braucht es auch mehr Empathie.

Die erste Cloud, mit der Sie Geheimnisse teilen können.

SINA Cloud – Souverän gedacht. Sicher gemacht.

QR-CODE SCANNEN
UND ZUM KOSTENFREIEN
WEBINAR ANMELDEN.

Die SINA Cloud für Verschlusssachen bis GEHEIM.
Beliebige Mandanten und Sicherheitslevel
auf einer Infrastruktur.

secunet.com protecting digital infrastructures

secunet

EDITORIAL

Liebe Leserin, lieber Leser

- **Kurz vor Redaktionsschluss** erreicht uns die aktuelle Erhebung des Digitalverbands Bitkom. Demnach müssen die deutschen Unternehmen noch größere Anstrengungen unternehmen, um den Datenschutz umzusetzen. In rund zwei Drittel hat der Aufwand für den Datenschutz im vergangenen Jahr zugenommen, und nirgendwo ist er zurückgegangen. 9 von 10 Unternehmen bezeichnen den aktuellen Datenschutz-Aufwand als hoch. Zugleich sind in rund zwei Drittel der Unternehmen in Deutschland in den vergangenen zwölf Monaten innovative Projekte aufgrund von Datenschutz-Vorgaben gescheitert oder gar nicht erst angegangen worden.

Angesichts des hohen Aufwands zieht fast die Hälfte der Unternehmen den Einsatz von künstlicher Intelligenz beim Datenschutz in Betracht. Zugleich sind gut zwei Drittel der Unternehmen der Meinung, dass der Einsatz von KI in den Unternehmen den Datenschutz vor ganz neue Herausforderungen stellt. Ist KI also das neue Yin und Yang der Cybersecurity?

In der aktuellen Ausgabe uneres „Sonderheftes Security" gehen wir Antworten auf diese Frage nach und zeigen zahlreiche Ansätze für eine erfolgreiche IT-Security auf.

Ihr
HEINER SIEGER, Chefredakteur
DIGITAL BUSINESS CLOUD
heiner.sieger@win-verlag.de

Wir brauchen eine diverse Cyber Security-Welt

Der Fachkräftemangel in der IT und speziell in dem Bereich Cyber Security ist allgegenwärtig. Doch Frauen sind in diesen Bereichen noch immer stark unterrepräsentiert. Um die Herausforderungen der digitalen Zukunft zu meistern, brauchen wir diversere Teams – und das beginnt bei der Förderung von Vielfalt und Chancengleichheit.

VON CHRISTIAN GÄBEL

Warum Diversität der Schlüssel zum Erfolg ist

Die IT-Branche treibt die digitale Transformation weltweit voran, doch sie bleibt in vielen Bereichen homogen und von Männern dominiert. Besonders im Bereich Cyber Security sind Frauen unterrepräsentiert, was nicht nur eine Frage der Geschlechtergerechtigkeit ist, sondern auch den Fortschritt behindert. Diversität in Teams, vor allem in der IT, ist entscheidend für den Erfolg von Unternehmen und die Zukunft der digitalen Gesellschaft.

DER AUTOR
Christian Gäbel
ist Teil der Geschäftsführung bei der pco GmbH & Co. KG, Gründer des Deutschen Incident Response-Teams (DIRT) und verantwortlich für die strategische Ausrichtung des Geschäftsbereiches Cyber Security und des Deutschen IT-Security Kongresses.

Der Status Quo: Frauen in der IT

Der Fachkräftemangel in der IT ist bekannt und Unternehmen suchen dringend nach qualifiziertem Personal. Dennoch ist der Frauenanteil in der Branche erschreckend niedrig.

Laut einer Bitkom-Studie von 2022 sind nur 17 Prozent der IT-Fachkräfte in Deutschland Frauen. In der Cyber Security, einem stark wachsenden Bereich, sind sie sogar noch seltener vertreten. Trotz hervorragender Leistungen in MINT-Fächern entscheiden sich viele Frauen gegen eine Karriere in der IT. Gründe dafür sind unter anderem Stereotypen, fehlende Vorbilder und strukturelle Barrieren, die Frauen den Zugang zu technischen Berufen erschweren.

Stereotypen und kulturelle Barrieren

Ein großes Problem sind verfestigte Geschlechter-Stereotypen, die bereits in der Schule beginnen. Technik wird oft als „Männerdomäne" betrachtet und Mädchen werden seltener dazu ermutigt, sich für Informatik zu interessieren. Dies prägt die Berufswahl junger Frauen und setzt sich in der Ausbildung und im Beruf fort. Frauen, die in der IT arbeiten, sehen sich oft mit Vorurteilen konfrontiert, was ihr technisches Verständnis betrifft, was entmutigend wirken kann.

Mangelnde Sichtbarkeit und Vorbilder

Ein weiteres Hindernis ist die geringe Sichtbarkeit weiblicher Vorbilder in der IT. Erfolgreiche Frauen in der Branche sind kaum präsent und in den Medien dominieren Männer als Experten. Dies verstärkt den Eindruck, dass IT-Berufe nichts für Frauen sind.

Tatsächlich gibt es jedoch viele Frauen, die in der IT herausragende Arbeit leisten – als Programmiererinnen, Datenwissenschaftlerinnen, Focus Sales-Mitarbeiterinnen oder CTOs. Doch sie stehen oft im Schatten ihrer männlichen Kollegen, was junge Frauen davon abhält, IT-Berufe in Betracht zu ziehen.

Strukturelle Hürden im Berufsumfeld

Neben kulturellen und psychologischen Hürden gibt es strukturelle Barrieren, die Frauen den Einstieg in die IT erschweren. In männerdominierten Teams ist es oft schwierig, ernst genommen zu werden. Zudem fehlen in vielen Unternehmen gezielte Maßnahmen zur Förderung von Frauen, und flexible Arbeitszeitmodelle – wichtig für Mütter und Väter – sind nicht überall etabliert.

Auch der Gender Pay Gap ist in der IT ein Thema: Frauen verdienen im Durchschnitt weniger als Männer, selbst bei gleicher Qualifikation und Erfahrung (z. B. laut dem Gender Pay Gap Report von Destatis). Dies wirkt abschreckend auf Frauen, die eine Karriere in der IT anstreben.

Erfolgreiche **Frauen in der IT sollten sichtbarer gemacht werden**. Vorbilder helfen dabei, stereotype Vorstellungen zu überwinden und jungen Frauen zu zeigen, dass sie in der Branche erfolgreich sein können.

Der Wert von Diversität in Teams

Warum ist es so wichtig, mehr Frauen in die IT zu bringen? Diversität ist ein Schlüssel zum Erfolg, sowohl wirtschaftlich als auch gesellschaftlich. Studien wie die McKinsey & Company-Studie „Diversity Wins" (2020) zeigen, dass diverse Teams kreativer, innovativer und produktiver sind. Unterschiedliche Perspektiven führen zu besseren Lösungen und stärken die Innovationskraft von Unternehmen. Besonders in der IT, einer Branche, die sich ständig verändert, ist dies entscheidend. In der Cyber Security beispielsweise, wo Cyber-Angreifer aus verschiedensten Kontexten kommen, ist es von Vorteil, wenn das Verteidigungsteam ebenfalls eine breite Vielfalt an Lösungs-Perspektiven bietet.

Positive Ansätze und Initiativen

Es gibt bereits zahlreiche Initiativen, um Frauen in der IT zu fördern. Mentoring-Programme, Schulungen und Stipendien helfen, Frauen den Einstieg zu erleichtern und sie zu vernetzen. Auch Unternehmen selbst können eine entscheidende Rolle spielen, indem sie Maßnahmen zur Förderung der Diversität ergreifen, etwa durch flexible Arbeitsmodelle und Programme zur Vereinbarkeit von Beruf und Familie.

Was kann die Branche tun?

Um die IT-Branche vielfältiger zu gestalten und Chancengleichheit zu fördern, sind meiner Meinung nach gezielte Maßnahmen erforderlich. Diese umfassen:

- Frühzeitige Förderung: Mädchen und junge Frauen (gleichermaßen aber auch junge Männer) sollten bereits in der Schule und im Studium für MINT-Fächer begeistert werden. Schulungen, Praktika und Workshops bieten Einblicke in die spannenden Karrieremöglichkeiten der IT.

- Vorbildfunktion: Erfolgreiche Frauen in der IT sollten sichtbarer gemacht werden. Vorbilder helfen dabei, stereotype Vorstellungen zu überwinden und jungen Frauen zu zeigen, dass sie in der Branche erfolgreich sein können.

- Inklusive Unternehmenskultur: Eine Arbeitskultur, die Vielfalt fördert, ist entscheidend. Flexible Arbeitsmodelle, faire Bezahlung und gezielte Förderprogramme tragen dazu bei, dass sich alle Mitarbeitenden unabhängig von Geschlecht oder Herkunft wohlfühlen.

- Mentoring und Netzwerke: Der Austausch zwischen erfahrenen IT-Fachkräften und Nachwuchstalenten durch Mentoring-Programme und Netzwerke unterstützt Frauen dabei, sich in der Branche zu etablieren und ihre Karrierechancen zu verbessern.

Der Fachkräftemangel in der IT, besonders in der Cyber Security, bleibt ein drängendes Problem. Um dieses zu bewältigen, müssen wir verstärkt auf Diversität und Chancengleichheit setzen. Frauen sind in der IT noch immer unterrepräsentiert, und es liegt in der Verantwortung der gesamten Branche, ein inklusives Umfeld zu schaffen.

Diversität ist nicht nur ein gesellschaftlicher Imperativ, sondern auch ein entscheidender Erfolgsfaktor für Unternehmen. Nur durch vielfältige Teams kann die IT-Branche die Herausforderungen der Zukunft meistern und gleichzeitig die Innovation vorantreiben.

Diversität ist keine Option, sondern eine Notwendigkeit – und die Zeit zu handeln ist jetzt. •

„Wesentlicher Mehrwert für die Diversität im Unternehmen“

Sophia Peterseim, Expertin Interne Revision bei Cancom, über die Rolle als Frau in einem IT-Security-Unternehmen und die Bedeutung von Einfühlungsvermögen und Empathie.

VON HEINER SIEGER

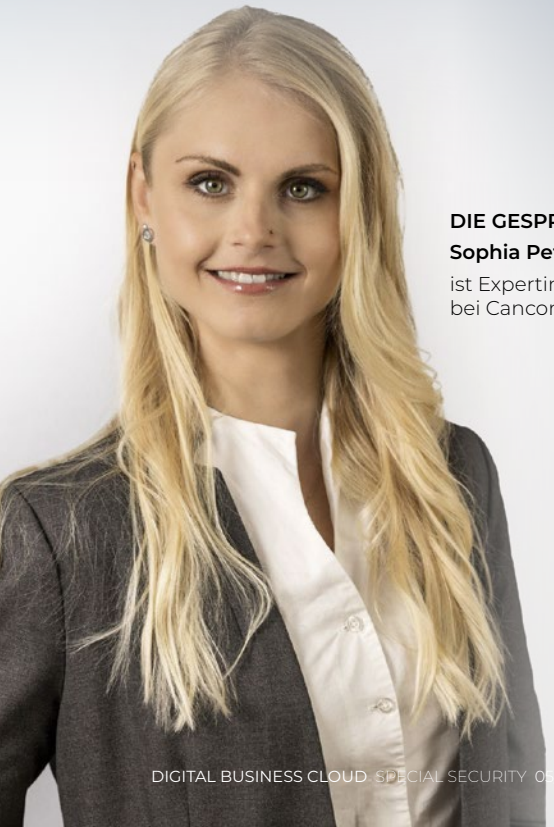
Was genau ist Ihre Aufgabe bei Cancom?
Ich bin seit knapp vier Jahren im Unternehmen, seit ca. drei Jahren arbeite ich in der internen Revision und bin dort für unsere internen Audits zuständig. Dazu führe ich mit den Kolleginnen und Kollegen Interviews, welche sowohl persönlich als auch online stattfinden. Hierbei beleuchte ich gemeinsam mit den Verantwortlichen den aktuellen Ist-Zustand des jeweiligen Bereichs, bezogen auf die existierenden Prozesse sowie Themen bezüglich dem Tool- und Mitarbeitereinsatz. Dabei wird die aktuelle Prozessdokumentation gemeinsam besprochen und wesentliche Prozesse untersucht, ob und wie diese funktionieren. In diesem Zusammenhang identifiziere ich dann den Handlungs- bzw. Optimierungsbedarf.

Wo liegen die Berührungspunkte in Richtung IT und IT-Security?
Im Unternehmen bin ich gestartet im Team Information Security Governance & Compliance (ISGC), welches unsere regulierten Kunden, also die beispielsweise von der BaFin reguliert und überwacht werden, in Bezug auf die Informationssicherheit betreut und berät. Über diese Tätigkeit bin ich zur IT gekommen. Anschließend habe ich mich entlang meiner persönlichen Interessen hin zur internen Revision entwickelt, wo ich heute tätig bin. Für uns als IT-Dienstleister ist dies sehr wichtig, da wir so Compliance gewährleisten, Risiken identifizieren, Prozesse optimieren, IT-Sicherheit überprüfen und Qualitätsstandards sichern.

Was gefällt Ihnen an dieser Aufgabe?
Es war mir ein Anliegen, eine Funktion im Unternehmen auszuüben, in welcher ich dazu beitragen kann, etwas zu verbessern. Die IT ist eine bekanntermaßen sehr dynamische Branche. Damit geht folglich einher, dass sowohl die Anforderungen unserer Kunden als auch unsere Produkte und Dienstleistungen, rechtliche Rahmenbedingungen sowie interne Prozesse einer kontinuierlichen Änderung unterliegen. Nichts ist so beständig wie der Wandel, sagte einst Heraklit. Dadurch ist es erforderlich, sich regelmäßig die existierenden Prozesse und Richtlinien anzusehen und zu evaluieren, ob Anpassungen erforderlich sind. Eine konstruktive, zielführende und offene Kommunikation ist hier von zentraler Bedeutung. Einfühlungsvermögen und Empathie sind äußerst hilfreiche Attribute, welche mir helfen, mich in die Herausforderungen der Kolleginnen und Kollegen hineinzudenken, um gemeinsam Lösungen zu erarbeiten. Mir ist es wichtig, den Weg zur Auflösung der Probleme sauber zu gestalten, um folglich auch den Kolleginnen und Kollegen den Arbeitsalltag zu erleichtern und Mehrwerte für sie zu schaffen.

Wie wichtig ist das Thema IT-Security in Ihrem Unternehmen?
Es ist eines unserer Fokus-Themen und hat bei uns zwei Dimensionen: Einerseits realisieren wir als ein führender IT-Dienstleister in der DACH-Region maßgeschneiderte und ganzheitliche Security-Lösungen und unterstützen unsere Kunden beim sicheren Betrieb ihrer IT-Infrastrukturen – bis hin zur vollständigen Betriebsübernahme. Es ist denke ich hinreichend bekannt, dass die IT-Sicherheitsvorfälle in den unterschiedlichsten Branchen stark zugenommen haben und der Bedarf nach IT-Sicherheitslösungen bei unseren Kunden immer größer wird. Das Thema ist vor allem dann besonders wichtig, wenn Unternehmen mit sensiblen Daten arbeiten. Gerade Banken und Versicherungen werden immer öfter Opfer von Cyberattacken, da können wir sehr gut unterstützen.

Andererseits hat IT-Security auch bei uns intern höchste Priorität, da digitales Vertrauen für uns und unsere Kunden von größter Bedeutung ist. Wie bereits angesprochen, haben wir zahlreiche Kunden im Banken- und Versicherungsumfeld sowie im Bereich öffentlicher Auftraggeber und Healthcare. Aus diesem Grund müssen wir selbst auch



DIE GESPRÄCHSPARTNERIN
Sophia Peterseim
ist Expertin Interne Revision bei Cancom.

ganzheitlich abgesichert sein, interne Schwachstellen minimieren und alle Einfallstore schließen.

Arbeiten noch andere Frauen bei Cancom im Bereich IT oder IT-Security?
Ja bereits einige, aber wir würden gerne noch mehr Frauen für die IT begeistern. Bei uns ist der Quereinstieg ohne weiteres möglich! Es gibt viele spannende Aufgabenbereiche mit und ohne IT-spezifischem Fachwissen. Und Letzteres kann man sich aneignen – unterstützt und geschult vom Arbeitgeber. Viele denken, man braucht Programmierkenntnisse oder muss technischer Spezialist sein, um in der IT zu arbeiten, und das schreckt natürlich ab. Aber es gibt so viel mehr. Besonders Frauen möchten wir ermutigen, den Quereinstieg in die IT zu wagen und neue berufliche Wege zu entdecken. Ich habe beispielsweise eine Berufsausbildung als Kauffrau für Versicherungen und Finanzen abgeschlossen und war im Anschluss für einen Distributor und anschließend für ein Cyberversicherungsunternehmen im Außendienst tätig. Hierbei konnte ich erste Erfahrungen im IT-Security-Bereich sammeln. Und da ich dieses Thema spannend fand, bin ich in die IT gewechselt. Meine bisherigen Erfahrungen habe ich dort sehr gut einbringen und weiter ausbauen können.

Wie konnten Sie sich für die Aufgabe fachlich vorbereiten bzw. aus- und weiterbilden? Ist das besonders schwierig?
Die Aus- und Weiterbildung im Bereich IT-Security ist zwar eine Herausforderung, aber nicht unmöglich. Es war auch für mich als Quereinsteigerin zu Beginn ein neues Themenfeld. Es ist jedoch gut machbar, vor allem, wenn einen das Thema sehr interessiert. Ich habe bei der Deutschen Gesellschaft für Informationssicherheit (DGI) in Berlin den Lehrgang zum Chief Information Security Officer, sowie den Riskmanager absolviert und in Frankfurt zusätzlich den Kurs zum Internal Audit Expert absolviert. Wenn man es können möchte, fleißig und zielstrebig ist, ist das durchaus möglich. Das Interesse am Thema ist eine wichtige Voraussetzung. Auch wenn es sich immer noch um eine Männerdomäne handelt, sollten Frauen sich nicht scheuen, diesen Berufsweg zu wählen. Einer erfolgreichen Karriere in diesem Berufsfeld steht nichts im Wege – man muss es nur machen.

Frauen sind in der IT-Security stark unterrepräsentiert. Wie könnte sich das ändern?
Mit dem Mut, sich auch neuen Dingen zuzuwenden. Aus Unternehmenssicht ist es wichtig, großen Wert auf die Ansprache und Unterstützung von jungen Menschen und Berufsanfängerinnen und -anfängern zu legen. Zum Beispiel sollte auf Berufs-Messen und in Schulen ein noch größerer Wert darauf gelegt werden, jungen Menschen und speziell jungen Frauen, schon früh mehr Informationen zu diesem spannenden Berufsfeld zu geben. Das kann dann das Interesse wecken und Frauen anregen, sich diesem Bereich zuzuwenden. Es geht letztendlich um das Interesse am Tätigkeitsfeld und das Fachwissen, welches man sich aneignen kann, wie in anderen Bereichen auch. Auch eine verstärkte Sichtbarkeit von Frauen, die bereits in der IT-Security tätig sind, kann dies unterstützen. Daher habe ich auch sehr gerne dieses Gespräch mit Ihnen geführt. •

Viele denken, man braucht Programmierkenntnisse oder muss technischer Spezialist sein, um in der IT zu arbeiten, und das schreckt natürlich ab. **Aber es gibt so viel mehr.** Besonders Frauen möchten wir ermutigen, den Quereinstieg in die IT zu wagen und neue berufliche Wege zu entdecken.

Cloud-Strategien gegen Cybergefahren

Technologische Souveränität ist das Rückgrat einer modernen, wettbewerbsfähigen Wirtschaft. Sie gewährleistet die Sicherheit und Resilienz von IT-Systemen, die für die digitale Infrastruktur unerlässlich sind. Technologien „Made in Germany" spielen eine zentrale Rolle und stärken die technologische Unabhängigkeit Europas.

VON ARI ALBERTINI

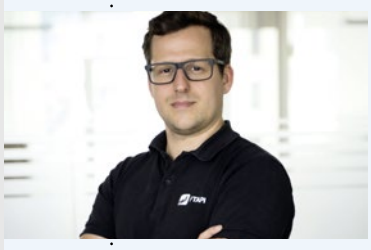
DIE EU HAT ERKANNT, dass technologische Souveränität entscheidend für die Zukunft Europas ist. Ein zentraler Baustein ist die NIS-2-Richtlinie, die bis Oktober 2024 in nationales Recht umgesetzt werden muss. Ziel ist es, ein einheitlich hohes Sicherheitsniveau in der gesamten EU zu gewährleisten und die Widerstandsfähigkeit der Mitgliedstaaten gegen Cyberangriffe zu erhöhen.

Cloud-Computing spielt eine zentrale Rolle in der Digitalisierung und bietet skalierbare IT-Ressourcen für Wirtschaft und öffentliche Verwaltung. Europäische Cloud-Lösungen sind besonders wichtig, um die technologische Souveränität zu stärken und die Abhängigkeit von außereuropäischen Anbietern zu verringern. Sie bieten nicht nur technologisch fortschrittliche Lösungen, sondern erfüllen auch die hohen Datenschutz- und Sicherheitsstandards, die in Europa gelten.

Vorteile für die Systemsicherheit

Cloud-Technologien bieten zahlreiche Vorteile für die IT-Sicherheit:

- Skalierbarkeit und Flexibilität: Unternehmen können ihre IT-Ressourcen flexibel und bedarfsgerecht skalieren. Dies ist besonders wichtig, um auf dynamische Bedrohungslagen schnell reagieren zu können.
- Zentralisierte Sicherheitsmaßnahmen: Cloud-Anbieter investieren erheblich in die Sicherheit ihrer Infrastrukturen. Dazu gehören fortschrittliche Verschlüsselungstechniken, kontinuierliche Überwachung und regelmäßige Sicherheits-Updates, die oft über das hinausgehen, was im On-Premise-Betrieb möglich ist.
- Erhöhte Cyberresilienz: Durch die Nutzung von Cloud-Diensten können Unternehmen ihre Resilienz gegenüber Cyberangriffen erhöhen. Cloud-Anbieter verfügen über umfangreiche Ressourcen und Fachwissen, um schnell auf Sicherheitsvorfälle zu reagieren und die Auswirkungen auf die Nutzer zu minimieren.



DER AUTOR
Ari Albertini ist CEO von FTAPI.

Resilienz durch Cloud-Lösungen

Cyberresilienz beschreibt die Fähigkeit, schnell und effektiv auf Cybervorfälle zu reagieren und die Betriebsfähigkeit aufrechtzuerhalten. Cloud-Lösungen ermöglichen es, auf skalierbare Sicherheitsressourcen zurückzugreifen. Die zentrale Verwaltung und die fortlaufende Aktualisierung der Sicherheitsmaßnahmen durch Cloud-Anbieter stellen sicher, dass Unternehmen stets gegen die neuesten Bedrohungen gewappnet sind. Außerdem können Cloud-Dienste die Wiederherstellungszeit nach einem Vorfall durch automatisierte Backup- und Wiederherstellungsprozesse erheblich verkürzen.

Fazit

Europäische Lösungen und Cloud-Technologien sind Schlüsselkomponenten für die technologische Souveränität und Sicherheit Europas. Durch die NIS-2-Richtlinie werden höhere Cybersicherheitsstandards etabliert, die Unternehmen und öffentliche Einrichtungen gleichermaßen betreffen. Die Vorteile der Cloud, wie Skalierbarkeit, zentrale Sicherheitsmaßnahmen und erhöhte Resilienz, tragen maßgeblich dazu bei, diese Standards zu erfüllen. Gleichzeitig wird die Unabhängigkeit von außereuropäischen Anbietern gestärkt. Indem Europa in Cloud-Lösungen und technologische Unabhängigkeit investiert, sichert es nicht nur seine digitale Zukunft, sondern schafft auch eine robuste Basis gegen wachsende Cyberbedrohungen. •

NIS2 im Fokus:

Was KRITIS-Betreiber wissen müssen

Marco Eggerling,
Global CISO bei Check Point Software Technologies GmbH

DIE GRUNDLAGE DES ÖFFENTLICHEN LEBENS sind Kritische Infrastrukturen (KRITIS). Sauberes Trinkwasser, volle Supermarktregale, medizinische Versorgung, Personentransport, Müllabfuhr und Energiegewinnung sind gekoppelt an die Sicherheit von KRITIS-Betreibern. Sie alle stehen unter dem Dauerfeuer von Hacker-Angriffen, denn die wichtigsten Versorgungsunternehmen verfügen über wertvolle Daten und sind deshalb immer wieder Ziel von Sabotage und Ransomware-Attacken.

Die EU hat gegen diese Bedrohung die NIS2-Richtlinie verabschiedet, die KRITIS-Betreiber der Mitgliedsländer auf ein höheres IT-Sicherheitsniveau hieven soll. Im Oktober 2024 wird NIS2 hierzulande in nationales Recht überführt. Ein Blick auf die Kernaspekte von NIS2 zeigt, was IT-Entscheider auf dem Zettel haben müssen.

Wen NIS2 betrifft – Drei Kenngrößen entscheiden im Wesentlichen darüber, ob man zu KRITIS zählt: Sektor-Zugehörigkeit, Mitarbeiterzahl und Jahresumsatz, oder Jahresbilanz-Summe. Diese Einstufungen bestimmen den Umfang der erforderlichen Cyber-Sicherheitsmaßnahmen und Meldepflichten. Betroffen sind aber nicht nur Konzerne, sondern auch Kleine und Mittlere Unternehmen (KMU), die in kritischen Sektoren tätig sind.

Risikomanagement und Sicherheitsmaßnahmen – Wen NIS2 betrifft, der muss umfassende Risikomanagement-Maßnahmen ergreifen. NIS2 verlangt den Einsatz moderner IT-Technologien und -Konzepte wie Zero Trust, Netzwerksegmentierung, MFA, Datensicherung und fortschrittliche Firewalls, um auch gegen unbekannte Bedrohungen geschützt zu sein.

Verantwortung der Führungskräfte – Ein zentraler Aspekt der NIS2 ist die Verantwortung der Unternehmensleitung. Führungskräfte müssen sicherstellen, dass Cyber-Sicherheitsstrategien entwickelt, umgesetzt und regelmäßig geprüft werden. Zudem müssen sie gewährleisten, dass im Falle eines Sicherheitsvorfalls alle betroffenen Parteien, einschließlich der zuständigen Behörden, innerhalb von 24 Stunden informiert werden.

Lieferketten und externe Unterstützung – Ein weiteres Kernelement ist die Überwachung der Lieferkette. Unternehmen müssen sicherstellen, dass auch Dienstleister und Zulieferer die Cyber-Sicherheitsstandards einhalten. Dies kann durch die Einbindung von Managed Security Service Provider (MSSP) geschehen, um die hauseigenen IT-Teams zu entlasten.

Sanktionen und Haftung – Versäumnisse bei der Einhaltung der NIS2 können schwerwiegende Konsequenzen haben. Unternehmen, welche die Anforderungen nicht erfüllen, drohen Bußgelder von bis zu 10 Millionen Euro oder zwei Prozent des weltweiten Jahresumsatzes. Zudem können Führungskräfte persönlich haftbar gemacht werden, wenn sie ihre Sorgfaltspflichten vernachlässigen.

Langfristige Compliance – Die NIS2-Konformität ist eine kontinuierliche Aufgabe. Ab 2028 müssen Unternehmen jährlich nachweisen, dass sie alle erforderlichen technischen, organisatorischen und operativen Maßnahmen getroffen haben, um den aktuellen Stand der Technik einzuhalten. Diese langfristige Perspektive soll sicherstellen, dass Unternehmen dauerhaft gegen Cyber-Bedrohungen gewappnet sind.

KRITIS-Betreiber müssen Vorreiter sein

Cyber-Angriffe werden in absehbarer Zeit nicht abflauen. Die Frage, ob man in Sachen IT-Sicherheit aufrüsten sollte oder es einfach riskiert, stellt sich daher nicht mehr. Es kann jeden treffen und Investitionen in die eigene Sicherheit werden sich immer auszahlen. Kundenbeziehungen, wichtige Daten, die eigene unternehmerische Reputation und Existenz sowie das öffentliche Leben sind in Gefahr, wenn KRITIS-Betreiber nicht auch Vorreiter der IT-Sicherheit sind. •

Schatten-IT – das unterschätzte Risiko

Die Grenzen zwischen privater und beruflicher Nutzung mobiler IT-Geräte verschwimmen, aber auch die Nutzung unautorisierter generativer KI- oder cloudbasierter Anwendungen nimmt weiter zu. IT-Teams müssen sich eine klare Strategie überlegen, wie sie die Herausforderung dieser Schatten-IT in ihren Unternehmen in den Griff bekommen.

VON WILLIAM FENDT

SCHATTEN-IT IST MEIST WENIGER ein eigenständiges Problem als vielmehr ein Symptom für generelle organisatorische Schwierigkeiten im IT-Bereich. Oft greifen Nutzer oder ganze Abteilungen auf alternative Lösungen zurück, weil etwa der interne IT-Support bei IT-Problemen nicht schnell genug reagieren kann, aber Abgabefristen nicht verschoben werden können. Die daraus resultierenden unkontrollierten IT-Prozesse schaffen Sicherheitslücken, die Cyberkriminelle ausnutzen können, wodurch das Risiko von Mal- und Ransomware-Angriffen steigt.

Schatten-IT wird immer komplexer und die Risiken höher

Die Kontrolle von IT-Ressourcen wird durch Schatten-IT erheblich komplexer, da diese nicht in zentrale Sicherheitskonzepte integriert sind. Das erschwert IT-Teams eine proaktive Sicherheitsüberwachung im Netzwerk und kann im Falle eines Sicherheitsvorfalls das Vertrauen von Kunden und Partnern sowie den Ruf des Unternehmens nachhaltig schädigen. Damit einher gehen auch Compliance-Verstöße, die zusätzlich rechtliche und finanzielle Konsequenzen für das Unternehmen nach sich ziehen können. Untersuchungen zeigen immer wieder, dass IT-Abteilungen den Anteil von Schatten-Anwendungen in ihren Netzwerken regelmäßig unterschätzen und Discovery-Checks offenbaren oft schwerwiegende Sicherheitslücken, die durch die Installation von Drittanbieter-Apps und deren unautorisierten Zugriff auf sensible Daten entstehen.

Gegenmittel: Klare Strategie und effektive Tools

Die wirksame Bekämpfung von Schatten-IT erfordert eine klare Strategie, die präventive Maßnahmen und schnelle Reaktionspläne umfasst. Tools wie Software Asset Management (SAM), Enterprise Mobility Management (EMM) und Unified Endpoint Management (UEM) spielen dabei eine zentrale Rolle. Diese Systeme schaffen umfassende Transparenz über die IT-Infrastruktur und ermöglichen es, unautorisierte Anwendungen und Geräte automatisiert zuverlässig zu identifizieren – sie helfen dem IT-Team so, die Nutzung schlecht konfigurierter Hardware, ungepatchter Software oder unautorisierter Cloud-Speicher-Anwendungen im Arbeitsalltag zu verhindern.

SAM stellt zum Beispiel sicher, dass wirklich nur lizenzierte Software im Unternehmensnetzwerk eingesetzt wird, während EMM und UEM die Verwaltung und Sicherheit mobiler Geräte und Endpunkte gewährleisten. Unternehmen können durch den Einsatz solcher Tools viele Einfallstore effizient schließen.

Keine Nebenrolle: Der menschliche Faktor

Neben technischen Lösungen ist aber auch die Schulung der Belegschaft entscheidend, um Schatten-IT effektiv zu bekämpfen. Klare Richtlinien sind unerlässlich, um das Bewusstsein für die Risiken der Nutzung unautorisierter Software und Apps zu schärfen – IT-Teams müssen mithelfen, dass ihre Kollegen verstehen, dass die Verwendung solcher Anwendungen die Sicherheit ihres Unternehmens gefährdet. Ein strategischer Ansatz, der Schatten-IT im Unternehmen effizient in den Griff bekommen will, stützt sich auf drei Säulen: Automatisierte Erfassung verwendeter Anwendungen im Netzwerk, Vorauswahl sicherer Software in Kombination mit Self-Service-Angeboten, um die Bedürfnisse der User zu erfüllen, sowie Aufklärung der Angestellten über die Risiken. So kann langfristig der Sumpf der Schatten-IT ausgetrocknet und die IT-Sicherheit im Unternehmen nachhaltig verbessert werden. •

DER AUTOR
William Fendt
ist Senior Product Manager bei baramundi Software.

Mehr Sicherheit für die Cloud

Es ist sinnvoll, einen Penetrations-Test einer Cloud-Umgebung mit einem interviewbasierten Security Assessment zu verbinden. So bekommt man einen Überblick über die Sicherheit der Cloud-Infrastruktur.

VON DANIEL HANKE

CLOUD-UMGEBUNGEN SIND HEUTE EIN ZENTRALER BESTANDTEIL der IT-Infrastruktur vieler Unternehmen. Sie bieten zahlreiche Vorteile wie Flexibilität, Skalierbarkeit und Kosteneffizienz. Doch mit diesen Vorteilen gehen auch erhöhte Sicherheitsanforderungen einher. Um die Sicherheit einer Cloud-Umgebung umfassend zu gewährleisten, ist es sinnvoll, einen Penetrations-Test mit einem interviewbasierten Security Assessment zu kombinieren. Diese Kombination bietet eine tiefgehende und umfassende Sicherheitsbewertung, die sowohl technische als auch organisatorische Aspekte abdeckt.

Ganzheitliche Risikobewertung

Ein Penetrations-Test hilft dabei, Schwachstellen der Cloud-Infrastruktur zu identifizieren, die von Angreifern ausgenutzt werden könnten. Während diese Penetrations-Tests technische Schwächen effektiv aufdecken, berücksichtigen sie aber nicht alle möglichen Risiken. Ein interviewbasiertes Security Assessment ergänzt diese Tests, indem es auch organisatorische und menschliche Faktoren untersucht. Durch Interviews mit Schlüsselpersonen im Unternehmen werden potenzielle Risiken ermittelt, die aus fehlerhaften Prozessen oder mangelnder Sicherheitskultur resultieren könnten. Zum Beispiel könnten unzureichende Schulungen zu erhöhten Risiken etwa durch Phishing-Angriffe führen, die durch technische Tests allein nicht erfasst werden.

Priorisierung von Maßnahmen

Die Ergebnisse eines Penetrations-Tests enthalten meist eine umfangreiche Liste von technischen Schwachstellen, die behoben werden müssen. Ein interviewbasiertes Security Assessment ermöglicht es, diese Ergebnisse in einen breiteren Kontext zu setzen. Durch gezielte Interviews können Risiken und ihre potenziellen Auswirkungen auf das Geschäft genauer verstanden und priorisiert werden. Dadurch wird eine gezielte und effektive Umsetzung von Sicherheitsmaßnahmen ermöglicht, die speziell auf die Bedrohungen des Unternehmens zugeschnitten sind.

Verbesserung der Sicherheitskultur

Die Sicherheit in einem Unternehmen wird durch verschiedene Faktoren beeinflusst, darunter technische, prozessuale und kulturelle Aspekte. Um ein umfassendes Sicherheitsbewusstsein zu schaffen, ist es wichtig, die Mitarbeiter in den Bewertungsprozess einzubeziehen. Ein interviewbasiertes Assessment kann dazu beitragen, Sicherheitslücken in allen Bereichen aufzudecken und eine Sicherheitskultur zu fördern, die über rein technische Maßnahmen hinausgeht.

Nachhaltige Sicherheits-Strategien

Mit diesem integrativen Ansatz helfen auf IT-Security spezialisierte Dienstleister Unternehmen, nachhaltige Sicherheitsstrategien zu entwickeln. Durch die Kombination technischer Tests mit organisatorischen Bewertungen können langfristige Sicherheitsmaßnahmen implementiert werden, die sowohl aktuelle als auch zukünftige Bedrohungen adressieren. Dies führt zu einer kontinuierlichen Verbesserung der Sicherheitslage und einer stärkeren Resilienz gegenüber Cyberangriffen. Heute, aber auch in Zukunft. •

DER AUTOR
Daniel Hanke
ist Practice Leader Application & Infrastructure Testing bei TÜV Rheinland i-sec.

KI revolutioniert die Cybersecurity

Die Integration von künstlicher Intelligenz hat die IT-Sicherheits-Landschaft grundlegend verändert. Unternehmen stehen komplexeren Bedrohungen gegenüber, die traditionelle Systeme oft nicht mehr abwehren können. Gleichzeitig ermöglicht KI eine schnellere und genauere Erkennung sowie eine proaktive Reaktion auf Sicherheitsvorfälle.

VON DANIEL EBERHORN

AUFSEITEN DER CYBERSECURITY haben KI-Technologien das Potenzial, herkömmliche Abwehrmaßnahmen wirkungslos erscheinen zu lassen. Die präzise Anomalie-Erkennung durch künstliche Intelligenz minimiert die Anzahl von Fehlalarmen und steigert die Qualität der Erkennungen exponentiell. Mit Algorithmen zur Mustererkennung kann die KI verdächtige Aktivitäten identifizieren, die für menschliche Analysten oder herkömmliche Sicherheits-Tools unsichtbar bleiben würden.

Beispielsweise kann ein KI-System ungewöhnliche Datenübertragungen oder unautorisierte Zugriffsversuche sofort erkennen und melden. Dies ermöglicht es Unternehmen, schneller auf potenzielle Bedrohungen zu reagieren, bevor sie zu ernsthaften Sicherheitsvorfällen eskalieren.

KI klassifiziert und priorisiert

In der aktuellen Wirtschaftssituation spielen Effizienz und Kosteneinsparungen eine zentrale Rolle. Durch den Einsatz von künstlicher Intelligenz können Security-Teams Fehlalarme um bis zu 75 Prozent reduzieren und die Reaktionszeit auf kritische Alarme um bis zu 50 Prozent verkürzen. KI automatisiert die Klassifizierung und Priorisierung von Ereignissen, filtert weniger relevante oder falsch-positive Warnungen heraus und identifiziert echte Bedrohungen schneller.

Dadurch bietet künstliche Intelligenz nicht nur eine effiziente Lösung für das Management großer Datenmengen, sondern trägt auch dazu bei, dem Fachkräftemangel entgegenzuwirken. Routineaufgaben werden automatisiert, die IT-Abteilung wird entlastet und Mitarbeiter können sich gezielt auf kritische Sicherheitsvorfälle konzentrieren.

Die Kehrseite: KI in den Händen Krimineller

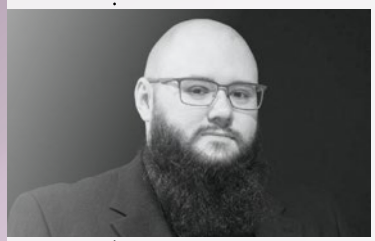
Während künstliche Intelligenz die Abwehr gegen Cyberbedrohungen verbessert, setzen auch Cyberkriminelle diese Technologie ein, um ihre Angriffe präziser und effektiver zu gestalten. Der Bereich der Phishing-Angriffe hat dadurch eine neue Dimension erreicht: KI-gestützte Algorithmen analysieren große Mengen an Daten, um hochgradig personalisierte und überzeugende Phishing-E-Mails zu erstellen. Diese E-Mails sind oft so gut gemacht, dass selbst geschulte Mitarbeiter Schwierigkeiten haben, sie als betrügerisch zu erkennen.

Zuletzt haben sich vermehrt sogenannte Deepfakes verbreitet: Diese Technologie ermöglicht es, Videos und Audioaufnahmen so zu manipulieren, dass Personen scheinbar Dinge sagen oder tun, die sie in Wirklichkeit nie gesagt oder getan haben. Deepfakes eignen sich somit für eine Reihe böswilliger Anwendungen wie die gezielte Verbreitung von Falschinformationen, Identitätsdiebstahl oder CEO-Fraud.

Innovation ermöglichen, Risiken minimieren

Die rechtlichen Rahmenbedingungen zur KI-Sicherheit wurden im Mai 2024 von der EU verabschiedet. Der AI Act der Europäischen Union stellt das weltweit erste umfassende Regelwerk dar, das den Einsatz von künstlicher Intelligenz reguliert. Generell gilt es, Innovation zu fördern und gleichzeitig Risiken zu minimieren. Während KI enorme Vorteile für die Effizienz und Effektivität von Sicherheitsoperationen bietet, erfordert sie auch Vorsicht und Verantwortung – sowohl bei der Anwendung von KI als auch bei der Entwicklung neuer KI-Modelle.

Die Schulung von Mitarbeitern im Umgang mit künstlicher Intelligenz ist unerlässlich, da neben IT-Sicherheitsaspekten auch datenschutzrechtliche Herausforderunge bestehen. •



DER AUTOR
Daniel Eberhorn
ist Lead Architect Cyber Security beim Bechtle IT-Systemhaus Würzburg.

Cyber-Security - ein Drama in fünf Akten

Viele Unternehmen gehen im Jahr 2025 von einem Paradigmenwechsel für die IT-Security aus. Eine Herkulesaufgabe für die Verantwortlichen. Die Strategie „vereinheitlichen, standardisieren, automatisieren“ kristallisiert bestimmt die Marschrichtung. Ohne XDR als umfassende Sicherheitslösung kaum möglich. Warum das klassische SOC wie wir es kennen, ausstirbt.

VON SVEN HILLEBRECHT

Ist die Gefahr allgegenwärtig?
Verantwortliche Akteure werden durch die steigende Anzahl von Cyberangriffen vor immer größere Herausforderungen gestellt. Gleichzeitig sehen sich die wenigsten Firmen auf diesen Paradigmenwechsel vorbereitet. Das erfordert eine Neuausrichtung der bisherigen IT-Sicherheitskonzepte. Geschäftsführung und Security-Verantwortliche sind gemeinsam gefordert die Herkulesaufgabe zu meistern.

Ein K.O.stenkriterium?
Nach wie vor liegt ein hoher Kostendruck auf den Firmen und gleichzeitig besteht ein enormer Bedarf an IT-Sicherheitsexperten. Die schiere Masse an Vorfällen und komplexe hybride Sicherheitsarchitekturen (mobile Endgeräte und Cloud-Lösungen eingeschlossen) überfordern zunehmend. Versäumnisse wie die Weiterentwicklung von modernen Infrastrukturen, Fortbildung der Verantwortlichen und die Sensibilisierung der ganzen Belegschaft zeigen sich nun in ganzem Ausmaß. Bestehende Sicherheitskonzepte sind intransparent, schlecht skalierbar und abhängig von menschlicher Performance.

Vereinheitlichen, standardisieren, automatisieren?
Der strategische IT-Ansatz „vereinheitlichen, standardisieren, automatisieren“ kristallisiert sich als Wendepunkt für die IT-Security. Was in der gesamten IT bereits transformiert wurde, ist im Bereich IT-Security überfällig. In den Vordergrund wird nicht mehr nur die Reaktion durch den Menschen gestellt, sondern eine Automatisierung, die rund um die Uhr greift und lernt. Incident Management als reaktives Werkzeug verschmilzt mit Business Continuity Management und wird so durch definierte Prozesse, smarte Übungen und pragmatische Methoden angereichert.

Warum nutzen so wenige Firmen die neuen Möglichkeiten von SOC?
Extended Detection & Response (XDR) als zeitgemäßer Ansatz beschreibt eine kontinuierliche Überwachung, Analysen, Reaktion und Prävention. Er erfasst und korreliert Daten automatisch auf mehreren Sicherheitsebenen – E-Mail, Endpunkt, Server, Cloud-Workload und Netzwerk. Dies ermöglicht eine schnellere Erkennung von Bedrohungen und verbesserte Untersuchungs- und Reaktionszeiten durch Sicherheitsanalysen. Zusätzlich werden präventive Maßnahmen vorgeschlagen, die eine mögliche Angriffsfläche von vorneherein verringern.

Wie halten Firmen den Fokus aufrecht?
Unternehmen sind gut beraten, ihr klassisches SOC zu einer modernen XDR-Lösung auszubauen. Durch ein strategisches Outsourcing werden Kräfte im Bereich Security weiter gebündelt und der Fokus auf Security als Hauptaufgabe sichergestellt. Abhängigkeit von Ressourcen, menschlicher Alarmmüdigkeit, fehlendem Knowhow oder gar fehlendem Fokus werden vermieden. Mit Managed Security sind die Anforderungen an einheitliche und transparente Prozesse genauso unterstützt wie notwendige Dokumentationspflichten. Davon profitiert unternehmerische Verantwortung, BCM/ISM, ISO und Stakeholder wie Gesellschafter oder Cyberversicherer. Es lohnt sich historisch gewachsene SOC-Strukturen aufzubrechen und die Möglichkeiten umfassender Sicherheitslösungen zu nutzen. •

DER AUTOR
Sven Hillebrecht
ist General Manager des IT-Beratungsunternehmens Adlon.

Ein Lehrstück für die Branche

Ein IT-Ausfall im Juli 2024 brachte weltweit Systeme zum Stillstand. Flieger blieben am Boden, der Zahlungsverkehr geriet ins Stocken, Züge fielen aus. Ein einziges fehlerhaftes Software-Update zeigt die Schwächen unserer digitalen Abhängigkeit. Warum dieser Vorfall mehr als nur ein Betriebsunfall ist.

VON KLAUS JETTER

ES WAR EIN MOMENT DES KOLLEKTIVEN AUFATMENS, als die Systeme nach dem fatalen IT-Ausfall wieder zum Leben erwachten. Was jedoch bleibt, ist die Erkenntnis: Ein einzelner Fehler kann ganze Unternehmen lahmlegen. Ein unscheinbares Update der Sicherheits-Software von CrowdStrike entpuppte sich in der Praxis als Desaster. Doch wie konnte es überhaupt so weit kommen? Der Fehler lag nicht nur in der Qualitätssicherung, sondern auch in der Art und Weise, wie Updates implementiert werden. Ein schrittweiser Roll-out, bei dem nur eine kleine Gruppe von Systemen aktualisiert wird, hätte den Schaden begrenzen können.

IT-Security-Software sicher ausrollen

Trotz des Vorfalls ist klar: Cybersicherheits-Software ist unerlässlich. Die Bedrohung durch Cyberangriffe ist real und nimmt stetig zu. Der Schlüssel liegt in einer besseren Verwaltung dieser Tools, um solche Vorfälle zu vermeiden. Was können Unternehmen also tun, um Update-Probleme zu vermeiden? Zunächst gilt es, in enger Partnerschaft mit dem Anbieter die Prozesse unter die Lupe zu nehmen:

1. Validieren Sie die Qualitätssicherungsverfahren für Updates und stellen Sie sicher, dass Ihr Anbieter sowohl automatisierte als auch manuelle Software-Tests verwendet. Zudem sollten Kompatibilitätstests mit anderen gängigen Software- und Systemkonfigurationen durchgeführt werden.
2. Überprüfen Sie, ob der Anbieter eine schrittweise Roll-out-Methode verwendet, um das Risiko zu minimieren.
3. Stellen Sie sicher, dass Anbieter-Updates nur während der regulären Support-Zeiten und nicht vor Wochenenden oder Feiertagen erfolgen.

DER AUTOR
Klaus Jetter
ist DACH-Chef von WithSecure.

Wenn ein Unternehmen über ausreichende Kapazitäten verfügt, dann können folgende Maßnahmen das Risiko von Software-Update-Problemen weiter reduzieren:

1. Bevor Sie Updates in Ihrem gesamten Netzwerk bereitstellen, testen Sie diese in einer kontrollierten Umgebung.
2. Ähnlich wie der Anbieter sollten Sie den Roll-out mit einer kleinen Gruppe von Systemen beginnen, bevor Sie das gesamte Netzwerk aktualisieren.
3. Führen Sie Updates zu Zeiten mit einer geringen Systemnutzung durch, um Störungen zu minimieren und sicherzustellen, dass Ihr IT-Personal bei Problemen verfügbar ist.
4. Sichern Sie kritische Systeme und Daten vor dem Ausrollen des Updates, um bei einem updatebedingten Ausfall diese schnell wiederherzustellen.

Monopole und ihre Gefahren

Der CrowdStrike-Vorfall ist nicht isoliert zu betrachten. Er spiegelt ein systemisches Problem wider: Die Abhängigkeit von wenigen großen Anbietern. Auch Microsofts dominante Stellung im Bereich der Betriebssysteme und Sicherheits-Software ist hier ein zweischneidiges Schwert. Auf der einen Seite bieten integrierte Systeme Effizienzvorteile, auf der anderen Seite bergen sie das Risiko, dass ein einzelner Fehler weitreichende Konsequenzen hat.

Die EU hat mit dem Digital Markets Act einen Rahmen geschaffen, der solche Monopolstellungen kritisch hinterfragt. Microsoft wurde als „Gatekeeper“ identifiziert, eine Rolle, die mit besonderen Verpflichtungen einhergeht. •

Wie Unternehmen durch Daten-Resilienz den IT-Bedrohungen trotzen können

Von Sebastian Lacour,
Senior Manager Channels Germany
bei Veeam

DIE BEDROHUNG DURCH RANSOMWARE-ANGRIFFE nimmt stetig zu. Das bestätigen Berichte wie der Veeam Ransomware Trends Report 2024. Er verdeutlicht, dass fast die Hälfte aller Unternehmensdaten betroffen sind, was zu erheblichen Datenverlusten führt und die Notwendigkeit einer soliden Daten-Resilienz-Strategie unterstreicht. Unternehmen stehen vor der Herausforderung, nicht nur auf Angriffe zu reagieren, sondern diese proaktiv abzuwehren.

Moderne Technologie strategisch nutzen

In der digitalen Landschaft spielen Technologien wie künstliche Intelligenz (KI), Cloud Computing und Automatisierung eine Schlüsselrolle. Sie bieten enorme Vorteile, bergen aber auch potenzielle Risiken. Organisationen sollten daher berücksichtigen, dass sie nicht nur die Effizienzvorteile dieser Technologien nutzen, sondern auch die Sicherheit, Verfügbarkeit und Integrität ihrer Daten weiterhin gewährleisten. Ein strukturierter Ansatz zur Verwaltung und Überwachung moderner Technologien ist unerlässlich geworden, um Sicherheitslücken frühzeitig zu erkennen und zu schließen. Doch wie gestaltet ein Unternehmen eine sinnvolle Strategie?

Die fünf Säulen der Daten-Resilienz

Eine erfolgreiche Strategie basiert auf fünf zentralen Prinzipien:

1. Datensicherung: Regelmäßige, unveränderliche Backups sind notwendig, um die Verfügbarkeit von Daten im Falle eines Angriffs sicherzustellen.
2. Wiederherstellung: Schnelle Wiederherstellungsprozesse minimieren Ausfallzeiten und ermöglichen eine rasche Wiederaufnahme des Geschäftsbetriebs.
3. Datenfreiheit: Unabhängig davon, ob die Daten in der Cloud oder lokal gespeichert sind, müssen sie jederzeit sicher und verfügbar sein.
4. Sicherheit: Moderne Sicherheitslösungen, wie Firewalls und Anti-Viren-Software, sind die erste Verteidigungslinie gegen Cyber-Bedrohungen. Backup und Recovery sind dagegen die letzte und beste Linie.
5. Datenintelligenz: Durch den Einsatz von KI können Unternehmen wichtige Einblicke in ihre IT-Umgebung gewinnen und Bedrohungen, wie Malware oder Ransomware, frühzeitig erkennen und stoppen, bevor diese größeren Schaden anrichten.

Die Bedeutung von Kommunikation für Daten-Resilienz

Technologie allein reicht nicht aus, um Daten effektiv zu schützen. Entscheidend für den Erfolg ist die Zusammenarbeit zwischen den IT-Abteilungen und der Unternehmensleitung. Häufig mangelt es an einer klaren Kommunikation über die Risiken und den geschäftlichen Nutzen von Datensicherheit. IT-Teams müssen daher in der Lage sein, den wirtschaftlichen Nutzen einer robusten Datenschutzstrategie verständlich zu vermitteln, um die notwendige Unterstützung und Budget zu erhalten. Gleichzeitig muss das Management erkennen, dass Investitionen in Datensicherheit langfristig die Kosten senken und das Unternehmen nachhaltig schützen.

Fazit

Unternehmen müssen präventiv handeln und dürfen nicht bloß auf Bedrohungen reagieren. Der Aufbau einer umfassenden Daten-Resilienz als Konzept erfordert Planung, regelmäßige Tests und die Schulung der Mitarbeiter. Dies ist keine einmalige Aufgabe, sondern ein kontinuierlicher Prozess, der Unternehmen auf Bedrohungen vorbereitet und Resilienz aufbaut. Wer rechtzeitig handelt, kann nicht nur Ausfallzeiten minimieren, sondern auch das Vertrauen seiner Kunden sichern und die Wettbewerbsfähigkeit steigern. Daten-Resilienz ist somit nicht nur eine technische Notwendigkeit, sondern ein strategischer Vorteil, der über Erfolg oder Misserfolg eines Unternehmens entscheiden kann. •

Wie Zero Trust Innovationen schützt

Netzwerk- und Security-Teams müssen heute an einem Strang ziehen, um die effektive Kontrolle und Transparenz aller Datenströme von Unternehmen zu erzielen. Das weltweit tätige Toyota Gazoo Racing World Rally Team setzt auf eine moderne Sicherheitsarchitektur auf Basis von Zero Trust zum Schutz der sensiblen Daten wie auch der Mitarbeiter.

VON PAUL HENNIN

WER SICH MIT ZERO TRUST BESCHÄFTIGT HAT, weiß, dass es sich dabei nicht um einen punktuellen Ansatz, sondern eine moderne Sicherheitsarchitektur handelt, die Fachabteilungen sowie Verantwortliche für Netzwerk- und Sicherheit gemeinsam erarbeiten. Zero Trust stellt die Basis für das Monitoring aller Datenströme als integrierten Ansatz bereit. Im Unterschied zu Netzwerksicherheit am Perimeter werden bei Zero Trust Nutzer und Anwendungen nicht von vornherein als vertrauenswürdig eingestuft. Vertrauen und damit der Zugriff auf Daten und Anwendungen werden erst dann ermöglicht, wenn die Identität des Users und der Kontext von einem Security Broker verifiziert und die sichere Verbindung auf Basis von Richtlinien durchgesetzt ist.

Auf dem Weg zur Implementierung einer Zero-Trust-Architektur müssen IT-Abteilungen einige Schritte berücksichtigen. Mit der Umsetzung eines Einführungsprozesses unterliegen alle digitalen Komponenten eines Unternehmens wie Nutzerzugänge, Endgeräte und IoT- und OT-Geräte sowie Workloads in der Cloud den gleichen granularen Kontrollmechanismen. Zur Umsetzung einer Zero-Trust-Architektur gilt es, die folgenden Schritte abzubilden: Verifizierung von Identität und Kontext, Kontrolle von Inhalt und Zugriff, Umsetzung von Richtlinien.

Zero Trust in sieben Schritten

Bei einer Zero-Trust-Architektur kappt wird im ersten Schritt die Verbindungsanfrage überprüft und dazu werden Identität und Kontext aufbauend auf den W-Fragen „wer", „was" und „wo" eines Zugriffsversuchs untersucht. Jedes Element in diesem Prozess leitet zum nächsten Schritt über und erstellt so einen dynamischen Entscheidungsablauf für jede Anfrage. Für jede Verbindung werden die Identität, das Risiko des Users und der Webseite, die Sicherheitslage und Inhalte als Entscheidungskriterien herangezogen und dann entschieden, ob die Verbindung hergestellt wird.

Toyota Gazoo setzt auf Zero-Trust-Plattform

Das Toyota Gazoo Racing World Rally Team (TGR-WRT) betreibt Programme für die World Rally Championship, den Motorsport und Young Driver Development. Da das finnische Unternehmen in rauen Umgebungen und häufig an abgelegenen Standorten rund um den Globus unterwegs ist, war der sichere Zugang zum Internet und zu Anwendungen eine Herausforderung für das IT-Team. TGR-WRT benötigt Anbindungen zu rund 100 Diensten, darunter Datenspeicherung, SaaS-Anwendungen sowie private Applikationen für sensible Entwicklungs- und Testdaten der Rallye-Fahrzeuge. Für das Unternehmen war die herkömmliche Sicherheitsinfrastruktur aus VPNs und Firewalls nicht mehr agil und sicher genug. Als TGR-WRT den IT-Betrieb auf eine Cloud-First-Strategie umstellte, waren eine effizientere Konnektivität und höhere Sicherheitfür die User gefragt.

Der IT-Dienstleister von TGR-WRT empfahl die Zscaler Security Cloud als passende Lösung für die besonderen Anforderungen. Nach dem Proof of Concept wurde die Einführung der Zscaler Zero Trust Exchange in einem engen Zeitplan umgesetzt. Dank der Cloud-nativen Sicherheitsplattform werden sichere Verbindungen zwischen Usern, Zweigstellen, Anwendungen und Workloads von überall aus und mit allen Geräten ermöglicht. Da die Anbindung nicht über das Netzwerk erfolgt, wird auf diese Weise die Angriffsfläche reduziert.

Riku Nykänen, Information Security Officer bei TGR-WRT, erläutert: „Zscaler ist eine der besten Entscheidungen, die wir getroffen haben. Die Zero-Trust-Exchange-Plattform vereinfacht unsere gesamte Architektur. Sie bildet den Kern unserer Sicherheitsstrategie für den Datenverkehr von unseren On-premise- und Cloud-Servern sowie mobilen Geräten, die unser Team weltweit während der Rallyes oder an Teststrecken von unterwegs aus nutzt. Unsere Anwender sind aufgrund der einfachen Bedienung und der nahtlosen, unterbrechungsfreien Konnektivität zufrieden mit der Lösung. Für die Datenübertragung von der Rennstrecke zählt schließlich jede Zehntelsekunde."

Sichere Übertragung von vertraulichen Daten

Während eines Rennens ist es von entscheidender Bedeutung, dass Daten von den Fahrzeugen und Serviceteams so schnell wie möglich zur Zentrale übertragen werden, um dort auf Performanz analysiert und optimiert zu werden und damit zur Zuverlässigkeit der Fahrzeuge beizutragen. Aufbauend auf der Plattform von Zscaler konnte TGR-WRT eine IT-Umgebung aufbauen, die die vertraulichen Daten von allen Standorten aus sicher überträgt.

TGR-WRT setzt dafür auf Zscaler for Users mit Zscaler Internet Access, um Anwendern von überall aus und mit jedem Gerät Zugang zum Internet und zu SaaS-Applikationen zu gewährleisten. Mithilfe von TLS-/SSL-Dateninspektion und KI-gesteuerter Abwehr werden Anwender in allen Stadien der Angriffskette geschützt, wird Datenschutzverletzungen vorgebeugt und die Ausbreitung von Bedrohungen unterbunden. Zusätzlich wurde die unzuverlässige VPN-Technologie durch Zscaler Private Access abgelöst, wodurch die sichere Anbindung zu privaten Anwendungen von jedem Standort möglich wird. Schließlich ermöglicht Zscaler Digital Experience dem Helpdesk-Team eine schnellere Problembehebung von User-Tickets bei Verbindungseinschränkungen.

Komplexität der IT-Architektur reduziert

Das Unternehmen vertraut auf die direkte Anbindung zur Cloud-Architektur über Zscaler Zero Trust SD-WAN, um die Daten aus den Fuhrparks und der Firmenzentrale über einen Branch-Connector direkt an die Zero-Trust-Exchange-Plattform weiterzuleiten und damit den sicheren Zugriff auf Anwendungen und das Internet zu ermöglichen. Damit kann einerseits die Komplexität der Architektur weiter eingeschränkt werden und andererseits wird auf diese Weise eine weitere Datensicherheits-Ebene eingeführt, da Site-to-Site VPNs überflüssig werden.

TGR-WRT ist mit der Zscaler-Lösung äußerst zufrieden. Von April bis Juni 2024 wurden über die Sicherheitsplattform rund 262 Millionen Transaktionen mit 13,7 TByte an Datenvolumen überwacht, was den Anstieg des Datenverkehrs um mehr als 1.400 Prozent im Vergleich zum Vorjahr emöglichte. In diesem Zeitraum wurden von der Cloud-Plattform etwa drei Millionen Richtlinienverletzungen gestoppt. •

DER AUTOR
Paul Hennin
ist Marketing Director für EMEA bei Zscaler.

Toyota Gazoo Racing World Rally Team beteiligt sich unter anderem an der World Rally Championship. (Bild: Pal Hennin)

Bild/Copyright: ngstock – stock.adobe.com

Nachhaltige Digitalisierung – by Design

Security by Design rückt spätestens mit dem Cyber Resilience Act auch in den Blickpunkt von Chefetagen. Aber was ist das überhaupt, was bringt es den Anwendern und was bedeutet es für Hersteller und Dienstleister?

VON STEFFEN ULLRICH

DIE DIGITALISIERUNG VON IMMER KRITISCHEREN GESCHÄFTSPROZESSN macht diese zu einem attraktiven Ziel für Erpressung, Spionage und Sabotage. Gleichzeitig wächst die Komplexität von Hardware, Software und digitalen Infrastrukturen und damit nehmen Fragilität und Angriffsfläche zu. Vom Einsatz Künstlicher Intelligenz profitieren sowohl Angreifer als auch Verteidiger. Diese bringt selbst eine hohe Komplexität mit sich und trägt damit zum Problem bei. Sichtbar werden diese Probleme durch die steigende Anzahl erfolgreicher Angriffe oder fehlerbedingter Ausfälle mit immer höheren Schäden. Patches für Schwachstellen kommen oft erst nach den Angriffen – und damit zu spät. Zudem führen hastig bereitgestellte Not-Patches zu ungeplanten Betriebsunterbrechungen.

Security by Design kann Abhilfe schaffen

Zur Verbesserung bietet sich Security by Design an: Dieser Ansatz zerlegt komplexe Systeme in einzelne Komponenten mit jeweils minimalen Rechten und einem klar definierten und verifizierten Zusammenspiel zwischen ihnen. Dies reduziert nicht nur die Komplexität, sondern durch den Fokus auf minimale Rechte auch die Angriffsfläche und das Schadenpotenzial. Ein weiterer Aspekt von Security by Design ist die Annahme, dass Fehler unvermeidlich sind, deren Auswirkungen sich aber durch ein robustes, fehlertolerantes Design minimieren lassen.

Für Infrastrukturen bedeutet das: Segmentierung und Mikrosegmentierung von Netzen, Systemen, Containern und Anwendungen, kombiniert mit Zero-Trust-Zugriffskontrollen. Je granularer die Segmente und je restriktiver die Zugriffskontrollen sowie das Filtern von Daten und Kommunikation sind, desto kleiner werden Angriffsfläche und Schadenpotenzial. Auch schränkt dies die Möglichkeit von Angreifern ein, sich ungebremst in der Infrastruktur auszubreiten. Dabei sollte man sich nicht auf einzelne Sicherheitsmaßnahmen verlassen, sondern Schwächen einzelner Maßnahmen durch eine mehrschichtige Verteidigung (Defense in Depth) sowie Angriffserkennung robust kompensieren.

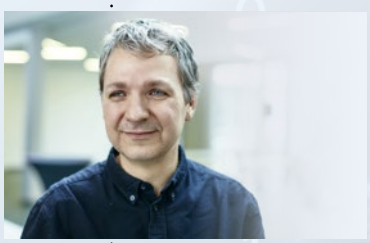
So profitiert die Software-Entwicklung

Das Zerlegen von Software in einzelne Komponenten mit strikt verifiziertem Zusammenspiel reduziert die Komplexität und erhöht die Wartbarkeit. Das Kapseln von Komponenten in Prozesse, Container, Sandboxen et cetera mit jeweils minimalen Rechten verringert das Schadenpotenzial zusätzlich. Besonders relevant ist dies beim Einsatz von Fremdkomponenten, bei denen man keinen Einfluss auf die Qualität hat. Die Kombination mehrerer dieser Sicherheitsschichten erhöht die Robustheit bei Fehlern.

Für Anwender verringert Security by Design die Risiken und sorgt für mehr Sicherheit . Weniger Unterbrechungen durch kritische Patches oder erfolgreiche Angriffe führen zu einer höheren Produktivität. Security by Design fungiert somit als Enabler einer nachhaltigen Digitalisierung.

Was bedeutet dies für Hersteller und Dienstleister?

Wie alle größeren Änderungen ist Security by Design initial kostspielig und zeitaufwendig. Neben dem Aufbau neuer Kompetenzen muss sich oft auch die Firmenkultur ändern. Mittelfristig jedoch kommen die Vorteile zum Tragen, etwa die bessere Wartbarkeit von Software und Infrastrukturen sowie weniger kritische Sicherheits- und Verfügbarkeitsprobleme, für die man gegenüber Kunden eventuell haften muss. •



DER AUTOR
Steffen Ullrich ist Technology Fellow bei genua.

Neue Sicherheitsstandards für KI:

Risiken erkennen und effektiv managen

Arnd Gille, Senior Manager Solutions Consulting Germany, Palo Alto Networks

KÜNSTLICHE INTELLIGENZ (KI) ENTWICKELT SICH in rasantem Tempo und findet immer häufiger Anwendung in Unternehmen. Die anfängliche Skepsis gegenüber der Technologie ist gewichen, zeigt der State of Cloud-Native Security Report 2024: Alle Befragten begrüßen demnach die Einführung von KI-basierten Anwendungen. Während der Einsatz von KI enorme Vorteile bringt, sollten Unternehmen die damit einhergehenden neuen Herausforderungen nicht unterschätzen, da herkömmliche Sicherheitsstrategien bisher nicht ausreichen.

Die Dynamik der KI-Landschaft

Angesichts der schnellen Fortschritte im Bereich der KI stehen Unternehmen unter enormem Druck, neue Technologien schnellstmöglich zu integrieren, um ihre Wettbewerbsfähigkeit zu sichern. Die Verfügbarkeit zahlreicher Tools über einfache Programmierschnittstellen (Application Programming Interface, API) und ein schnell wachsendes Ökosystem an Tools und Frameworks beschleunigen diese Entwicklung zusätzlich. Gerade diese Geschwindigkeit erschwert zunehmend eine gründliche Risikobewertung und die Einführung geeigneter Sicherheitsmaßnahmen, wodurch Sicherheitsteams oft gezwungen sind, Entscheidungen ohne etablierte Standards zu treffen. Daher ist es entscheidend, Sicherheits- und Governance-Aspekte frühzeitig in den KI-Entwicklungsprozess zu integrieren, um Risiken proaktiv zu mindern und widerstandsfähigere Systeme zu schaffen.

Neue Anforderungen an Sicherheit und Compliance

Herkömmliche Cybersicherheitsstrategien, die auf Vertraulichkeit, Integrität und Verfügbarkeit von Daten basieren, müssen im Umfeld der KI um Dimensionen wie Fairness, Transparenz und Verantwortlichkeit erweitert werden. Regulatorische Neuerungen wie der EU AI Act erfordern zudem, dass Unternehmen die mit KI-Anwendungen verbundenen Risiken bewerten und mindern. Dies ist insbesondere in risikobehafteten Bereichen wie dem Personal- und Kreditwesen sowie der Strafverfolgung relevant. Sicherheitsteams müssen daher eng mit Rechts- und Compliance-Teams zusammenarbeiten und Mechanismen zur Überwachung und Validierung der Ergebnisse von KI-Modellen schaffen. Darüber hinaus ist die Prävention und Früherkennung von KI-Schwachstellen von entscheidender Bedeutung, da eine reaktive Behebung sowohl kostspielig als auch zeitintensiv sein kann.

Transparenz und Kontrolle als Schlüssel

Um Risiken KI-gestützter Anwendungen langfristig erfolgreich zu bewältigen, sollten Unternehmen zusätzlich auf Transparenz und Kontrolle setzen. Transparenz erfordert zunächst ein umfassendes Verständnis über den Einsatz von KI im gesamten Unternehmen. Dazu zählen die Erfassung aller verwendeten KI-Modelle, die Nachverfolgung der zugehörigen Trainings- und Betriebsdaten sowie die detaillierte Dokumentation von Funktionen und Zugriffsrechten. Ohne diese grundlegende Transparenz lassen sich Risiken nicht zuverlässig bewerten oder Richtlinien effektiv durchsetzen. Kontrolle bezieht sich auf die Implementierung von Richtlinien, Prozessen und technischen Sicherheitsvorkehrungen, die sicherstellen, dass KI verantwortungsvoll und im Einklang mit den Werten der Organisation eingesetzt wird.

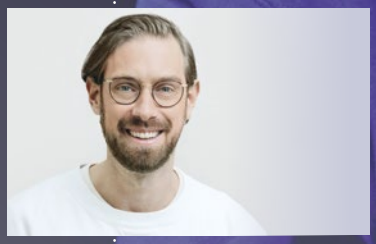
Fazit

Mit der rasanten Verbreitung von KI stoßen herkömmliche Sicherheitsstrategien an ihre Grenzen. Daher müssen Unternehmen einen strukturierten Ansatz für Sicherheitsverantwortliche bereitstellen, der eine Zusammenarbeit zwischen allen Interessenvertretern ermöglicht – einschließlich Sicherheits-, Compliance- und Tech-Teams. So können sie geeignete Governance-Mechanismen für KI entwickeln und implementieren, angepasst an die jeweiligen Anforderungen, Prioritäten und rechtlichen Vorgaben. •

Cyberangriffe bedrohen Unternehmen

Deutsche Unternehmen kämpfen gegen steigende Cyberkriminalität. Über drei Viertel der Experten sehen die Bedrohung als kritisch, laut Prognosen zielen 90 Prozent der Angriffe auf menschliche Emotionen ab. Trotz dieser Gefahr wächst das Budget für Cybersicherheit nur langsam. Doch der Aufbau einer nachhaltigen Sicherheitskultur ist essenziell.

VON NIKLAS HELLEMANN



DER AUTOR
Dr. Niklas Hellemann
ist CEO von SoSafe.

ANGRIFFE AUF IT-INFRASTRUKTUREN, Datendiebstahl und Erpressung durch Ransomware können finanzielle Verluste und nachhaltige Schäden für Reputation und Betriebsfähigkeit bedeuten. Als besonders erfolgreich stellt sich für Angreifer der Fokus auf menschliche Emotionen durch Social-Engineering-Methoden heraus. Das Marktforschungsunternehmen Forrester prognostiziert für 2024, dass der Faktor Mensch in 90 Prozent der Cyberangriffe involviert sein wird. Die Sicherheit von Organisationen hängt also entscheidend von der menschlichen Verteidigungslinie ab. Dass die Bedrohung sich nochmals verschärft hat, zeigt der SoSafe Human Risk Review 2024: 77 Prozent der Sicherheitsexperten im DACH-Raum sind der Meinung, dass die Bedrohungslandschaft am kritischsten Punkt der letzten fünf Jahre ist, und mehr als jede zweite Organisation (52 Prozent) war bereits selbst betroffen.

KI und die geopolitische Lage verschärfen die Gemengelage

Durch das Aufkommen von Künstlicher Intelligenz haben Cyberkriminelle heute einfachen Zugang zu raffinierten Methoden und verbinden diese mit kreativen Social-Engineering-Taktiken. Angriffe sind längst nicht mehr auf den ersten Blick zu erkennen. Der menschliche Faktor wird zusehends stärker an- und ausgespielt, und fortschrittliche technologische Verteidigungsmaßnahmen werden umgangen. 79 Prozent der befragten Sicherheitsbeauftragten schätzen die Nutzung generativer KI für Social-Engineering-Angriffe für ihre Organisation als besorgniserregend ein. Verschärft wird die Situation durch die komplexe geopolitische Lage, die laut 75 Prozent der Befragten zunehmend verwundbar macht.

Unternehmen kennen das Risiko – investieren aber nicht genug

Die Prävention von Cyber-Angriffen ist Management-Sache, dem stimmten 99 Prozent der Befragten zu: Sowohl leitende Angestellte als auch ihr Board sind in Cybersicherheits- und Governance–Entscheidungen involviert. Gleichzeitig gaben nur etwa die Hälfte der Befragten (53 Prozent) an, dass das Budget für Cybersecurity in den letzten zwei Jahren gestiegen sei. Zum Vergleich: In Spanien sind es 66 Prozent und in Großbritannien ganze 73 Prozent.

Mitarbeiter als beste Verteidigung

Obwohl die Verbreitung neuer Angriffsformen zunimmt, bleibt das traditionelle Phishing eine der effektivsten Methoden. SoSafe stellte fest, dass zu Beginn eines Cybersecurity-Trainings 37 Prozent der Menschen auf schädliche Links klicken und 38 Prozent dieser Personen anschließend weiter interagieren, indem sie beispielsweise Formulare ausfüllen und persönliche Daten preisgeben. 80 Prozent der Malware- und Ransomware-Angriffe beginnen mit menschlicher Manipulation durch Phishing oder andere Formen. Gleichzeitig finden Angriffe zunehmend auch über Soziale Netzwerke, Anrufe, Messaging Apps, oder Kollaborations-Tools – oder über mehrere dieser Kanäle gleichzeitig – statt.

Technische Lösungen sind schon lange nicht mehr ausreichend: Um Mitarbeiter als aktivsten Teil ihrer Cybersicherheit einzusetzen, müssen Unternehmen eine nachhaltige Verhaltensveränderung fördern. Sicherheit muss zur Intuition werden. Das ist bei vielen auch bereits angekommen: 89 Prozent der Befragten gaben an, dass der Aufbau einer Sicherheitskultur in ihrem Unternehmen für sie Priorität hat. Der Handlungsbedarf ist jedoch gegeben, um im Katz-und-Maus-Spiel mit Cyberkriminellen dauerhaft die Oberhand behalten zu können. •

MEHR SCHUTZ
durch ein adaptives Security-Ökosystem

DIE ZUNEHMENDE BEDROHUNGSLAGE IM CYBERRAUM erfordert, dass Unternehmen ihre IT-Sicherheitslösungen kontinuierlich aktualisieren. Gleichzeitig stellt der Mangel an Fachkräften im Bereich Cybersicherheit Unternehmen vor große Herausforderungen. Um diese Bedingungen zu adressieren, gewinnen zentralisierte IT-Sicherheitsinfrastrukturen und proaktive Security-Ansätze zunehmend an Bedeutung. Ein adaptives Security-Ökosystem bietet eine effektive Lösung, indem es verschiedene Sicherheitsfunktionen konsolidiert und die Effizienz und Flexibilität in der Verwaltung von IT-Sicherheitsprozessen steigert.

Ein Beispiel für ein solches System ist das adaptive Security-Ökosystem von Sophos, das Unternehmen unterstützt, ihre Cybersicherheit auf ein neues Niveau zu heben. Dieses Ökosystem deckt die gesamte Palette an Sicherheitsanforderungen ab. Die integrierte Lösung ermöglicht eine zentrale Verwaltung, wodurch der Verwaltungsaufwand reduziert und die Zusammenarbeit zwischen Endpoint- und Netzwerkschutz verbessert wird.

Durch die zentrale Verwaltung können Bedrohungen schneller erkannt und abgewehrt werden, was zu einer spürbaren Entlastung der IT-Abteilung führt. Dies ist besonders wichtig angesichts des Fachkräftemangels im Bereich Cybersicherheit. Die Automatisierung und Integration von Sicherheitsprozessen ermöglichen eine effizientere Nutzung vorhandener Ressourcen und optimieren gleichzeitig den Schutz vor modernen Cyberangriffen. Zudem bietet das System die Flexibilität, schnell auf neue Bedrohungen zu reagieren und die Sicherheitsmaßnahmen kontinuierlich anzupassen.

Mehr Kontrolle und Transparenz durch MDR

Ein weiteres zentrales Element des Security-Ökosystems von Sophos ist Managed Detection and Response (MDR). Diese Lösung bietet Unternehmen maximale Kontrolle und Transparenz über ihre Sicherheitsprozesse. Mit MDR können IT-Teams potenzielle Sicherheitsvorfälle in Echtzeit überwachen und festlegen, wie und wann diese eskaliert werden sollen. Maßgeschneiderte Maßnahmenpläne ermöglichen eine gezielte Reaktion auf Vorfälle, was die Effizienz der Sicherheitsmaßnahmen erhöht. MDR bietet zudem eine zusätzliche Schutzebene, indem es eine proaktive Überwachung und Analyse von Bedrohungen ermöglicht. Dies minimiert das Risiko von Sicherheitsvorfällen und reduziert gleichzeitig die Belastung der internen IT-Ressourcen.

In einer Zeit, in der Cyberbedrohungen immer komplexer werden, ist ein adaptives Security-Ökosystem von entscheidender Bedeutung für den Schutz moderner IT-Infrastrukturen. Die Kombination von zentralisiertem Management, umfassendem Schutz und der Möglichkeit, Bedrohungen in Echtzeit zu überwachen, bietet Unternehmen eine Lösung, die sowohl Effizienz als auch Sicherheit maximiert. Unternehmen, die ihre IT-Sicherheitsstrategie zukunftssicher gestalten wollen, finden in diesem adaptiven Security-Ökosystem einen verlässlichen Partner. •

▸▸▸

Auf der it-sa 2024 vom 22. bis 24. Oktober in Nürnberg zeigt Sophos am Stand 7-227, wie integrierte Sicherheitslösungen den steigenden Anforderungen an die Cybersicherheit gerecht werden.

Cyber-Gefahren durch KI – kann man sich davor schützen?

Das Facettenreichtum an Angriffsmöglichkeiten ist durch KI exponentiell gewachsen. Viele Unternehmen sind sich dieser Gefahren laut AI-Security Report noch nicht bewusst. Ebenfalls besorgniserregend: Rund die Hälfte der Führungskräfte bewerten die Lösungen nicht adäquat, die sie von ihre Cybersicherheitsanbietern oder IT-Dienstleistern kaufen.

VON DR. YVONNE BERNARD

KÜNSTLICHE INTELLIGENZ (KI) ist mittlerweile ein wichtiger Bestandteil von Cybersecurity-Produkten. Auch Cyberkriminelle nutzen KI-Techniken, um ihre Strategien zu optimieren und komplexe Cyberangriffe zu entwickeln. Der AI-Security Report 2024 von Hornetsecurity, eine repräsentative Umfrage unter 514 deutschen Entscheidungsträgern, die in Zusammenarbeit mit YouGov durchgeführt wurde, zeigt die Bedenken hinsichtlich des Einflusses von KI auf die Cybersicherheit. Besonders besorgt sind die Befragten in Bezug auf KI-gestütztes Phishing (54 %), Deepfakes (39 %) und Angriffe, die sich mithilfe von KI leichter skalieren lassen (37 %).

DIE AUTORIN
Dr. Yvonne Bernard
ist CTO bei Hornetsecurity.

Generative KI als Helfer für E-Mail-Angriffe

Phishing gehört noch immer zu den häufigsten Angriffsmethoden. Für die Empfänger ist es schwierig festzustellen, ob bösartige E-Mails von Large Language Models (LLMs) erstellt oder verbessert wurden. Diese sind, sofern sie gut gemacht sind, kaum mehr von einer „menschlichen" Phishing-E-Mail zu unterscheiden.

- Höhere Code-Produktivität: Tools wie GitHub Copilot ermöglichen es Malware-Entwicklern Schadcode effizient zu erstellen.
- Anspruchsvolles Phishing: Mit LLMs lassen sich überzeugende und zielgerichtete Phishing-E-Mails erstellen, die selbst von erfahrenen Nutzern schwierig zu erkennen sind. Zudem können Angriffe in verschiedene Sprachen übersetzt werden.
- Gezielte Recherche: KI-basierte Suchmaschinen helfen Angreifern, Informationen über Unternehmen und Einzelpersonen zu sammeln, um sie für Spear-Phishing-Angriffe und Social Engineering zu verwenden.

Copilot als Einfallstor

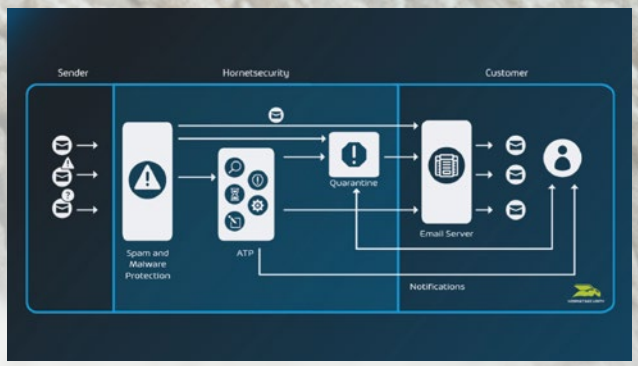
Für Unternehmen birgt die Integration von Copilot in Microsoft 365 Risiken, da das Tool Zugriff auf sensible Daten erhält. Der Grund: Um auf Daten zuzugreifen nutzt Copilot sämtliche Berechtigungen des angemeldeten Benutzers, auch wenn er diese selbst gar nicht alle kennt. Ohne ein robustes Zugriffsmanagement öffnen Unternehmen Bedrohungsakteuren so das Tor zu ihren Unternehmensdaten.

Der Umgang mit privaten und sensiblen Daten

Der Einsatz von KI-Tools wie ChatGPT oder anderen LLMs wirft datenschutzrechtliche Bedenken auf, die Unternehmen und Endbenutzer berücksichtigen sollten. Auch wissen wir noch nicht, welche Daten zur Modellschulung verwendet werden. Zudem zeigt ein Blick in die Nutzungsbedingungen, dass die Inhalte der Benutzer standardmäßig für das Training der Modelle genutzt werden. Rechtlich ungeklärt ist auch die Frage, was passiert, wenn GenAI urheberrechtlich geschütztes Material zur Verfügung stellt und wem diese Inhalte gehören. Unternehmen müssen daher eine Strategie zum Umgang mit internen Daten in LLM-Systemen entwickeln.

Letztendlich müssen sich auch die Anbieter der AI-Dienste mit Cyber-Risiken auseinandersetzen, etwa mit sogenanntem Poisoning. Hier „vergiftet" ein Angreifer die Antworten der LLMs, um ein gewünschtes Ergebnis für böswillige Zwecke zu erzeugen. Für große KI-Akteure sind zudem Modell-Diebstähle eine Gefahr, denn ein gestohlenes LLM kann zu effektiveren Dark-Web-KIs wie WormGPT führen.

Schutz vor Cyberangriffen und Bedrohungen wie Ransomware, Phishing, Spear-Phishing oder auch CEO-Betrug bieten Technologien wie Phishing Detection, Advanced Threat Protection (ATP) und Automated Incident Response.



Advanced Threat Protection (ATP) von Hornetsecurity erweitert die Filtermechanismen für Spam und Malware und führt verdächtige Anhänge in einer Quarantäne-Umgebung aus, um deren Verhalten zu untersuchen.

Letztendlich müssen sich auch die Anbieter der AI-Dienste mit Cyber-Risiken auseinandersetzen, etwa mit sogenanntem Poisoning. Hier „vergiftet" ein Angreifer die Antworten der LLMs, um ein gewünschtes Ergebnis für böswillige Zwecke zu erzeugen.

Next Gen-Cyberabwehr:
Den Angreifern einen Schritt voraus

KI ist ein mächtiges Werkzeug, das auch die Umsetzung von Sicherheitsrichtlinien signifikant erleichtern kann. Laut AI-Security Report planen 60 % der Entscheidungsträger Investitionen in KI zur Stärkung der eigenen Cybersicherheit in den kommenden zwei Jahren zu priorisieren, um u.a. die Gefahrenerkennung und Reaktionsmöglichkeiten zu verbessern und Störfälle besser untersuchen zu können.

KI-gestütztes ATP beispielsweise ergänzt herkömmliche mehrstufige Filtersysteme für E-Mails. Dabei werden durch sogenanntes Sandboxing Dateien, Codes oder Software in einer kontrollierten und isolierten Umgebung überprüft und bewertet, um nach verdächtigen Aktivitäten zu suchen. Mithilfe von Machine Learning (ML) und mehr als 500 verhaltensanalytischen Sensoren wird anschließend entschieden, ob die Datei oder E-Mail legitim ist.

Die menschliche Firewall

Dennoch ist kein System in der Lage, jede einzelne bösartige E-Mail zu erkennen. Es bedarf eines mehrstufigen Schutzsystems, das die menschliche Firewall einschließt. Der AI-Security Report zeigt, dass hier noch Nachholbedarf besteht. So bietet noch rund ein Viertel der Unternehmen (25,7%) ihren End-Usern keine Security Awareness Schulung an.

Der Wille und das Grundverständnis für KI sind zwar da, dennoch muss noch an vielen Stellschrauben gedreht werden. Fest steht: Sind Unternehmen bereit, sich auch auf Security-Lösungen mit KI einzulassen, befinden sie sich auf dem richtigen Weg zu mehr Sicherheit. •

Künstliche Intelligenz – das neue Yin und Yang der Cybersecurity

Technologien mit künstlicher Intelligenz beeinflussen viele Bereiche der IT, so auch die Cybersecurity. Anlässlich der diesjährigen it-sa in Nürnberg haben wir Experten ausgewählter Security-Lösungsanbieter folgende zwei Fragen gestellt: Ist künstliche Intelligenz das neue Yin und Yang der Cybersecurity? Und welche Gefahren, aber auch welche Chancen ergeben sich durch KI für Unternehmen?

VON STEFAN GIRSCHNER

POTENZIAL VON KÜNSTLICHER INTELLIGENZ VERANTWORTUNGSVOLL NUTZEN

Sebastian Lacour,
Senior Manager Channels Germany bei Veeam

KI KÖNNTE TATSÄCHLICH ALS DAS NEUE YIN UND YANG der Cybersecurity betrachtet werden. Hierbei stehen sich zwei gegensätzliche, aber dennoch miteinander verbundene Kräfte gegenüber. Einerseits bietet KI enorme Potenziale zur Stärkung der Cybersicherheit. Sie ermöglicht die schnelle Analyse großer Mengen an Daten, die Erkennung von Anomalien und die Automatisierung von Reaktionsmaßnahmen. Mithilfe von maschinellem Lernen können Bedrohungen frühzeitig identifiziert und Angriffsmuster erkannt werden, was Sicherheitslösungen effizienter und proaktiver macht.

Andererseits birgt die gleiche Technologie auch erhebliche Risiken. So nutzen Cyberkriminelle KI, um Angriffe zu verstärken und zu automatisieren. Sie entwickeln raffinierte Phishing-Techniken, Malware und andere Angriffsmethoden, die schwerer zu erkennen und zu stoppen sind. So wie KI die Verteidiger stärkt, bietet sie auch den Angreifern neue Werkzeuge und Möglichkeiten. Die Herausforderung besteht darin, das Potenzial von KI verantwortungsvoll zu nutzen und gleichzeitig die damit verbundenen Risiken zu minimieren. Letztlich bieten sich durch KI erhebliche Chancen zur Transformation und Optimierung, aber der Erfolg hängt stark davon ab, wie gut Unternehmen die damit verbundenen Risiken managen. Eine sorgfältige Planung, transparente Prozesse und eine ethische Verantwortung sind unerlässlich, um das volle Potenzial von KI auszuschöpfen und gleichzeitig die Gefahren zu minimieren. •

MODERNE ABWEHRMECHANISMEN MÜSSEN AUF KI-TECHNOLOGIEN SETZEN

Kevin Schwarz,
CTO in Residence International bei Zscaler

KOMPLEXITÄT IST DER FEIND VON IT-SICHERHEIT. Künstliche Intelligenz, kombiniert mit Cloud-basierter Sicherheit, kann durch Automatisierung diese Komplexität reduzieren. KI verrichtet schon heute wichtige Dienste, um bisher nicht erkannte Malware (Zero Days) zu erkennen. Letztlich müssen Angreifer nur einmal erfolgreich sein, um Schaden in einem Unternehmen anzurichten, wohingegen die Abwehr kontinuierlich eingreifen muss angesichts sich stetig wandelnder Angriffsmuster, die durch KI noch zusätzlich beschleunigt werden. Wenn Angreifer aufrüsten und ihre Phishing-Angriffe mit Hilfe von GenAI-Tools personalisiert gestalten, hat der User noch weniger Chancen, diese zu erkennen. Dementsprechend müssen auch die modernen Abwehrmechanismen auf KI-Technologien setzen. Dabei verrichtet die KI sehr gute Dienste bei der Korrelation der immensen Datenmengen, um Anomalien schneller zu erkennen.

Mit Breach Prediction geht Zscaler den Schritt von der reaktiven zur proaktiven Sicherheit. Durch die intelligente Analyse des Netzwerkdatenverkehrs und der Korrelation von Verhaltensmustern mit schädlichen Aktivitäten lassen sich die Angriffswahrscheinlichkeit und Schritte zur Verhinderung vorhersagen. Durch die Benachrichtigung der IT-Abteilung können Sicherheitsvorfälle unterbunden und die die Kosten von Angriffen oder Imageschäden abgefedert werden. Die KI kommt zur Risikomitigierung zum Einsatz und beugt Schäden durch (KI-basierte) Angriffe vor. •

DATEN FÜR KI-INNOVATIONEN ZUGÄNGLICH MACHEN

Marc Kleff,
Director Solutions Engineering bei NetApp

KÜNSTLICHE INTELLIGENZ VERÄNDERT DEN ALLTAG: Sie erleichtert und automatisiert viele Routine-Aufgaben und treibt damit gleichzeitig mehr denn je das Datenwachstum voran. Um KI-Projekte auch wirklich erfolgreich voranzubringen, sind zielgerichtetes Datenmanagement und eine intelligente Dateninfrastruktur von entscheidender Bedeutung. Damit Unternehmen möglichst viel Wert aus Daten und ihrem Einsatz in KI-Tools ziehen können, ist es zum einen unerlässlich, Daten effizient zu speichern und Cloud-ready zu machen. Die wichtigste Herausforderung für die Wertschöpfung bleibt jedoch, verteilte Daten in hybriden Multi-Cloud-Umgebungen für KI-Innovationen compliant zugänglich und nutzbar zu machen.

Allerdings dürfen Unternehmen vor diesem Hintergrund keinesfalls Abstriche bei ihrer Cybersicherheit machen, die mittlerweile ebenfalls ein zentraler Faktor im Geschäftsbetrieb ist. Denn das ist die Schattenseite von künstlicher Intelligenz: Auch Bedrohungsakteure nutzen sie immer häufiger in hochprofessioneller Weise für gezielte Hacks. So erhöht die Schlüsseltechnologie KI, bereits erfolgreich erprobt in Security-Tools oder Entwicklungs-Projekten, gleichzeitig selbst das Risiko von Cyberangriffen.

Für Verteidiger wird daher die Dateninfrastruktur zur letzten Verteidigungslinie im Unternehmen. KI und Maschinelles Lernen (ML), die in den Primärspeicher integriert sind, unterstützen dabei, Ransomware in Echtzeit zu bekämpfen, unabhängig vom Speicherort der Daten. Das erhöht das Level der Data Protection, beschleunigt die Wiederherstellung und verbessert so die gesamte Cyber-Resilienz im Unternehmen. •

AUFBAU EINER STRATEGIE FÜR ERHÖHTE CYBERRESILIENZ

Frank Schwaak,
Field CTO EMEA bei Rubrik

SO WIE KI VIELE ASPEKTE DES LEBENS des Lebens verändert hat, hat sie auch die Bedrohungslandschaft verändert. Cyberangreifer nutzen jetzt KI, um ihre Hacks gezielter, professioneller und individueller zu gestalten. Dies erhöht das Risiko eines erfolgreichen Cyberangriffs für Unternehmen und die Notwendigkeit, sich darauf vorzubereiten, dramatisch.

KI hat verändert, womit Unternehmen rechnen sollten: Ich glaube, es ist nicht die Frage, ob ein erfolgreicher Cyberangriff stattfinden wird, es ist nicht einmal eine Frage wann, sondern wie oft. Daher sollten Unternehmen für den schlimmsten Fall planen. Sie müssen das Worst-Case-Szenario bedenken: Wie lange wird es dauern, bis mein Unternehmen nach einem Cybervorfall wieder betriebsbereit ist? Die Priorisierung der Geschäftskontinuität in der aktuellen Bedrohungslandschaft ist ein wesentlicher Bestandteil einer Cyber-Resilienz-Strategie.

Dazu sollten sich Unternehmen die Frage stellen: Welche Daten habe ich, und welche Daten benötige ich, um meine Geschäfte fortzuführen? Eine gute Lösung kann dabei helfen und den Unterschied ausmachen, ob ein Unternehmen innerhalb von Stunden oder Monaten wieder einsatzbereit ist. Dieselbe Technologie, die das Risiko eines Angriffs erhöht, kann bei der Wiederherstellung nach einem Angriff helfen. KI-generierte Workflows können beispielsweise den Wiederherstellungsprozess erleichtern. KI kann IT-Teams auch dabei helfen, die Entscheidungsfindung während eines Cybervorfalls zu optimieren und schneller auf neue Bedrohungen zu reagieren. KI-basierte Wiederherstellungsprozesse können zur schnellen Wiederherstellung von Daten und Anwendungen genutzt werden. Dies macht Unternehmen widerstandsfähiger, da sie den potenziellen Schaden minimieren. •

SECURITY-BY-DESIGN ALS STANDARD BEI JEDER KI-ANWENDUNG

Claus Gründel,
General Manager Embedded IoT Solutions bei Swissbit AG

KÜNSTLICHE INTELLIGENZ WIRD GEFÜHLT in nahezu jedem Bereich als das neue Yin und Yang betrachtet. Die Beantwortung der Frage ist allerdings nicht einfach, da sie viele Facetten umfasst. Denn KI kann einerseits Sicherheitsprobleme lösen, andererseits aber auch neue Bedrohungen mit sich bringen.

Ein oft übersehener Aspekt bei der Einführung von KI in Unternehmen ist die Frage, ob Implementierungen unter Sicherheitsaspekten betrachtet wurden. Wo werden die enormen Datenmengen, die für das Training von KI-Modellen verwendet werden, gespeichert? Wie wird die IP von KI-Modellen separat in einer sicheren (lokalen) Domäne auf Geräten gespeichert? Wie und wo sammelt beispielsweise ein autonomer Roboter seine Daten? Diese Fragen sind entscheidend, denn ohne geeignete Sicherheitsvorkehrungen könnten diese Daten zu einem Ziel für Cyberkriminelle werden. Berücksichtigen Unternehmen, die KI-Lösungen entwickeln oder einsetzen, dies nicht ausreichend, läuft die KI Gefahr, selbst zum Einfallstor für Cyberangriffe oder Datenlecks zu werden.

Neben den potenziellen Risiken bietet KI jedoch auch zahlreiche Chancen. So kann diese genutzt werden, um Bedrohungen schneller zu erkennen und Sicherheitslücken effizienter zu schließen. Allerdings gilt dies auch umgekehrt: Hacker können ebenfalls KI verwenden, um Schwachstellen in IT-Systemen noch schneller aufzuspüren. Diese Dynamik stellt Unternehmen vor die Herausforderung, stets einen Schritt voraus zu sein. Daher sollte der Grundsatz „Security-by-Design" bei jeder KI-Anwendung zum Standard werden. In diesem Fall kann beispielsweise die Gewichtung eines KI-Modells in einem Security-Modul im Speicher abgesichert werden. Unternehmen müssen sich intensiv damit auseinandersetzen, wie eine Lösung mit den Themen Datenschutz, Datenhaltung und Datensicherheit umgeht, bevor sie sich für eine Implementierung entscheiden. •

DURCH ZERO-TRUST DEN DATENFLUSS KONTROLLIEREN

Udo Schneider,
Governance, Risk & Compliance Lead, Europe bei Trend Micro

AN DER SPITZE DER CYBERRISIKEN, die mit KI einhergehen, stehen Deep Fakes und Phishing. Diese Angriffe sind zwar nicht neu und werden von Cyberkriminellen schon seit Jahren eingesetzt, aber die Qualität der Angriffe hat sich durch generative KI erheblich verbessert. KI ist für cyberkriminelle Akteure deswegen besonders attraktiv, weil es dadurch quasi unmöglich wird, natürliche und künstliche Inhalte voneinander zu unterscheiden. Daher liegt der Schwerpunkt der Sicherheit nicht auf der Erkennung der KI selbst – was bereits schwierig ist und immer schwieriger wird – sondern auf auffälligen Aktionen, die beispielsweise an einen Meeting-Call oder eine E-Mail-Interaktion anknüpfen.

Für Unternehmen ist es zudem wichtig zu wissen, ob Mitarbeiter öffentliche KI-Tools nutzen und dabei interne Daten ungewollt zum Training dieser Tools beitragen. Der Sicherheitsfokus in Unternehmen sollte daher auf der Kontrolle des Datenflusses sowie auf verdächtigen Aktionen liegen, die an scheinbar natürliche Kommunikationen anschließen.

Ein Zero-Trust-Ansatz schafft einen sicheren Rahmen, um KI-basierte Prozesse in Unternehmensstrukturen zu integrieren und gleichzeitig die Kontrolle über den Datenfluss zu gewährleisten. Echtzeit-Überwachung und zentrale Zugriffsverwaltung verhindern Datenlecks und wehren Bedrohungen wie Prompt-Injection ab.

Zusätzlich unterstützt KI die Automatisierung von Security-Information-and-Event-Management (SIEM)-Systemen und erweitert Security Operations Center (SOC) durch automatisierte Erkennungs- und Reaktionsvorschläge. So verschmelzen traditionelle Sicherheitslösungen mit modernen KI-Anwendungen, was die Widerstandsfähigkeit gegen die komplexen Bedrohungen der heutigen Zeit stärkt. •

KI STEIGERT DEN REIFEGRAD VON SECURITY-PROGRAMMEN

Marco Eggerling,
Global CISO bei Check Point Software

KÜNSTLICHE INTELLIGENZ IST KEINE ERFINDUNG der Neuzeit, sondern geht auf Alan Turing zurück, ist also über 70 Jahre alt. Seither sind gerade im Kontext der Zunahme von Rechenleistung und der Geschwindigkeit, in welcher wir auf Daten zugreifen, viele technologische Fortschritte verzeichnet worden. KI benötigt die Cloud und vice versa. Jedoch erleben wir mit KI aus meiner Sicht den Oppenheimer Effekt der Informationssicherheit, weil die Entwicklung von KI aus anderen Gründen erfolgte als sie aktuell genutzt wird. Als Teil von Automatisierung in der Behandlung von Sicherheitsvorfällen ist KI eine feine Sache und hilft den Security-Analysten, die Arbeitslast zu reduzieren. Dennoch wird der Mensch weiterhin die letzte Instanz bleiben, der die finale Entscheidung trifft, wie mit einem Vorfall umzugehen ist.

Aus diesen Anamnesen lernt KI für künftige Vorfälle und wird mit jedem Vorfall besser. KI wird positiv dazu beitragen, den Reifegrad des Security-Programms einer Organisation zu steigern und zu stabilisieren. Aufbauend auf der Steigerung des Reifegrades eines Security-Programms liegt ein weiterer Mehrwert von KI. Dies setzt jedoch voraus, dass die Qualität der Datenstrukturen hoch ist und bleibt. Solange die Integrität der Datenbasis also rein bleibt, kann und wird die KI eine gute Arbeit leisten.

Aber auch Cyberkriminelle nutzen Large Language Models als Angriffsmethode. Check Point Research sieht aktuell eine deutliche Zunahme von Vorfällen, welche auf KI-basierte Attacken verweisen. Durch die Zunahme sollten Unternehmen in der Verteidigungslinie auf Technologie-Komponenten setzen, welche auf KI basieren. Es wird aus meiner Sicht also zunehmend zu einem „Wettrüsten" kommen, in welchem die künstliche Intelligenz beiden Seiten zur Verwendung steht und es sich dabei herausstellen wird, wer die Nase vorn haben wird. •

DURCH KI wird SIEM NIE MEHR SO SEIN WIE ZUVOR

Jörg Hesske,
Area Vice President EMEA Central bei Elastic

IM TAGESGESCHÄFT DES SOC kann es herausfordernd sein, schnelle Reaktionszeiten zu gewährleisten. Nicht nur wegen der zunehmenden Angriffe, sondern auch wegen unterbesetzter Teams sowie Arbeitsabläufen, die immer noch monotone Routinearbeit erfordern. Mit dem Aufkommen von KI wird es für Unternehmen zur Priorität, ihr SOC zu überdenken. Um schnell neue Bedrohungen zu erkennen, zu untersuchen und auf sie zu reagieren, müssen Unternehmen ihr SOC modernisieren. Der Schlüssel dazu liegt in KI-getriebenen Sicherheitsanalysen.

Jeder Schritt zu einem modernen SOC sollte die Arbeitserfahrung für Sicherheitsanalysten grundsätzlich verbessern. Generative KI (GenAI) kann dabei helfen, Alerts zu filtern und die Anzahl der Alerts, die Analysten manuell untersuchen müssen, von Hunderten auf einige wenige zu reduzieren. Dadurch können Analysten Angriffe priorisieren, nicht Alerts. Sie haben die Ressourcen, um schnell zu reagieren, mit einem klaren Fokus und strategischen Schritten.

Im Falle eines echten Cyberangriffs liefern KI-Assistenten Sicherheitsanalysen in natürlicher Sprache, um Alerts zu überprüfen und auf Vorfälle zu reagieren. So wird jeder Benutzer zu einem extrem leistungsstarken Benutzer. Künstliche Intelligenz hat einen erheblichen Einfluss auf die sich ständig weiterentwickelnde Dynamik zwischen Angreifern und Verteidigern. Sowohl Hacker als auch Sicherheitsexperten können von KI profitieren – zum Nachteil der jeweils anderen Seite. Da Angreifer KI nutzen, um sowohl die Anzahl als auch die Raffinesse ihrer Angriffe zu erhöhen, wird es für Verteidiger entscheidend, KI strategisch in ihre Verteidigungssysteme zu integrieren. Wenn Verteidigungssysteme versagen, sind schnelle Reaktionszeiten der Schlüssel, um Schäden zu minimieren. •

CVEs, Bären und sichere Lieferketten

Umfragen unter IT-Entscheidern benennen Security regelmäßig als Top-Thema. Schnell kommt die Sprache auf CVEs (Common Vulnerabilities and Exposures), einen Industriestandard zur Benennung und Dokumentation von Sicherheitslücken in Computersystemen. 2023 gab es deren 28.961; im ersten Quartal 2024 mit 8.697 knapp einen Fall pro Viertelstunde.

VON DR. GERALD PFEIFER

Under Attack – das neue Normal

Letztlich sind es Menschen, nicht CVEs, die sich als Probleme erweisen: Jene nämlich, die Schwachstellen ausnutzen, sei es kriminell oder politisch bedingt. So berichtete der Bitkom im Mai, dass 46 Prozent der betroffenen Unternehmen in Deutschland Angriffe nach Russland zurückverfolgen konnten (halb so viele 2021), und 42 Prozent nach China (30 Prozent im Jahr 2021).

Dem Österreichischen Rundfunk ORF zufolge gab es im Juli 100.000 staatliche Hacker in China (Haupteinsatzgebiet Spionage) und 30.000-50.000 in Russland (Fokus auf Desinformation). Auch Nordkorea ist aktiv: Ende 2023 platzierten Hacker gut zwei Dutzend Pakete auf NPM, einer Bibliothek mit mehreren Millionen JavaScript-Paketen, die von gut 17 Millionen Entwicklern im Jahr verwendet wird. Die Pakete: allesamt inklusive Backdoors mit dem Ziel, sich auf den Systemen der Entwickler von Crypto-Zahlungsplattformen einzunisten und von dort die Umgebung ihrer Arbeitgeber zu infizieren – ein klassischer Angriff über Software Supply Chains.

DER AUTOR
Dr. Gerald Pfeifer
ist CTO bei SUSE sowie Chair des openSUSE Board.

> Ein wesentlicher Schritt ist es, den Menschen in den Mittelpunkt zu stellen, aufzuklären, gemeinsam Richtlinien zu erarbeiten, Praktiken zu etablieren und Policies zu setzen, aus welchen Quellen Code bezogen wird, unter welchen Voraussetzungen, und mit welchen Vorgehensweisen.

Angreifer wie Verteidiger wenden sich zunehmend intelligenten und automatisierten Ansätzen zu. Attacken finden am laufenden Band statt. Laut Gartners „2023 Supply Chain Risk Management Survey" sind „Angriffe auf die Software-Lieferkette auf dem Vormarsch": 63 Prozent der Befragten gaben an, im vergangenen Jahr betroffen gewesen zu sein. Damit ist die Frage letztlich nicht, ob eine Organisation einen Angriff auf ihre Software-Lieferketten erlebt, sondern wie häufig und wie effektiv.

Ziel oder Kollateralschaden?

Angreifer gehen, wie wir anhand der NPM-Attacke gesehen haben, oft sehr raffiniert und geduldig vor. Manchmal haben sie ein spezifisches Ziel im Visier, manchmal wer-

fen sie ein weites Netz aus und suchen nach verwundbaren Systemen.

Deshalb gilt es, besser abgesichert zu sein als die Mehrzahl der anderen potentiellen Opfer. Oder um es mit einem amerikanischen Sprichwort zu sagen: „SIe müssen nicht schneller laufen als der Bär, sondern nur schneller als die langsamsten Camper." Klassische Ansätze wie Firewalls, Netzwerksegmentierung, Multi-Factor-Authentication, Intrusion Detection und natürlich das regelmäßige Scannen auf CVEs sind die Norm geworden.

Um diese Bollwerke zu umgehen, bedienen sich Angreifer „weicherer" Angriffsvektoren, vor allem wenn es gegen konkrete Ziele geht: Über Menschen, durch Social Engineering, Erpressung und Bestechung, andererseits über Software Supply Chains. So gelingt ein Eindringen, ohne Aufmerksamkeit zu erwecken, gar auf Einladung hin: Entwickler und andere Mitarbeiter laden aktiv neue Komponenten, Programme oder Updates in ihre Umgebungen und somit in das Herz der IT.

Moderne Programmiersprachen – JavaScript, Go, Python, Ruby, etc. – bieten Portale mit Unmengen an Modulen und anderen nützlichen Ergänzungen, aus denen Entwickler gerne schöpfen. Der Platzhirsch GitHub alleine bedient 100 Millionen Entwickler und bietet mehr als 420 Millionen Repositories an, darunter mindestens 28 Millionen öffentliche. Dazu kommen Anwendungen von Softwareherstellern (ISVs), die sich mittlerweile ebenfalls häufig aus dem Fundus öffentlicher Bibliotheken bedienen, und natürlich eigenständige Open Source-Projekte. Insgesamt eine Vielfalt, die gern und oft konsumiert wird.

So praktisch (und auch sinnvoll) die Nutzung all dieser Quellen ist, sie birgt das Risiko, sich ein Problem ins Haus zu holen: Böswillige Hacker können Schadcode einpflanzen, sei es direkt oder durch das Hacken des Accounts eines etablierten Entwicklers. Dazu kann bei mangelhafter Sicherheit durch eine sogenannte „Man-in-the-Middle" Attacke auf dem Weg vom ursprünglichen Entwickler zum Portal oder vom Portal zum Anwender etwas verändert werden. Ähnlich können übel wollende (ehemalige) Mitarbeiter oder Dienstleister mit Insiderwissen Systeme kompromittieren. Und letztlich machen selbst die besten Entwickler Fehler, die Dritte entdecken und melden oder (im Fall von Open Source) gar direkt beheben oder die Kriminelle ausnutzen und zu Geld machen können.

Was nun?

Ein wesentlicher Schritt ist es, den Menschen in den Mittelpunkt zu stellen, aufzuklären, gemeinsam Richtlinien zu erarbeiten, Praktiken zu etablieren und Policies zu setzen, aus welchen Quellen Code bezogen wird, unter welchen Voraussetzungen, und mit welchen Vorgehensweisen. Dem klassischen „Trust but verify" folgend mag das in kritischen Umgebungen bis hin zur Inspektion von Quellcode durch Spezialisten führen, oder zumindest einem schnellen Durchsehen und Testen in einer isolierten Umgebung. Natürlich wird man auf bekannte Muster bzw. bekannte CVEs scannen. Sicherheit, und insbesondere die Suche nach bekannten Schwachstellen, ist ein ständiger Prozess, keine einmalige Aktion. Es gilt also laufend zu überprüfen: auf Entwicklungssystemen, in Produktionsumgebungen und in der Infrastruktur selbst.

Wichtig ist es, bei eigenen Entwicklern und auch in Open Source-Communities mehr Bewusstsein für Sicherheit zu schaffen und entsprechende Werkzeuge und Angebote zur Verfügung zu stellen.

Ein weiterer Ansatz sind Zertifizierungen, die bestätigen, dass Hersteller bei der Entwicklung, Wartung und Verteilung ihrer Software bestimmten Prinzipien folgen und ein entsprechendes Maß an Sorgfalt an den Tag legen. Dazu zählen detaillierte Code Reviews, das Signieren der Software sowie aller Updates und kryptographisch gesicherte Lieferwege, wie es etwa Googles SLSA beschreibt.

Zwar hat die EU mit der NIS2 (Network and Information Security) Richtlinie und dem Cyber Resilience Act eine erste Grundlage für mehr IT-Sicherheit sowie den Schutz kritischer Infrastruktur geschaffen, aber:

Nobody is Perfect

Letztlich müssen wir einer Wahrheit ins Auge schauen: Absolute Sicherheit existiert nicht. Wir können uns nur so gut wie möglich schützen und lernen, auf Unerwartetes und Unerwünschtes zu reagieren.

Eine hundertprozentig sichere Supply Chain ist illusorisch. Wie gehen wir also damit um, wenn doch einmal etwas durchrutscht? Wie können wir allzu großen Schaden verhindern und selektiv Maßnahmen ergreifen, ohne den gesamten Betrieb einzustellen? Hier sind Zero Trust-basierte Ansätze vielversprechend und Notfallpläne (inklusive Kommunikationsmaßnahmen), die auch geübt werden. •

Zu viel Cyber – zu wenig Security

Die Zahl der Cyberangriffe nehmen zu. Dadurch wächst der Security-Markt schneller als jede andere Branche. Dies führt jedoch auch dazu, dass Anbieter auf dem Markt erscheinen, die nicht seriös sind. Um einen guten Security-Dienstleister zu erkennen, sollten objektive Bewertungskriterien herangezogen werden.

VON FLORIAN HANSEMANN

WENN EIN UNTERNEHMEN ZIEL EINER HACKERATTACKE WIRD, dann wird es schnell teuer: IT-Ausfälle, Ausgaben für externe Dienstleistungen zur Wiederherstellung des Geschäftsbetriebs sowie durch entgangene Geschäfte. Vorbeugen ist daher der richtige Schritt. Doch vor allem Mittelständlern fehlen hier oft die personellen Ressourcen für die IT-Sicherheit und man setzt externe Dienstleister. Diese gibt es mittlerweile zuhauf – umso schwerer ist es, einen seriösen Anbieter zu finden. Doch ein paar objektive Bewertungskriterien helfen.

Zero Day & Tools

Ein Dienstleister mit speziellen Kompetenzen in technischer Sicherheit strebt oft danach, seine Reputation in der Community zu erhöhen oder die Informationssicherheit allgemein zu verbessern. Zwei anerkannte Methoden dafür sind die Veröffentlichung von Sicherheitslücken und die Entwicklung von Tools: Security-Dienstleister können bislang unbekannte Schwachstellen identifizieren und veröffentlichen, um sogenannte CVEs (Common Vulnerabilities and Exposures) zu beantragen. Während der Arbeit an Projekten stehen Dienstleister oft vor Herausforderungen, für die es keine bekannten Lösungen gibt. Daher entwickeln diese häufig kleine Tools oder Skripte, um bestimmte Aufgaben zu erleichtern. Die Tools oder Skripte werden oft über Plattformen wie GitHub der Community zur Verfügung gestellt.

Fachbeiträge

Fachbeiträge in Blogs können Informationen zu aktuellen Sicherheitsthemen, Anleitungen zum Hacken oder News zur Entwicklung und Verschleierung von Malware enthalten. Solche Beiträge bieten oft Einblicke in frühere Projekte eines Dienstleisters. Beispielsweise könnte ein Blog-Beitrag über das Injizieren von Malware in eine gängige Software darauf hindeuten, dass der Dienstleister diese Technik bei einem Penetrations-Test verwendet hat.

Daher sollte man prüfen, ob ein Security-Dienstleister ein eigenes Blog betreibt. Und behandelt der Blog hauptsächlich technische Themen der Sicherheit oder konzentriert er sich mehr auf strategische und managementlastige Inhalte? Wenn Letzteres der Fall ist, dann ist der potenzielle Dienstleister möglicherweise besser für konzeptionelle Aufträge als für technische Sicherheitsanalysen geeignet.

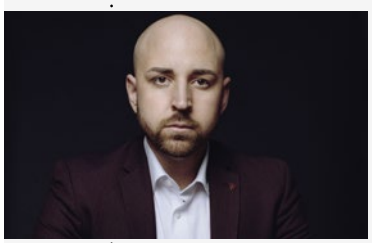
Soziale Medien

Der Community-Gedanke und die Vernetzung haben einen hohen Stellenwert im Bereich der IT-Sicherheit. Auf der Plattform X bleiben Interessierte im Bereich der IT-Sicherheit über aktuelle Entwicklungen wie Malware, Angriffsvektoren und Sicherheits-Tools informiert.

Die Anzahl der Follower kann Hinweise darauf geben, ob ein Dienstleister oder Berater einen Mehrwert für die Community bietet. Ein weiterer Punkt ist, auf die Reaktionen der Posts zu achten, also Likes und Retweets. So lassen sich gekaufte Follower ausschließen. So ist zum Beispiel ein Account mit 10.000 Followern und nur wenigen Likes pro Post verdächtig.

Konferenzen

Cybersecurity-Dienstleister, die auf renommierten Konferenzen sprechen, zeigen in der Regel auch bei Projekten eine hohe Leistungsfähigkeit. Veranstaltungen, bei denen Redner sich einkaufen oder für den eigenen Vortrag bezahlen, werden nicht besucht. Renommierte technische Konferenzen in Deutschland sind unter anderem Troopers Conference, BlackHat, Munich Cyber Tactics, Techniques and Procedures (MCTTP), Offensive Con oder vom Chaos Computer Club (CCC). •



DER AUTOR
Florian Hansemann
ist Geschäftsführer bei HanseSecure.

Perfekte Strategie statt Rechts-Korsett

In Anbetracht der zunehmenden Digitalisierung sehen sich Unternehmen mit einer sich stetig verschärfenden Bedrohungslage konfrontiert. Regulatorische Vorgaben wie NIS-2 oder DORA sollen hier Leitplanken bieten und für mehr IT-Sicherheit sorgen. Doch eine unreflektierte Umsetzung dieser Vorgaben birgt die Gefahr einer Checkbox Security.

VON DANIEL TREMMEL

GEMEINHIN WIRD UNTER CHECKBOX SECURITY die Praxis verstanden, Sicherheitsmaßnahmen lediglich aufgrund ihrer Erfüllung von Compliance-Anforderungen zu implementieren, ohne die tatsächlichen, operativen Risiken und Bedürfnisse der Organisation zu berücksichtigen. Dies führt zu einer Reihe von Problemen, denen die Verantwortlichen begegnen müssen.

So besteht die Gefahr unverhältnismäßiger Kosten bei gleichzeitig geringem Return on Investment (ROI), wenn Sicherheitslösungen nicht auf die spezifischen Risiken des Unternehmens abgestimmt sind. Dadurch werden Ressourcen gebunden, ohne die Sicherheitslage tatsächlich zu verbessern.

Hinzu kommt das erhöhte Risiko durch zentrale Sicherheitslösungen. Denn viele dieser Lösungen, wie beispielsweise EDR-Systeme (Endpoint Detection and Response) oder Schwachstellen-Scanner, erfordern umfangreiche Zugriffsrechte auf kritische Systeme und können so selbst zum Einfallstor für Angreifer werden oder technische Fehlfunktionen hervorrufen.

Beispiele wie der kürzliche Update-GAU bei CrowdStrike oder die Supply-Chain-Attacken bei Solarwinds zeigen, dass selbst etablierte Anbieter vor solchen Vorfällen nicht gefeit sind. Daher sollte bei jeder Implementierung kritisch hinterfragt werden, welche Zugriffsrechte tatsächlich notwendig sind.

Vorsicht vor Schatten-IT

Auch die Anwender dürfen nicht außer Acht gelassen werden. Denn überbordende Sicherheitsmaßnahmen, die nicht auf die Bedürfnisse der Benutzer abgestimmt sind, führen zu komplexen Prozessen und geringer Usability. Die Folge: Frustration bei den Mitarbeitern und eine erhöhte Wahrscheinlichkeit, dass Sicherheitsrichtlinien umgangen und im schlimmsten Fall Schatten-IT-Lösungen genutzt werden, die zusätzliche Sicherheitsrisiken bergen.

Ganzheitliche Sicherheitsstrategie

Ein ganzheitlicher Cybersecurity-Ansatz sollte die Balance zwischen Compliance und tatsächlichen Sicherheitsbedürfnissen finden. Statt blind Vorgaben abzuarbeiten, gilt es für Unternehmen mehrere Aspekte zu berücksichtigen. Unerlässlich ist dabei die Durchführung regelmäßiger Sicherheits-Assessments, um ein genaues Bild der aktuellen Sicherheitslage zu erhalten und potenzielle Schwachstellen frühzeitig zu identifizieren.

Diese Sicherheits-Assessments sollten jedoch nicht als einmalige Maßnahme betrachtet werden, sondern als kontinuierlicher Prozess, der sich an die sich ständig ändernde Bedrohungslage anpasst.

Wahl der Sicherheits-Lösungen

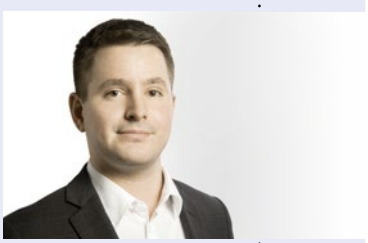
Auch bei der Auswahl von Sicherheits-Lösungen muss genau hingesehen werden. So müssen diese auf die spezifischen Risiken und Bedürfnisse des Unternehmens zugeschnitten sein.

Um jedoch eine möglichst hohe Wirksamkeit aller Sicherheitsmaßnahmen zu gewährleisten, darf nicht nur die Technik, sondern muss viel mehr auch der Faktor Mensch berücksichtigt werden. Hier gilt es auf Sensibilisierungsmaßnahmen und Schulungen für Mitarbeiter zu setzen, um ein sicherheitsbewusstes Verhalten zu fördern und die gewünschte Sicherheitskultur im Unternehmen zu etablieren.

Fazit

Eine effektive IT-Sicherheit erfordert mehr als nur die Erfüllung von Compliance-Anforderungen. Sie bedarf stattdessen eines ganzheitlichen Ansatzes, der die spezifischen Risiken und Bedürfnisse des Unternehmens berücksichtigt und auf einem kontinuierlichen Prozess der Risikoanalyse und -management basiert. •

DER AUTOR
Daniel Tremmel
ist Security Solutions Architect bei A1 Digital.



Risiko Mensch in der IT-Security

Die Digitalisierung hat die Arbeitswelt für die meisten Menschen grundlegend verändert: Cloud-Technologien, mobiles Arbeiten und der Einsatz von künstlicher Intelligenz bieten Vorteile ebenso wie Herausforderungen für die Cybersicherheit. IT-Sicherheitsverantwortliche sind weltweit in höchster Alarmbereitschaft.

VON MIRO MITROVIC

DER MENSCH IST WEITERHIN das größte Einfallstor für Cyberkriminelle. Das geht aus der aktuellen Studie „Voice of the CISO" von Proofpoint hervor. 72 Prozent der befragten deutschen Sicherheitsverantwortlichen (Chief Information Security Officer, CISO) sehen menschliches Fehlverhalten als größte Schwachstelle – Tendenz steigend.

Das ist nachvollziehbar, denn durch mobiles Arbeiten und die Nutzung von Cloud-Anwendungen vergrößert sich die Angriffsfläche für Cyberkriminelle. Schon ein unachtsamer Klick auf einen schädlichen Link oder der Download einer infizierten Datei kann schwerwiegende Folgen nach sich ziehen.

Mitarbeiterfluktuation endet in Datenverlust

Ein weiteres Risiko geht von der Mitarbeiterfluktuation aus. Verlassen Mitarbeiter das Unternehmen, dann besteht die Gefahr, dass sie sensible Daten unbefugt kopieren oder weitergeben. Obwohl die meisten Unternehmen von ihren Sicherheitsvorkehrungen überzeugt sind, berichtet fast die Hälfte der Chief Information Security Officer weltweit von Datenverlusten im letzten Jahr. Davon geben 73 Prozent an, dass die Datenverluste durch scheidende Mitarbeiter verursacht wurden. In Deutschland ist dieser Anteil mit 77 Prozent sogar noch höher.

KI: Zwei Seiten einer Medaille

Künstliche Intelligenz spielt eine immer wichtigere Rolle – sowohl für Cyberkriminelle als auch für die Abwehr von Cyberangriffen. KI-basierte Angriffe werden zunehmend raffinierter und schwieriger zu erkennen. KI bietet aber auch neue Möglichkeiten, um Sicherheitslösungen zu verbessern und Unternehmen besser zu schützen. Um menschlichen Fehlern und komplexen, personalisierten Cyberangriffen zu begegnen, setzen 87 Prozent der befragten Sicherheitsverantwortlichen auf den Einsatz von KI-gestützten Sicherheitsfunktionen.

CISO: Stärkerer Druck

Die Rolle des IT-Sicherheitsverantwortlichen hat in den vergangenen Jahren an Bedeutung gewonnen. Der Austausch mit dem Vorstand hat sich verbessert und Sicherheitsfragen werden heute auf höchster Ebene debattiert. Chief Information Security Officer sehen sich aber auch einem immer höheren Druck ausgesetzt. Budgetkürzungen, Personalmangel und die ständige Gefahr von Cyberangriffen führen zu Stress und Überlastung. Gerade Burnout ist ein ernstes Problem unter den IT-Sicherheitsverantwortlichen: 53 Prozent waren nach eigenem Bekunden im vergangenen Jahr betroffen, in Deutschland waren es sogar 60 Prozent. Erschwerend kommen überzogene Erwartungen hinzu, mit denen sich 66 Prozent konfrontiert sehen.

Awareness und Technologie

Um Unternehmen effektiv vor Cyberangriffen zu schützen, ist ein ganzheitlicher Ansatz erforderlich, der sowohl technologische als auch menschliche Faktoren berücksichtigt. Nur wenn Unternehmen die Bedeutung des Faktors Mensch erkennen und in moderne Sicherheitstechnologien investieren, können sie sich effektiv schützen. Ein leistungsfähiges Dokumenten-Management-System (DMS) trägt nicht nur zur Einhaltung gesetzlicher Vorgaben und zur Optimierung interner Prozesse bei. Durch weitergehende Digitalisierung reduzieren Unternehmen langfristig Kosten und realisieren Produktivitätssteigerungen. •

DER AUTOR

Miro Mitrovic ist Area Vice President DACH bei Proofpoint.

Malware-Check für USB-Sticks und Co.

Mobile Speichergeräte wie USB-Sticks oder externe Festplatten spielen bei einem persönlichen Besuch noch immer eine große Rolle. Auf mobilen Datenträgern kann jedoch unbemerkt Malware in Unternehmensnetzwerke gelangen – ein erhebliches Sicherheitsrisiko.

VON ROBERT KORHERR

DER AUTOR
Robert Korherr ist CEO von Prosoft.

MOBILE SPEICHER spielen in der Unternehmenswelt noch immer eine große Rolle. Traditionell regeln DLP- (Data Loss Prevention) sowie Port-Blocker-Lösungen den Einsatz von externen Speichergeräten und lassen ausschließlich registrierte und freigegebene USB-Speichergeräte zu. Zudem ist es sinnvoll, nur verschlüsselte mobile Speichergeräte zu erlauben. Aber das schützt das Netzwerk per se nicht vor der Infektion durch Malware.

Kompliziert wird es, wenn zum Beispiel ein externer Geschäftspartner ein mobiles Speichergerät mitbringt, etwa der Service-Techniker mit der Diagnose-Software oder der neuen Firmware für eine Produktionsanlage. In solchen Fällen stoßen herkömmliche Ansätze schnell an ihre Grenzen – selbst bei vorhandener Client-Antiviren-Lösung. Denn Evasive- und Zero-Day-Malware können trotzdem über das Endgerät ins Netzwerk gelangen und sich ausbreiten.

Stand der Technik: Datenschleusen

Datenschleusen bieten eine fortschrittliche und vor allem sichere Alternative zu herkömmlichen Methoden. Diese Systeme kombinieren im Idealfall mehrere Antiviren-Engines und ermöglichen eine parallele Überprüfung auf Malware außerhalb des Netzwerk-Perimeters.

Manche Datenschleusen wie MetaDefender Kiosk von Opswat nutzen bis zu 35 Anti-Malware-Engines verschiedener Hersteller gleichzeitig. Das erhöht die Malware-Erkennungsrate auf über 99 Prozent und spart zudem wertvolle Zeit.

So funktionieren moderne Datenschleusen:

- Mehrfach-Scans für höhere Sicherheit: Datenschleusen nutzen mehrere Antiviren-Engines verschiedener Hersteller. Dies maximiert die Malware-Erkennungsrate und reduziert damit das verbleibende Risiko. Der parallele Malware-Check spart viel Zeit im Vergleich zu seriellen Scans der Dateien.
- Sicherer Workflow: Datenschleusen arbeiten isoliert vom Netzwerk – infizierte Dateien gehen daher in Quarantäne oder werden gelöscht, die Malware kann sich also nicht im Netzwerk verbreiten. Unkritische Dateien können entweder direkt ins Netzwerk übertragen oder auf sichere, freigegebene Datenträger kopiert werden. Dies minimiert das Risiko durch manipulierte Hardware, zum Beispiel durch BadUSB, einer versteckten und gefährlichen Malware.
- Schutz vor Evasive- und Zero-Day-Malware: Schad-Software, welche Antiviren-Engines mangels Signatur noch nicht erkennen, ist besonders kritisch. Einige Datenschleusen-Hersteller bieten ein optionales Datei-Desinfektionsmodul an. Dieses entfernt sämtliche potenziell gefährlichen Inhalte wie Makros oder eingebettete Links und wandelt riskante Dateitypen in sichere Formate um.

Einsatzbereiche von Datenschleusen

Datenschleusen werden gerade in sicherheitskritischen Bereichen häufig eingesetzt. Zwei Beispiele sind Sicherheitsbehörden oder kritische Infrastrukturen, deren Systeme dauerhafte Integrität und Verfügbarkeit erfordern. Ein weiteres Beispiel sind industrielle Steuerungssysteme und Produktionsanlagen, die nur ein geringes Schutzniveau haben und keine Ausfallzeiten erlauben.

Fazit

Gegenüber herkömmlichen Methoden bieten Datenschleusen deutliche Vorteile: Sie überprüfen mobile Speichergeräte effizient und sicher auf Malware.

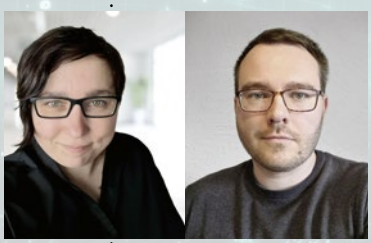
Datenschleusen haben sich deshalb besonders in sicherheitskritischen Umgebungen als unverzichtbar etabliert. •

Manuelles versus automatisiertes Pentesting

Das Pentesting hat sich weiterentwickelt – von manuellen Überprüfungen hin zu automatisierten Lösungen inklusive Cybersicherheits-Validierung des gesamten Netzwerks. Wie unterscheiden sich diese Methoden und was können Unternehmen damit erreichen? Ein Vergleich.

VON MAREEN DOSE UND DANIEL HOYER

WENN ES UM CYBERSICHERHEIT GEHT, gilt es, die Verteidigungsmechanismen kontinuierlich auf Herz und Nieren prüfen. Penetrationstest (Pentesting) haben sich als bewährte Methode etabliert, um die Wirksamkeit der Sicherheitsmaßnahmen zu validieren und potenzielle Angriffsvektoren aufzudecken. Doch wie sich die Bedrohungslandschaft weiterentwickelt, so wandelt sich auch die Art und Weise, wie die Tests durchgeführt werden. Traditionell dominierten manuelle Ansätze, bei denen erfahrene Sicherheitsexperten die Perspektive von Angreifern einnehmen und versuchen, in Unternehmensnetzwerke einzudringen. Heute jedoch gewinnen automatisierte Lösungen zunehmend an Bedeutung. Mit ihnen lässt sich die Sicherheit kontinuierlich überprüfen, ohne externe Spezialisten zu beauftragen.



DIE AUTOREN
Mareen Dose und Daniel Hoyer
sind Presales Consultants bei indevis.
Sie beraten Kunden in allen Belangen rund um die Abwehr und Bekämpfung von Cyberbedrohungen.

Manuelles Pentesting bietet Momentaufnahme

In der Vergangenheit beauftragten Unternehmen meistens externe Dienstleister, die dann Netzwerke, Anwendungen und Prozesse auf Schwachstellen untersuchten. Die Experten führen realistische Angriffe durch und versuchen, in die Systeme einzudringen. Dieser Ansatz hat einige Vorteile: Spezialisierte Pentester bringen ihre langjährige Erfahrung und ihr Fachwissen ein und können auch Social-Engineering-Szenarien prüfen.

Allerdings hat diese Methode auch Grenzen. Sie liefert lediglich eine Momentaufnahme der aktuellen Sicherheitslage – und die veraltet rasch. IT-Umgebungen und Angriffstechniken entwickeln sich ständig weiter, was die Angriffsfläche und das Risikoprofil unablässig ändert. Außerdem hängen die Ergebnisse stark von den individuellen Fähigkeiten des beauftragten Experten ab – das erschwert eine einheitliche Bewertung.

Automatisierte Sicherheitsvalidierung: Kontinuierlich und standardisiert

Im Gegensatz dazu eröffnet die „Automated Security Validation" oder einfach „automatisiertes Pentesting" eine laufende Kontrolle. Mithilfe von KI-gestützter Software scannen diese Plattformen die IT-Umgebung auf ausnutzbare Sicherheitslücken und führen realistische Angriffe durch. Dabei greifen sie auf eine umfangreiche Datenbank mit aktuellen Bedrohungsinformationen zurück.

Einer der Hauptvorteile des automatisierten Pentesting ist die Möglichkeit, Penetrationstests rund um die Uhr und in regelmäßigen Abständen durchzuführen. Auf diese Weise können Unternehmen ihre Angriffsfläche und Risikoexposition kontinuierlich überwachen und schnell auf Veränderungen reagieren. Darüber hinaus liefern die Lösungen einheitliche Berichte, die es erlauben, den Sicherheitsstand über mehrere Standorte hinweg konsistent zu bewerten.

Wann ist welcher Ansatz empfehlenswert?

Beide Methoden – manuelles und automatisiertes Pentesting – haben ihre Berechtigung und ergänzen sich in der Praxis oft gegenseitig. Manuelle Überprüfungen eignen sich besonders für komplexe Szenarien, die nur schwer automatisierbar sind, wie beispielsweise Social-Engineering-Angriffe oder umfangreiche Red-Teaming-Übungen.

Automatisierte Lösungen hingegen sind ideal, um Standardszenarien kontinuierlich zu validieren und gro-

ße Testumfänge zu bewältigen. Sie helfen außerdem dabei, Schwachstellen richtig zu priorisieren und dort zu patchen, wo es am nötigsten ist. Denn Vulnerability-Management-Systeme reichen dafür oft nicht aus..

Compliance-Anforderungen: Pentesting wird zur Pflicht

Doch Pentesting ist nicht nur eine empfehlenswerte Praxis, sondern für viele Unternehmen auch gesetzlich gefordert. Die NIS2-Verordnung, die bis Oktober 2024 in nationales Recht umgesetzt werden muss, verlangt von Einrichtungen kritischer Infrastrukturen (KRITIS) und deren Lieferkette regelmäßige Sicherheitsüberprüfungen, ein Cyberrisiko- und ein Business-Continuity-Management. Pentesting gilt hierbei als wichtiges Instrument.

Auch der Digital Operational Resilience Act (DORA), der Anfang 2023 in Kraft trat, schreibt Penetrationstests explizit als Maßnahme vor. Das Gesetz gilt ab Anfang 2025 verbindlich für alle europäischen Unternehmen des Finanzsektors. Gartner hat unter anderem deshalb Pentesting unter „Adversial Exposure Validation" in seinem aktuellen Hype Cycle 2024 für Security Operations aufgenommen und als Innovation-Treiber eingestuft.

Chancen für den Mittelstand

Soll Pentesting erfolgreich sein, müssen jedoch einige Voraussetzungen erfüllt sein: Ein solides Sicherheitsniveau und etablierte Best Practices. Beides stellt sicher, dass die Menge der gefundenen Sicherheitslücken Unternehmen nicht überfordert. Zudem gilt es, Berichte zu verstehen und geeignete Maßnahmen umzusetzen. Bisher war die Praxis der Penetrationstest hauptsächlich großen Unternehmen vorbehalten. Doch als Managed Security Service wird es künftig auch für kleinere und mittelständische Unternehmen zugänglich. •

Soll Pentesting erfolgreich sein, müssen jedoch einige Voraussetzungen erfüllt sein: Ein **solides Sicherheitsniveau und etablierte Best Practices**. Beides stellt sicher, dass die Menge der gefundenen Sicherheitslücken Unternehmen nicht überfordert.

GenAI – der Turbo für IT-Security?

Künstliche Intelligenz liegt im Trend. Gefühlt beansprucht inzwischen jeder Technologieanbieter für sich, KI in irgendeiner Art und Weise zu verwenden – die Security-Branche bildet hier keine Ausnahme. Dabei lohnt sich ein genauer Blick, wo und wie KI aktuell tatsächlich IT-Security-Prozesse unterstützt und die Automatisierung vorantreibt.

VON MICHAEL HAAS

KI-TECHNOLOGIEN SIND INZWISCHEN EIN ELEMENTARER BAUSTEIN vieler moderner sogenannter Detection-and-Response-Lösungen –Endpoint Detection and Response (EDR), Network Detection and Response (NDR) oder Managed Detection and Response (MDR) sind hier klassische Beispiele. Diese Produkte nutzen oftmals Machine Learning und Deep Learning, um anomale Verhaltensweisen zu erkennen, die auf eine potenzielle Bedrohung oder einen Angriff innerhalb einer IT-Umgebung hinweisen.

GenAI noch im Reifeprozess

Im Gegensatz zu diesen bereits weitreichend erprobten Technologien ist generative KI (GenAI) das Nesthäkchen im KI-Umfeld. Tools wie ChatGPT gibt es erst seit knapp zwei Jahren, somit hatte diese Form der Künstlichen Intelligenz noch nicht die gleiche Zeit, sich zu etablieren und weiterzuentwickeln. Während sich andere KI-Technologien vor allem auf das Lernen aus großen Datensätzen konzentriert haben, zeigt GenAI seine Stärken bei der Erstellung schriftlicher, visueller und auditiver Inhalte unter Verwendung von Prompts oder Eingabedaten.

Auch wenn derzeit erst 24 Monate verstrichen sind, um GenAI im Zuge unterschiedlicher Anwendungsfälle dediziert auf Herz und Nieren zu prüfen: Es besteht wohl keinerlei Zweifel daran, dass sich die Technologie in einer Hype-Phase befindet und breite öffentliche Aufmerksamkeit genießt. Inwieweit, wann und wie schnell der Weg ins „Tal der Desillusionierung“ führt und welche konkreten Einsatzszenarios sich am Ende bewähren und durchsetzen werden, bleibt abzuwarten.

Aktuell steht die IT-Security-Branche noch ganz am Anfang. Es wird erprobt, wie sich die neuen Möglichkeiten von GenAI bei der Erkennung und Abwehr von Bedrohungen bestmöglich ausspielen lassen. In dem Zusammenhang kristallisieren sich jedoch bereits ein paar offensichtliche Ansatzpunkte für den praktischen Einsatz von Gen AI heraus:

- E-Mail:
  Möglicherweise liefert GenAI eine stichhaltige Antwort auf die uralte Frage, wie sich Phishing-Versuche blockieren lassen, bevor entsprechende Mails im Posteingang des Empfängers landen. Bestehende Lösungen verlassen sich momentan noch stark darauf, dass Mitarbeiter Phishing-Nachrichten identifizieren und melden. GenAI-basierte Produkte, die darauf trainiert sind, Anomalien in geschriebener Sprache und E-Mail-Adressen zu erkennen, könnten die von Spam- und Phishing-Nachrichten ausgehende Gefahr drastisch reduzieren. Leider nutzen aber auch die Cyberkriminellen GenAI, um die Qualität ihrer Phishing-Nachrichten zu verbessern, so dass wir im gleichen Zug auch einige einfache Möglichkeiten, die heute bei der Erkennung von Phishing-Nachrichten Wirkung entfalten, verlieren werden.

> „GenAI steht **eine glänzende Zukunft bevor** und viele Akteure der IT-Sicherheitsbranche testen die Möglichkeiten, um die Funktionalität gewinnbringend auszuspielen.“

- Identität
  Cyberkriminelle setzen inzwischen auf GenAI-basierte Werkzeuge, die ihnen helfen, andere Menschen zu imitieren, einschließlich der Nachahmung ihrer Stimme, ihres Bildes und ihres Schreibstils. Die Ergebnisse sind jedoch oftmals nicht hundertprozentig exakt. Daher kann es hilfreich sein, GenAI auch in Sicherheitsprodukten einzusetzen, um genau die Details zu beleuchten, die nicht mit der tatsächlichen Person übereinstimmen. Auf diese Weise lassen sich GenAI-basierte Angriffe aufspüren und abwehren, Sicherheitssysteme gewinnen bei der Authentifizierung von Benutzern so weiter an Schlagkraft.

- Reporting
  Bei der Erstellung individueller Berichte kann GenAI klar punkten. Mit wenigen Eingaben sind zum Beispiel benutzerdefinierte Reports generierbar, die die Einhaltung und Wirksamkeit von Sicherheitsprotokollen aufzeigen. Selbst wenn die heutigen GenAI-Funktionen noch nicht so weit ausgereift sind, um diesen Prozess vollständig zu automatisieren und händische Nacharbeit erforderlich ist: Schneller geht es allemal.

- Verbesserte Assistenten zur Sicherheitsanalyse
  Mit GenAI-Tools lassen sich beispielsweise identifizierte Vorfälle oder andere sicherheitsrelevante Erkenntnisse effektiv zusammenzufassen. Technische Sprache kann in verständliche Formulierungen gegossen werden, empfohlene Maßnahmen werden dadurch nachvollziehbarer. Der Einsatz ist aber auch in anderer Richtung denkbar: So können IT-Verantwortliche über Prompts Vorschläge zur verbesserten Konfiguration ihrer Sicherheitsplattform abfragen. Dies ermöglicht die Reaktion auf eine neue Bedrohung, sobald diese in den Nachrichten für Schlagzeilen sorgt.

Fazit

GenAI steht eine glänzende Zukunft bevor und viele Akteure der IT-Sicherheitsbranche testen die Möglichkeiten, um die Funktionalität gewinnbringend auszuspielen. Das Potenzial ist offensichtlich, vor allem im Hinblick auf interne Effizienzsteigerungen bei Programmierung, Kunden-Support und der Erstellung von Vertriebs- beziehungsweise Marketinginhalten. Bei der Integration in Produkte ist die Branche noch nicht ganz so weit, schließlich zählt im Rahmen der Cybersicherheit ein hohes Maß an Vorhersagbarkeit, um Kundenbedürfnisse erfüllen zu können. Hier braucht GenAI wohl noch ein wenig Zeit, um diese hohen Standards zu erreichen.

GenAI wird Cybersicherheitsprodukte also nicht von jetzt auf gleich neu erfinden. Es sollte jedoch nicht vergessen werden, wie positiv sich etabliertere KI- und ML-Technologien schon heute im Zuge einer modernen Cyberabwehr auswirken. •

DER AUTOR
Michael Haas
ist Regional Vice President Central Europe bei WatchGuard Technologies.

NEUE STUDIE ZU CYBER SECURITY – DIGITALISIERUNG VERSCHÄRFT DIE BEDROHUNGSLAGE

Das Risiko von Unternehmen, Opfer eines Cyber-Angriffs zu werden, bleibt hoch: 82 Prozent der befragten IT- und Security-Verantwortlichen von 150 Unternehmen in Deutschland beobachten seit Anfang 2023 eine Zunahme der Cyber-Sicherheitsrisiken. Die Digitalisierung führt laut 40 Prozent der Befragten zu einer neuen Qualität der Bedrohungen: Da Software praktisch alle Unternehmensbereiche durchdringt und immer mehr Geschäftsprozesse in die Cloud verlagert werden, erhöht sich die Zahl der Angriffsmöglichkeiten für Hackerinnen und Hacker. Auch die geopolitische Lage trägt zu einem Anstieg der Bedrohungen bei. Trotz der Zunahme des IT-Sicherheitsrisikos haben 33 Prozent der befragten Unternehmen keinen vollständigen Überblick über ihren konkreten Cyber-Security-Status, so die Ergebnisse der neuen Lünendonk-Studie 2024 „Von Cyber Security zu Cyber Resilience. •

KRYPTO-AGILITÄT: DER SCHLÜSSEL ZUR ABWEHR ZUKÜNFTIGER CYBERBEDROHUNGEN

In der modernen Cybersicherheitslandschaft stellt Krypto-Agilität einen essenziellen Bestandteil dar, um zukünftige Bedrohungen abzuwehren und die Sicherheit von Unternehmen jeder Größe zu gewährleisten. „Unternehmen müssen sich immer wieder neuen Herausforderungen stellen, insbesondere im Hinblick auf den Schutz von sensiblen und unternehmenskritischen Daten“, so Ari Albertini, CEO bei FTA-PI. „Cyberangriffe werden immer ausgefeilter und Entwicklungen wie Cybercrime-as-a-Service ermöglichen es, Cyberangriffe auch ohne IT-Kenntnisse zu starten.“ Krypto-Agilität ist die Fähigkeit, schnell und flexibel auf sich verändernde Bedrohungen reagieren zu können. Dafür werden alternative Verschlüsselungstechnologien in einem System implementiert. Eine solche Infrastruktur ermöglicht es, zwischen mehreren kryptografischen Algorithmen zu wechseln beziehungsweise die Algorithmen getrennt voneinander zu aktualisieren. So wird die Sicherheit der Daten sowie der Kommunikation gewährleistet. •

NEWS

Bild/Copyright: Rawpixel.com – stock.adobe.com

IMPRESSUM

DIGITAL BUSINESS CLOUD Magazin
www.digitalbusiness-cloud.de

Herausgeber und Geschäftsführer:
Matthias Bauer, Günter Schürger

So erreichen Sie die Redaktion:
Chefredaktion: Heiner Sieger (v. i. S. d. P.), heiner.sieger@win-verlag.de
Tel.: +49 (89) 3866617-14
Redaktion:
Konstantin Pfliegl, konstantin.pfliegl@win-verlag.de
Tel. +49 (89) 3866617-18
Stefan Girschner, stefan.girschner@win-verlag.de
Tel.: +49 (89) 3866617-16

Mitarbeiter dieser Ausgabe:
Ari Albertini, Dr. Yvonne Bernard, Mareen Dose, Daniel Eberhorn, William Fendt, Christian Gäbel, Michael Haas, Daniel Hanke, Florian Hansemann, Dr. Niklas Hellemann, Sven Hillebrecht, Paul Hennin, Daniel Hoyer, Klaus Jetter, Robert Korherr, Miro Mitrovic, Dr. Gerald Pfeifer, Daniel Tremmel, Steffen Ullrich

Stellvertretende Gesamtanzeigenleitung:
Bettina Prim, bettina.prim@win-verlag.de, Tel.: +49 (89) 3866617-23

Mediaberatung:
Gabriele Leyhe, gabriele.leyhe@win-verlag.de, Tel.: +49 (89) 3866617-24

Anzeigendisposition:
Chris Kerler, dispo@win-verlag.de, Tel.: +49 (89) 3866617-32,
Sabine Immerfall, dispo@win-verlag.de, Tel.: +49 (89) 3866617-33

So erreichen Sie den Abonnentenservice:
Leserservice:
WIN-Verlag GmbH & Co. KG
Max-Planck-Str. 7/9, 97070 Würzburg
Tel: +49 89 3866617 46
Fax: +49 89 3866617 47
abovertrieb@win-verlag.de

Vertrieb:
Sabine Immerfall, sabine.immerfall@win-verlag.de,
Tel.: +49 (89) 3866617-33

Produktion/Herstellung:
Jens Einloft, jens.einloft@win-verlag.de, Tel.: +49 (89) 3866617-36

Artdirection/Titelgestaltung:
DesignConcept Dagmar Friedrich-Heidbrink

Bildnachweis/Fotos:
stock.adobe.com, shutterstock.com, Werkfotos

Vorstufe + Druck:
C. Maurer GmbH & Co. KG, Geislingen/Steige

Anschrift Anzeigen, Vertrieb und alle Verantwortlichen:
WIN-Verlag GmbH & Co. KG
Balanstraße 73, Gebäude Nr. 21A, EG, 81541 München
Telefon +49 (89) 3866617-0

Verlags- und Objektleitung:
Martina Summer, martina.summer@win-verlag.de,
Tel.: +49 (89) 3866617-31

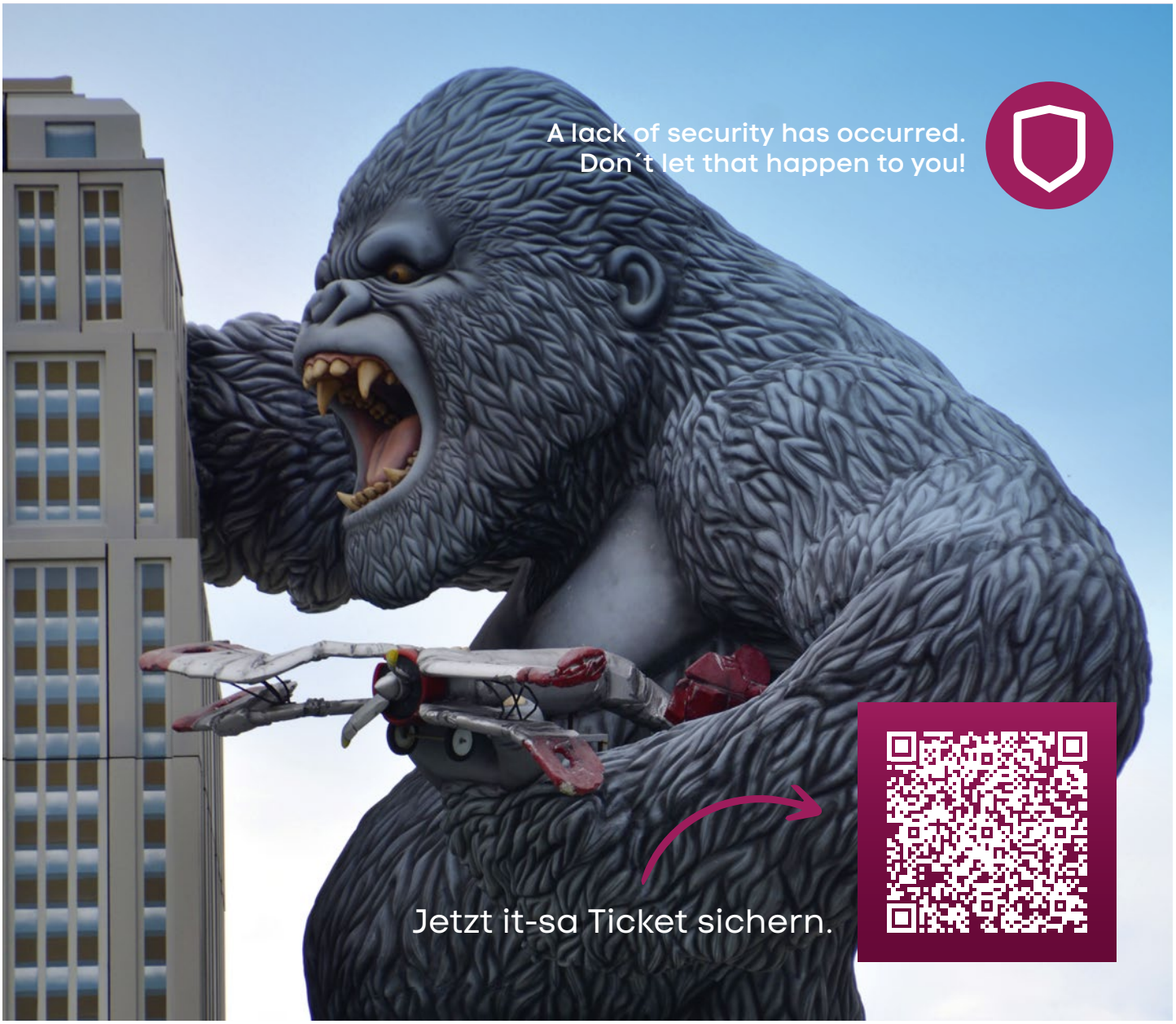
Bezugspreise:
Einzelverkaufspreis: 11,50 Euro in D, A, CH und 13,70 Euro in den weiteren EU-Ländern inkl. Porto und MwSt. Jahresabonnement (6 Ausgaben): 69,00 Euro in D, A, CH und 82,20 Euro in den weiteren EU-Ländern inkl. Porto und MwSt. Vorzugspreis für Studenten, Schüler, Auszubildende und Wehrdienstleistende gegen Vorlage eines Nachweises auf Anfrage. Bezugspreise außerhalb der EU auf Anfrage.

28. Jahrgang
Erscheinungsweise: 6-mal jährlich

Einsendungen: Redaktionelle Beiträge werden gerne von der Redaktion entgegen genommen. Die Zustimmung zum Abdruck und zur Vervielfältigung wird vorausgesetzt. Gleichzeitig versichert der Verfasser, dass die Einsendungen frei von Rechten Dritter sind und nicht bereits an anderer Stelle zur Veröffentlichung oder gewerblicher Nutzung angeboten wurden. Honorare nach Vereinbarung. Mit der Erfüllung der Honorarvereinbarung ist die gesamte, technisch mögliche Verwertung der umfassenden Nutzungsrechte durch den Verlag – auch wiederholt und in Zusammenfassungen – abgegolten. Eine Haftung für die Richtigkeit der Veröffentlichung kann trotz Prüfung durch die Redaktion vom Herausgeber nicht übernommen werden.

ISSN 2510-344X, VKZ B31383F
Dieses Magazin ist umweltfreundlich auf chlorfrei gebleichtem Papier gedruckt.

Außerdem erscheinen beim Verlag:
AUTOCAD Magazin, BAUEN AKTUELL, r.energy, DIGITAL ENGINEERING Magazin, DIGITAL MANUFACTURING, e-commerce Magazin, DIGITAL BUSINESS CLOUD, DIGITAL PROCESS INDUSTRY, DIGITAL HEALTH INDUSTRY



Security

JETZT ZU M365 WECHSELN – FÜR MAXIMALE SICHERHEIT IM DIGITALEN WORKSPACE!

Treffen Sie uns auf der it-sa 2024 in Nürnberg
Stand: 6-446 - Halle: 6

Microsoft 365

TAROX
tarox.de

TREND MICRO™

Cybersecurity
neu gedacht

Reduzieren Sie die Komplexität. Steigern Sie Ihre Resilienz.

Das Management von Cyberrisiken ist essentiell für Ihren Geschäftserfolg. Unsere KI-gestützte Cybersicherheitsplattform Trend Vision One™ hilft Ihnen, Cyberrisiken besser zu verstehen, zu kommunizieren und zu minimieren

Entdecken Sie, was möglich ist unter TrendMicro.com/visionone