EURO SECURITY Special

Das Sicherheitsmagazin für Planer, Errichter und Anwender für die DACH-Region

Experten Ausblick

Das Potenzial generativer KI für den Sicherheitssektor; Cyberangriffe: Mehr Daten diebstahl statt Erpressung

Videotechnik

Die vier wichtigsten Trends für Videoüberwachung 2024; Mehr Videodaten verarbeiten Dank Edge-Bereich

Cloud-Sicherheit

Eine Studie unterstreicht, dass Zero-Trust-Segmentierung für die Cloud-Sicherheit unverzichtbar ist

ISSN 09481249 • 12-2023 • ZKZ 16724 Postvertriebsstück bezahlt • 80383 BAY Germany ©SEC Global • euro-security.de

Inhalt

Inhalt

euro-security.tv euro-security.de

Editorial

Sicherheitsprognosen von allen Seiten beleuchtet

In diesem Special haben wir eine große Anzahl von Meinungen zusammengetragen, die Sicherheitsrisiken und Antworten auf Entwicklungen in Industrie, Wirtschaft und Gesellschaft aufzeigen. Viele Autoren haben ihre Strategien in fünf oder mehr Punkte zusammengefasst. Manches überschneidet sich, andere Beiträge schaffen neue Perspektiven.

Beim Rückblick auf das Jahr 2023 wird schnell deutlich: Die wichtigsten Trends in Industrie und Wissenschaft bestimmen auch in den Bereich physischer und IT-basierter Sicherheitslösungen die Lage. So nimmt die Rolle der Künstlichen Intelligenz eine wirklich starke Rolle ein – sowohl im Hinblick auf Sprachmodelle und generativer KI. Sprachgestützte Lösungen können eine Entlastung des Kundendienstes in einem Unternehmen eröffnen und auch einen Mehrwert für die Kunden bei ihren Anfragen im Komfort bieten. Die Rolle der KI bei Sicherheitsanwendungen eröffnet Chancen, die Lösungen genauer und effizienter machen werden. Damit kann die Mensch-Maschine-Beziehung das Betreiben von Sicherheitslösungen fehlerfreier, aber auch kostengünstiger gestalten. Auch im nächsten Jahr wird die automatische Erkennung von Objekten ein wichtiges Thema. In Anbetracht des bestehenden Fachkräftemangels werden sich hier weitere Wachstumschancen eröffnen und auch die Akzeptanz wird weiter zunehmen.

Cloud-Technologie, SaaS oder BYOD-Modelle sind für die IT-Sicherheit wichtige Bereiche, die es abzusichern gilt. In diesem Special gehen viele Experten unter Berücksichtigung verschiedener Aspekte auf die richtigen Sicherheitsmaßnahmen und bestehende Sicherheitsrisiken ein. Die Sicherheit von Endgeräten und darauf abgestimmte Phishing-Techniken sind ein Top-Thema. Das Jahr 2024 sollte dafür genutzt werden, spezifisch auf mobile Endgeräte zugeschnittene Maßnahmen Sicherheitsstrategien zu erarbeiten.
Im Hinblick auf klassische Malware, prognostiziert ein Experte, dass der Schutz vor Cyber-Kriminellen zunehmend von der Fähigkeit eines Unternehmens abhängig sein wird, qualifizierte Mitarbeiter zu finden. Also auch hier schlägt der Fachkräftemangel negativ auf die Sicherheitslage durch.
Generell müssen sich Anbieter von Sicherheitslösungen auch verstärkt mit der klassischen IT-Sicherheit auseinandersetzen, weil die Digitalisierung auch hier Anbieter und Anwender fordert.

Wir wünschen viel Spaß beim Lesen, besinnliche Feiertage und einen guten Rutsch ins neue Jahr.

Dr Claudia Mrozek

Impressum

Euro Security Fachmedien (Verlagsvertretung); Grabenfeldstrasse 25, 83083 Riedering, Tel: +49 (0)8036 3035071; Email: redaktion@euro-security.de
Redaktion: ***Dr. Claudia Mrozek, Chefredak. (V.i.S.d.P., Herausgeber)***, *Caroline Best, Angela Kloose, Dirk Lehmanski, Maria Lehmen, Anne, Schneider, Heiko Scholz, Patricia Ovo, Cathy Thomens, Sophie Mrozek, Alexander Mrozek, Mariam Nassreddin; Marcus Smid, Angela Thorn*
Druckerei *D+L Print, Dorsten / Schmidl & Rotaplan Druck, Regensburg*
Aboverkauf *DCMN Marketing Agentur, Email: abo@sec-global.org*
Anzeigenverwaltung/-vertretung *DCMN Marketing Agentur Oberbayern, Bestellungen und Druckvorlagen: anzeigen@euro-security.de*
Copyright: *Der Markenverwerter SEC Global ist urheberrechtlich verantwortlich für Inhalt, Design und die Herstellung von Druckmaterialien/-erzeugnissen für die Fachzeitschriften Euro Security, Middle East Security und African Security. Ebenfalls betreffen allgemeine Copyrightrechte und -pflichten die Webseite ‚www.eurosecglobal.de' und alle angeschlossenen Seiten, digitalen Services und Publikationen. Ohne Zustimmung des Verlags können weder ganze Artikel noch große Teile von Texten per E-Mail, über ‚Social Media'-Netzwerke oder auf andere Weise veröffentlicht werden. Eine wirtschaftliche Verwertung oder eine andere kommerzielle Benutzung ist nicht zulässig. In Verbindung mit der gedruckten Zeitschrift oder den veröffentlichten Texten auf der Website bzw. digitalen Anwendungen ist das Reproduzieren oder die Vervielfältigung von Marken/ Logos (wie "Euro Security" [ES] oder "Middle East Security" [MES] Name genauso wie andere verlagseigene Logos oder Handelsnamen nur mit schriftlicher Genehmigung der Verlagsleitung möglich. Das Kopieren oder die Verlinkung ganzer Textpassagen unter eigenem Namen sind ausschließlich für den persönlichen und nicht-kommerziellen Gebrauch zulässig. Der Ausdruck eines Artikels auf Papier ist zulässig, eine Vervielfältigung nicht. Genauso ist eine Speicherung für den privaten Gebrauch zulässig. Eine Verwendung, die über den nicht-kommerziellen Gebrauch hinausgeht, ist nicht erlaubt. Digitale Anwendungen sind pro Lizenz nur auf bis zu fünf getrennten Geräten zu verwenden. Auch aus diesen Quellen ist eine Reproduktion, Veränderung oder eine kommerzielle Verwendung nicht gestattet. Die Übertragung der Inhalte auf andere Webseiten, Newsgroups, Mailinglisten, elektronische Bulletins, Servern oder andere Medien, die mit einem Netzwerk verbunden sind oder regelmäßig oder systematisch Inhalte in elektronischer (einschließlich der im Rahmen jeder Bibliothek, Archiv oder ähnliche Dienstleistung) speichern, ist nicht gestattet. Jede Verwendung der im Druck oder Online publizierten Inhalte sind ausdrücklich untersagt. Anfragen auf Genehmigung bitte an eines unserer SEC Global unter copyright@sec-global.org senden. Eine Freigabe oder ein kostenpflichtiges Angebot wird Ihnen umgehend zugehen. © Sec Global*

EURO SECURITY Fachverlage und - medien ist förderndes Mitglied im BHE/Deutschland. BHE-Mitglieder erhalten im Rahmen ihrer Mitliedschaft regulär erscheinende Ausgaben der Euro Security DACH kostenlos.

17. – 20. September 2024

SECURE YOUR BUSINESS

Sonder- und Spezialeinheiten

Geschlossener Bereich für behördliche Sicherheitskräfte

50 years

security essen

Die Leitmesse für Sicherheit

www.security-essen.de

MESSE ESSEN

SICHERHEIT 2024

Das Potenzial generativer KI für den Sicherheitssektor

„2023 war das Jahr, in dem große Sprachmodelle (Large Language Models, LLM) als Grundlage für generative KI in das öffentliche Bewusstsein rückten. Jedes Unternehmen untersucht potenzielle Anwendungs- fälle für generative KI und der Sicherheitssektor ist da keine Ausnahme. Im Jahr 2024 werden wir sicherheitsorientierte Anwendungen sehen, die auf dem Einsatz von LLMs und generativer KI basieren.

Dazu werden wahrscheinlich Assistenten für Bediener gehören sowie ein interaktiver Kundensupport. Erstere unterstützen Unternehmen dabei, Videomaterial genauer und effzienter zu interpretieren, letzterer liefert nützliche und umsetzbare Antworten auf Kundenanfragen. Darüber hinaus hat generative KI ihren Wert in der Softwareentwicklung bereits unter Beweis gestellt, was sich im gesamten Sicherheitssektor als vorteilhaft erweisen wird."

Jochen Sauer, Architect & Engineering Manager bei Axis Communications (©Axis)

KI-Automatisierung und Cloud-Transformation für die IT-Sicherheit

„In Sachen IT-Sicherheit stehen zahlreiche Unternehmen nach wie vor am Anfang der Cloud-Transformation und haben die verschiedenen Möglichkeiten, die sich hierdurch für die Verbesserung ihrer IT-Sicherheitsstrategie ergeben, noch nicht ausgeschöpft. Konkret wird sich der Trend zu modernen SASE-Architekturen noch einmal verstärken, da diese im Vergleich zu den bestehenden SD-WAN-Modellen sowohl ein höheres Maß an Flexibilität und Sicherheit als auch Kosteneinsparungspotenzial im Betrieb bieten. Ein weiteres großes Thema, das wir sehen, ist künstliche Intelligenz als Ergänzung bestehender Prozesse, insbesondere für die automatisierte Prüfung, Bearbeitung und Nachbearbeitung von Sicherheitsvorfällen, um IT-Sicherheits-Teams zu entlasten und so insbesondere in Unternehmen mit begrenzten IT-Ressourcen Kapazitäten für komplexere Aufgaben freizumachen. Dementsprechend wird die Nachfrage nach KI-basierten Plattform- und Automatisierungslösungen für die IT-Sicherheit in Zukunft noch weiter steigen, sowohl auf Kunden- als auch auf Managed Services-Anbieterseite."

Ulrich Brüll, CTO bei Conscia Deutschland, ©Conscia Deutschland

Mehr BYOD-Modelle erfordern zusätzliche Sicherheitsmaßnahmen für mobile Endgeräte

„In immer mehr Unternehmen werden Bring Your Own Device-Modelle (BYOD) eingeführt und Mitarbeiter nutzen zunehmend private Smartphones und Tablets für Berufliches. Für die IT-Sicherheit ergeben sich dadurch neue Risiken, da Cyberkriminelle ihre Methoden spezifisch an mobile Endgeräte anpassen – zum Beispiel durch Phishing-Techniken, die auf kleineren Bildschirmen ganz besonders schwer zu erkennen sind und Social Engineering, das sich die legerere Handhabung von mobilen Endgeräten zu Nutze macht. Dementsprechend muss ‚Mobile First' in Zukunft auch ‚Mobile Security First' bedeuten: IT-Sicherheitsverantwortliche müssen die Risiken der mobilen Endgeräte im Unternehmen neu bewerten und im nächsten Schritt entsprechende, spezifisch auf mobile Endgeräte zugeschnittene Maßnahmen treffen, da schon ein einziges kompromittiertes Gerät schwerwiegende Folgen für die gesamte Unternehmenssicherheit haben kann."

Henrik Nitsche, Security Solution Manager bei Jamf; ©Jamf

Cyberangriffe: Zunehmend auf Datendiebstahl statt Erpressung

„Anstatt nur auf Ransomware zu setzen – sprich, die Daten eines kompromittierten Unternehmens zu verschlüsseln und für die Entschlüsselung ein Lösegeld zu verlangen – werden Cyberkriminelle in Zukunft auch verstärkt auf subtilere Methoden setzen. Sobald sie sich Zugang zu einem Unternehmensnetzwerk verschafft haben, können Angreifer beispielsweise die Verwaltungsanwendungen, die bereits im Netzwerk aktiv sind, nutzen, um nach und nach über einen längeren Zeitraum hinweg und größtenteils unbemerkt Daten zu entwenden. Die Vorteile dieses Ansatzes sind klar: Jedes Unternehmen hat potenziell Zugriff auf Technologien zur Erkennung und Beseitigung von Malware, aber wenn keine Malware verwendet wird, sind diese nicht effektiv. Stattdessen braucht es aufmerksame Mitarbeiter, die Unstimmigkeiten im Netzwerk erkennen und melden – Schutz vor Cyberkriminellen wird also in Zukunft zunehmend von der Fähigkeit eines Unternehmens abhängig sein, qualifizierte Mitarbeiter zu finden."

Mark Stockley, Cybersecurity Evangelist bei Malwarebytes, © Mark Stockley

IT-Sicherheit entwickelt sich vom Kostenpunkt zum Wachstumstreiber

„Mit der kontinuierlichen Eskalation von Cyberbedrohungen in den vergangenen Jahren haben Führungskräfte in Unternehmen zunehmend verstanden, wie wichtig IT-Sicherheit ist. Nach wie vor zählt sie jedoch immer noch als ein in sich geschlossener Bereich im Unternehmen und die IT-Sicherheitsteams als separate Abteilungen, die außerhalb des Tagesgeschäfts agieren. Auch dahingehend wird ein Umdenken notwendig werden.Führungskräfte müssen IT-Sicherheit als wichtigen Geschäftsfaktor verstehen, nicht als reinen Kostenpunkt wie bislang. IT-Sicherheitsteams müssen enger in die Abläufe und Prozesse des Geschäftsalltags integriert werden und IT-Sicherheit als strategische Priorität definiert werden. Tatsächlich ist IT-Sicherheit aufgrund der voranschreitenden Digitalisierung nämlich bereits mit den meisten Aspekten des Geschäftsbetriebs eng verflochten und kann deshalb nicht mehr außen vor bleiben. Unternehmen, die dies erkennen und eine entsprechende Transformation einleiten, können IT-Sicherheit umso schneller zu einem Wachstumstreiber machen."

Michael Armer, CISO bei RingCentral; ©RingCentral,

20. WELT-ANTIKORRUPTIONSTAG

Erfolgreich gegen Korruption

Seit dem 9. Dezember 2003 wird jährlich der Welt-Antikorruptionstag begangen. In diesem Jahr feiert der Internationale Tag gegen Korruption nunmehr sein 20-jähriges Bestehen. Mit diesem Tag soll an das Übereinkommen der Vereinten Nationen gegen Korruption (UNCAC) vom 31.Oktober 2003 erinnert und auf die Gefahren, das Ausmaß und die Konsequenzen von Korruption hingewiesen werden.

Das UN-Übereinkommen wurde mittlerweile von 190 Vertragsparteien unterzeichnet (Stand: 10. Oktober 2023). Darin verpflichten sich die beigetretenen Länder, verschiedene Formen der Korruption zu bestrafen und bei deren Bekämpfung international zusammenzuarbeiten. Es umfasst fünf Hauptbereiche: Präventivmaßnahmen, Kriminalisierung und Strafverfolgung, internationale Zusammenarbeit, Vermögensabschöpfung sowie technische Hilfe und Informationsaustausch. Die Konvention deckt die unterschiedlichen Formen von Korruption ab. Hierzu gehören insbesondere Bestechung, Vorteilsgewährung, Einflussnahme, Amtsmissbrauch und verschiedene Korruptionshandlungen im privaten Sektor.

Korruption wirkt sich negativ auf alle Bereiche der Gesellschaft aus, ist eng mit Konflikten und regionaler Instabilität verflochten, gefährdet die soziale und wirtschaftliche Entwicklung und untergräbt demokratische Institutionen und Rechtsstaatlichkeit.

Auf dem aktuellen Korruptionswahrnehmungsindex (CPI) von Transparency International, einer gemeinnützigen und parteipolitisch unabhängigen Bewegung, die sich dem globalen Kampf gegen die Korruption verschrieben hat, erreicht Deutschland 79 von 100 Punkten. Der CPI gibt den Grad der wahrgenommenen Korruption wieder. Je höher die Punktzahl eines Landes ist, desto integrerer ist sein Ruf. Unter den gelisteten 180 Ländern rangiert Deutschland auf Platz 9 der Rangliste. Am 3. März 2005 gründeten das Innenministerium und das Justizministerium des Landes Brandenburg die ressortübergreifende gemeinsame Ermittlungsgruppe Korruption (GEG Korruption), in welcher die Schwerpunktabteilung der Staatsanwaltschaft Neuruppin und das LKA 138 konzentriert mit landesweiter Zuständigkeit Kor- ruptionsstraftaten verfolgen.

Innenminister Michael Stübgen: „Korruption ist ein grenzenloses Übel und schädigt das Gemeinwohl. Korruption behindert die Innovationskraft der Wirtschaft und untergräbt das Vertrauen der Menschen in die Funktionsfähigkeit und Integrität der öffentlichen Verwaltung. Wichtige Faktoren für eine erfolgreiche Korruptionsprävention und -bekämpfung sind daher Transparenz und gemeinschaftliches Engagement von Bürgerschaft, Politik, Verwaltung und Wirtschaft."

Das Landeskriminalamt des Landes Brandenburg veröffentlicht jährlich das Lagebild „Korruptionskriminalität im Land Brandenburg". Es richtet sich in erster Linie an die politische und polizeiliche Führungs- und Entscheidungsebene und soll dazu beitragen, das Gefahren- und Schadenspotenzial von Korruption und deren Bedeutung für die Kriminalitätslage im Land Brandenburg einzuschätzen und den erforderlichen Handlungsbedarf zu erkennen. Dem Lagebild für das Jahr 2022 zufolge ist die Anzahl der Korruptionsverfahren im Vergleich zum Vorjahr um 125 auf 55 Verfahren (2021: 180 Verfahren) bzw. um 69,4 %, das diesbezügliche Straftatenaufkommen um 683 auf 190 Fälle (2021: 873 Fälle) bzw. um 78,2 %, gesunken.

Dieser Rückgang ist vor allem auf statistische Effekte zurückzuführen, da sich einzelne Umfangsverfahren mit der Erfassung einer hohen Anzahl von Einzelfällen in den jeweiligen Jahren statistisch stark auswirken, was im Vorjahr 2022 ebenfalls zu beobachten war.

In der langjährigen Betrachtung ist ohnehin die Tendenz zu beobachten, dass sich das beobachtete Geschehen auf Sachverhalte komplexer struktureller Korruption konzentriert, für deren Aufklärung die Strafverfolgungsbehörden auf Hinweisgeber angewiesen sind.

Den Schwerpunkt der Korruptionsermittlungen bildeten dabei erneut Fälle der strukturellen Korruption, insbesondere klassische Bestechungs- und Bestechlichkeitsdelikte im Zusammenhang mit dienstpflichtwidrigen Handlungen von tatbereiten Nehmern (Amtsträgern).

Bei der Betrachtung der tatverdächtigen Geber fällt auf, dass die Bauwirtschaft mit 20 % den größten Anteil einnimmt und der Anteil der privaten Geber nach einem Hoch im Vorjahr wieder deutlich gesunken ist. Der Hauptzielbereich der korruptiven Handlungen bleibt unverändert die öffentliche Verwaltung.

messe frankfurt

light+building

3. – 8. 3. 2024
Frankfurt am Main

Intelligent. Vernetzt. Sicher!

Sicherheitstechnik im Gebäude: unverzichtbar! Erfahren Sie, wie wegweisende Innovationen die Gebäudesicherheit auf ein neues Level heben.

Weltleitmesse für Licht und Gebäudetechnik

Jetzt schnell Ticket sichern!

Die vier wichtigsten Trends für Videoüberwachung 2024

Schnelle Einführung von künstlicher Intelligenz und Fortschritte bei der kantenbasierten Verarbeitung, mehr Kontrolle über geschlossene Plattformen und höhere Anforderungen an den Schutz der Privatsphäre und der Cybersicherheit

i-PRO Co., Ltd. (ehemals Panasonic Security), ein weltweit führender Anbieter professioneller Sicherheitslösungen für Überwachung und öffentliche Sicherheit, hat heute seine vier wichtigsten Prognosen für die physische Sicherheitsbranche im Jahr 2024 vorgestellt.

Anpassbares KI-Lernen vor Ort als nächste Stufe der KI-Einführung

2024 wird der Einsatz von KI auf dem Markt für physische Sicherheit weiter zunehmen. Während KI-basierte Sicherheitskameras schon seit einiger Zeit in der Lage sind, Fehler durch die zuverlässige Erkennung von Menschen und Fahrzeugen erheblich zu reduzieren, wird die nächste Phase der KI für datenhungrige Unternehmen unwiderstehlich sein. Die heutige Technologie ermöglicht es Integratoren und Endanwendern, die KI-Analyse einer Ka-

mera vor Ort zu trainieren, um einzigartige Objekte zu erkennen, die für ein Unternehmen wichtig sind, um sie zu verfolgen oder zu zählen. Die KI-Schulung von Edge-Geräten vor Ort kann die Genauigkeit weiter erhöhen, indem sie Logos auf Fahrzeugen oder Uniformen erkennt, Flugzeuge, Gabelstapler, Kinderwagen usw. zählt. Dieser neue Strom von Business-Intelligence-Daten, der direkt durch die Edge-Verarbeitung in Sicherheitskameras gewonnen wird, wird automatisierte Arbeitsabläufe ermöglichen und gleichzeitig die betriebliche Effizienz und die Servicequalität verbessern. KI-basierte Systeme werden bald in der Lage sein, zu erkennen, wenn Personen Hilfe benötigen, oder zu melden, wenn ein Boden nass ist, um beispielsweise ein Ausrutschen zu verhindern.

Die sich schnell verändernde Technologie erfordert skalierbare, flexible und zukunftssichere Investitionen

Unternehmen werden im Jahr 2024 unter erhöhtem Druck stehen, in Lösungen zu investieren, die nicht schon kurz nach der Installation veraltet sind oder durch geschlossene Plattformen eingeschränkt werden. i-PRO rät, Anbieter und Hersteller mit offenen Plattformen zu suchen, die frei mit mehreren Drittherstellern zusammenarbeiten. Die Geräte sollten so konzipiert sein, dass sie von den Entwicklungen in den Bereichen KI und Analytik profitieren können, ohne dass die Gabelstapler aufgerüstet werden müssen. Indem sie sich auf die Nachrüstung, Aufrüstung und Integration bestehender Geräte mit neuer Technologie in einem schrittweisen Ansatz konzentrieren, können Unternehmen die Lebensdauer bestehender Geräte maximieren und gleichzeitig neue Funktionen hinzufügen, wie z. B. die Nutzung von KI auf Geräten ohne KI.

Mehr Leistung für den Edge-Bereich

Im Jahr 2024 wird noch mehr Leistung in den Randbereichen zur Verfügung stehen. Kameras mit leistungsstarken Prozessoren werden in der Lage sein, mehr Videodaten zu verarbeiten als je zuvor. Edge-Geräte werden bald in der Lage sein, zusammenzuarbeiten und ihre Rechenressourcen auf ähnliche Weise zu kombinieren, wie es heute mit Server-Racks in der Cloud möglich ist. Dies wird deutlich mehr Verarbeitungsfunktionen ermöglichen, ohne das Netzwerk und die unterstützende Infrastruktur zu überlasten. Die Kosten für Bakkend-Server werden relativ niedrig bleiben, da die Verarbeitung von KI-basierten Analysen vermehrt in Edge-Geräten wie Kameras stattfindet und weniger Videomaterial zur Analyse zurück auf Server gestreamt wird. Durch die verbesserte Edge-Verarbeitung werden auch Cloud-basierte Systeme effizienter und weniger kostspielig zu betreiben sein.

Datenschutz und Cybersicherheit werden noch stärker unter die Lupe genommen

KI und ihre Untergruppen werden im nächsten Jahr noch genauer unter die Lupe genommen, da weltweit Durchführungsverordnungen und Gesetze erlassen werden, um die Verletzung der Privatsphäre und des Eigentums an persönlichen Daten weiter zu verringern. Der Artificial Intelligence Act des Europäischen Parlaments und der U.S. Blueprint for an A.I. Bill of Rights sind erste Beispiele für einen Trend, der die Sicherheitsbranche beeinflussen wird. Unternehmen benötigen Transparenz und Compliance angesichts gesetzlicher Änderungen und bewährter Verfahren, die sich schnell ändern können. Aus diesem Grund ist es von entscheidender Bedeutung, mit Anbietern und Herstellern zusammenzuarbeiten, die eine nachgewiesene Erfolgsbilanz bei der Entwicklung haben, bei der "Privacy by Design" und ein verantwortungsbewusster Umgang mit KI zu den wichtigsten Grundsätzen gehören.

Da mit Hilfe von KI so viele nützliche Daten gesammelt werden, muss sichergestellt werden, dass private Daten auch privat bleiben. Videoüberwachungsanlagen müssen die sich weiterentwickelnden Standards wie NIST FIPS 140-2 Level 3 und den neueren 140-3 Standard unterstützen, um sicherzustellen, dass das Sicherheitssystem nicht zu einem Angriffsvektor wird.

Weltweit werden zunehmend Zero-Trust-Praktiken gefordert, bei denen jede Transaktion zwischen Geräten und Personen validiert wird. So hat beispielsweise das Weiße Haus der USA die Einhaltung von Zero-Trust-Architekturen und -Designs auf Bundesebene bis 2024 vorgeschrieben. Diese Änderung der US-Bundespolitik wird sich auf alle Unternehmen auswirken, die in den USA tätig sind. i-PRO geht außerdem davon aus, dass die USA im Jahr 2022 eine Version des "American Data Privacy and Protection Act" verabschieden werden, die den US-Bürgern einige GDPR-ähnliche Schutzmaßnahmen bietet.

Wir erwarten ein sehr arbeitsreiches Jahr 2024, da immer mehr Unternehmen weltweit Upgrades und Erweiterungen von Sicherheitssystemen in Auftrag geben", sagte Hiroshi (Huey) Sekiguchi, CMO, i-PRO Co., Ltd. "Angesichts des schnellen technologischen Wandels ist es wichtiger denn je, die Branche darüber aufzuklären, wie diese spannenden Technologien zum Schutz von Vermögenswerten und zur Erzielung von Einnahmen eingesetzt werden können, während gleichzeitig Datenschutzbestimmungen und bewährte Verfahren zur Cybersicherheit eingehalten werden."


Rainer Sturm / pixelio.de

Lünendonk-Blitzumfrage

B2B-Service-Unternehmen blicken überwiegend optimistisch in das Jahr 2024

Umsätze sollen 2024 durchschnittlich um 9,5 Prozent zulegen • 91 Prozent der Dienstleister planen Honorarerhöhungen • Gehälter sollen 2024 im Mittel um 4,7 Prozent steigen • Dienstleister experimentieren mit generativer KI

Deutsche B2B-Service-Unternehmen blicken trotz vieler wirtschaftlicher Herausforderungen optimistisch auf das Jahr 2024. Führende Dienstleister der Segmente Managementberatung, Digitales und IT, Wirtschaftsprüfung und Steuerberatung, Personaldienstleistungen und Real Estate Services rechnen für das Jahr 2024 mit einem Umsatzplus von durchschnittlich 9,5 Prozent. Während Anbieter von Real Estate Services von einem Umsatzplus im Mittel von 3,7 Prozent ausgehen, liegt die Spanne bei Digital- und IT-Dienstleistern bei durchschnittlich 14,4 Prozent. Consulting-Häuser erwarten im Mittel ein Wachstum von 10,5 Prozent, Wirtschaftsprüfer von 8,0 Prozent und Personaldienstleister von 6,0 Prozent. Für das laufende Jahr 2023 prognostizieren die B2B-Service-Anbieter branchenübergreifend ein Umsatzplus von durchschnittlich 8,3 Prozent.

Das sind Ergebnisse einer Blitzumfrage des Research- und Beratungsunternehmens Lünendonk & Hossenfelder, die Ende November bis Anfang Dezember 2023 durchgeführt wurde. Mit der Umfrage am Jahresende überprüft Lünendonk die Prognosen aus den Studien des ersten Halbjahres.

Mitarbeiterwachstum hält mit dem Umsatzwachstum nicht mit

Im Vergleich zum Umsatz erwarten die Unternehmen jedoch ein geringeres Mitarbeiterwachstum: Auf durchschnittlich 4,8 Prozent beziffert sich dieses für das aktuelle Jahr 2023 – beeinflusst durch eine angespannte Lage im Personaldienstleistungsmarkt. Hier wird 2024 eine Entspannung erwartet, sodass über alle B2B-Service-Märkte hinweg die Zahl der Mitarbeitenden um 7,7 Prozent zulegen soll.

Honorare und Gehälter steigen aufgrund Inflation und Nachfrage

Die Inflation stellt für viele Unternehmen weiterhin eine Herausforderung dar. Für 2023 wird eine durchschnittliche Preissteigerung in Deutschland von 6 Prozent erwartet, für 2024 von circa 3 Prozent. Dies spiegelt sich auch in den Preisen und Gehältern der Dienstleistungsunternehmen wider: 86 Prozent haben 2023 ihre Preise erhöht – überwiegend zwischen 2 und 10 Prozent. Auch 2024 planen 91 Prozent, ihre Preise zu erhöhen – jedoch in einem geringeren Umfang. Mitarbeitergehälter steigen 2023 um durchschnittlich 6,2 Prozent und sollen 2024 im Mittel um 4,7 Prozent zulegen. „Zwar hat die Inflation einen signifikanten Einfluss auf die Entwicklung der Honorare und Gehälter der Dienstleister. Gleichzeitig besteht nahezu in allen B2B-Service-Märkten eine hohe Nachfrage im Markt, sodass höhere Preise durchsetzbar sind", kommentiert Lünendonk-Geschäftsführer Jörg Hossenfelder die Ergebnisse. „Aufgrund Inflation, Gehaltserhöhungen und Technologieinvestitionen bleibt jedoch von der Honorarerhöhung wenig übrig."

Dienstleister befassen sich mit generativer KI

Die Entwicklungen im Bereich der generativen Künstlichen Intelligenz (KI) beeinflussen ebenfalls das Geschäft der Dienstleister. 11 Prozent der Teilnehmenden befassen sich bereits intensiv mit KI, 68 Prozent bereits vereinzelt und weitere 15 Prozent planen, sich in Zukunft stärker damit zu befassen. Branchenabhängig werden Potenziale zur Effizienzsteigerung in Form von KI-gestützten Textzusammenfassungen, der Erstellung von neuem Content oder intelligenten Chatbots für Mitarbeitende oder Kundinnen und Kunden gesehen. IT-Dienstleister setzen zudem große Hoffnungen in die KI-Unterstützung bei der Programmierung und im Coding.

B2B-Dienstleister profitieren von Herausforderungen der drei „Ds"

„Der deutsche B2B-Dienstleistungsmarkt bleibt auch zukünftig ein hoch spannender Markt mit vielfältigen Entwicklungsmöglichkeiten. Unternehmen suchen Antworten auf die Herausforderungen der drei „Ds" – Digitalisierung, Dekarbonisierung und Demografie. B2B-Service-Unternehmen spielen hier eine wichtige Rolle und können auch weiterhin von Wachstumsmöglichkeiten profitieren", fasst Hossenfelder die Ergebnisse zusammen.

Über die Blitzumfrage

An der Online-Befragung von Lünendonk & Hossenfelder nahmen insgesamt 116 Personen aus B2B-Dienstleistungsunternehmen der Märkte für Managementberatung, Wirtschaftsprüfung und Steuerberatung, Digitales und IT, Engineering Services, Personaldienstleistungen und Real Estate Services teil. 61 Prozent der Teilnehmenden sind Vorstände oder haben eine Geschäftsführungsposition inne, 25 Prozent fungieren als leitende Angestellte. Zeitraum der Befragung war 29. November bis 8. Dezember 2023. **[www.luenendonk.de]**

Fünf IT-Trends 2024

Ökologie trifft auf Ökonomie – immer seltener in der Cloud

Mit scharfem Blick auf Effizienz: Hybride Szenarien erfahren vermehrt Zulauf

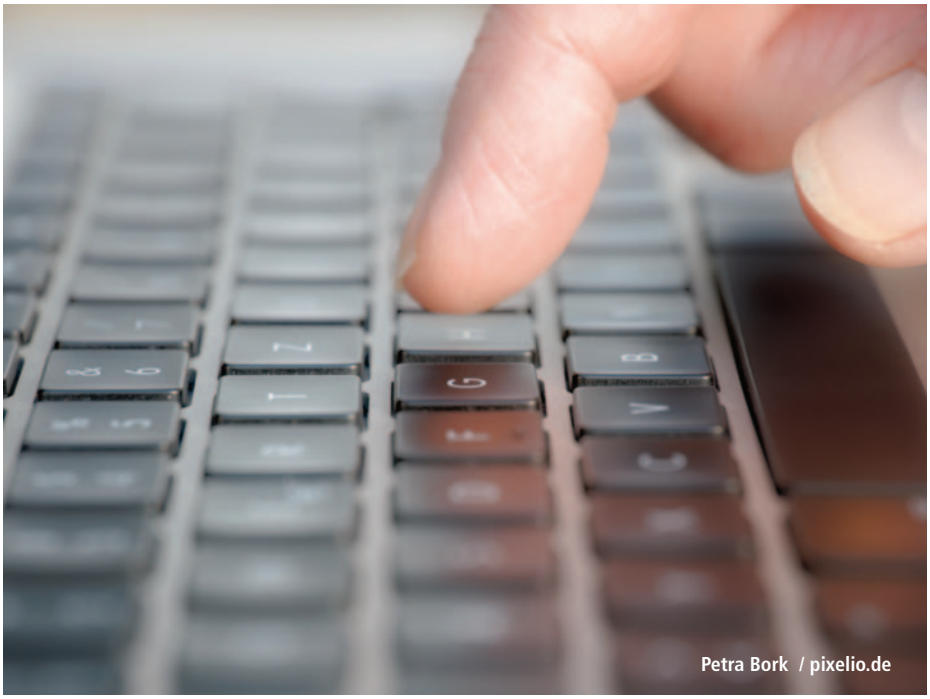
Die Lernkurve aus so manchem Cloud-Projekt führt immer öfter zu einem zumindest teilweisen Cloud-Exit – dieser Trend wird 2024 weiter Fahrt aufnehmen. Nachhaltigkeit bei Kosten und Energieeinsatz werden zentrale Faktoren bei der Beschaffung sein, so die Einschätzung der Thomas-Krenn.AG. Weitere Prioritäten seien nächstes Jahr demnach Edge Computing sowie engere Kooperationen zwischen Kunden, Herstellern und Systemhäusern.

Die deutsche Wirtschaft bildet 2023 mit einem negativen Wachstum das wirtschaftliche Schlusslicht der Eurozone. Diese Rezession wird sich auch auf die IT-Branche auswirken: Ein Selbstläufer wird das kommende Jahr damit nicht, jedoch wird es durchaus Chancen für die Unternehmen dieser Industrie geben. Sie liegen insbesondere in technologischen Schüben sowie den nach wie vor hohen Energiekosten. Die Thomas-Krenn.AG hat auf dieser Basis fünf IT-Trends für das Jahr 2024 identifiziert:

1 **Trend 1 – Cloud-Exit:** Der generell zu hinterfragende Total Cost of Ownership (TCO) sowie intransparente und komplexe Preismodelle gerade bei den großen Hyperscalern führen dazu, dass vornehmlich kleine und mittlere Unternehmen (KMU) nicht wie erhofft von der Cloud profitieren. Hinzu kommen nach wie vor Datenschutz-Fragezeichen im Hinblick auf US-Anbieter. Bereits 2023 ist daher die Zahl von Exit-Szenarien aus reinen Cloud- hin zu hybriden Umgebungen gestiegen. Dieser mit dem starken Wachstum bei HCI-Lösungen begonnene Trend wird 2024 bei KMU weiter an Fahrt aufnehmen. Das gilt umso mehr, da solche Hybrid-Clouds durchaus die Potenziale von Künstlicher Intelligenz (KI) abrufen können.

2 **Trend 2 – Hardware-Kosten:** Zwar wird 2024 nach derzeitigen Prognosen eine gewisse wirtschaftliche Erholung einsetzen; diese wird jedoch von überschaubarer Größe sein und auch erst im Lauf des Jahres auftreten. Gleichzeitig steht 2024 nach dem Ausrüstungshoch während der Covid-Pandemie eine weitere Modernisierungswelle an; zudem endet der Support unter anderem für Windows Server 2019. Die Unternehmen werden demnach Investitionsbereitschaft zeigen, dabei jedoch noch stärker auf die Kosten bei der Hardware-Beschaffung achten. Das gilt gleichermaßen für Server, Storage samt Unified-Systemen sowie für Clients.

3 **Trend 3 – Energieeffizienz:** Was seit dem Beginn der aktuellen geopolitischen Krisen gilt, wird auch 2024 weiterhin eines der zentralen Themen bleiben – Energie. Das gilt für Gas wie für elektrischen Strom. Die 2024 erwartete Modernisierungswelle bei der IT wird Unternehmen dabei durchaus Gelegenheiten geben, Fortschritte zu erzielen. Dafür sorgen unter anderem nochmals optimierte Prozessoren sowie neue Player in diesem Bereich. Entsprechend sparsame Systeme werden besonders gefragt sein, denn sie zahlen nicht nur auf die Kosten ein, sondern auch auf die immer weiter greifenden gesetzlichen Vorgaben, Stichwort „ESG".


Petra Bork / pixelio.de

4 **Trend 4 – Edge Computing:** Alles andere als ein neues Phänomen, kann Edge Computing im Jahr 2024 signifikant an Bedeutung gewinnen. Ein Grund dafür liegt in den Maßnahmen rund um Cloud Exit und hybride Szenarien; Unternehmen, die hier Veränderungen anstoßen, werden diese vermehrt bis zur Edge führen. Auch die Energieeffizienz ist hier ein treibendes Element. Insbesondere werden die zunehmenden Digitalisierungsbestrebungen eine zentrale Rolle spielen, dem Edge-Ansatz noch mehr in die Breite zu verhelfen.

5 **Trend 5 – Zusammenarbeit:** Nicht nur die Collaboration innerhalb von Unternehmen hat sich seit der Coronapandemie geändert, sondern auch über die Unternehmensgrenzen hinaus. Agile Low-Code-Systeme und das Ansinnen nach mehr Digitalisierung spielen hierbei eine Rolle. Zudem wird sich die Zahl der Systemhäuser 2024 weiter konsolidieren; die verbliebenen werden dabei größer werden und mehr Services anbieten. Kommt eine Zusammenarbeit zustande, wird diese daher enger sowie intensiver und damit eine umfangreiche Bandbreite abdecken: Hersteller und Systemhäuser werden mehr denn je die Rolle von vertrauensvollen Ratgebern einnehmen.

„Vielleicht ist es auf den ersten Blick erstaunlich, dass KI nicht zu den Trendthemen des Jahres 2024 zählt. Für uns liegt das nicht daran, dass die Relevanz nicht vorhanden wäre, ganz im Gegenteil. KI ist als Trend dominant und gleichzeitig diffus. Zudem ist es ein Werkzeugkasten, es gibt ja nicht die eine KI", erläutert Christoph Maier, CEO der Thomas-Krenn.AG. „Daher sehen wir andere Trends, die vielfach KI nutzen oder zur sicheren, rechtskonformen, effizienten Bereitstellung beitragen können.

Ökologie und Ökonomie sind dabei aus unserer Sicht zentral, und das mit weniger Cloud-Beitrag. Es werden vielfach eher evolutionäre Schritte sein, auch vor dem Hintergrund der Rezession. Einmal mehr wird gelten: Wer die richtigen Entscheidungen trifft, wird als Gewinner hervorgehen."

KI im Cyberkampf: Intelligente Sicherheit für die Cloud-Ära

Arne Jacobsen, Director of Sales EMEA bei Aqua Security

KI-gesteuerte Tools sind zunehmend in der Lage, komplexen Code zu erzeugen. Cyberkriminelle können diesen für ausgeklügelte Malware und Exploit-Programme umfunktionieren – und das in einer Geschwindigkeit und Effizienz, die zuvor undenkbar war. Dies senkt zudem die Hürde für einen schnellen Einstieg in die Cyberkriminalität, auch für Personen mit minimalen Programmierkenntnissen. KI-Systeme können bekannte Angriffsmethoden schnell adaptieren und verbessern, wodurch die Umsetzung fortschrittlicher Bedrohungen erleichtert wird. Diese Demokratisierung von Angriffsmöglichkeiten wird zu einer Verbreitung fortschrittlicher Malware führen – häufigere und effektivere Cyberangriffe sind die Folge.

Die Reaktion auf diese Veränderung erfordert von der Cybersicherheitsbranche differenzierte, verhaltensorientierte Sicherheitsmaßnahmen. Auch hierbei spielen KI und maschinelles Lernen eine zentrale Rolle, um normales Nutzerverhalten zu verstehen, Anomalien zu erkennen und innovative Bedrohungen zu bewältigen. Proaktive und intelligente Systeme, die Speicher-Scanning und Prozessüberwachung integrieren, sind entscheidend, um Bedrohungen zu identifizieren und zu entschärfen. In einem sich ständig weiterentwickelnden Cloud-Ökosystem gewährleisten sie eine robuste Sicherheit. **www.aquasec.com**

Unternehmen sollten Security als fortlaufenden Prozess leben - aber nicht versuchen, über Nacht 100% zu erreichen

Stefan Schachinger, Product Manager Network Security Barracuda Networks

2024 wird Unternehmen vor die Situation stellen, ob Cyberkriminelle mit der Einführung von KI schneller sein könnten als die Sicherheitsbranche. Durch Werkzeuge wie generative KI hat die Qualität von Angriffen ein neues Niveau erreicht, das es uns Menschen fast unmöglich macht, zwischen echt und gefälscht zu unterscheiden. Für die Industrie und ihre Sicherheitslösungen ist es wichtig, diese neue Technologie schnell zu übernehmen. Denjenigen, die ihre Sicherheitslage nicht verbessern, stehen schwierige Zeiten bevor.

Denn die meisten Organisationen sind nicht darauf vorbereitet, sich gegen gezielte und qualitativ hochwertige Angriffe zu verteidigen, die wir früher nur auf Nationalstaaten- und Geheimdienst-Ebene gesehen haben. Dazu gehören Social Engineering und technische Angriffsvektoren. Im Hinblick auf KI wird klar, dass immer mehr Unternehmen mit ausgeklügelten Angriffen konfrontiert sein werden. So können robuste Zero-Trust-Maßnahmen Unternehmen vor ernsthaftem Schaden schützen.

Wir Security-Anbieter sollten uns neben der Prävention auf die Erkennung laufender Angriffe und die entsprechende Reaktion konzentrieren, zum Beispiel mit dezentraler Sicherheit an den Randbereichen eines Netzwerks oder eines Systems – also an den Endpunkten.

Wir werden bei der Einführung neuer Sicherheitslösungen wie SASE oder Zero-Trust-Konzepten einen großen Schritt sehen. Es besteht kein Zweifel daran, dass wir eine weitere Welle schwerwiegender Sicherheitsvorfälle erleben werden, und die unsichere geopolitische Lage in vielen Teilen der Welt tut ihr Übriges. Im Jahr 2024 werden wir erkennen, dass moderne Lösungen erforderlich sind, um sich gegen moderne Bedrohungen zu verteidigen. Unternehmen sollten Security als fortlaufenden Prozess leben, aber nicht versuchen, über Nacht 100 Prozent zu erreichen. Werden Projekte zu groß, zu kompliziert oder zu teuer, können sie scheitern. Skalieren ist die richtige Vorgehensweise.

www.barracuda.com

Wirtschaftlich motivierte Cyberkriminelle werden kompetenter und agiler – KI-basiertes Scamming-as-a-Service skaliert Cyberbetrug im sechsstelligen Bereich

Martin Zugec, Technical Solutions Director bei Bitdefender

Auch im Jahr 2024 werden sich die Trends in der Cyberkriminalität weiter fortschreiben, welche vor Jahresfrist schon aktuell waren. Cyberkriminelle mit finanziellen Beweggründen, insbesondere Ransomware-Affiliates und -Operatoren, werden ihre Fähigkeiten weiter verbessern und in Sachen Raffinesse das Niveau staatlich unterstützter Hacker erreichen. Die Cyberkrimi- nellen werden sich weiter rasch neue Fähigkeiten aneignen, die es ihnen ermöglichen, neu entdeckte Schwachstellen sofort auszunutzen. Dabei sind sie bestrebt, Schwachstellen innerhalb von 24 Stunden nach Bekanntwerden der ersten Proof-of-Concept (PoC)-Codes auszunutzen.

Diese Agilität fordert die Cybersicherheitsteams in hohem Maße heraus und erhöht die Notwendigkeit proaktiver Maßnahmen. Darüber hinaus gehen wir davon aus, dass die Angreifer immer geschickter darin werden, sich vor der Abwehr zu verbergen. Sie werden verbesserte Techniken wie DLL-Sideloading einsetzen, um ihre Aktivitäten zu verschleiern. Diese Entwicklungen unterstreichen die zentrale Rolle fortschrittlicher Cybersicherheit durch Technologien wie zum Beispiel Extended Detection and Response (XDR) sowie durch die externen Sicherheitsdienste einer Managed Detection and Response. Da Unternehmen jeder Grösse und Branche weiterhin Ziel von Angriffen sind, wird der Bedarf an robusten Cybersicherheitsmaßnahmen im Jahr 2024 und darüber hinaus immer weiter steigen. Darüber hinaus wird Künstliche Intelligenz die Bedrohungslandschaft weiter massiv umgestalten. Der spektakuläre Fortschritt bei Large Language Models (LLM) wird höchstwahrscheinlich automatisierte Scamming-Toolkits hervorbringen, die Opfer im sechsstelligen Bereich in verschiedenen Sprachen gleichzeitig angreifen können.

Zugleich wachsen die Schwierigkeiten, einen Scam an einfachen Äußerlichkeiten zu erkennen. Toolkits werden Scamming-as-a-Service-Angebote zusammen mit KI-basierter Bild- und Ton-Manipulation verkaufen, vermieten oder verwalten. Die Bedrohungsakteure werden die Möglichkeit haben, perfekt zu chatten, mit überzeugenden Bildern zu hinterlegen und eventuell sogar zu Echtzeit-Video-Unterhaltungen übergehen. Zugleich wird KI auch Video-Content generieren können. Erste Beispiele liefern schon Instagram-Influenzer. Cyberkriminelle und politisch motivierte Hacker mit staatlichem Hintergrund werden hier nicht zurückstehen und Fehlinformationen zu streuen versuchen – insbesondere im Vorfeld der bevorstehenden US-Wahlen. **www.bitdefender.de**

Ein gemischter KI-Ansatz verändert auch die IT-Security

Bernd Greifeneder, CTO und Gründer von Dynatrace

Im Jahr 2024 tritt die generative KI in die letzten Phasen ihres Hype-Zyklus ein und Unternehmen werden erkennen, dass die Technologie zwar transformativ ist, aber für sich allein keinen signifikanten Wert liefern kann. Infolgedessen werden sie zu einem gemischten KI-Ansatz übergehen, der generative KI mit anderen Arten von künstlicher Intelligenz und zusätzlichen Daten- quellen kombiniert. Dieser Ansatz ermöglicht tiefgehende Schlussfolgerungen und verleiht den von generativer KI erzeugten Ergebnissen Präzision, Kontext und Bedeutung. Dies hat Auswirkun-

gen in vielen Bereichen des Unternehmens inklusive der IT-Sicherheit. Mit Blick auf Security werden Unternehmen alte SIEM-Lösungen (Security Information and Event Management) ausmustern, da Sicherheitsteams nach intelligenteren Threat-Analysen suchen. Diese modernen Lösungen ermöglichen es Sicherheitsteams, ihre Fähigkeiten über die Logauswertungen hinaus zu erweitern. Sie können auf den dazugehörigen Kontext zugreifen, der durch ein breites Spektrum an Datenmodalitäten und verschiedene Arten von KI – einschließlich einem Zusammenspiel aus generativen, kausalen und prädiktiven Techniken – bereitgestellt wird. Dadurch erhalten Unternehmen Zugang zu tieferen, präziseren, intelligenten und automatisierten Bedrohungsanalysen, die sie dabei unterstützen, ihre Anwendungen und Daten vor immer raffinierteren Bedrohungen zu schützen.
www.dynatrace.com

Sicher Daten zu teilen wird zu einer Kernaufgabe für die Cyberresilienz digitalisierter Unternehmen in der Cloud

Ari Albertini, CEO von FTAPI Software GmbH

Cyberangriffe werden weiter zunehmen und 2024 sogar noch raffinierter werden. Proaktive Abwehrmaßnahmen unterstützt von innovativen Technologien wie Künstlicher Intelligenz spielen daher in Zukunft eine wichtige Rolle. Auch das Thema Quantencomputing wird im Blickfeld der Cybersicherheitsforschung bleiben. Mittels Krypto-Agilität, also der Fähigkeit, alternative Verschlüsselungstechnologien in einem System zu implementieren, wird es möglich sein, schnell und flexibel auf sich verändernde Bedrohungen zu reagieren. Der Einsatz verschiedener Verschlüsselungsverfahren erleichtert es, den sich ständig ändernden Angriffsmethoden standzuhalten und neuen Bedrohungen gezielter entgegenzuwirken. Langfristig könnte sich Krypto-Agilität zu einer festen Disziplin in der Cyberabwehr entwickeln.

Infrastrukturen, die nicht zusammenhängende Abläufe durch die logische und physische Trennung klar voneinander abgrenzen und im Falle eines Angriffs nicht vollständig ausfallen, werden zunehmend an Bedeutung gewinnen. Durch Umbau ihrer IT-Landschaft können Unternehmen die Cyberresilienz ihrer Systeme langfristig stärken.

Die Cloud wird sich von einer einfachen Speicherlösung immer mehr zu einem Grundpfeiler für eine sichere, dezentrale und skalierbare Infrastruktur entwickeln. Durch vermehrten On-Demand-Betrieb werden Kernservices zunehmend dezentralisiert. Umso entscheidender wird es daher, die Resilienz der IT gegenüber Angriffen von außen zu stärken. In diesem Zusammenhang werden umfassende Plattformen zum sicheren Teilen und Speichern von Daten und Informationen eine immer wichtigere Rolle spielen. Anstatt wie bisher nach dem „Best-of-Breed"-Ansatz einzelne Lösungen für Problemstellungen und Anforderungen von verschiedenen Herstellern zu beschaffen, lassen sich über ganzheitliche Plattformen mehrere Prozesse sicher abbilden. Durch das Bündeln von sicherem Datentransfer, virtuellen Datenräumen und automatisierten Prozessen ist die Sicherheit, Vertrauenswürdigkeit und Integrität der erhobenen, übermittelten und weiterverarbeiteten Daten jederzeit gegeben.
www.ftapi.com

„KI bedingt den Einsatz von KI – Ein Ansatz zur Bekämpfung von Finanzkriminalität"

Roy Prayikulam, Bereichsleiter Risk&Fraud und Mitglied der Geschäftsleitung bei Inform

Aktuelle Umfragen der Verbraucherzentralen zeigen, dass 30 % der Internetnutzer in Deutschland bereits Opfer von Cyberangriffen geworden sind. Heutzutage reichen die Bedrohungen jedoch über traditionelle Malware hinaus; sie umfassen ausgeklü-

gelte Schemata wie SIM-Swapping oder Phishing, mit denen sich auch starke Authentifizierungsmethoden umgehen lassen. SIM-Swapping ist beispielsweise eine Täuschung, bei der ein Hacker illegal eine Telefonnummer übernimmt und so Zugang zu privaten Daten erlangt.

Besorgniserregend ist der Anstieg an „Social Engineering"-Betrug, bei dem Betrüger sich als vertrauenswürdige Kontakte oder Autoritäten (wie Familie, Freunde oder Behörden) ausgeben, um Menschen zu Geldüberweisungen oder zur Preisgabe sensibler Informationen zu verleiten. Diese Betrügereien nutzen das menschliche Vertrauen aus und umgehen damit selbst robuste Sicherheitsmaßnahmen wie die Zwei-Faktor-Authentifizierung. Doch selbst hier nutzen die Kriminellen moderne Technologie in der Umsetzung: So hat die Verbreitung von generativen KI-Tools ungewollt zu einem Anstieg von schwer erkennbaren, mittels KI generierter Phishing-Angriffe geführt, wie der dramatische Anstieg an Vorfällen seit der öffentlichen Verbreitung von ChatGPT beweist.

Natürlich sind Aufklärung und Bildung wichtige Werkzeuge im Kampf gegen derartige Finanzkriminalität. Wenn aber doch einmal etwas passiert, müssen Banken in der Lage sein, betrügerische Finanztransaktionen als solche zu erkennen und zu verhindern. Digitale Abwehrmechanismen bzw. „Fraud Detection-Lösungen" kommen zwar schon seit längerer Zeit zum Einsatz, es fehlt aber häufig an der Fähigkeit, auch komplexen, kanalübergreifenden Szenarien (Multi-Channel-Fraud) auf die Schliche zu kommen.
Das sind Betrugsmuster, bei denen Kriminelle ihre Aktivitäten auf mehrere Medien und Kanäle ausweiten. Haben sie sich beispielsweise Zugang zum Konto eines Opfers verschafft, überweisen sie das Geld nicht einfach direkt auf ihre Konten, sondern nutzen den Zugang, um zum Beispiel Kreditkartendaten oder andere Informationen abzugreifen. Damit können sie dann – von der starren Betrugserkennungslösung der Bank unbemerkt – beim Kreditdienstleister des Opfers einen Kredit aufnehmen. Banken müssen daher echtzeitfähige KI-Lösungen implementieren, die sämtliche Daten und Datenquellen vom Online und Mobile Banking über das Nutzerverhalten, Kontakte mit dem Kundenservice, bis hin zu Transaktionen im elektronischen Geschäftsverkehr zusammenhängend prüfen, bewerten und daraus automatisiert Handlungen oder Handlungsempfehlungen ableiten können. Wenn wir Finanzkriminalität effektiv bekämpfen wollen, müssen wir den Kriminellen auch technologisch einen Schritt voraus sein. **www.inform-software.com**

Ransomware und NIS-2 steigern den Bedarf an Managed Security Services

Tom Haak, CEO bei Lywand

Ransomware-Angriffe werden im kommenden Jahr weiterhin und in vielerlei Hinsicht die IT-Sicherheitsstrategie von Unternehmen beeinflussen. In jüngster Vergangenheit haben die Angriffswellen eine neue Dimension erreicht, sowohl was die Menge als auch die Qualität anbelangt.Neben äußerst ausgereiften Social Engineering-Taktiken sind zunehmend Schwachstellen der Schlüssel zum Erfolg von Attacken. Dafür machen Angreifer sich die Fähigkeiten von KI zu Nutze. Ist es ihnen gelungen, Zugang zum System ihrer Opfer zu erlangen, macht sich der nachgeladene Schadcode eigenständig auf die Suche nach gängigen Schwachstellen, um schließlich die Kontrolle zu erlangen. Und von diesen gibt es viele: Laut dem diesjährigen Lagebericht des BSI zur IT-Sicherheit befindet sich die Zahl der Schwachstellen in Software auf einem beunruhigenden Niveau. Doch was bedeutet dies für Unternehmen?
Zunächst, dass sich ihre Angriffsfläche vergrößert hat. Ist es Cyberkriminellen gelungen, mittels Social Engineering IT-Sicherheitsmaßnahmen zu umgehen, können nicht durchgeführte Updates in beliebiger Software über den Erfolg des Angriffs entscheiden. Um dies zu verhindern, müssen Unternehmen ihr Patch-Management verbessern und eingehend überprüfen. Denn bereits eine einfache Fehlkonfiguration kann dafür sorgen, dass ein Patch zwar installiert, aber nicht wie vorgesehen angewendet wird, womit Schwachstellen dennoch bestehen bleiben.

Erhöhten Druck, Kontrolle über ihre Angriffsfläche zu bekommen, verspüren einige Unternehmen außerdem durch die NIS-2-Richtlinie, die im Oktober 2024 in Kraft treten soll. Diese dehnt die Vorgaben für kritische Infrastrukturen auf weitere Branchen aus, wodurch nun auch bestimmte KMUs davon betroffen sind.

NIS-2 verlangt von ihnen nicht nur eine zuverlässige Auskunftsfähigkeit über den Status ihrer IT-Security, sondern legt ihnen auch Verant- wortung bei Sicherheitsvorfällen auf. Vor dem Hintergrund dieser Entwicklungen ist zu erwarten, dass sich im kommenden Jahr die Nachfrage nach Managed Security Services, die diese Herausforderungen adressieren, steigern wird. Dies gilt voraussichtlich vor allem für KMUs, da bei ihnen der Bedarf an Professionalisierung größer ist. **www.lywand.com**

Sicher scheitern: Schutzschilde hochziehen reicht nicht mehr aus

Dr. Christian Polster, Mitgründer und CEO bei Materna Radar Cyber Security

Geopolitische Konflikte werden zunehmend auch im digitalen Raum ausgetragen, was zu einer Erhöhung der Bedrohungslage von Staaten, Unternehmen, Behörden und Organisationen führt. Der Vergleich durch IT-Sicherheitsmaßnahmen eine sichere Burg zu errichten ist heutzutage überholt: Bis vor kurzem war es der Ansatz durch eine reine Verstärkung der Verteidigungsanlage mit all ihren Mauern, Gräben, Toren und Wehrtürmen die Angreifer fernzuhalten. Doch die Metapher der sicheren Burg veraltet gerade:

Erstens sind IT-Infrastrukturen heute notwendigerweise in viele Richtungen hin offen – man denke nur an die Themen Cloud, Software-as-a-Service, Home-Office und Verbindungen zu Lieferanten.

Zweitens haben die Angreifer ausreichend Expertise, Zeit, Technologien und Ressourcen, um selbst die größten Hindernisse zu überwinden. Wir müssen uns eingestehen: Der zu schützende Bereich wird zunehmend größer, die notwendigen Mauern immer länger und zunehmend löchrig.

Deshalb braucht es einen Paradigmenwechsel in der Cyber-Security: Es reicht nicht länger, Schutzschilde hochzuziehen. Wir brauchen eine Strategie des „sicheren Scheiterns". Wir müssen akzeptieren, dass wir nicht alle Gefahren im Vorfeld abwehren können und uns darauf konzentrieren, Angriffe schnell zu erkennen, professionell zu managen und die Auswirkungen zu minimieren.

Es geht um Cyber-Resilienz. Dafür bedarf es eines Cyber-Resilienz-Konzepts mit klaren Prozessen und Notfallplänen. Die Sensibilisierung der eigenen Mitarbeiter - nach wie vor der Hauptangriffsvektor für Attacken - sowie ein strukturierter Zugang zum Information Security Management System (ISMS) mit einem Security Operations Center (SOC) im Zentrum sind entscheidend, um die eigene Cyber-Resilienz zu stärken.

Die Vorgaben der Europäische Union mit der Richtlinie zur Sicherheit von Netz- und Informationssystemen (NIS-2) sieht Maßnahmen vor, die bis Oktober 2024 von Unternehmen und Behörden mit mindestens 50 Beschäftigten oder zehn Millionen Euro Jahresumsatz umzusetzen sind. Die Umsetzung dieser Vorgaben werden europäischen Unternehmen und Institutionen helfen, sich für die neue Realität zu wappnen.

www.materna.com

KI-basierte Angriffstechniken erfordern verstärkten Schutz von Identitäten

Guido Grillenmeier, Principal Technologist bei Semperis

Seit Jahren nutzen Angreifer erfolgreich dieselben zentralen Schwachstellen aus. Nehmen wir als Beispiel Active Directory, den zentralen Identitätsdienst von Microsoft, der von Hackern verwendet wird, um Benutzerrechte zu erlangen und tiefer in das Netzwerk ihrer Opfer einzudringen. Während Active Directory sich seit seiner Einführung kaum verändert hat, werden die Methoden der Angreifer, sich dazu Zutritt zu verschaffen, immer fortschrittlicher. KI-Technologien ermöglichen es Cyberkriminellen, immer ausgereiftere und überzeu- gendere Phishing-Kampagnen zu erstellen, die gekonnt mit den Emotionen ihrer Opfer spielen.
Derartig ausgeklügelte Phishing-Versuche können nun selbst Nutzer mit hohem Sicherheitsbewusstsein überlisten. Die Veröffentlichung von Windows Server 2025 gegen Ende 2024 erkennt die Notwendigkeit an, die Identitätssicherheit durch die Einführung einiger zusätzlicher Sicherheitsfunktionen in Active Directory zu stärken. Es ist gut zu sehen, dass der Identitätsschutz stärker in den Fokus gerückt wird.

www.semperis.com

Cybersecurity-Trends für 2024

Fußball-EM in Deutschland und KI sorgen für Zunahme von Angriffen

Von Paul Bauer, Regional Sales Director bei Illumio

Hackerangriffe und Ransomware-Gruppen haben auch in diesem Jahr wieder für zahlreiche Schlagzeilen gesorgt und viele Unternehmen wie beispielsweise Motel One, die Deutsche Leasing oder Lürssen betroffen. Keine Branche ist davor gefeit. Wie jedes neue Jahr bringt auch das Jahr 2024 sowohl Chancen als auch Herausforderungen für die IT-Sicherheit mit sich. Illumio geht davon aus, dass die folgenden Themen eine wichtige Rolle spielen.

Hochkarätige Veranstaltungen wie die Fußball-Europameisterschaft in Deutschland – aber auch die Olympischen Spiele in Paris und die Europawahlen – sind nicht nur logistische und organisatorische Herausforderungen, sondern bieten eine gute Gelegenheit für groß angelegte Angriffe auf kritische Infrastrukturen. Ransomware-Gruppen werden versuchen, diese als Chance auf hohe Lösegeld-Summen zu nutzen, da sie wissen, dass sich Unternehmen während dieser Veranstaltungen keine Ausfälle leisten können. Zugleich werden Cyberkriminelle und staatlich geförderte Hacker versuchen, Chaos und wirtschaftliche Instabilität herbeizuführen. Besonders gefährdet sind die Sektoren Energie, Verkehr, Kommunikation und öffentliche Dienste.

Künstliche Intelligenz und damit einhergehende Anwendungen können die IT-Sicherheit stärken, allerdings birgt diese Technologie auch zahlreiche Gefahren. So macht es KI unglaublich einfach und vor allem schneller, Social Engineering und Manipulation zu optimieren. Dadurch sind bessere und realistischere Techniken bei Phishing und Deep Fakes zu erwarten, die Stimmen und Videos simulieren und versuchen, die biometrische Authentifizierung zu umgehen, um Zugang zu Unternehmen zu erhalten. Algorithmen werden Kommunikationsmuster und Nachrichten imitieren, die so legitim erscheinen, dass Angreifer damit das Vertrauen gewinnen können. Gleichzeitig wird die KI zur Datenauswertung eingesetzt, um die Erfolgswahrscheinlichkeit zu erhöhen.

Darüber hinaus birgt KI weitere Gefahren: So wird die rasche Einführung von KI in Unternehmen zu einem starken Anstieg unbeabsichtigter Cyber-Vorfälle führen. Die Mitarbeiter nutzen vermehrt KI-Tools, um ihre Arbeit besser und schneller erledigen zu können. Allerdings verstehen die meisten noch nicht, wie sie diese nutzen oder die Antworten interpretieren können, was zu einem enormen Anstieg unbeabsichtigter Cyber-Vorfälle führen wird. Verschärft wird das Ganze durch frei zugängliche Anwendungen, die aber nicht ausdrücklich an die angemessenen unternehmensinternen Sicherheitsgrenzen der Compliance, Vertraulichkeit und Geheimhaltungsvereinbarungen gebunden sind. Insbesondere auch dann, wenn die Nutzer der Technologie mit kritischen Informationen in Forschung und Entwicklung, geistigem Eigentum oder sensiblen Daten arbeiten.

Unabhängig davon, ob KI oder internationale Ereignisse die treibende Kraft sind, eines ist sicher: Im nächsten Jahr wird es mehr Cyberangriffe geben, und diese werden raffinierter sein und wahrscheinlich Erfolg haben.

Es stellt sich nicht mehr die Frage, ob und wann man angegriffen wird, sondern wie stark man betroffen ist. Das Ziel sollte daher sein, den Betrieb auch angesichts von Angriffen aufrechtzuerhalten. Dies bedeutet, dass man akzeptiert, dass es zu Angriffen kommen wird, und sich auf die Stärkung der Cyberresilienz konzentriert, und zwar durch bewährte Strategien wie Zero Trust und der Eindämmung von Angriffen. Durch die Implementierung von Technologien wie Zero-Trust-Segmentierung – Mikrosegmentierung unter dem Aspekt von Zero Trust – können sich Unternehmen besser schützen und die Auswirkungen von Angriffen abmildern.

Zero-Trust-Segmentierung

- **Hälfte aller Cyberangriffe haben ihren Ursprung in der Cloud und kosten Unternehmen im Schnitt 3,76 Millionen Euro**
- **Die Studie unterstreicht, dass Zero-Trust-Segmentierung für die Cloud-Sicherheit unverzichtbar ist**

Illumio, Inc., Anbieter für Zero-Trust-Segmentierung, präsentiert seinen neuen Cloud Security Index: „Redefine Cloud Security with Zero Trust Segmentation". Die weltweite Studie informiert über den aktuellen Stand der Cloud-Sicherheit, die Auswirkungen von Angriffen auf die Cloud und die Gründe für das Versagen herkömmlicher Cloud-Sicherheitstechnologien beim Schutz von Unternehmen in der Cloud. Vanson Bourne, ein unabhängiges Forschungsunternehmen, befragte 1.600 IT- und Sicherheitsentscheider in neun Ländern und stellte fest, dass die Cloud-Risiken immer größer werden, herkömmliche Cloud-Sicherheitstools nicht mehr ausreichen und dass Zero-Trust-Segmentierung (ZTS) für die moderne IT-Infrastruktur unerlässlich ist.

Die wichtigsten Erkenntnisse sind:

- Die traditionelle Cloud-Sicherheit lässt moderne Unternehmen im Stich: Im letzten Jahr hatte fast die Hälfte aller Datenschutzverletzungen (47 Prozent) ihren Ursprung in der Cloud, und mehr als sechs von zehn Befragten glauben, dass die Cloud-Sicherheit unzureichend ist

und ein ernsthaftes Risiko für ihre Geschäftsabläufe darstellt.

- Datenschutzverletzungen in der Cloud kosten Unternehmen jedes Jahr Millionen: Im Durchschnitt hat ein Unternehmen, das im letzten Jahr von einem Angriff auf die Cloud betroffen war, fast 4,1 Millionen Dollar Schaden erlitten. 26 Prozent der Befragten gehen davon aus, dass Sicherheitsverletzungen nicht unvermeidlich sind, was ein ernstes Risiko für Unternehmen und deren Kunden darstellt.

- ZTS ist entscheidend für die Resilienz der Cloud: 93 Prozent der Befragten stimmen zu, dass ZTS ein wesentlicher Bestandteil jeder Cloud-Sicherheitsstrategie ist, da es das digitale Vertrauen erhöht (61 Prozent), die Geschäftskontinuität gewährleistet (59 Prozent) und die Cyberresilienz stärkt (61 Prozent).

Cloud-Probleme sind in der komplexen, hybriden Welt von heute allgegenwärtig

In dem Moment, in dem Unternehmen ihre sensibelsten Daten in die Cloud verlagern, steigt die Komplexität und das Risiko für sie. 98 Prozent der Unternehmen speichern ihre sensibelsten Daten in der Cloud, darunter Finanzdaten, Business Intelligence und personenbezogene Daten von Kunden oder Mitarbeitern. Dennoch sind mehr als 9 von 10 Unternehmen besorgt, dass unnötige oder unautorisierte Verbindungen zwischen Cloud-Diensten die Wahrscheinlichkeit einer Kompromittierung erhöhen.

Laut der Studie sind die Hauptbedrohungen für die Cloud-Sicherheit von Unternehmen folgende: Arbeitslasten und Daten, die klassische Systemgrenzen überschreiten (43 Prozent); mangelndes Verständnis für die Aufteilung der Verantwortung zwischen Cloud-Anbietern und -Händlern (41 Prozent); Social-Engineering-Angriffe (36 Prozent); mangelnde Transparenz bei Multi-Cloud-Implementierungen (32 Prozent) und zunehmende Malware- und Ransomware-Angriffe (32 Prozent).

Wo herkömmliche Cloud-Sicherheitstools versagen

Die überwältigende Mehrheit der Befragten ist der Meinung, dass der derzeitige Ansatz ihres Unternehmens in Bezug auf die Cloud-Sicherheit erhebliche Risiken birgt:

- 95 Prozent geben an, dass sie eine bessere Übersicht über die Konnektivität mit Software von Drittanbietern benötigen.
- Dieser Mangel an Transparenz wirkt sich auf die Fähigkeit der Unternehmen aus, auf Angriffe zu reagieren. 95 Prozent der Befragten gaben an, dass sie ihre Reaktionszeit auf Cloud-Angriffe verbessern müssen.

Die Befragten machen sich Gedanken über die geschäftlichen Auswirkungen eines Cloud-Angriffs – die drei größten Sorgen sind:

- Rufschädigung und Vertrauensverlust in der Öffentlichkeit (39 Prozent), Verlust sensibler Daten (36 Prozent) und Verlust von umsatzbringenden Diensten (35 Prozent).

Zero-Trust-Segmentierung ist ein unverzichtbares Element

93 Prozent der IT- und Sicherheitsentscheider sind der Meinung, dass die Segmentierung kritischer Assets ein notwendiger Schritt ist, um Cloud-basierte Projekte zu sichern. Darüber hinaus haben Unternehmen mit spezieller Mikrosegmentierungstechnologie im letzten Jahr mit geringerer Wahrscheinlichkeit einen Cloud-Angriff erlebt (35 Prozent) als Unternehmen ohne diese Technologie (43 Prozent). Und ZTS geht auf die Sichtbarkeit und Sicherheitsbedenken von Unternehmen ein, durch:

- Kontinuierliche Überwachung der Konnektivität zwischen Cloud-Anwendungen, Daten und Arbeitslasten (55 Prozent); Minimierung der Reichweite und der Auswirkungen eines Angriffs durch Eindämmung seiner Ausbreitung (51 Prozent); und Einblicke in unnötige Konnektivität, die zu einer erhöhten Anfälligkeit führen könnte (45 Prozent).

„Da Cloud-Umgebungen dynamisch und vernetzt sind, wird es für Sicherheitsteams immer schwieriger, mit herkömmlichen Lösungen zurechtzukommen", sagt John Kindervag, Chief Evangelist bei Illumio. „Unternehmen brauchen moderne Sicherheitsansätze, die ihnen standardmäßig Echtzeittransparenz und -eindämmung bieten, um Risiken zu minimieren und die Möglichkeiten der Cloud zu optimieren. Ich bin optimistisch, dass nahezu jedes Sicherheitsteam der Verbesserung der Cloud-Sicherheit in den kommenden Monaten Priorität einräumt, und dass sie Lösungen wie ZTS als einen wesentlichen Bestandteil ihrer Zero-Trust-Journey betrachten."

Illumio stellt mit CloudSecure zudem die branchenweit umfassendste ZTS-Plattform vor, die Sicherheitsteams bei der Bewältigung der dringendsten Cybersecurity-Herausforderungen in hybriden und Multi-Cloud-Umgebungen, an Endpunkten und in Rechenzentren unterstützt. Die ZTS-Plattform von Illumio visualisiert die Verbindungen in der gesamten Umgebung eines Unternehmens. Illumio ZTS macht es für Sicherheitsteams einfach, Prioritäten zu setzen und ihre Mikrosegmentierungsrichtlinien zu erstellen, um die Angreifer daran zu hindern, sich in der gesamten IT-Umgebung auszubreiten und kritische Ressourcen und Daten zu erreichen. Dies reduziert das Risiko und erhöht die Resilienz.

Der vollständige Cloud Security Index „Redefine Cloud Security with Zero Trust Segmentation" steht hier zur Verfügung:

Methodik der Studie

Im September 2023 beauftragte Illumio Vanson Bourne mit der Durchführung einer weltweiten Studie unter 1.600 IT- und Sicherheitsentscheidern über den aktuellen Stand der Cloud-Sicherheit und die Auswirkungen der Segmentierung. In die Ergebnisse flossen die Meinungen von leitenden Informationssicherheits- und IT-Fachleuten in den USA, Großbritannien, Frankreich, Deutschland, Australien, Japan, Singapur, Saudi-Arabien und den Vereinigten Arabischen Emiraten ein.

Cybersecurity-Studie: Sind IT-Sicherheits-teams zu selbstsicher?

Während die IT-Teams von Unternehmen externe Experten klar befürworten, lehnt die Mehrheit der internen Cybersecurity-Verantwortlichen diese ab.

Die Rolle der Cybersicherheit im geschäftlichen Kontext hat einen bedeutenden Wandel vollzogen: Einst als Verhinderer angesehen, wird sie zunehmend als Katalysator für Digitalisierung und Geschäftsentwicklung erkannt. Dies geht aus einer Studie hervor, die Trend Micro gemeinsam mit dem Brandenburgischen Institut für Gesellschaft und Sicherheit (BIGS) durchgeführt hat. Obwohl Unternehmen demnach die Bedeutung der IT-Security für den Geschäftserfolg mittlerweile anerkennen, offenbart die Studie eine überraschende Diskrepanz: 56,9 Prozent der firmeneigenen IT-Teams halten es für notwendig, die Expertise externer Sicherheitsspezialisten heranzuziehen, aber lediglich 14,7 Prozent der IT-Security-Verantwortlichen teilen diese Ansicht.

Spiegelt dieses Ergebnis ein überdimensioniertes Vertrauen der internen IT-Security-Verantwortlichen in die Fähigkeiten der eigenen Abteilung wider? Das könnte man annehmen. Denn fast die Hälfte der CISOs schätzt das Risiko eines Cyberangriffs auf ihr Unternehmen in den nächsten zwölf Monaten als hoch oder sehr hoch ein. Warum wollen sie dann kaum Hilfe von außen anfordern?

Mögliche Gründe für die Ablehnung externer Security-Expertise

Die Hintergründe, warum der CISO externe Unterstützung ablehnt, sind für die Unternehmensleitung von großer Bedeutung. Denn überschätzen hauseigene Security-Verantwortliche ihre Fähigkeiten tatsächlich, ist die Gefahr hoch, dass Sicherheitslücken entstehen. Eine mögliche Erklärung für die Skepsis gegenüber Managed Security Services sieht die Studie darin, dass die Inhouse-IT-Sicherheitschefs ungern Verantwortung abgeben oder Einflüsse von außen in ihrem Arbeitsbereich akzeptieren. Außerdem könnten negative Erfahrungen dafür verantwortlich sein und kostspielige externe Berater einen Cyberangriff in der Vergangenheit nicht verhindern konnten. Einen weiteren Grund konstatiert das BIGS darin, dass, nach einem bekannt gewordenen Vorfall, Firmen mit Anfragen von IT-Sicherheitsdienstleistern überschwemmt werden und bei der Vielzahl an Angeboten den Überblick verlieren und entscheidungsmüde werden.

IT-Security-Teams sind überlastet

Die Anforderungen an ein umfassendes Sicherheitskonzept steigen stetig. Cyberkriminelle organisieren sich zunehmend unternehmerisch und verfolgen hochmoderne Angriffsstrategien, während IT-Infrastrukturen immer komplexer und schwerer zu überschauen werden. Diese Entwicklungen erfordern einen ganzheitlichen Schutzansatz, dem nur komplex gestaltete Sicherheitstechnologien gerecht werden. Für Unternehmen reicht es nicht aus, in den Erwerb führender Cybersecurity-Lösungen zu investieren. Um diese in einen ganzheitlichen Sicherheitsansatz zu integrieren, müssen sie sorgfältig konfiguriert, professionell verwaltet und rund um die Uhr überwacht werden. Für die IT-Teams bedeutet das eine hohe Belastung – nicht zuletzt auch mental. Der globale Fachkräftemangel, der laut einer aktuellen (ISC)2-Studie in der Cybersecurity mit 3,4 Millionen fehlenden Experten beziffert wird, verstärkt die Überlastung der Branche

Studie: https://tinyurl.com/5xvwp7sy

Über die Studie

Das Marktforschungsunternehmen Mindfacts befragte im Auftrag von Trend Micro 300 leitende Angestellte aus der IT und IT Security in Unternehmen mit mehr als 250 Mitarbeitern aus verschiedenen Branchen. Je 30 Prozent der Teilnehmer stammen aus dem Gesundheitswesen und aus Behörden. Die Umfrage fand im September und Oktober 2022 statt. Auf Basis der Ergebnisse führte das Brandenburgische Institut für Gesellschaft und Sicherheit BIGS eine empirische Analyse durch. Es untersuchte Zusammenhänge und ermittelte unter anderem, welche Faktoren zu eher strategischen oder reaktiven Investitionen in IT-Sicherheit führen.

Top Software & Testing Trends

2023 stand ganz im Zeichen von ChatGPT. Der KI-Hype wird sich auch 2024 fortsetzen und bringt für Entwicklungsunternehmen sowohl neue Chancen als auch Herausforderungen. Welche Trends sich für das kommende Jahr im Software Testing abzeichnen, erklärt Viktoria Praschl, VP Sales Central Europe bei Tricentis.

Software & Testing Trends

1. Anforderungen an das Testing von KI-Modellen steigen

Mit ChatGPT hat sich generative KI breitflächig durchgesetzt. Aber das Potenzial der neuen Technologie ist noch lange nicht ausgeschöpft. 2024 werden sich sowohl generative KI als auch allgemeine KI-Modelle weiterentwickeln. Gleichzeitig macht auch die Regulierung Fortschritte. Auf dem AI Saftey Summit im November vereinbarten die teilnehmenden Länder, künftige KI-Modelle einiger der weltweit größten Technologieunternehmen vor ihrer Veröffent- lichung zu testen. 2024 soll außerdem der EU AI Act in Kraft treten. Unternehmen werden daher neue Tools und Technologien einführen, um Risiken von KI-Systemen zu bewerten, Compliance-Vorgaben einzuhalten und trotzdem Innovationen voranzutreiben.

2. KI-gestützte Test-Automatisierung ist auf dem Vormarsch

2024 bleibt die wirtschaftliche Lage angespannt. Unternehmen müssen gut mit ihren Budgets haushalten, trotzdem aber wachsende Kunden-Anforderungen erfüllen und ihre Release-Geschwindigkeit steigern. Sie können es sich nicht mehr leisten, unnötig Zeit und Ressourcen mit manuellen Aufgaben zu verschwenden. Testautomatisierung wird daher unverzichtbar. Immer mehr Unternehmen nutzen dabei das Potenzial von KI. Die neue Technologie kann zum Beispiel beim Test-Case-Design unterstützen, die Fehlersuche erleichtern und oder UI-Tests automatisieren, indem sie menschliches Nutzerverhalten simuliert. Richtig trainiert kann generative KI sogar selbst Test Cases schreiben. Mitarbeitende müssen allerdings lernen, die KI so anzuleiten, dass sie die gewünschten Ergebnisse liefert.

3. Generative KI-Anwendungen erfordern Continuous Testing

Immer mehr Unternehmen integrieren generative KI in ihre Produkte und Services. Das wirft auch die Frage auf, wie man solche Anwendungen testet. Da sich selbstlernende Systeme kontinuierlich verändern, kann es passieren, dass sie im Laufe der Zeit abdriften und anders reagieren als erwartet. Um Fehlverhalten zu erkennen, brauchen Unternehmen eine neue Testing-Strategie, die eher einem kontinuierlichen Monitoring gleicht. Außerdem sollten sie in einer simulierten Umgebung prüfen, welche Auswirkungen Veränderungen der KI auf kritische Prozesse haben.

4. Tests zur Datenintegrität gewinnen an Bedeutung

Experten prognostizieren, dass sich das Datenvolumen im nächsten Jahr verdoppeln wird. Umso wichtiger wird es für Unternehmen, diese Flut effizient zu meistern und die Datenintegrität sicherzustellen. Sie müssen in der Lage sein, schnell hochqualitative Daten für die täglichen Prozesse und Geschäftsentscheidungen bereitzustellen. Der Trend geht daher zu herstellerunabhängigen Datenintegritätslösungen, die es ermöglichen, die gesamten Datenströme in der IT-Landschaft zu testen. Dabei spielen KI-Unterstützung und Automatisierung eine wichtige Rolle, um die geforderte Geschwindigkeit zu erzielen, die Mitarbeitenden zu entlasten und das Risiko für Fehler zu minimieren.

5. Der Einsatz von Low-Code/No-Code Tools nimmt weiter zu

Der Fachkräftemangel wird sich noch verschärfen. In den kommenden Jahren müssen Unternehmen weiterhin versuchen, mit knapp besetzten Teams mehr zu erreichen. Low-Code-Tools erweisen sich als wertvolle Hilfe, um die verfügbaren Ressourcen optimal einzusetzen. Sie ermöglichen es, ohne Programmierkenntnisse Tests zu designen, zu managen und durchzuführen. So können auch weniger technisch versierte Mitarbeiter bei der Qualitätssicherung unterstützen, während erfahrene Entwickler mehr Zeit für strategische Aufgaben gewinnen. 71 Prozent der IT-Entscheider in Deutschland, Österreich und der Schweiz gehen davon aus, dass der Einsatz von Low-Code/No-Code in den nächsten drei Jahren zunehmen wird, so eine KPMG-Studie.

6. Quality Engineering wird stärker in den Software-Lebenszyklus integriert

Unternehmen sind heute mit einem volatilen Umfeld konfrontiert, in dem sich Kunden- und Marktanforderungen ständig ändern. Sie müssen in der Lage sein, schnell zu reagieren, dürfen dabei aber keine Kompromisse bei der Qualität machen. Daher wird es immer wichtiger, Quality Engineering in alle Phasen des Software-Lebenszyklus zu integrieren. 2024 werden Unternehmen verstärkt eine ganzheitliche Strategie zur Qualitätssicherung verfolgen. Mit KI-gestützter Testautomatisierung und einem Low-Code/No-Code-Ansatz lässt sich das effizient umsetzen.

7. Der Mobile-Trend setzt sich fort

Fast 59 Prozent des Online-Traffics erfolgt heute bereits über mobile Endgeräte. Künftig wird der Anteil weiter steigen. Mobile Anwendungen bereitzustellen, wird daher entscheidend für den Geschäftserfolg. Die Nutzererwartungen sind hoch: Unternehmen müssen dafür sorgen, dass ihre Apps performant mit verschiedenen Endgeräten und Browsern funktionieren. Dafür benötigen sie eine Strategie, um ihre Software schnell und einfach in vielen verschiedenen Szenarien zu testen – sowohl mit physischen als auch virtuellen Smartphones und Tablets.

Fazit

Neben dem KI-Hype sind Entwicklungsunternehmen 2024 weiterhin mit alt bekannten Herausforderungen konfrontiert: Sie müssen trotz Fachkräftemangel und knappen Budgets immer schnellere Release-Zyklen meistern und wachsende Qualitätsanforderungen erfüllen.

Viktoria Praschl, VP Sales Central Europe bei Tricentis, fasst zusammen: „Unternehmen sollten alle Möglichkeiten ausschöpfen, um Quality Engineering agil, effizient und ganzheitlich zu gestalten.

Dazu gehört Testautomatisierung ebenso wie der Einsatz von KI und Low-Code/No-Code. Künstliche Intelligenz kann im Software Testing heute schon wertvolle Unterstützung leisten. Hier wird sich in den kommenden Jahren noch viel tun. Andererseits erfordern KI-Anwendungen selbst eine neue Testing-Strategie."

[www.tricentis.com]

Gestohlene Daten und Zugänge
von jedem dritten Unternehmen im Darknet

Weltweit taucht jedes dritte Unternehmen im Zusammenhang mit dem Verkauf gestohlener Daten im Darknet auf, wie eine Stichprobe der Kaspersky-Experten [1] zeigt. Über einen fast zweijährigen Untersuchungszeitraum hinweg entdeckten sie fast 40.000 Nachrichten, die kompromittierte Unternehmensdaten zum Kauf, Verkauf oder zur Weitergabe angeboten haben. Der Verkauf von Zugängen zu Unternehmensinfrastrukturen im Darknet stellt eine zunehmende Bedrohung für Unternehmen dar: Kaspersky verzeichnete eine Zunahme um 16 Prozent im Vergleich zum Vorjahr.

Insgesamt entdeckte die Kaspersky Digital Footprint Intelligence zwischen Januar 2022 und November 2023 etwa 40.000 Nachrichten in Foren, Blogs und Telegram-Schattenkanälen, die sich um den Handel von internen Unternehmensdatenbanken sowie Dokumenten drehten.

In einigen Nachrichten wurde jedoch auch der Zugang zu Unternehmensinfrastrukturen angeboten. Mehr als 6.000 solcher Nachrichten identifizierten die Kaspersky-Experten während des fast zweijährigen Untersuchungszeitraums – und die Angebote nehmen zu. Die durchschnittliche Anzahl monatlicher Nachrichten dieser Art stieg zwischen dem vergangenen Jahr und 2023 um 16 Prozent von 246 auf 286. Hinsichtlich der für 2024 prognostizierten Gefahr durch Supply-Chain-Angriffe könnten auch Daten-Leaks bei kleineren Unternehmen erhebliche Folgen für eine Vielzahl von Menschen und Unternehmen weltweit haben.

Weiterhin untersuchten die Kaspersky-Experten, zu welchen Unternehmen die Zugänge verkauft wurden. Hierzu wählten sie 700 Unternehmen zufällig aus, die im Jahr 2022 im Zusammenhang mit kompromittierten Unternehmensdaten standen. In 233 Beiträgen tauchten Angebote zu diesen im Darknet auf. Diese erwähnten explizit Daten-Leaks, gestohlene Zugänge zu Infrastrukturen oder gehackte Konten.

„Nicht jede Nachricht im Darknet enthält neue oder einzigartige Informationen", erklärt Anna Pavlovskaya, Expertin bei Kaspersky Digital Footprint Intelligence. „Manche Angebote können sich doppeln. Möchten Cyberkriminelle Daten zum Beispiel besonders schnell verkaufen, veröffentlichen sie die Angebote in verschiedenen Untergrund-Foren, um ein größeres Publikum potenzieller Käufer zu erreichen. Zudem können bestimmte Datenbanken kombiniert und erneut angeboten werden. Solche kombinierten Angebote fassen beispielsweise Informationen aus verschiedenen zuvor geleakten Datenbanken zusammen, wie etwa Passwörter für E-Mail-Adressen."

Kaspersky-Empfehlungen zur Risikominimierung bei Daten-Leaks

- Darknet kontinuierlich auf Posts zu Daten-Leaks überwachen. Services wie Kaspersky Digital Footprint Intelligence [2] helfen dabei, den Überblick zu behalten.
- Schnelle Identifikation von und Reaktion auf Daten-Leaks ist essenziel. Bei einem solchen Vorfall sollte zunächst die Ursache verifiziert, interne Daten und die Authentizität der Informationen geprüft werden. Unternehmen müssen Beweismittel sammeln, um zu bestätigen, dass der Angriff stattgefunden hat und Daten kompromittiert wurden.
- Umfassende Incident-Response-Pläne für die Vorfallreaktion vorab entwickeln, die zuständigen Teams, Kommunikationskanäle und Protokolle festlegen, um bei einem Daten-Leak schnell und effektiv handeln zu können [3]. Hierzu zählt auch ein Plan bezüglich der Kommunikation an Kunden, Journalisten und Behörden bei solchen Vorfällen.

Fußnoten

[1] https://securelist.com/what-to-do-if-your-company-was-mentioned-on-darknet/111358/
[2] https://content.kaspersky-labs.com/se/media/en/business-security/enterprise/kaspersky-digital-footprint-intelligence-datasheet.pdf
[3] https://www.kaspersky.de/enterprise-security/incident-response

Nützliche Links:

- Kaspersky-Untersuchung zu Daten-Leaks: https://securelist.com/what-to-do-if-your-company-was-mentioned-on-darknet/111358/
- https://content.kaspersky-labs.com/se/media/en/business-security/enterprise/kaspersky-digital-footprint-intelligence-datasheet.pdf > Kaspersky Digital Footprint Intelligence
- Kaspersky Incident Response Service: https://www.kaspersky.de/enterprise-security/incident-response
- Kaspersky Threat Intelligence: https://go.kaspersky.com/test-threat-intelligence-de.html

Kaspersky-Untersuchung unter: https://tinyurl.com/3m2v8a63

IT-Trends 2024: 5 Prognosen zwischen Hyper-Personalisierung und KI-Inzucht

- **PAC, das führende europäische Marktanalyse- und Beratungsunternehmen für die IT-Branche, hat die wichtigsten Trends für die IT-Verantwortlichen im Jahr 2024 zusammengefasst.**
- **Neben strikterem Cloud-Kostenmanagement wird es in Zukunft u.a. auf ein effektives Sicherheitsmanagement ankommen.**
- **Zugleich wird GenAI die Chancen für eine Hyper-Personalisierung im Rahmen der Customer Experience von Unternehmen erhöhen.**

Zum Jahreswechsel veröffentlichen die PAC-Analysten auf Basis fundierter Analysen ihre wichtigsten Prognosen für das neue Jahr. Sie zeigen die entscheidenden Trends und Marktentwicklungen auf, die sich auf unterschiedliche Weise auf den IT-Markt auswirken werden.
Fünf zentrale Trends sind es, die nach den Erkenntnissen der Analysten in 2024 und darüber hinaus für Unternehmen überdurchschnittliches Wachstum, Effizienzsteigerung und mehr Nachhaltigkeit bringen werden – und wie zu erwarten war, haben viele mittelbar oder unmittelbar etwas mit dem Themenfeld der Künstlichen Intelligenz zu tun.

1. FinOps für GenAI: Verwaltung von Cloud-Kosten im KI-Zeitalter wird für Unternehmen zur Herausforderung.

Das Jahr 2023 markierte einen Wendepunkt für KI-Services, insbesondere resultierend aus der wachsenden Bedeutung von Generative AI (GenAI). stehen nun vor einem neuen FinOps-Wendepunkt, da GenAI hohe Rechen- und Datenverarbeitungskapazitäten erfordert, die nur durch Cloud-Dienste erschwinglich realisiert werden können. PAC sieht GenAI als das, was die Tech-Industrie eine „Killer-Applikation" nennt, da es sich um eine Innovation handelt, deren Anwendungsfall sowohl das private als auch das berufliche Leben von Menschen weltweit verändert und beeinflusst.
Gleichzeitig sehen die Analysten aber auch ein erhebliches Risiko für Unternehmen, dass die Nachfrage nach solchen Diensten zu unerwarteten Kostensteigerungen führt – in einer Größenordnung und Geschwindigkeit, die weitaus gravierender ist als die anfänglichen Kostenprobleme bei der Ausbreitung der Cloud. „Unternehmen müssen daher die Cloud-Service-Kosten für KI in allen Geschäftsbereichen durch FinOps effektiv verwalten und eine Kultur der finanziellen Transparenz und Verantwortlichkeit schaffen", rät Spencer Izard, Principal Analyst von PAC.

2. MLSecOps: Effektives Sicherheitsmanagement wird in einer von „Multi-Hops" geprägten KI-Landschaft zum Muss.

Mit der Zunahme der KI-Nutzung steigt auch die Notwendigkeit, Sicherheitspraktiken an ML-bezogene Workflows anzupassen. Viele Unternehmen stehen vor der Herausforderung, KI in einer Vielzahl von IT-Lösungen zur Unterstützung von Geschäftsmodellen zu etablieren – und Unternehmen, die ihre Cybersicherheitsstrategie nicht parallel zu ihrer KI-Strategie anpassen, gehen hohe Risiken ein. MLSecOps-Rahmenwerke werden daher für die Absicherung von KI-Lösungen und -Diensten zunehmend einen höheren Stellenwert bekommen. Eine besondere Herausforderung aufgrund der in vielen Unternehmen zu beobachtenden breiten Palette an KI-Services, ist dabei die sogenannte „Multi-Hop-KI".
Darunter versteht man die Verkettung mehrerer KI-Lösungen oder -Dienste und ihrer Datensätze zu einer integrierten Pipeline oder Lieferkette, wobei bei jedem Hop eine andere, oft cloudbasierte KI-Lösung oder ein anderer Dienst genutzt wird. Diese KI-Nutzung wird Lösungen und Dienste von einer Vielzahl von IT-Anbietern umfassen. Zwischen den einzelnen „Hops" wird es

keine menschliche Interaktion geben, sodass der Mensch nur den anfänglichen Input liefert und dann den Multi-Hop-Output erhält. PAC hält dies für einen revolutionären Schritt, aber auch ein Risiko bei der Nutzung von KI. „Dem Mehrwert von KI für Unternehmen steht das Potenzial für neue Formen von Sicherheitsverletzungen gegenüber. Denn Daten sind aus Sicht der Cybersicherheit das wertvollste Gut, das sich böswillige Akteure aneignen können – und da sie das Herzstück aller KI sind, ist dies ein Bereich, mit dem sich CxOs in den kommenden Jahren intensiv befassen müssen", weiß Spencer Izard.

3. Umgang mit der KI-Inzucht: Wie die Anwendung von verantwortungsvoller und erklärbarer KI für Validität sorgt.

Ein zunehmend relevantes Problem im Zusammenhang mit Künstlicher Intelligenz ist die sogenannte „KI-Inzucht". Dieses Phänomen tritt auf, wenn KI-Systeme überwiegend von anderen KI-generierten Inhalten lernen, was zu einer Verzerrung und Entfremdung von der menschlichen Perspektive führen kann. Während etwa die aktuellen Versionen des ChatGPT-Modells auf einer relativ sauberen Bandbreite von überwiegend menschengenerierten Datenpunkten trainiert wurden, könnten zukünftige KI-Modelle immer mehr Daten generieren (und von ihnen lernen), die sich über viele Verarbeitungsiterationen hinweg von der Relevanz für menschliche Perspektiven unterscheiden.

Diese Entwicklung, besonders sichtbar im Bereich der generativen KI (GenAI), könnte die Langzeitwirksamkeit von KI-Lösungen beeinträchtigen. „Wir von PAC halten dies für ein sehr ernstes Warnsignal für eine potenzielle Zukunft mit schwerwiegenden Auswirkungen auf den Nutzen der KI sowohl für Organisationen als auch für die Gesellschaft", warnt Spencer Izard. Verantwortungsvolle und erklärbare KI-Tools und Frameworks können indes als geeignete Instrumente zur Bewältigung dieses Problems angesehen werden.

4. Hyper-Personalisierung: Digitale Assistenten schaffen mit Hilfe von GenAI eine individuelle Kundenansprache.

Seit Jahren streben Unternehmen im B2C- oder D2C-Geschäft danach, digitale Einkaufserlebnisse ähnlich einem persönlichen Einkaufsberater mit möglichst präziser Personalisierung zu bieten. Generative KI eröffnet Chancen Hyper-Personalisierung zu erreichen, die darauf abzielt, eine möglichst enge und langfristige Beziehung zum Kunden zu entwickeln, die das Engagement und die Loyalität erhöht und Cross- und Upselling-Möglichkeiten eröffnet. In der Vergangenheit waren die Kosten für einen Einkaufsberater, der den Kunden so passgenau beraten konnte, angesichts der unzureichenden Datenlage zu hoch und die Skalierbarkeit nicht gegeben.

Auch waren vor GenAI die Chatbot-Style-Schnittstellen nicht ausgeklügelt genug, um Kaufberatungen oder Steuerungen ähnlich einem traditionellen persönlichen Einkaufsberater zu bieten. PAC prognostiziert, dass ab 2024 die Integration von GenAI in digitale Erlebnisse auf Mitarbeitergeräten zur Unterstützung persönlicher Interaktionen und durch ähnliche Erlebnisse direkt auf den Geräten der Kunden vermehrt erfolgen wird. „Dadurch wird GenAI den Zugang zu digitalen Assistentendiensten im Stil eines persönlichen Einkaufsberaters für die Verbraucher demokratisieren, den Kaufzyklus von Unternehmen vereinfachen und neue Umsatzmöglichkeiten schaffen", prognostiziert Spencer Izard.

5. Neue ESG-Regulierung: Die CSRD verschärft die Anforderungen an Unternehmen für eine nachhaltige IT-Landschaft.

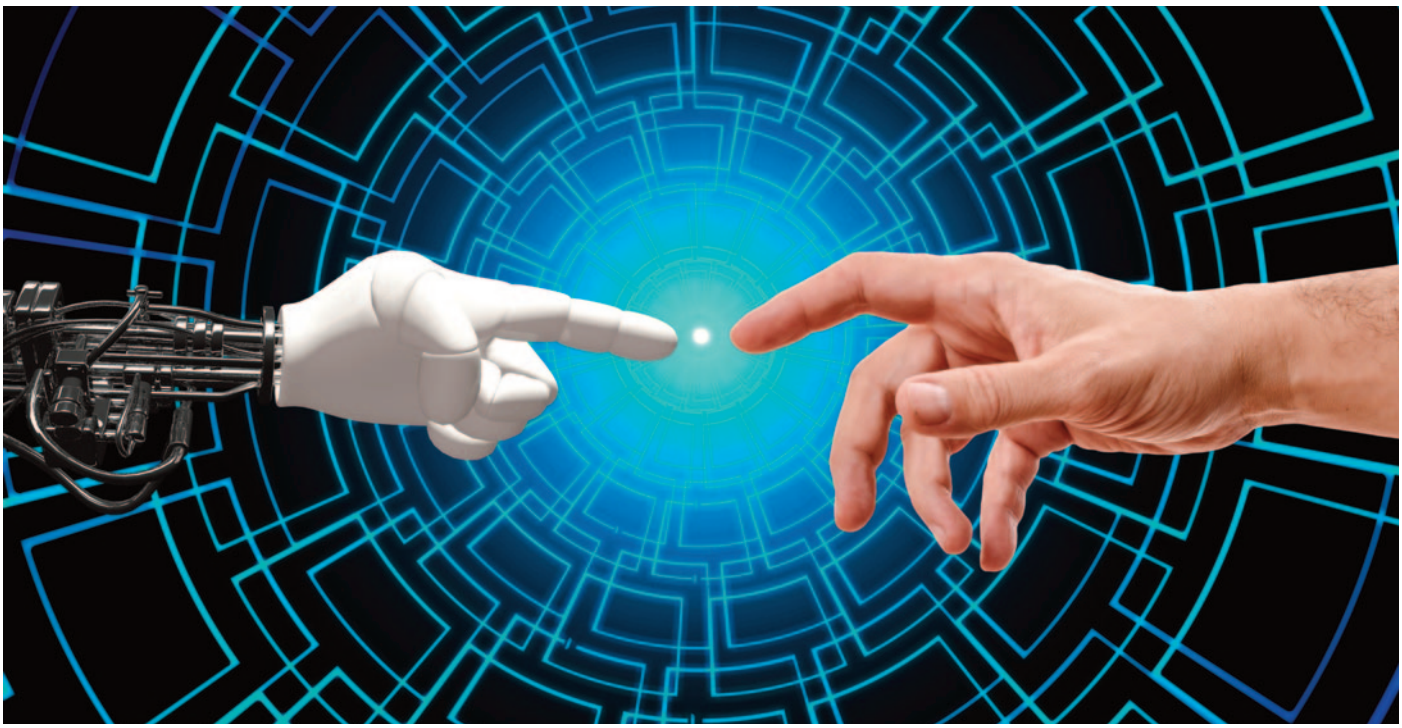
Die Corporate Sustainability Reporting Directive (CSRD) regelt ab 2024 EU-weit die Umweltberichterstattung und forciert damit die internationalen ESG-Bestrebungen. Die Experten von PAC sehen das Inkrafttreten der CSRD als Beschleuniger des Wandels hin zu mehr Nachhaltigkeit in Unternehmen. Waren diese in der Vergangenheit an Nachhaltigkeit vor allem deshalb interessiert, weil ihre Kunden danach fragten und es die Gelegenheit bot, Umsätze zu steigern, besteht nun eine Verpflichtung mit rechtlichen, rufschädigenden und kommerziellen Komponenten. „Unternehmen werden vermehrt nach Partnern suchen, die ihnen helfen, die richtigen Softwarelösungen und Prozesse zu implementieren, um Daten im Zusammenhang mit ESG effizient zu verfolgen, zu sammeln und zu analysieren", sagt Mopia Kamdoum, Analystin von PAC.

Gleichzeitig wird die Vergleichbarkeit der Berichte die Unternehmen dazu drängen, zu zeigen, dass sie mindestens so nachhaltig ausgerichtet sind wie ihre direkten Mitbewerber. Der Trend zu mehr Nachhaltigkeit wird Unternehmen zudem weiter zu einer Cloud-First-Strategie ermuntern.

Neben der Möglichkeit, einzelne Workloads mit vertretbarem Aufwand und Betriebskosten in die Cloud zu migrieren, werden Organisationen zunehmend fragen, wie nachhaltig verschiedene Cloud-Angebote sind. Bei der Auswahl eines Cloud-Anbieters wird Nachhaltigkeit neben der Verfügbarkeit von Dienstleisterressourcen und angemessenen Funktionen in der PaaS-Umgebung ein Schlüsselfaktor sein. Zudem werden auch die Cloud-Anbieter Effizienzparameter für Interessenten bereitstellen, um die Nachhaltigkeit der Angebote zu belegen.

*PAC hat sich als das führende europäische Marktanalyse- und Beratungsunternehmen für die IT-Branche einen Namen gemacht. Mit der klaren Fokussierung auf die teils speziellen Marktentwicklungen in Europa decken die Expertinnen und Experten mehr als 30 Ländermärkte im Detail ab.

Mehr zu diesen und einigen weiteren Prognosen im folgenden ausführlichen Beitrag: https://sitsi.pacanalyst.com/pacs-predictions-for-2024/



Die 5 wichtigsten KI-Trends

- **Liz Centoni, CCSO bei Cisco, nennt fünf Technologiefelder, in denen KI im neuen Jahr verstärkt Einzug halten wird.**
- **Generative KI wird 2024 vor allem in Geschäftsanwendungen allgegenwärtig sein.**
- **Die Fortschritte in der KI bergen neue Cyberrisiken aber auch Chancen für Umwelt und Unternehmen.**
- **Ethik und Frameworks werden beim Einsatz von KI eine zentrale Rolle spielen.**

KI-Technologien entwickeln sich in einem noch nie dagewesenen Tempo. Die Fortschritte Künstlicher Intelligenz, insbesondere der generativen KI (GenAI), eröffnen neue Möglichkeiten, die unsere Wirtschaft, Arbeits- und Lebensweisen maßgeblich verändern werden. Der Cisco AI Readiness Index zeigt jedoch, dass zwar 95 Prozent der deutschen Unternehmen über eine KI-Strategie verfügen oder sie entwickeln, aber nur 7 Prozent bestmöglich auf den Einsatz von KI vorbereitet sind. Liz Centoni, Chief Strategy Officer und EVP/GM of Applications bei Cisco, nennt fünf Technologiefelder, in denen KI im neuen Jahr verstärkt Einzug halten wird.

1 APIs vereinfachen die Nutzung von KI

Unternehmen haben einen wachsenden Bedarf, Daten, Automatisierung und Innovation schnell und einfach zu nutzen. Laut Cisco AI Readiness Index priorisieren allerdings nur 17 % der deutschen Unternehmen Budgets für die KI-Einführung gegenüber anderen Technologieinvestitionen. Eine Lösung wird die verstärkte Verwendung von Schnittstellen (API) sein. Über diese Abstraktions-Ebene werden im kommenden Jahr viele KI-Tools und -Services integriert werden. Solche „API-Abstraktionen" ermöglichen eine kostengünstigere Einbindung von KI in Geschäftsprozesse, ohne dass EntwicklerInnen tief in die technischen Details der KI-Einführung eingreifen oder eigene Large Language Models (LLM) entwickeln zu müssen. Durch den Zugriff auf eine Vielzahl von KI-Funktionen über APIs können sich wiederholende Aufgaben automatisiert werden und Entscheidungen auf besseren Datengrundlagen getroffen werden.

Ebenfalls werden sich 2024 APIs durchsetzen, die eine kundenindividuelle Umsetzung von KI ermöglichen. Unternehmen kombinieren dazu Schnittstellen verschiedener Anbieter und erzeugen damit KI-Lösungen für ihre individuellen Anforderungen. Die Verzahnung unterstützt zugleich die Zusammenarbeit mit externen KI-Experten, Start-ups und Forschungseinrichtungen. Aktuell sind bereits erste Modelle solcher kuratierten KI-Ökosysteme erkenn-

bar – Modelle, die wir im kommenden Jahr häufiger erleben werden.

2 KI-gestützte Cyberangriffe erfordern Zusammenarbeit von Politik, Wirtschaft und Zivilgesellschaft

2024 werden Unternehmen, Politik, NGOs und Zivilgesellschaft zunehmend durch KI-generierte Desinformation gefährdet sein. Laut dem Cybersecurity Readiness Index 2023 von Cisco sind nur 11 % der deutschen Unternehmen resilient genug, um gegen Cyberangriffe zu bestehen – und nur 29 % haben überhaupt ein gutes Verständnis zu den verschiedenen Cyberbedrohungen durch KI. Technologieunternehmen und Regierungen werden darum 2024 gemeinsam daran arbeiten, Lösungen gegen KI-gestützte Bedrohungen wie

Deepfakes, KI-Social-Bots oder geklonte Sprachaufnahmen zu schärfen und geeignete Cybersicherheitsmaßnahmen zu implementieren. Auch werden Investitionen in die Risikoerkennung und das Training von KI-Modellen mit großen Datensätzen zunehmen. Um Bedrohungen frühzeitig zu erkennen, müssen Unternehmen daher 2024 in fortschrittliche Sicherheitstechnologien investieren und dem Datenschutz höhere Priorität einräumen.

3 Generative KI hält vollständig Einzug in die Geschäftswelt – auch im B2B-Bereich

Um wettbewerbsfähig zu bleiben, müssen Unternehmen innerhalb des kommenden Jahres KI implementieren. Darum stehen 2024 natürliche, sprachliche Schnittstellen (NLIs) für neue Produkte im Fokus, die von GenAI unterstützt werden. Die Hälfte der neuen Produkte wird solche Interfaces standardmäßig integriert haben. GenAI wird ebenso die Interaktionen im B2B-Geschäft verbessern, Schnittstellen und Dienste für Datenzugriffe bieten und in vielen Geschäftsanwendungen eingesetzt werden. Dies betrifft vor allem Unternehmensaufgaben, die Daten analysieren und visualisieren, beispielsweise im Projektmanagement, in der Bewertung von Softwarequalität oder der Analyse von Compliance-Feldern sowie bei HR-Aufgaben. Es ist weiterhin abzusehen, dass spezialisierte KI-Modelle stärker in den Fokus rücken. Damit wird eine Verlagerung hin zu kleineren LLMs mit höherer Genauigkeit, Relevanz, Präzision und Effizienz gehen.
So können beispielsweise LLaMA-7B-Modelle für Sprachaufgaben wie das Schreiben und Vervollständigen von Code oder die Klassifizierung von Bildern mit wenigen Aufnahmen („few-shotting") eingesetzt werden. Darüber hinaus wird die Multimodalität, bei der verschiedene Datentypen wie Bilder, Text, Sprache und numerische Daten kombiniert werden, die B2B-Anwendungsfälle in Bereichen wie Geschäftsplanung, Medizin und Finanzdienstleistungen erweitern und dort für kontinuierlich bessere Ergebnisse sorgen.

4 Verbesserte Energieeffizienz beim KI-Einsatz ist wichtiger denn je

Kleinere, auf spezifische Anwendungsfälle zugeschnittene KI-Modelle reduzieren schon 2024 im Vergleich zu generischen Systemen die Energiekosten beim Einsatz von KI. Diese speziellen Systeme werden auf hochpräzisen Datensätzen trainiert und erledigen die spezifische Aufgaben deutlich effizienter. Im Gegensatz dazu müssen bei Deep-Learning-Modellen große Datenmengen verarbeitet werden, um Ergebnisse zu erzielen.

Weiterhin wird die stark wachsende Anwendung der Energievernetzung zu einer besseren Energieeffizienz beitragen. Gemeint ist die Kombination von Software Defined Networking mit Gleich- strom-Mikronetzen. Dies wird Unternehmen 2024 dabei helfen, den Energieverbrauch und die Emissionen genauer zu messen. Viele Funktionen in der IT und in intelligenten Gebäuden können mit IoT-Sensoren automatisiert und durch integrierte Energiemanagement-Fähigkeiten effizienter gestaltet werden.

5 Ethik und Frameworks spielen eine zunehmende Rolle für KI

Die Einführung von KI ist ein bis heute einmaliger technologischer Wandel, der gleichermaßen Innovationskraft und Vertrauen braucht. Allerdings: Laut Cisco AI Readiness Index fehlen bei 76 % aller Unternehmen weltweit umfassende Richtlinien, die die Nutzung von KI regeln. Angesichts der Risiken von GenAI herrscht weitgehend Konsens, dass solche Richtlinien und eine freiwillige Selbstkontrolle der KI-Branche generell nötig sind.

Ebenfalls muss sichergestellt sein, dass Verbraucher Zugang zu ihren Daten und Kontrolle über sie behalten – ganz im Sinne der aktuellen EU-Datenverordnung. Dabei sind die Unternehmen selbst gefordert: Mit der wachsenden Bedeutung von KI-Systemen werden öffentlich verfügbare Daten für das Training der KI-Modelle bald nicht mehr ausreichen. Hochwertige Sprachdaten werden voraussichtlich vor 2026 erschöpft sein, sodass bald ein Umstieg auf private oder synthetische Daten notwendig wird.

Das birgt allerdings das Risiko von unerlaubtem Zugriff und Datenschutz-Verletzungen. Die Verantwortlichen für den Einsatz für KI werden sich darum zu mehr Transparenz und Vertrauensarbeit in Bezug auf die Entwicklung, Nutzung und Ergebnisse von KI-Systemen verpflichten. Gerade Technologieunternehmen werden sich im kommenden Jahr darauf einstellen müssen, ein neues Maß an Offenheit zu zeigen – beispielsweise, welche Governance-Prozesse die interne Entwicklung, Anwendung und Nutzung von KI steuern. Sind sie in der Breite nicht in der Lage, einen vertrauenswürdigen Umgang mit KI glaubhaft nachzuweisen, wird auch der ordnungspolitsche Rahmen im kommenden Jahr enger gefasst werden.

Über die Studien
Der Cisco AI Readiness Index basiert auf einer Doppelblind-Umfrage unter 8.161 Geschäfts- und IT-Führungskräften aus dem privaten Sektor in 30 Ländern im Jahr 2023. Sie wurde von einem unabhängigen Dritten durchgeführt, der die Teilnehmenden aus Unternehmen mit 500 oder mehr MitarbeiterInnen befragte. Der Index bewertet die KI-Bereitschaft der Unternehmen in sechs zentralen Bereichen: Strategie, Infrastruktur, Datenhaltung, Governance, Fachpersonal und Unternehmenskultur. Für Deutschland wurden 300 ExpertInnen befragt. Der Cisco Cybersecurity Readiness Index 2023 basiert ebenfalls auf einer Doppelblind-Umfrage unter 6.700 Führungskräften in 27 Ländern, die in ihren Unternehmen für Cybersicherheit zuständig sind. Die Untersuchung wurde Ende 2022 mittels Online- und Telefoninterviews durchgeführt. Für Deutschland wurden 300 ExpertInnen befragt.

Die 7 wichtigsten IT-Technologien und -Themen

NTT blickt ins neue Jahr

Von Networking über Edge Computing und Private 5G bis hin zu Rechenzentren und Cloud – die großen Themen, mit denen sich Unternehmen im Jahr 2024 auseinandersetzen müssen, sind dieselben wie im Jahr 2023. Auch die als Wunderwaffe gehandelte generative KI wird in den kommenden Monaten ganz oben auf der Agenda stehen. Doch welche konkreten Lösungen, Ansätze und Services werden wir sehen? NTT Ltd., ein führendes IT-Infrastruktur- und Dienstleistungsunternehmen, verrät, was Unternehmen im neuen Jahr erwartet.

Aus Sicht von NTT spielen 2024 folgende Themen eine wichtige Rolle für den IT-Betrieb:

1. Der Begriff „Dark NOC" geht in das Lexikon der Netzwerkwelt ein.

In der Geschwindigkeit, in der sich AIOps weiterentwickelt hat, ist ein Network Operations Center (NOC) zur idealen Lösung für die Netzwerküberwachung und -kontrolle geworden. „Dark" bedeutet in diesem Zusammenhang, dass alle bestehenden operativen Geschäftsprozesse mithilfe fortschrittlicher KI-Algorithmen vollständig automatisiert werden können. Um die Netzqualität weiter zu verbessern, die Techniker zu unterstützen und die Infrastrukturen zu modernisieren, werden in den nächsten zwölf Monaten immer mehr Unternehmen AIOps-Methoden in den allgemeinen IT-Betrieb einbinden. Obwohl die Automatisierung das Herzstück eines „Dark NOC" ist, ist menschliche Expertise jedoch der Schlüssel zum Erfolg. Firmen müssen also nicht nur die notwendigen technologischen Vorbereitungen treffen – von der Standardisierung der APIs bis zur Optimierung von Datenprozessen –, sondern auch in die Weiterbildung ihrer Mitarbeitenden investieren.

2. Künstliche Intelligenz erfordert Investitionen in die disruptive Energieversorgung von Rechenzentren.

Klassische Racks verbrauchen etwa sechs bis acht Kilowattstunden (kWh) Strom. Mit dem Voranschreiten von KI erhöht sich die Leistungsdichte eines einzelnen Rack-Schranks und damit der Stromverbrauch deutlich – schon heute sind 50 bis 100 kWh üblich. Schätzungen zufolge wird sich der durchschnittliche Stromverbrauch in den kommenden Jahren verdoppeln oder sogar verdreifachen. Racks, die mehr Wärme erzeugen und folglich mehr Kühlung benötigen, machen den Netto-Null-Zielen der Unternehmen aber einen Strich durch die Rechnung. Unternehmen werden deshalb nach nachhaltigeren Optionen suchen müssen – nicht nur aus Kostengründen, sondern auch weil immer strengere Vorschriften greifen. NTT beispielsweise nutzt bereits Techniken wie die Flüssigkeitstauchkühlung (Liquid Immersion Cooling), unterstützt Fernwärmeprojekte und erforscht Solarpaneele im Weltraum.

3. Nachhaltigkeit ist integraler Bestandteil aller Lösungen.

Das Thema Sustainability wird angesichts verschärfter Auflagen einen großen Einfluss darauf haben, in welche Technologien und in welche Bereiche Unternehmen künftig investieren. Bereits zum 1. Januar 2024 müssen beispielsweise 50 Prozent des verbrauchten Stroms in deutschen Rechenzentren aus erneuerbaren Energiequellen stammen, der Strom darf jedoch nicht schon nach dem Erneuerbare-Energien-Gesetz (EEG) gefördert sein. 2027 steigt der Anteil dann auf 100 Prozent. Auf ihrem Weg zu einem Netto-Null-Betrieb setzen aber auch immer mehr Unternehmen Technologien wie Private 5G ein. LyondellBasell und Schneider Electric etwa nutzen 5G-Campusnetze, um Smart-Factory-Anwendungen rund um ihre ESG-Initiativen voranzutreiben. Das reicht von der Verringerung des Kohlenstoffausstoßes bis hin zur Kreislaufwirtschaft für Hardware.

4. Optische Netzwerke werden zum Mainstream.

Angesichts hoher Anforderungen in Bezug auf Effizienz, Zuverlässigkeit, Nachhaltigkeit und Zukunftsfähigkeit wird die optische Vernetzung 2024 stärker in den Mittelpunkt rücken. Aktuelle Tests, bei denen Übertragungsraten von 1,2 Tbit/s erreicht wurden, belegen das Potenzial. Gleichzeitig wollen über alle Branchen hinweg mehr als 90 % der Führungskräfte ihre Netzwerke modernisieren und so sicherstellen, dass sie für aktuelle wie auch künftige Herausforderungen gerüstet sind. Daneben gibt es umfassende Anstrengungen, die Grenzen bestehender Infrastrukturen mit Hilfe von optischen Technologien zu überwinden. So haben sich über 100 Organisationen zusammengeschlossen, um IOWN (Innovative Optical and Wireless Network) voranzutreiben.

5. IoT-Ökosysteme treiben die Einführung von P5G und Edge voran.

Die Kombination von IoT, Private 5G und Edge Computing ermöglicht es Unternehmen, Echtzeit-Einblicke zu gewinnen und darauf aufbauend fundiertere Entscheidungen zu treffen. Müssen riesige Datenmengen direkt am Netzwerkrand verarbeitet und mittels KI/ML analysiert werden, sind intelligente Edge-Funktionen und -Technologien unabdingbar. Dazu zählt die zunehmende Automatisierung aufgrund des Fachkräftemangels, aber auch Computer Vision oder Digitale Zwillinge. Ohne Hilfe von außen werden die wenigsten Firmen solche Anwendungsfälle realisieren können. Acht von zehn Unternehmen gehen deshalb

davon aus, dass ihre Abhängigkeit von Edge-Services durch Drittanbieter in den nächsten zwei Jahren zunehmen wird. Das Partner-Ökosystem von NTT bündelt die vorhandene Expertise rund um 5G-fähige Geräte, die Anwendungsfälle wie Push-to-Talk Devices, Augmented-Reality-Headsets, Computer-Vision-Kameras und Sensoren in der Fertigungs-, Automobil-, Logistik- und weiteren Branchen unterstützen.

6. Menschliche Fähigkeiten sind für KI unerlässlich.

Die Mehrheit der CX (Customer Experience)-Interaktionen ist nach wie vor auf menschliche Unterstützung angewiesen – sie ist und bleibt laut dem 2023 Global CX Report von NTT aus Sicht der Führungskräfte ein wichtiger Teil der Customer Journey. Daran ändert auch die Tatsache nichts, dass vier von fünf Unternehmen in den nächsten zwölf Monaten KI in die CX-Bereitstellung integrieren wollen. Ein grundlegendes Verständnis für KI und Big-Data-Analytik wird für die meisten Arbeitsplätze unabhängig von der Branche zur Grundvoraussetzung. Die Neueinstellung entsprechender Experten ist eine Möglichkeit, wird sich aber angesichts des Fachkräftemangels schwierig gestalten. Eine Studie von NTT DATA hat ergeben, dass Unternehmensleiter in den letzten drei Jahren durch Investitionen in Umschulungs- und Weiterbildungsinitiativen eine Rentabilität von mehr als 25 Prozent erzielt haben.
Dieser Trend wird sich 2024 fortsetzen – ohne Qualifikationslücken zu schließen, werden Unternehmen das Potenzial neuer Technologie nicht ausschöpfen können.

7. „Unsichtbare" Wolken werden vertikal.

Wenn sie gut funktionieren, werden Cloud-Umgebungen unsichtbar, sodass die Anwendungen im Vordergrund stehen. Was bei Office-Applikationen, Projektmanagement-Tools oder CRM-Lösungen bereits weitgehend funktioniert, ist in anderen Bereichen oftmals noch nicht ausgereift.

2024 werden zunehmend branchenspezifische Clouds, die Software, PaaS- und IaaS-Ebenen vereinen, auf den Markt kommen, um dedizierte Anwendungsfälle bereitzustellen. Diese konzentrieren sich nicht auf die Technologie an sich, sondern auf das Geschäftsergebnis.

„2023 hat Unternehmen quer durch alle Branchen vor viele Herausforderungen gestellt. Auch 2024 wird die eine oder andere Überraschung bereithalten. Generative KI, die sich in diesem Jahr zum absoluten Hype-Thema entwickelt hat, verspricht für die unterschiedlichsten Einsatzszenarien Abhilfe, indem Prozesse effizienter gestaltet und gleichzeitig der Zeit- und Ressourcenaufwand für die Tätigkeiten spürbar reduziert wird", erklärt Kai Grunwitz, CEO Germany und Regional Leader DACH bei der NTT Ltd.

„Fakt ist: Künstliche Intelligenz wird in den nächsten Jahren in immer mehr Bereiche vordringen. Gleichzeitig werden von Networking über Edge Computing und Private 5G bis hin zu Rechenzentren und Cloud neue Technologien und Lösungen auf den Markt kommen, die Unternehmen bei der Erreichung ihrer Geschäftsziele maßgeblich unterstützen."

Kai Grunwitz, CEO Germany und Regional Leader DACH NTT Ltd. (Quelle: NTT Ltd.)

Handel an Flughäfen

EHI-Studie „Travel Retail 2023": Passagierfrequenz und Mieterstruktur an Flughäfen

Bahnhöfe und Flughäfen sind attraktive Standorte für Einzelhandel, Gastronomie und Dienstleistungen und haben sich im Laufe der Zeit zu interessanten Einkaufsstätten entwickelt. Die EHI-Studie „Travel Retail 2023" untersucht 25 ausgewählte Bahnhöfe (in Kooperation mit MyTraffic) und die 15 größten Flughäfen in Deutschland hinsichtlich ihrer Mieterstruktur und Frequentierung im Jahr 2022 und ersten Halbjahr 2023.

Dabei haben die Flughäfen mit den meisten Passagieren – Frankfurt/Main, München, Berlin und Düsseldorf – auch die größte Anzahl an Einzelhandelsmietern, zeigt die Studie. „An Flughäfen ist der Branchenmix im öffentlichen Bereich von Dienstleistungsanbietern geprägt – Autovermietungen und Reisebüros sind hier weit verbreitet. Nach der Sicherheitskontrolle dominieren Einzelhandel und Gastronomie", erklärt Studienautor Björn Stelzenmüller.

Einzelhandel dominiert im Sicherheitsbereich

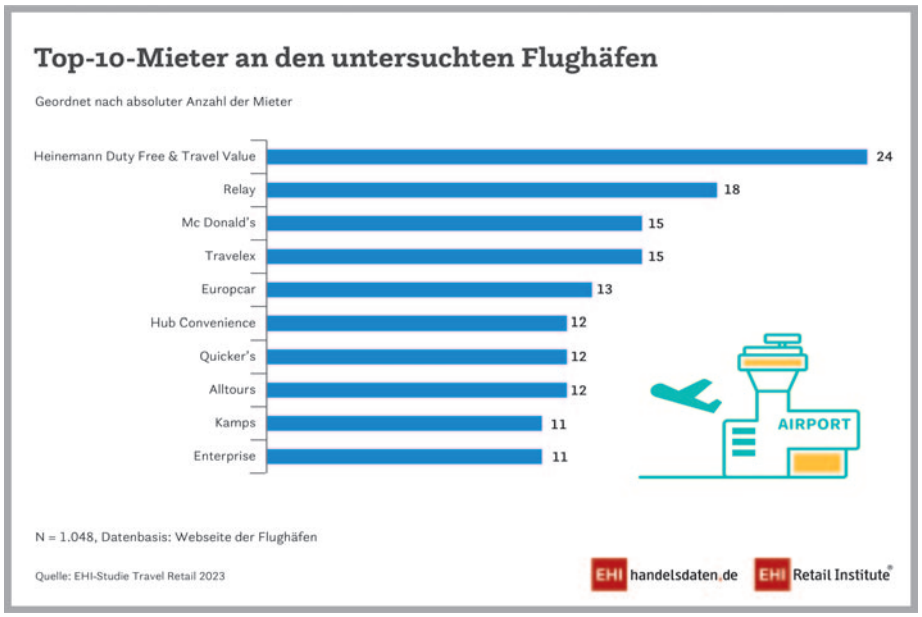
Betrachtet man den gesamten Branchenmix an Flughäfen nach der EHI-Branchensystematik*, so hat der Einzelhandel mit 37 Prozent den größten Anteil, gefolgt von Dienstleistungen mit 35 Prozent und der Gastronomie mit 28 Prozent. Im öffentlichen Bereich der Flughäfen dominiert der Dienstleistungssektor mit 53 Prozent, im Sicherheitsbereich ist der Einzelhandel mit 55 Prozent führend. Hier sind vor allem Mieter aus den Bereichen Accessoires, Entertainment und Bekleidung sowie Duty-Free angesiedelt.

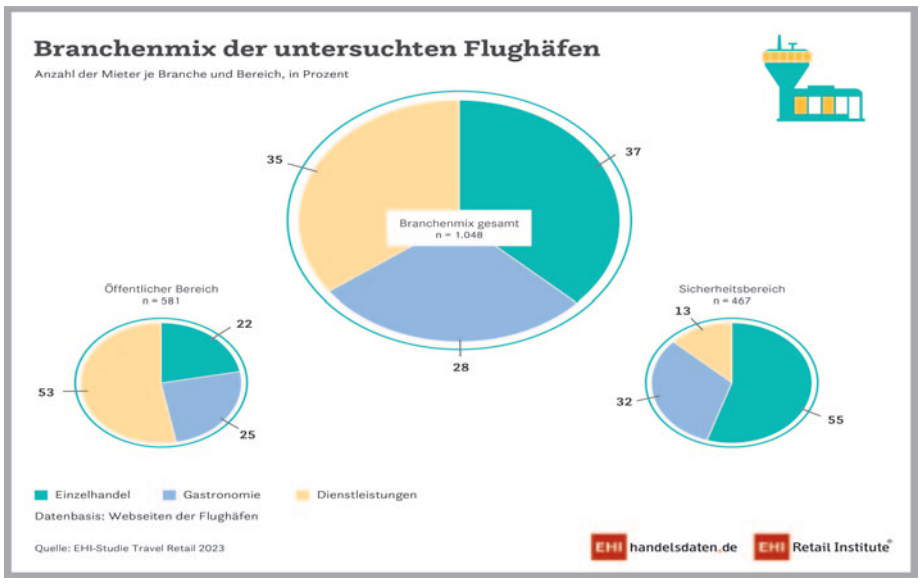
Top-Mieter an Flughäfen

Der Frankfurter Flughafen ist mit 48,9 Mio. Passagieren im Jahr 2022 der frequenzstärkste deutsche Flughafen, gefolgt von München (31,6 Mio.), Berlin (19,8 Mio.) und Düsseldorf (16,1 Mio.). Auch bei den Mietern aus dem Einzelhandel führt Frankfurt (133) das Ranking an – vor München (92), Berlin (45) und Düsseldorf (33). Die Hälfte der Top-10-Mieter an den untersuchten Flughäfen sind mit Heinemann (24 Shops), Relay (18), Hub Convenience, Quicker's (je 12) und Kamps (11) Einzelhandelsunternehmen.

Die Studie ist zum Download verfügbar und für EHI-Mitglieder kostenlos.

Methodik: Für die Studie wurden die 15 größten Flughäfen in Deutschland hinsichtlich ihrer Frequentierung und Mieterstruktur untersucht. Die jährlichen Passagierzahlen dieser Flughäfen hat der Flughafenverband ADV ermittelt. *EHI-Branchensystematik: Kategorisierung nach Einzelhandel, Gastronomie und Dienstleistung (außer von Bahnhöfen und Flughäfen selbst betriebene Flächen, Geldautomaten, Hotels und Toiletten)





Vertrauen in der digitalen Welt:
Was wird 2024 wichtig?

Vertrauen im Internet ist ein wichtiger Faktor bei der Bekämpfung von Cyber-Bedrohungen. Im kommenden Jahr werden einige neue Regularien umgesetzt, Entwicklungen vorangetrieben und neue Technologien weiterentwickelt. Ingolf Rauh, Head of Product und Innovation Management bei Swisscom Trust Services, hat vier Trends für 2024 identifiziert.

Neue Regularien DORA und NIS2

NIS2 (Network and Information Security 2) zielt darauf ab, die Cybersicherheitsanforderungen für wichtige Infrastrukturen zu harmonisieren, während DORA (Digital Operational Resilience Act) die betriebliche Widerstandsfähigkeit im Finanzsektor betont. Beide Vorschriften nehmen besonders Lieferketten in die Pflicht und legen Verpflichtungen für Softwareanbieter fest. NIS2 ist eine Richtlinie, die bis Oktober 2024 in nationales Recht umzusetzen ist. Jedes Land der EU kann diese Umsetzung allerdings anders realisieren, was multinationalen Unternehmen wie Banken häufig Probleme bereitet.

DORA hingegen ist eine Verordnung der EU und tritt voraussichtlich 2025 unmittelbar in den Mitgliedsstaaten in Kraft. DORA konzentriert sich auf die Betriebsstabilität im Finanzsektor, sodass diese einem Cyberangriff standhalten kann und Finanzdienstleistungen weiter verfügbar bleiben.

Unternehmen sollten sich frühzeitig mit den neuen Regularien vertraut machen, da insbesondere die Compliance ansonsten Probleme bereiten könnte. Für NIS2 entfällt die Prüfkompetenz in Deutschland auf das BSI bzw. die BaFin. Artikel 46 von DORA enthält eine ganze Reihe von Behörden, die

darüber hinaus die Einhaltung der Regularien garantieren sollen – bestenfalls die EZB, beziehungsweise auch die BaFin.

eIDAS 2.0 und EU-Wallets

Im Februar 2024 wird das EU-Parlament über eine Verordnung zur Einführung von digitalen Wallets abstimmen. Passiert der Gesetzesvorschlag das Parlament und den europäischen Rat, könnte die Verordnung bereits im Frühjahr 2024 in Kraft treten. Der Vorschlag besagt unter anderem, dass alle 27 Mitgliedsstaaten ihren Bürgern bis 2026 eine digitale Brieftasche anbieten müssen, mit der diese sich elektronisch ausweisen können. Bis zum Jahr 2030 sollen 80 Prozent der EU-Bevölkerung über eine solche Wallet verfügen, so der Wille der EU-Kommission. Kritik gibt es allerdings von Datenschützern und Sicherheitsexperten, die unter anderem die anonyme Nutzung digitaler Dienste gefährdet sehen.

Vollständige Digitalisierung von Arbeitsverträgen

Im deutschen Nachweisgesetz soll eine Regelung geschaffen werden, wonach wie bereits bisher bei schriftlichen Arbeitsverträgen die Verpflichtung des Arbeitgebers, einen Nachweis der wesentlichen Vertragsbedingungen zu erteilen, entfallen kann, wenn der Arbeitsvertrag beispielsweise in einer gültigen elektronischen Form geschlossen wurde. Die Pflicht zur schriftlichen Niederlegung wurde im letzten Gesetzesentwurf hierzu immer wieder kritisiert und verhinderte eine vollständige Digitalisierung von HR-Prozessen.

Hier bietet sich die Nutzung elektronischer Dokumente an, die mit einer qualifizierten elektronischen Signatur nach § 126a BGB versehen sind und damit einen adäquaten Ersatz für die Schriftform bieten können. Nicht nur aufgrund dieser legislativen Initiative, sondern auch aus ganz praktischen Gründen im digitalen Raum wird die qualifizierte elektronische Signatur immer mehr zum Standard werden und die händische Unterschrift auf Papier sukzessive ablösen.

Post-Quantenkryptografie

Quantencomputer machen in der letzten Zeit immer wieder Schlagzeilen und die Technologie nähert sich immer mehr dem praktischen Einsatz. Wann die überlegene Rechenleistung allgemein zur Verfügung stehen wird, ist aktuell schwer abzuschätzen, doch es scheint nur noch eine Frage der Zeit zu sein. Dann wird die Technologie zwangsläufig auch in falsche Hände gelangen und Kriminelle können sie nutzen, um Verschlüsselungen zu knacken, die bisher als sicher galten. Die Quantenrechner erlauben die Verwendung neuartiger Algorithmen, die die Rechenzeit für die Lösung komplexer mathematischer Probleme, wie sie in der Kryptografie verwendet werden, erheblich verkürzt.

Das bedeutet, es braucht auch für die Verschlüsselung neue Algorithmen, die so komplex sind, dass sie auch Angriffen mit Quantenrechnern standhalten können. IT-Sicherheitsanbieter und Vertrauensdienste müssen ihre Hard- und Software daher bereits heute so designen, dass sie zukünftig neue, quantensichere Algorithmen integrieren können.

In der DACH-Region zeichnen sich für 2024 verschiedene Trends im Bereich Cybersecurity ab, die Unternehmen im Auge behalten sollten. Die voranschreitende Digitalisierung eröffnet nicht nur neue Horizonte und gestaltet Prozesse und Abläufe in Unternehmen oder auch in Behörden um. Sie rückt auch die Sicherheit digitaler Systeme als entscheidenden Faktor für den Erfolg von Organisationen zunehmend in den Fokus.

Folgende fünf Trends bestimmen unserer Meinung nach die nähere Zukunft des sicheren Teilens und Übertragens von Daten:

1. Wachsende Cyberbedrohungen

In der angespannten gesamtpolitischen Lage verlagern sich Konflikte zunehmend in den digitalen Raum. Die Zahl der sichtbaren und spürbaren Cyberangriffe auf Unternehmen und Behörden steigt. Insbesondere Sektoren wie die öffentliche Verwaltung und das Gesundheitswesen hinken beim Thema sichere Digitalisierung aber noch hinterher. Nachholbedarf besteht vor allem bei Themen wie Effizienz und Cybersicherheit. Laut Bericht zur Lage der IT-Sicherheit des BSI 2023 (1) werden kommunale Betriebe immer häufiger Opfer eines Ransomware-Angriffs. Auch aktuelle Beispiele wie die Angriffe auf Kommunen in Südwestfalen und Oberbayern zeigen, dass die Bedrohungslage für Behörden immer akuter wird. Einige Betriebe waren mehrere Monate offline. Hinzukommt, dass im neuen Jahr wichtige politische Ereignisse wie die Präsidentschaftswahl in den USA anstehen, die globale Auswirkungen haben und hohe Anforderungen an die IT-Sicherheit stellen. Falschinformationen und Fake News, die mithilfe von Künstlicher Intelligenz erstellt werden, sind nur eine mögliche Herausforderung. Das wird langfristig zu einer erhöhten Sensibilität und einem verstärkten Fokus auf die Sicherheit digitaler Systeme führen.

2. Regulierungen und digitale Souveränität

Neue Regulierungen und gesetzliche Vorgaben werden Themen wie Cybersicherheit

Sicherheit im Wandel

Die Top-Cybersecurity-Trends für 2024

und Souveränität auf die digitale Agenda stellen. Cloud-Umgebungen, deren Besitzer souverän mit ihren Daten umgehen und damit auch die Compliance mit einer DSGVO sicherstellen können, sowie die Unabhängigkeit von nicht-europäischen Akteuren werden dabei im Mittelpunkt der Bemühungen stehen. Jüngste Beispiele wie die Übernahme der deutschen Software-Anbieter Dracoon und ownCloud durch Kiteworks verdeutlichen die Notwendigkeit einheitlicher Regulierungskriterien. Diese sollten das Ziel haben, die Souveränität von Unternehmen und Behörden über ihre Informationen zu gewährleisten und auch inländische Angebote zum sicheren Datenaustausch und Datenübertragung zu fördern. In diesem Zusammenhang wird im nächsten Jahr auch die Umsetzung der NIS2-Richtlinie (Network and Information Systems Directive 2) der Europäischen Union eine zentrale Rolle spielen. NIS2 stellt einen langfristigen strategischen Ansatz dar, um die digitale Autonomie europäischer Unternehmen zu stärken, anhaltende Unsicherheiten zu vermeiden und einen nachhaltigen Weg zur digitalen Souveränität Europas zu ebnen.

3. Technologien zur Cyberabwehr

Künstliche Intelligenz wird bei Cyberbedrohungen eine immer größere Rolle spielen und die Entwicklung proaktiver Abwehrmaßnahmen entscheidend prägen. In Zeiten, in denen sich die Bedrohungslandschaft rasant weiterentwickelt und verändert, kommt schnellen und effektiven Abwehrmaßnahmen eine immer stärkere Bedeutung zu.

Auch das Thema Quantencomputing wird im Blickfeld der Cybersicherheitsforschung bleiben. Mittels Krypto-Agilität, also der Fähigkeit, alternative Verschlüsselungstechnologien in einem System zu implementieren, werden Systeme in der Lage sein, schnell und flexibel auf sich verändernde Bedrohungen zu reagieren. Der Einsatz verschiedener Algorithmen und Verschlüsselungsverfahren erleichtert es, den sich ständig ändernde Angriffsmethoden standzuhalten und neuen Bedrohungen gezielter und quasi ohne Downtime entgegenzuwirken. Damit hat Krypto-Agilität das Potenzial, zu einer festen Disziplin in der Cyberabwehr zu werden.

4. Dezentralisierung und Resilienz

In der sich ständig weiterentwickelnden Welt der Cybersicherheit wird sich die Cloud von einer einfachen Speicherlösung immer mehr zu einem Grundpfeiler für eine sichere, dezentrale und skalierbare Infrastruktur entwickeln. Durch vermehrten On-Demand-Betrieb ist es möglich, Kernservices zunehmend zu dezentralisieren und die Resilienz gegenüber Angriffen von außen zu stärken. Unternehmen können auf diese Weise Ausfälle durch Cyberangriffe minimieren.

Das Risiko, Opfer eines Cyberangriffs zu werden, wird in den nächsten Jahren weiter zunehmen. Unternehmen sollten sich daher rechtzeitig auf den Notfall vorbereiten und robuste Infrastrukturen entwickeln, die im Falle eines Angriffs nicht vollständig ausfallen. Es empfiehlt sich daher, nicht zusammenhängende Abläufe durch die logische und physische Trennung von Infrastrukturen klar voneinander abzugrenzen. Auf diese Weise werden die Auswirkungen von Sicherheitsereignissen und die Gesamtintegrität der Systeme sichergestellt.

5. Herausforderungen im Umgang mit Fachkräften

Im Zuge des anhaltenden War-for-Talents werden intuitive und innovative Technologienlandschaften eine immer größere Rolle spielen. Intelligente Tools ermöglichen es Unternehmen, vorhandene personelle Ressourcen optimal zu nutzen und beispielsweise durch das Automatisieren wiederkehrender Prozesse die Effizienz zu steigern und dem Fachkräftemangel zu begegnen.

Umfassenden Plattformen wird dabei eine zentrale Rolle zukommen. Anstatt wie bisher nach dem „Best-of-Breed"-Ansatz vorzugehen und einzelne Lösungen für Problemstellungen und Anforderungen herstellerunabhängig zu beschaffen, lassen sich über ganzheitliche Plattformen mehrere Prozesse sicher abbilden. Durch das Bündeln vom sicheren Datentransfer, virtuellen Datenräumen und Lösungen zur Prozessautomatisierung ist die Vertrauenswürdigkeit und Integrität der erhobenen, übermittelten und weiterverarbeiteten Daten jederzeit gegeben.

2024 wird für die Cybersecurity-Landschaft ein facettenreiches Jahr. Ob es um regulatorische Änderungen wie NIS2 geht, dem Integrieren neuer Technologien oder dem Optimieren von Personalstrategien, um die kommenden Herausforderungen bewältigen zu können, müssen Unternehmen agil und widerstandsfähig bleiben. Nur so werden sie es schaffen, im sich entwickelnden digitalen Zeitalter auf Dauer erfolgreich zu sein.

Autor: Ari Albertini, CEO FTAPI Software GmbH

Quellen: (1) Bundesamt für Sicherheit in der Informationstechnik „Die Lage der IT-Sicherheit in Deutschland 2023"

Wann und Wie

Trends 2024: Keine Frage mehr des „Ob“, sondern des „Wann“ und „Wie“

Andreas Junck, Senior Sales Director DACH bei Gigamon, stellt die vier größten Herausforderungen vor, die 2024 auf IT-Sicherheitsteams zukommen werden, und verrät, welche Rolle Visibility dabei spielt.

So sehr wir es uns auch wünschen: Die Anzahl von Cyber-Angriffen wird so bald nicht abflachen – im Gegenteil. Vielmehr müssen sich Unternehmen darauf vorbereiten, dass es auch sie bald treffen wird. Es ist nur eine Frage der Zeit, wann Akteure zuschlagen, und dann muss schnell gehandelt werden. Allerdings trüben sogenannte Blind Spots innerhalb der IT-Infrastruktur die Reaktionsfähigkeit. Im nächsten Jahr wird es also das übergeordnete Ziel sein, besonders die folgenden Blind Spots sichtbar zu machen und somit die IT-Sicherheit im Unternehmen zu stärken.

Verschlüsselter und lateraler Datenverkehr: Die toten Winkel im Netzwerk

Firewalls, Endpoint Detection and Response oder Security Information and Event Management: Auf dem Markt gibt es zahlreiche Sicherheitslösungen, die umfangreichen Schutz vor Cyber-Bedrohungen versprechen. Cyber-Akteure arbeiten jedoch unaufhaltsam an neuen Methoden und Tools, mit denen sie die herkömmlichen Sicherheitsperimeter clever umgehen. So versteckt sich laut einer Untersuchung von Watchguard Threat Lab 93 Prozent der Malware hinter einer SSL- oder TLS-Verschlüsselung. Betroffene Unternehmen bemerken ihr Vorhandensein erst, wenn es bereits zu spät und der Schaden angerichtet ist. Man sollte meinen, dass dieser beliebte Angriffsvektor zu höherer Vorsicht ermahnt. Die Realität sieht allerdings anders aus. Laut einer aktuellen Hybrid-Cloud-Studie von Gigamon lassen 79 Prozent der befragten Unternehmen verschlüsselten Datenverkehr ungeprüft durch ihr Netzwerk wandern. Der laterale Datenstrom (East-West Traffic) ist dabei besonders gefährdet; 47 Prozent der Unternehmen mangelt es hier an Einblick.

Was lange Zeit als Heiliger Gral der Datensicherheit galt, wird nun also konsequent von Cyber-Kriminellen ausgenutzt, um sich ungesehen Zugang zu sensiblen Daten zu verschaffen. Folglich müssen Unternehmen im kommenden Jahr einen Weg finden, ihren gesamten Traffic transparenter zu machen.

Komplexität entwirren – trotz kleinem Budget

Seit Jahren müssen Unternehmen mit einer wachsenden IT-Landschaft zurechtkommen. Doch mit jeder weiteren Technologie und unternehmenskulturellen Veränderung nimmt die damit verbundene Komplexität neue Dimensionen an. So tragen der Wechsel zu Hybrid- und Multi-Cloud-Umgebungen, Remote Work, Schatten-IT sowie stark vernetzte IoT- und OT-Systeme massiv dazu bei, dass Unternehmen den Überblick darüber verlieren, was sich genau in ihrer Infrastruktur abspielt.

Auch Legacy-IT, die sich nur schwer updaten und schützen lässt, hat einen Einfluss auf die Komplexität. Dabei ist besonders im Produktionsumfeld künftig mit mehr Cyber-Angriffen auf Herstellungsprozesse und Lieferketten zu rechnen.

Gleichzeitig sind Unternehmen gezwungen, zahlreiche Regulierungen und Datenschutzgesetze einzuhalten. Dafür müssen ihre Strukturen und Systeme allerdings tief blikken lassen – und das trotz limitiertem Sicherheitsbudget. Wenn das nötige Investment für mehr Sichtbarkeit nicht gemacht wird, bleibt die Sicherheitslage riskant.

Künstliche Intelligenz, das zweischneidige Schwert

Der Hype um (Generative) KI-Anwendungen flacht allmählich ab. Auch wenn sie in vielen Bereichen noch in den Kinderschu-

hen stecken, werden sich Einsatz und Fähigkeit im kommenden Jahr auf eine Bandbreite an Use Cases ausweiten. Es ist davon auszugehen, dass Unternehmen die Stärken von KI und Automatisierung zunehmend und gezielter in die eigene IT-Sicherheit einbinden werden.

Als verlängerter Arm von Cyber-Sicherheitsteams könnten KI-Systeme künftig nicht nur das Internet durchforsten, um auffällige Angriffsmuster und neue Bedrohungen zu finden, sondern auch die eigene IT-Landschaft – und zwar ganzheitlich. Alles, was sie dafür brauchen: Daten aus wirklich allen Ecken der Infrastruktur. Angesichts dessen werden Security Data Lakes, mithilfe derer sich KI-Anwendungen mit qualitativ hochwertigen Daten speisen lassen, in Zukunft wesentlich an Bedeutung gewinnen. Allerdings wird es zunehmend zur Herausforderung, die notwendigen Daten selbst in den versteckten Bereichen und komplexen Umgebungen ausfindig zu machen und heranzutragen.

Doch KI kann auch zum Risiko werden. So trägt sie zum einen zur Komplexität von IT-Landschaften bei. Zum anderen werden Cyber-Kriminelle sie zu ihren Gunsten nutzen – von wesentlich authentischer wirkenden Phishing-Mails bis hin zu ausgeklügelter Malware.

In Sachen Zero Trust ist noch Luft nach oben

Als Antwort auf die wachsende, immer dynamischere Bedrohungslandschaft werden immer mehr Unternehmen auf einen Zero-Trust-Ansatz setzen. Die Idee des Konzepts hat sich unlängst herumgesprochen: Alle Anwender und Geräte, die sich mit dem Unternehmensnetzwerk verbinden, sind potenzielle Einfallstore und daher nicht unbedingt vertrauenswürdig. Deshalb erhalten die Mitarbeitenden lediglich Zugang zu jenen Ressourcen, die sie für ihre Arbeit brauchen, und müssen ihre Identität zusätzlich verifizieren.

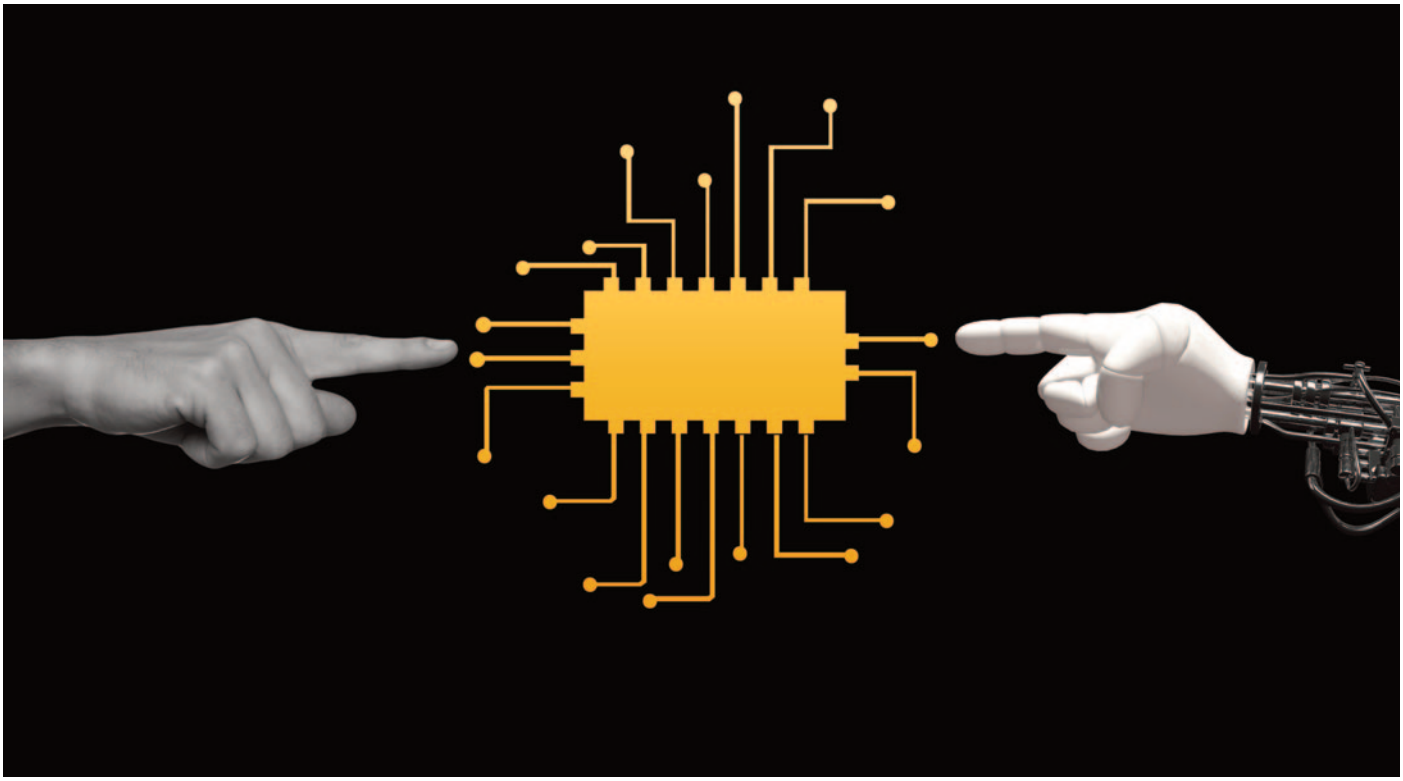
Vor allem in Deutschland sind viele Unternehmen erst am Anfang ihrer Zero-Trust-Reise. Dabei fällt auf, dass sie oftmals lediglich das Access-Management einrichten und denken, damit sei es getan. Vollständige Sichtbarkeit wird häufig vernachlässigt – und das, obwohl sie das grundlegende Fundament für Zero Trust bildet. Schließlich müssen Sicherheitsteams wissen, wo sich die (sensiblen) Daten im Netzwerk befinden und wer Zugriff darauf hat.

Cyber-Angriffe in verschlüsselten Daten, Komplexität, IT-Sicherheit mithilfe von KI sowie die erfolgreiche Etablierung von Zero Trust: All diese Herausforderungen haben eins gemeinsam. Sie lassen sich mithilfe eines hohen Grads an Sichtbarkeit meistern. Laut Gigamon haben aber nur 28 Prozent der deutschen Unternehmen einen holistischen Überblick über ihre IT-Landschaft. Herkömmliche Sicherheits- und Monitoring Tools können das Defizit nicht ausgleichen.

Für diesen Zweck gibt es Deep Observability: Entsprechende Lösungen analysieren sämtliche Daten, die in das Netzwerk kommen oder es verlassen. Auf diese Weise offenbaren sie Datenströme selbst in hochkomplexen IT-Umgebungen und machen verschlüsselten Datenverkehr einsehbar. Davon profitieren auch weitere Systeme wie Access-Management-Tools oder KI-Anwendungen. Vormals versteckte Daten werden transparent, wodurch sie zur Verbesserung der IT-Sicherheit beitragen.
können moderne Unternehmen vollständig in die Cloud migrieren. Gigamon unterstützt mehr als 4.000 Kunden weltweit, darunter über 80 % der Fortune 100 Unternehmen, neun der zehn größten Mobilfunkanbieter sowie hunderte von Regierungen und Bildungseinrichtungen weltweit. **[www.gigamon.com]**

KI wird der Co-Pilot im Lebens- und Arbeitsalltag

Dr. Jörg Herbers, Geschäftsführer der Inform GmbH, prognostiziert sieben wichtige KI-Trends für 2024



Künstliche Intelligenz (KI) ist längst mehr als ein Hype, sie etabliert sich zunehmend als integraler Bestandteil von immer mehr Lebens- und Geschäftsbereichen. Die Experten der Inform GmbH als weltweit führender Anbieter von fortschrittlichen KI-basierten Optimierungssoftwarelösungen prognostizieren sieben entscheidende KI-Trends, die 2024 und darüber hinaus eine Vielzahl von Branchen und gesellschaftlichen Praktiken beeinflussen werden: Dr. Jörg Herbers, CEO der Aachener Inform, stellt fest: „Während die KI-Technologie rasant voranschreitet, holt auch die menschliche Akzeptanz auf." Der Experte für KI, Operations Research und Cloud Transformation erwartet, dass „mit der zunehmenden Verbreitung und Reife von KI in den Bereichen Sprache, Bild- und Tonverarbeitung die Akzeptanz diese Technologien durch die Nutzer deutlich zunehmen wird".

Folgende sieben Trends werden künstliche Intelligenz 2024 und darüber hinaus bestimmen:

1. **Intuitive KI-Nutzung:**

   Das kommende Jahr läutet den Beginn eines Paradigmenwechsels in der Interaktion zwischen Mensch und KI ein, der von Visionären der Branche inspiriert ist. Mit der Unterstützung von Masayoshi Son, Softbank, will der ehe-

malige Apple-Designer Jony Ive ein „iPhone der künstlichen Intelligenz" entwickeln. Es soll eine natürlichere Anwendererfahrung schaffen und eine Abkehr von bildschirmzentrierten Schnittstellen signalisieren. Diese Entwicklung spiegelt den Trend zur nahtlosen Integration von KI in unsere täglichen Arbeitsmittel wider und verbessert die Art und Weise, wie Menschen arbeiten, kommunizieren und mit Technologie interagieren. Inform rechnet damit, dass künftig selbst komplexe Geschäftssoftware über Spracheingabe einfach zu bedienen sein muss, um den Kundenwünschen gerecht zu werden.

2. Generative KI-Integration:

KI wird immer mehr zu einem integralen Bestandteil von Softwareprodukten. Dies hat auch schon der Apple-CEO Tim Cook beobachtet, der begonnen hat, KI und maschinelles Lernen als „grundlegende Technologien" zu bezeichnen, die integraler Bestandteil eines jeden Produktes sein muss. Inform geht davon aus, dass die generative KI diesem Beispiel folgend als Co-Pilot in verschiedene Plattformen eingebettet werden wird. Sie wird die Nutzerinteraktionen mit diesen Plattformen und deren Funktionalitäten in verschiedenen Wirtschaftsbereichen verbessern.

3. Mensch-KI-Interaktion:

I Alterative KI-Interaktionen werden zur Norm werden. Die Nutzer werden sich an kontinuierliche Feedbackschleifen in verschiedenen Anwendungen gewöhnen. Das umfasst ein breites Spektrum von kreativen Aktivitäten mit Tools wie Midjourney bis hin zu technischen Lösungen, welche die großen Technologieunternehmen intern entwickeln. Entwicklungen wie die Integration von KI in Produkten wie Microsoft Office, das Apple iPhone oder in die Optimierungs- und Entscheidungsfindungssoftware von Inform deuten eine Zukunft an, in der KI im Zusammenspiel mit dem Menschen sowohl eine kollaborative als auch eine unterstützende Rolle spielen wird.

4. Ausweitung auf neue Bereiche:

Mit dem Erfolg von Modellen, die Texte und Bilder generieren, wird sich der Schwerpunkt nach und nach auf Modelle verlagern, die aus Videomaterial Texte erstellen. Das könnte eine Revolution sein, da sie das Lernen aus alltäglichen menschlichen Aktivitäten ermöglichen würde. Darüber hinaus werden KI-Systeme aus vielfältigeren und immer repräsentativeren Daten lernen. Pionierarbeit in anderen Bereichen, wie zum Beispiel die Proteinfaltung von AlphaFold, deutet auf das transformative Potenzial von KI-Anwendungen jenseits der derzeitigen Paradigmen hin. Im logisch nächsten Schritt werden sich Unternehmen mit KI-Systemen ausstatten, die ihnen helfen, ihre Geschäftsprozesse dynamisch anzupassen und zu optimieren.

5. Demokratisierung von Daten:

Die Veröffentlichung des Open-Source-Datensatzes SORDI (Synthetic Object Recognition Dataset for Industries) durch die BMW Group unterstreicht den Wandel hin zu offenen Datenökosystemen: Wenn Unternehmen gemeinsam hochwertige Prozessdaten nutzen, fördert dies ein kollaboratives Umfeld und forciert dadurch weitere KI-Innovationen. In deren Folge kann eine gerechtere Zukunft gestaltet werden, in der Daten den Fortschritt für alle vorantreiben.

6. Bedenken in Bezug auf die Cybersicherheit:

Allerdings haben die neu bereitgestellten KI-Tools unbeabsichtigt auch die Möglichkeiten für Cyberkriminelle massiv erhöht, wie der dramatische Anstieg von Phishing-Angriffen nach dem Start von ChatGPT zeigt. Um den ausgefeilten Bedrohungen durch böswillige KI-Nutzung zu begegnen, müssen alle Beteiligten dringend ebenso intelligente wie fortschrittliche Cybersicherheitsmaßnahmen etablieren.

7. Ethische KI:

Der jüngste Protest gegen die unautorisierte Verwendung von Scarlett Johanssons Konterfei für einen Avatar in einer Deepfake-Werbung ist nur ein Beispiel für die wachsenden ethischen Bedenken rund um den Einsatz von Künstlicher Intelligenz. Mit deren zunehmenden Fähigkeiten wächst auch ihr Missbrauchspotenzial. Das erfordert eine erhöhte Wachsamkeit und einen soliden ethischen Rahmen für ihre Anwendungen. Entwicklungen wie das KI-Gesetz der EU, die KI-Verordnung von US-Präsident Biden und der Hiroshima-Prozess der G7-Staaten weisen darauf hin, dass die Einführung weltweiter Regulierungsrahmen bevorsteht.

„Wir stehen an der Schwelle zu transformativen KI-Fortschritten und Inform bleibt vorne dabei, nicht nur bei der Vorhersage von Trends, sondern auch bei der aktiven Gestaltung der Zukunft von KI für die Optimierung von Geschäftsprozessen", so Herbers. Gleichzeitig positioniert sich das Softwareunternehmen klar für eine verantwortungsvolle und ethische KI-Entwicklung und hat deshalb im September 2023 seine Richtlinien zum verantwortungsvollen Umgang mit KI veröffentlicht. Darin geht es um einen „transparenten, verantwortungsvollen Umgang mit künstlicher Intelligenz, bei dem die Verantwortung immer beim Menschen verbleibt".

Dr. Jörg Herbers ist Geschäftsführer der Aachener Inform GmbH, ein weltweit führender Anbieter von fortschrittlichen KI-basierten Optimierungssoftwarelösungen.
©Inform GmbH

Vom Cyberrisiko zur Cyberresilienz

Bitdefender erinnert an zehn bewährte „Gebote" für die IT-Sicherheit in Unternehmen

Auch die komplexesten Attacken – neben den opportunistischen – starten oft mit ganz einfachen Werkzeugen. Viele Cybersicherheitsverantwortliche vergessen aber zu häufig, dass auch einfache, grundlegende Sicherheitsmaßnahmen die eigene Abwehr stärken können.

Grundsätzliche Verhaltensmaßregeln für einen sicheren Umgang mit IT verhindern nicht wenige Versuche, in Unternehmensnetze einzudringen. Die folgenden zehn Gebote zur IT-Sicherheit bieten einen durchaus weitreichenden Schutz für Systeme, Applikationen und Informationen. Viele davon sind bekannt und werden trotzdem immer wieder vernachlässigt.

Regel 1: Sich sicher im Internet bewegen

Von Trojanern mit E-Mail-Anhängen bis hin zu täuschend ähnlich nachgemachten Log-In-Seiten oder zum gezielten Sammeln von Informationen durch Social Engineering: Am Anfang auch komplexer und umfassender Infiltrationen in das Unternehmensnetz stehen Verstöße gegen einfachste Richtlinien der Internetsicherheit. Sich an diese zu halten, kann gar nicht oft genug betont werden.
IT-Sicherheitsverantwortliche müssen Ihre Mitarbeiter davor warnen:

- keine Links auf unbekannte Quellen anzuklicken;
- keine Software aus nicht vertrauenswürdigen Quellen herunterzuladen; sowie
- Richtlinien für den Umgang mit Unternehmensinformationen in soziale Medien herausgeben.

Regel 2: Mit Routine Phishing-Kampagnen abwehren

Neun von zehn Attacken beginnen mit einer oft gut als solche erkennbaren Phishing-Mail. Diese zu erkennen, sollten Mitarbeiter daher regelmäßig üben. Unternehmen sollten intern regelmäßig Phishing-Kampagnen simulieren, um beim Mitarbeiter das Bewusstsein für die Gefahr wachzuhalten und um Betroffene gleichzeitig auf neueste Gefahren hinzuweisen.

Regel 3: Software-Sparsamkeit

Zentral sind der Überblick und die Kontrolle über die tatsächlich im Unternehmen eingesetzte Software. Beides ist aber nicht immer gegeben. Je weniger Software im Einsatz, umso unwahrscheinlicher sind unnötige Komplikationen durch potenzielle Software-Schwachstellen. IT-Administrationen sollten zudem wissen, welche Software in welcher Version vorhanden ist, um Software-bedingte Schwachstellen schließen zu können. Auch wenn IT-Administratoren nicht die vollständige Kontrolle gerade über Schatten-IT-Tools aufrechterhalten können, empfiehlt es sich:

- eine zentrale Repository zu pflegen, die nur die für den täglichen Betrieb notwendige Software des Unternehmens in aktueller Version bereitstellt;
- nicht autorisierte Software nicht zu verbieten, aber zu überwachen und festzulegen, welcher Gebrauch akzeptiert ist; sowie
- Legacy-Software zu entfernen, ehe sie zum Sicherheitsrisiko werden kann.

Regle 4: Die Umgebung auf den neuesten Stand halten

Aktuelle Sicherheitspatches einzuspielen, ist eine der einfachsten und immer noch

am häufigsten vergessenen Abwehrmöglichkeiten. Zentral ist es daher:
- auch die Benutzer regelmäßig auf Software-Updates hinzuweisen;
- das Patch-Management über Active Directory und PowerShell-Skripte zu automatisieren; sowie
- Tools wie Microsoft Intune zu nutzen, um die nötigen Update-Prozesse sicherzustellen.

Regel 5: Privilegien-Sparsamkeit

Nicht jeder Nutzer muss über sämtliche Funktionalitäten und Rechte einer Anwendung verfügen. Ein Mitarbeiter im Vertrieb benötigt in der Kommunikation in der Regel nur einige unumgängliche Funktionalitäten etwa für die E-Mail-Korrespondenz mit Dateianhängen. Er benötigt aber keine Rechte zu Power-Shell-Skripten, durch die Hacker mit Makros infizierte Office-Dokumente in Anhängen implementieren und ausführen können. Es gilt daher nicht nur hier:

- so wenig Rechte wie möglich zu vergeben;
- Gruppenrichtlinien festzulegen oder uneingeschränkte Benutzer-Rechte einzuschränken oder zu löschen;
- lokale Benutzer möglichst ohne Administratorrechte anzulegen; sowie
- sofern möglich Nutzerrollen in der Organisation zu trennen, um den Zugriff auf Tools und Informationen einzuschränken.

Regel 6: Nicht nur auf externe Experten bauen und auf Basis-Technologien der IT-Abwehr verzichten

Kein IT-Unternehmen kommt ohne externe Hilfe aus. Doch auch diese Sicherheitsexperten benötigen lokale Unterstützer-Technologien. Ein externes Security Operation Center (SOC)etwa im Rahmen eines Managed-Detection-and-Response-Dienstes erkennt Seitwärtsbewegungen und komplexe Attacken, wenn deren Urheber bereits im Netz Fuß gefasst haben und versuchen, sich weiter im Opfernetz auszubreiten. Eine MDR ersetzt aber nicht den Schutz durch diese IT-Abwehrtechnologien.
Sicherheit auszulagern, ist eine Illusion. IT-Sicherheitsverantwortliche solltenvnicht auf Folgendes verzichten:

- eine flächendeckende Endpoint Detection and Response;
- eine Perimeter-Firewall für öffentlich verfügbare Server-Endpunkte oder eine Web-Application-Firewall für externe Anwendungen sowie für Anmelde- oder Administrator-Portale;
- einen Next-Generation-Malware-Schutz auch gegen Phishing; sowie
- eine zwingend vorgeschriebene VPN-Verbindung für alle Remote-Arbeitsvorgänge anstelle ungesicherter Fernzugriffsprotokolle wie Secure Shell (SSH), File Transfer Protocol (FTP), Remote Desktop Protocol (RDP) und Server Message Block (SMB), die möglicherweise dem öffentlichen Internet ausgesetzt sind.

Regel 7: Passwortdisziplin

Nutzer machen sich wenig Mühen mit Passwörtern und entscheiden sich zu oft für den einfachsten Weg, um Anmeldeinformationen zu erstellen und zu verwalten. Eine Multi-Faktor-Authentifizierung (MFA) und die Vorschrift, starke Passwörter zu verwenden, senken erheblich die Wahrscheinlichkeit, dass Hacker Benutzerkonten kom- promittieren.IT-Administratoren müssen zwischen verschiedenen Angeboten abwägen. Für eine MFA können je nach Unternehmen physische Token, Applikationen oder SMS-basierte Tools das geeignete Mittel der Wahl sein, unter Umständen mit anderen Diensten verbunden werden und Kosten sparen.

Regel 8: Hygiene für Wechseldatenträger

Wechseldatenträger lassen sich im Geschäftsalltag nicht immer vermeiden. Dennoch sollten IT-Verantwortliche durch Alternativen ihren Gebrauch reduzieren oder zumindest den vorsichtigen, sorgfältigen Umgang fordern. Dazu gehören:

- ein Pflicht-AV-Scan nach jedem Nutzen;
- SharePoint oder DSGVO-konforme Cloud-Dienste zum Speichern und Teilen von Dateien; sowie
- das Blocken von Wechseldatenträgern aus unbekannten oder nicht vertrauenswürdigen Quellen.

Regel 9: Mit Backup für den Ernstfall vorbereitet sein

Keine IT-Sicherheit kann einen erfolgreichen Angriff für alle Zukunft ausschließen. Backup und Recovery können in diesem Fall die Informationen retten, sofern Unternehmen der Datensicherung die angemessene Aufmerksamkeit entgegenbringen. Dazu gehören:

- eine redundante Sicherung der Daten an verschiedenen Orten;
- zusätzliche, regelmäßig verwaltete Bakkups durch Remote- und/oder Cloud-Backup-Dienste; sowie
- das Testen der Sicherheitskopien und der notwendigen Abläufe, um Daten wiederherzustellen.

Regel 10: Physische Sperren und Aufsicht über Hardware

Dieser letzte Tipp mag offensichtlich erscheinen, wird aber in vielen Unternehmen völlig vernachlässigt. Der unerlaubte physische Zugriff auf einen Rechner ist aber sowohl im Büro wie auch bei Mitarbeitern im Außendienst eine Gefahr. IT-Sicherheitsverantwortliche sollten ihre Mitarbeiter hinsichtlich Hardwaresicherheit unterstützen, indem sie Sicherheitsschlösser etwa für Notebooks anschaffen. Vorgesetzte sollten Mitarbeiter daran erinnern, ihre mobilen Geräte zu sichern, wenn sie das Büro verlassen.

Auch eine Verschlüsselung lokaler Daten at Rest bietet einen wichtigen Grundschutz der Informationen. Sowohl mit kleinen Maßnahmen als auch mit grundlegenden Sicherheits- und Managementtechnologien lässt sich die Sicherheit der Unternehmens-IT deutlich erhöhen. Gerade in der Vorbeugung von Angriffen tragen schon einfache Maßnahmen einiges bei, um eine große Zahl von Attacken ins Leere laufen zu lassen.

Industrielle Steuerungssysteme

GLOBAL: Sicherheitsmarkt für industrielle Steuerungssysteme erreicht bis 2030 32,88 Milliarden Dollar

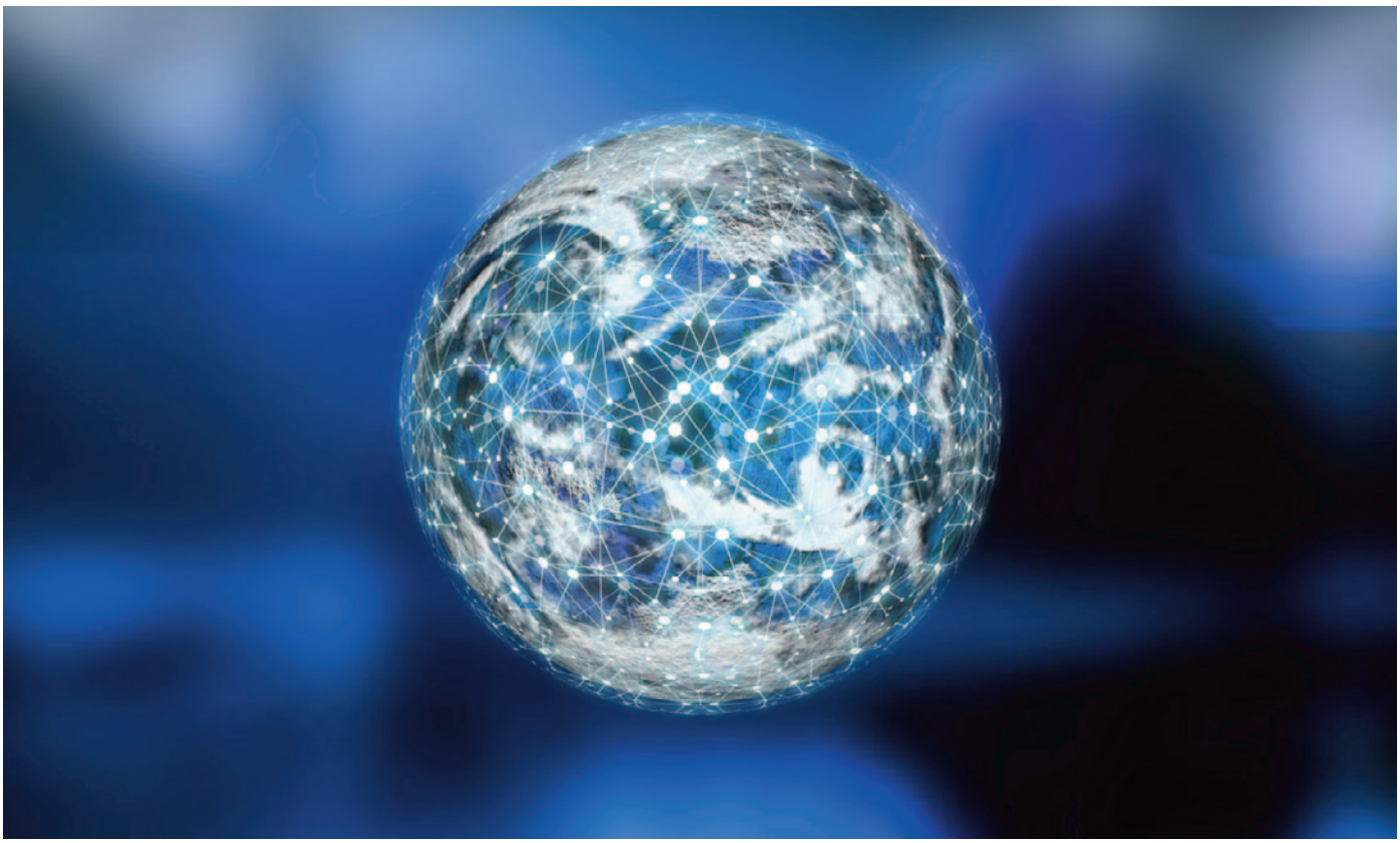
Der globale Sicherheitsmarkt für industrielle Steuerungssysteme wird bis 2030 voraussichtlich 32,88 Milliarden US-Dollar erreichen und während des Prognosezeitraums voraussichtlich mit einer CAGR von 8,2 % wachsen, so ein neuer Bericht von Grand View Research, Inc. Die zunehmende Einbindung digitaler Technologien in Geschäftsabläufe und industrielle Infrastrukturen hat zu einem deutlichen Anstieg des Risikos von Cyberangriffen geführt. Die Branche wird aufgrund des wachsenden Bedarfs an kreativen Lösungen zum Schutz angeschlossener Geräte und der steigenden Akzeptanz von SCADA-Systemen (Supervisory Control and Data Acquisition), die eine lokale und ferngesteuerte industrielle Prozesskontrolle ermöglichen, weiter expandieren. Dadurch wird das Gesamtwachstum des Marktes vorangetrieben.

Die Sicherheitssysteme für industrielle Steuerungssysteme bieten eine Reihe von Vorteilen, wie z. B. verbesserte Active Query-Funktionen für die Transparenz von Anlagen in allen Netzwerksegmenten und eine bessere Verwaltung von Sicherheitssensoren. Verschiedene Unternehmen führen verschiedene Produkte und Dienstleistungen ein, um auf dem Markt wettbewerbsfähig zu bleiben. So kündigte Tenable, Inc., ein Unternehmen für Cybersicherheitslösungen, im März 2023 Verbesserungen bei Tenable OT Security an, die den Schutz für kritische Infrastrukturen, industrielle Kontrollsysteme und Betriebstechnologie (OT) unabhängig von der Konfiguration oder dem Einsatz optimieren. Die verbesserten Funktionen ermöglichen es Anwendern, die gesamte Angriffsfläche mühelos abzusichern und zu kontrollieren, indem sie einheitliche Tools und Verfahren in ihrer gesamten Infrastruktur einsetzen, einschließlich Cloud, IoT, OT und IT-Systeme. Es wird erwartet, dass solche strategischen Initiativen das Marktwachstum im prognostizierten Zeitraum vorantreiben werden.

Es wird erwartet, dass Cyber-Bedrohungen erheblich reduziert werden, da sich das Internet der Dinge (IoT) auf dem Markt für Sicherheitslösungen für industrielle Steuerungssysteme immer weiter verbreitet. Intelligente, vernetzte und durch maschinelles Lernen (ML) gesteuerte Systeme reduzieren Cyberangriffe. Chief Information Security Officers (CISOs) im Transportwesen, in der Öl- und Gasindustrie sowie in der Medizintechnik sind führend bei Investitionen in Sicherheitssysteme mit IoT- und ML-Funktionen. Es besteht ein wachsender Bedarf an Produkten, die Sicherheit in Lösungen bieten, die speziell für Betriebstechnologien (OT) und industrielle Kontrollsysteme (ICS) entwickelt wurden, was das Wachstum des Marktes fördert.

Höhepunkte des Marktberichts über die Sicherheit industrieller Kontrollsysteme

- Das Dienstleistungssegment wird im Prognosezeitraum voraussichtlich eine hohe Wachstumsrate von mehr als 8,6 % aufweisen. Die ICS-Dienstleistungen sichern die Vermögenswerte. Vermögenswerte können durch Vorbeugung geschützt werden; zum Beispiel kann die Gefährdung von Transformatoren durch Überspannung reduziert werden, wenn ein Fehler, wie z. B. ein Überspannungszustand, erkannt wird. Daher wird davon ausgegangen, dass die Endnutzer zunehmend Sicherheitsdienste für industrielle Kontrollsysteme einführen.
- Das Verschlüsselungssegment wird bis 2030 voraussichtlich eine CAGR von mehr als 9,5 % verzeichnen. Verschlüsselungslösungen helfen bei der Umwandlung von Daten in ein Format, das nicht lesbar ist und nur mit einem geheimen Algorithmus oder Schlüssel entschlüsselt werden kann. Nur Personen, die über den entsprechenden Algorithmus oder Schlüssel verfügen, können die ursprüngliche Bedeutung der in verschiedenen Anwendungen, Dateien, Datenbanken und Netzwerken gespeicherten Daten entschlüsseln. Die Verschlüsselung kann Angreifer davon abhalten, ICS-Daten zu verändern, zu stehlen oder abzufangen, und stellt gleichzeitig deren Integrität und Authentizität sicher.
- Es wird erwartet, dass das Segment der verwalteten Dienste die schnellste CAGR-Wachstumsrate während des Prognosezeitraums verzeichnen wird. ICS Managed Service Provider konzentrieren sich auf ein breiteres ausgelagertes IT-Systemmanagement. Die Managed Services bieten Echtzeitüberwachung von Endpoint Detection and Response (EDR) und andere Lösungen zur Erkennung von Be-



drohungen durch Security Operations Centres (SOCs), was das Marktwachstum des Segments antreibt.

- Es wird erwartet, dass das Endpunkt-Segment auf dem Markt für industrielle Kontrollsysteme (ICS) während des Prognosezeitraums die höchste Wachstumsrate aufweisen wird. Die Marktteilnehmer entwickeln auf maschinellem Lernen (ML) basierende Methoden zum Aufspüren von Cyberangriffen durch verhaltensbasierte Techniken.

  Die Technologie des maschinellen Lernens (ML) hilft Unternehmen dabei, unbefugte Aktivitäten an Endgeräten zu erkennen und das System darüber zu informieren. Es wird erwartet, dass KI auch bei der Identifizierung von Zero-Day-Angriffen entscheidend sein wird. Daher wird erwartet, dass der Einsatz dieser fortschrittlichen Technologien die Nachfrage auf dem Markt im Prognosezeitraum ankurbeln wird.

- Es wird erwartet, dass das Segment der Energie- und Versorgungsunternehmen im Markt für industrielle Kontrollsysteme (ICS) während des Prognosezeitraums die höchste Wachstumsrate aufweisen wird. ICS-Software überbrückt die Lücke zwischen IT und OT im Energie- und Versorgungssektor, um einen umfassenden Überblick über die Sicherheit zu bieten und die lebenswichtige Infrastruktur der Endnutzer vor externen Bedrohungen zu schützen. Außerdem vereinfacht sie die Berichterstattung über die Einhaltung von NERC CIP und anderen Standards. Dies treibt das Marktwachstum in diesem Segment an.

- Es wird erwartet, dass der asiatisch-pazifische Markt für industrielle Kontrollsysteme während des Prognosezeitraums eine CAGR verzeichnen wird. Die Automobilindustrie in der Region hat aufgrund mehrerer bemerkenswerter Initiativen einen starken Fokus auf Digitalisierung und Industrie 4.0 erfahren. Dazu gehören u.a. Singapurs Smart Nation, die mit Indonesiens "2020 Go Digital Vision" verwandt ist, Thailands "Thailand 4.0"-Initiative und die Industrie 4.0-Initiativen der vietnamesischen Regierung. Dies treibt das Marktwachstum in der Region an.

Die Marktteilnehmer wenden verschiedene Geschäftsstrategien an, um potenzielle Kunden zu gewinnen und eine höhere Rentabilität auf diesem potenziellen Markt für industrielle Kontrollsysteme (ICS) zu erzielen. So hat die CPX Holding, ein Anbieter von Cybersicherheitslösungen und -dienstleistungen, im November 2023 die CPX Intelligent Threat Detection Platform auf den Markt gebracht, eine Cybersicherheitslösung, die intern entwickelt wurde und fortschrittliche Technologien zur Erkennung von Cyberbedrohungen einsetzt, um Kunden vor den sich ständig ändernden Bedrohungen zu schützen. Es wird erwartet, dass solche strategischen Initiativen das Marktwachstum im prognostizierten Zeitraum vorantreiben werden.

Mehr Informationen:
www.grandviewresearch.com/press-release/global-industrial-control-systems-security-market

Social-Media-Nutzung im Job mindert Leistung

Experiment der RUB zeigt Steigerung der Produktivität bei Reduktion um 30 Minuten pro Tag

Der Verzicht auf Social Media während der Arbeitszeit macht zufriedener und produktiver. Schon 30 Minuten weniger am Tag hat in einer einwöchigen Studie die psychische Gesundheit, die Arbeitszufriedenheit und das Engagement der Teilnehmer verbessert, berichten Forscher der Ruhr-Universität Bochum (https://www.rub.de) (RUB).

Hemmschuh Abhängigkeit

"Wir vermuten, dass Menschen dazu neigen, sich in sozialen Netzwerken positive Emotionen zu holen, die sie in ihrem Arbeitsalltag vermissen, insbesondere dann, wenn sie sich überarbeitet fühlen. Darüber hinaus bieten manche Plattformen wie LinkedIn auch die Möglichkeit, nach anderen Jobs zu suchen, wenn man mit seiner derzeitigen Tätigkeit unzufrieden ist", erklärt RUB-Forscherin Julia Brailovskaia.

Kurzfristig mag die Flucht vor der Realität in die Welt der sozialen Netzwerke die Stimmung tatsächlich heben - langfristig könne sich aber auch ein Abhängigkeitsverhalten einstellen, das gegenteilige Effekte mit sich bringe. Das Team hat ein Experiment gewagt. 166 Personen, die einer Teil- oder Vollzeitbeschäftigung in verschiedenen Sektoren nachgingen und mindestens 35 Minuten täglich nicht arbeitsbezogen Social-Media-Kanäle nutzten, nahmen daran teil.

Deutlich zufriedener im Job

"Bei der Gruppe, die 30 Minuten weniger täglich in sozialen Kanälen verbrachte, haben sich die Arbeitszufriedenheit und die psychische Gesundheit deutlich verbessert. Die Versuchspersonen in dieser Gruppe fühlten sich weniger überarbeitet und

waren engagierter bei der Arbeit als die Kontrollgruppe", so Brailovskaia. Auch das Gefühl, etwas zu verpassen, sank. Die Effekte hielten nach dem Ende des Experiments mindestens eine Woche an.

Die Forscher vermuten, dass eine verringerte Social-Media-Nutzung den Probanden mehr Zeit für Arbeitsaufgaben verschafft, sodass das Gefühl der Überarbeitung sinkt, und eine geteilte Aufmerksamkeit verringert.

"Mit ständiger Ablenkung von einer Aufgabe kann unser Gehirn nicht gut umgehen. Wer sich häufig unterbricht, um in Social Media auf dem neusten Stand zu bleiben, erschwert sich das konzentrierte Arbeiten und erreicht schlechtere Resultate.

Ransomware

Claroty-Studie: 75 Prozent der Industrieunternehmen wurden im vergangenen Jahr Opfer eines Ransomware-Angriffs

Kosten von Sicherheitsvorfällen und Prämien für Cyber-Versicherungen steigen / Neue Technologien wie generative KI werden zunehmend auch in OT-Umgebungen eingesetzt

Drei von vier Industrieunternehmen weltweit wurden im vergangenen Jahr Opfer eines Ransomware-Angriffs. Dies ist eines der Ergebnisse des neuen Reports „The Global State of Industrial Cybersecurity 2023: New Technologies, Persistent Threats, and Maturing Defenses" von Claroty, Spezialist für die Sicherheit von cyber-physischen Systemen (CPS). Dieser basiert auf einer weltweiten, unabhängigen Befragung von 1.100 Sicherheitsexperten, die in kritischen Infrastrukturen und Industrieunternehmen für Informationstechnologie (IT) und Betriebstechnik (OT) verantwortlich sind. Die Studie zeigt dabei die Herausforderungen, mit denen die Sicherheitsverantwortlichen im vergangenen Jahr kon- frontiert waren, ihre Auswirkungen auf OT-Sicherheitsprogramme und die Prioritäten für die Zukunft.

Der neue Report zeigt, dass Ransomware-Angriffe immer häufiger Auswirkungen auf OT-Umgebungen haben. Gemäß der letzten Studie aus dem Jahr 2021 betrafen 32 Prozent der Ransomware-Angriffe nur die IT, während 27 Prozent sowohl die IT als auch die OT erfassten. 2023 beschränkten sich 21 Prozent der Ransomware-Angriffe auf die IT, während 37 Prozent sowohl die IT als auch die OT betrafen.

Dies entspricht einem signifikanten Anstieg von 10 Prozentpunkten innerhalb der letzten zwei Jahren und verdeutlicht die wachsende Angriffsfläche und das steigende Risiko von Betriebsstörungen, die mit der IT/OT-Konvergenz einhergehen.

Neben den zunehmenden betrieblichen Auswirkungen von Ransomware sind auch die finanziellen Auswirkungen nach wie vor beträchtlich. 69 Prozent der im vergangenen Jahr von Ransomware-Angriffen betroffenen Unternehmen haben dabei das geforderte Lösegeld bezahlt, was bei mehr als der Hälfte zu finanziellen Einbußen von über 100.000 USD geführt hat. Entsprechend steigt die Nachfrage nach Cyber-Versicherungen: Eine große Mehrheit (80 %) der Unternehmen hat eine Cyber-Versicherung abgeschlossen, wobei sich etwa die Hälfte (49 %) für eine Police mit einer Dekkungssumme von einer halben Million Dollar oder mehr entschieden hat.

Verstärkt wird der zunehmende Druck bei der Bekämpfung von Bedrohungen und die Gefahr finanzieller Verluste durch die Integration neuer Technologien in OT-Umgebungen. So nutzen derzeit 61 Prozent der Befragten Sicherheitstools, die generative KI verwenden. Bei jedem zweiten (47 %) steigen hierdurch jedoch die Sicherheitsbedenken.

Angesichts dieser Herausforderungen, die durch die Bekämpfung von Ransomware und die Integration neuer Technologien entstanden sind, wächst die Notwendigkeit von Branchenvorschriften und -standards, welche die Prioritäten und Investitionen im Bereich der OT-Sicherheit bestimmen. 43 Prozent der befragten deutschen Unternehmen gaben an, dass die TSA-Sicherheitsrichtlinien den größten Einfluss auf die Sicherheitsprioritäten und -investitionen des Unternehmens haben, gefolgt von ISA/IEC-62443 (40 %) und NERC CIP (37 %). Die im nächsten Jahr in Kraft tretende NIS2 spielt bei lediglich 30 Prozent eine entscheidende Rolle.

„Unsere Studie zeigt, dass es sicherlich keinen Mangel an Herausforderungen gibt,

mit denen sich OT-Sicherheitsexperten konfrontiert sehen. Wir haben aber auch festgestellt, dass es ein enormes Potenzial und einen großen Willen gibt, die Sicherheitslage in industriellen Umgebungen zu verbessern", sagt Yaniv Vardi, CEO von Claroty.

„Die meisten Unternehmen arbeiten daran, ihre Maßnahmen zur Risikobewertung, zum Schwachstellenmanage- ment und zur Netzwerksegmentierung zu verstärken, um ihre cyber-physischen Systeme proaktiv zu schützen."Auch wenn die Implementierung generativer KI derzeit Zeit und Ressourcen in Anspruch nimmt, sind einige Fortschritte und Weiterentwicklungen zu verzeichnen, um Prozess- und Technologielücken zu schließen:

• Netzwerksegmentierung ist für die Reduzierung der lateralen Bewegung von Cyberangriffen (einschließlich von IT zu OT) von wesentlicher Bedeutung. 77 Prozent der Befragten bezeichnen ihren Ansatz hierfür als „angemessen" oder „ausgereift".

• Schwachstellen- und Risikomanagement: 78 Prozent der Befragten bezeichnen ihren Ansatz zur Identifizierung von Schwachstellen als „angemessen" oder „äußerst" proaktiv – ein deutlicher Anstieg gegenüber 66 Prozent im Jahr 2021. Die Geschwindigkeit, mit der Schwachstellen aufgedeckt und Patches veröffentlicht werden, übersteigt jedoch die Fähigkeit der Unternehmen, diese zu beheben. Daher verwenden die Unternehmen eine Reihe von Risikobewertungsmethoden, um eine Priorisierung vorzunehmen. Die gängigsten Methoden sind das Common Vulnerability Scoring System (CVSS), das von 52 Prozent der Befragten weltweit verwendet wird, gefolgt von den Risikobewertungen bestehender Sicherheitslösungen (49 %), dem Exploit Prediction Scoring System (EPSS) (46 %) und dem Known Exploited Vulnerabilities (KEV) Catalog (45 %).

• Geplante Maßnahmen: Die wichtigsten OT-Sicherheitsinitiativen, die die Befragten im nächsten Jahr umsetzen wollen, sind Risikobewertung (43 %), dicht gefolgt von Asset-, Change- und/oder Lifecycle-Management (40 %) und Schwachstellenmanagement (39 %).

Der komplette Report „The Global State of Industrial Cybersecurity 2023" zum Herunterladen: https://tinyurl.com/mvrevvxe

Methodik
Claroty beauftragte Pollfish mit der Durchführung einer Umfrage unter 1.100 Sicherheitsexperten für Informationstechnologie (IT) und Betriebstechnik (OT) in Nordamerika (500), Lateinamerika (100), EMEA (250) und Asien-Pazifik (250). An der Umfrage nahmen nur Personen teil, die hauptberuflich im Bereich IT-Sicherheit, OT-Sicherheit oder als OT-Ingenieur/Techniker tätig sind. Mehr als ein Dutzend Branchen sind dabei vertreten, wie die Automobilindustrie, Chemie, Stromversorgung, Lebensmittel- und Getränke, Öl- und Gas, Pharmazeutik und Biotechnologie, Transportwesen, Wasser- und Abfallwirtschaft, Konsumgüter, Bergbau und Werkstoffe, IT-Hardware sowie Forstwirtschaft, Zellstoff und Papier. Die Umfrage wurde im November 2023 abgeschlossen.

Cybersicherheitsrichtlinie NIS2

Wie Observability-basierte Automatisierung bei der Einhaltung unterstützt

Gesetzliche Vorschriften wie die DSGVO und seit kurzem die NIS2-Richtlinie sollen für mehr Datenschutz und Cybersicherheit in der Europäischen Union sorgen. NIS2 ist die bisher umfassendste Cybersicherheitsrichtlinie der EU und eine Aktualisierung der 2016 eingeführten Vorschriften. Sie soll strengere Anforderungen an das Risikomanagement und die Meldung von Cybersecurity-Vorfällen für ein breiteres Spektrum von Sektoren durchsetzen, wobei die Strafen bei Nichteinhaltung nun wesentlich härter ausfallen. Bis zum 17. Oktober 2024 soll NIS2 in nationales Recht umgesetzt werden. Da die typischen Compliance-Prozesse etwa 12 Monate dauern, ist keine Zeit zu verlieren.

Enorme Herausforderung für Unternehmen

Mit der zunehmenden Intelligenz und Leistungsfähigkeit von Technologien werden auch die Methoden der Angreifer immer ausgefeilter. NIS2 soll dafür sorgen, dass Unternehmen besser gegen die Flut an fortschrittlichen Cyberangriffen geschützt sind. Die strengen Anforderungen sind jedoch eine enorme Herausforderung, vor allem für die Sektoren und Organisationen, die bisher keine derart strengen Vorschriften einhalten mussten.

So sieht NIS2 beispielsweise sehr enge Fristen für die Meldung von Cybersicherheitsvorfällen vor.

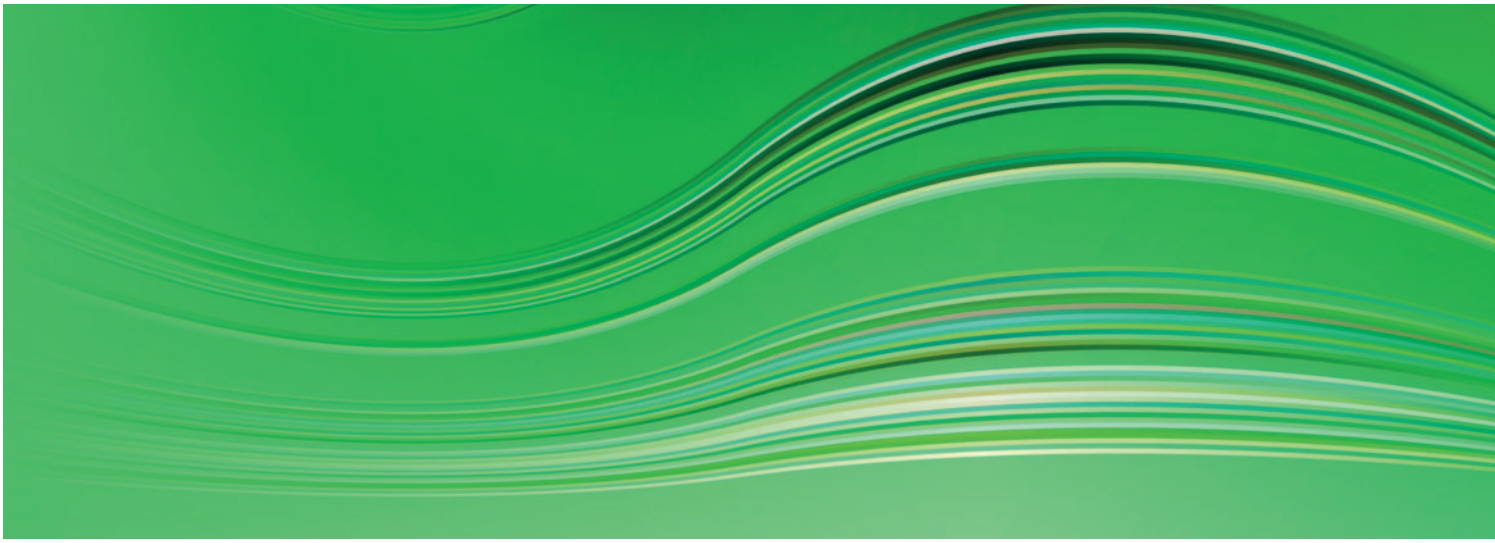
Organisationen sind verpflichtet, innerhalb von 24 Stunden eine Frühwarnung über einen Cybersicherheitsvorfall abzugeben und innerhalb von 72 Stunden eine ausführlichere Meldung zu machen.

Diese muss eine erste Bewertung des Vorfalls mit Angaben zu Schweregrad, Auswirkungen und Indikatoren für eine Kompromittierung enthalten. Nach einem Monat ist ein Abschlussbericht vorzulegen, der sicherstellen muss, dass Lehren aus früheren Vorfällen gezogen werden können.

Diese Anforderungen unterstreichen, dass es nicht mehr ausreicht, wenn eine Organisation nur fähig ist nachzuweisen, dass sie bei Bedarf einem Audit unterzogen werden kann. Unternehmen müssen Sicherheitsvorfälle schnell und effektiv untersuchen und darauf reagieren können. Diese Fristen sind fast unmöglich einzuhalten, wenn Sicherheitsteams nicht über die richtigen Werkzeuge verfügen.

NIS2 wird Fachkräftemangel weiter verschärfen

Wenn Unternehmen mit neuen Sicherheits- und Compliance-Anforderungen konfrontiert werden, besteht ihre erste Reaktion allzu oft darin, das Problem mit mehr Personal zu lösen. Es ist zwar wichtig, dass die richtige Expertise im Unternehmen vorhanden ist, um eine Einhaltung der Vorschriften zu erreichen und aufrechtzuerhalten, aber mehr Personal ist keine langfristige oder nachhaltige Lösung, da es einfach nicht genügend Sicherheitsspezialisten gibt. NIS2



wird den Fachkräftemangel noch weiter verschärfen, da eine große Anzahl von Organisationen betroffen ist. Die Unternehmen, die es sich leisten können, große Sicherheitsteams einzustellen, werden sich alle auf dem Markt verfügbaren Fachkräfte sichern, bevor andere eine Chance dazu bekommen.

Die Komplexität von Multi-Cloud-Umgebungen und Cloud-Native-Delivery-Praktiken stellt eine weitere Herausforderung für die NIS2-Compliance dar, da sie die Art und Weise, wie Sicherheitsteams an die Cybersicherheit herangehen, dramatisch verändert hat. Die Softwareentwicklung erfolgt nun kontinuierlich, mit mehr Releases und kürzeren Testzyklen für Sicherheitsteams. Infolgedessen ist die Wahrscheinlichkeit größer, dass Teams Schwachstellen übersehen.

Intelligente Automatisierung

Um die Anforderungen von NIS2 zu erfüllen und ein robustes Schwachstellen- und Vorfallmanagement zu ermöglichen, müssen die Sicherheitsanalyse- und Berichterstattungsprozesse optimiert und automatisiert werden. Es ist unmöglich, die von NIS2 geforderte Detailliertheit und Genauigkeit bei Cybersecurity-Vorfällen innerhalb des vorgegebenen Zeitrahmens durch manuelle Ansätze zu erreichen. Unternehmen benötigen Echtzeitdaten über ihre Sicherheitslage und einen durchgängigen Einblick in ihre hybride Multi-Cloud-Umgebung.

Dies kann nur durch die Verbindung von Sicherheits- und Observability-Daten und die Automatisierung von Runtime-Schwachstellenanalysen erreicht werden, um Erkenntnisse über den Schweregrad und die Auswirkungen von Sicherheitsvorfällen zu gewinnen. Mit diesen Erkenntnissen können Teams sofort die Dringlichkeit von Schwachstellen einschätzen und feststellen, welche Systeme während eines Vorfalls betroffen waren – eine wichtige Voraussetzung für Frühwarnberichte.

Außerdem erhalten sie Einblicke in die Priorisierung und Lösung von Problemen und können so schnell handeln. Um diese Informationen in dem kurzen Zeitrahmen zu sammeln, der für die Einhaltung von NIS2 erforderlich ist, müssen Sicherheitsteams jedoch den Prozess automatisieren, um diese Erkenntnisse zu gewinnen und sie in Berichten und Meldungen zu Sicherheitsvorfällen zusammenzufassen.

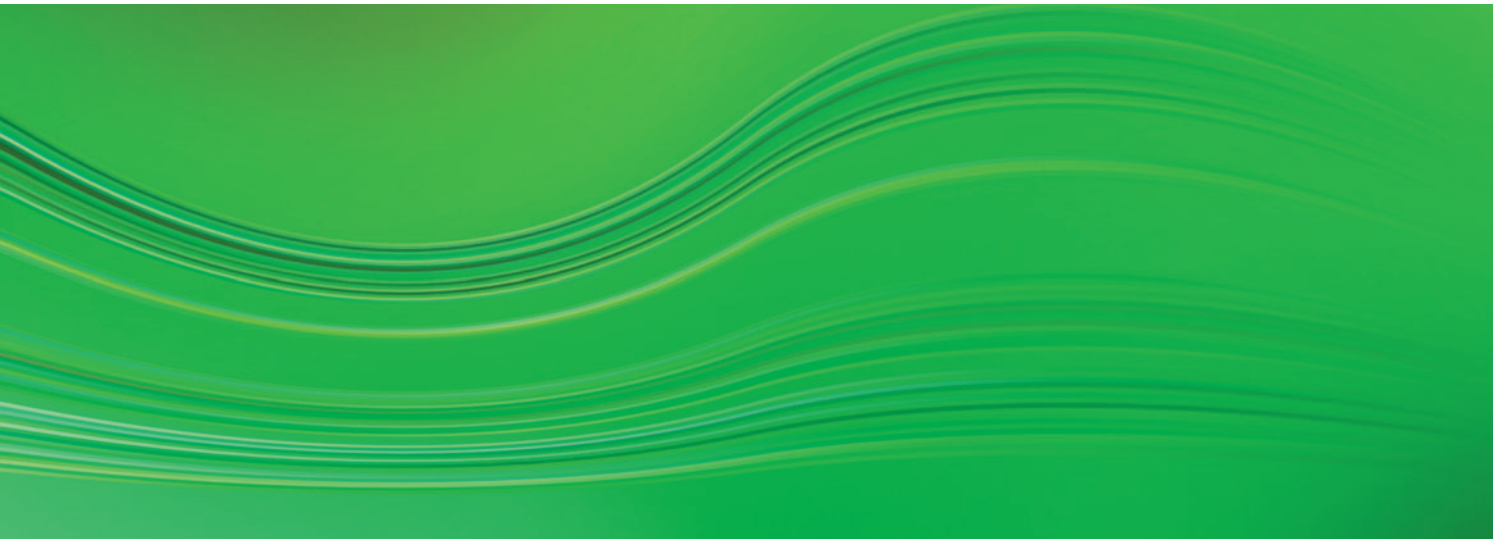
Über die Einhaltung von Vorschriften hinausgehen

Anstatt sich nur darauf zu konzentrieren, Probleme aufzuspüren und zu melden, sollten Unternehmen versuchen zu verhindern, dass diese Probleme überhaupt erst entstehen. Das bedeutet, dass die Sicherheit zu einer kritischen Komponente im Lebenszyklus der Softwareentwicklung wird. Viele Unternehmen würden behaupten, dass sie diesen Ansatz bereits umsetzen, aber die meisten tun dies manuell und ohne End-to-End-Transparenz, was die Effektivität einschränkt.

So müssen beispielsweise Security- und Entwicklungsteams zusammenarbeiten, um sicherzustellen, dass Software nicht bereits in frühen Entwicklungsphasen durch die Pipeline weitergeschickt wird, wenn nicht beide Teams davon überzeugt sind, dass sie sicher ist. Automatisierte Qualitäts- und Sicherheitskontrollen sind eine gute Möglichkeit, manuelle Arbeit in diesem Prozess zu vermeiden.
Durch die Kombination dieser Funktionen mit Observability-Daten können Schwachstellen oder Fehler automatisch erkannt werden, so dass Entwickler sie beheben können, bevor der Code in die nächste Phase der Bereitstellung geht.

Die Frist für NIS2 rückt rasch näher, daher ist es für Unternehmen jetzt an der Zeit zu handeln und sicherzustellen, dass sie über die nötige Transparenz verfügen, um angemessen auf die Compliance-Anforderungen vorbereitet zu sein.

Autor: Ben Todd, Dynatrace, RVP Security Solutions, EMEA



Veränderte Bedrohungslage – ganzheitlich Denken

2024: Die Trends in der IT-Security

Umwälzende Technologien, zunehmende Vernetzung, Globalisierung – so wie sich die digitale Welt wandelt, verändern sich auch die Methoden und Motivationen der Hacker. Deutsche Firmen sehen sich einer komplexer werdenden Bedrohungslandschaft gegenüber, die fortgeschrittenste Technik, politische Motivation und monetäre Interessen vereint. Darauf müssen sie sich vorbereiten. Welche Trends zeichnen sich für 2024 ab? Wolfgang Kurz, Geschäftsführer und Gründer indevis, erklärt.

1.Hacker: Zu monetärer Motivation kommtdie politische hinzu

Die Weltlage verändert das Verhalten der Cyberkriminellen. Schon mit dem Ukraine-Krieg wurden verstärkt Angriffe von russischen Hackergruppen auf deutsche Firmen verzeichnet. Mit dem Israel-Palästina-Konflikt sind die politisch motivierten Attacken weiter gestiegen und werden im nächsten Jahr noch zunehmen. In der Cybersicherheit kann sich niemand mehr darauf verlassen, nur mit Erpressern zu verhandeln. Jetzt müssen die Betriebe damit rechnen, dass hinter dem Angriff terroristische Vereinigungen stehen, deren Ziel es ist zu zerstören. Es geht darum, Systeme zu infiltrieren und Informationen zu löschen, anstatt zu verschlüsseln und Daten zu versilbern. Deutsche Unternehmen sind für terroristisch motivierte Attacken attraktiv – immerhin arbeiten sie in einer der größten europäischen Volkswirtschaften. Deutschland ist demokratisch und hat eine ernst zu nehmende Rüstungsindustrie. Alles Punkte, die es zum Feindbild machen. Leider ist eine National Cyber Defense auf Landesebene praktisch inexistent, daher sind Unternehmen selbst im Zugzwang.

2. Künstliche Intelligenz: Angriffe nähern sich der Perfektion

Auch die kommerziell motivierte Cyberattacke erfährt eine radikale Transformation dank der KI-basierten Technologien. Denn sie hebt diese auf eine bisher ungekannte Stufe der Raffinesse und Täuschung. Phishing-Attacken, die vor allem durch Rechtschreibfehler, mangelnde Personalisierung und offensichtliche Unstimmigkeiten auffielen, erfahren durch KI nun eine dramatische Steigerung an Komplexität. Generative KI-Tools wie WormGPT können heute hochgradig personalisierte E-Mails und Dokumente erstellen, sodass Hacker einen täuschend echten Mailverkehr kreieren können, der sich von einem authentischen Austausch kaum unterscheiden lässt. Deep Fakes und realistisch nachgeahmte Stimmen verstärken das Problem noch: Angreifer können damit Anrufe fälschen und Sicherheitsprotokolle umgehen. Traditionelle Sicherheitsmaßnahmen, die auf gesundem Misstrauen und menschlicher Überprüfung beruhen, stoßen an ihre Grenzen: Selbst Rückrufe auf bekannten Telefonnummern oder Codewörter können nicht mehr als sichere Verifikationsmethoden betrachtet werden.

Auf der Abwehrseite versuchen Sicherheitsanbieter und Technologiegiganten ebenfalls KI für ihre Zwecke einzusetzen: Es gilt, in Echtzeit Anomalien zu erkennen, Muster zu analysieren und proaktiv auf potenzielle Bedrohungen zu reagieren. Dies könnte einen Wendepunkt in der Defense markieren: Waren bisher die Angreifer im Vorteil, könnten die Sicherheitsexperten bald vorne liegen, insbesondere wenn sie Zugang zu den Ressourcen und Rechenleistungen der großen Technologieplattformen haben. Leider hat die Vergangenheit gezeigt, dass die Verteidiger viel zu spät auf neue Bedrohungen und Technologien reagieren. Daher wird KI vermutlich in nächster Zeit eher den Angreifern helfen. Die Ressourcen und Rechenleistung der großen Technologieplattformen unterscheiden nicht, an welche Seite sie ihre Leistung verkaufen.

3. Auch der Mittelstand braucht SASE

Secure Access Service Edge (SASE), dessen Fokus auf dem sicheren Zugriff und Endpoint-Schutz liegt, hat sich bei großen Organisationen weitgehend etabliert. Denn sie sehen sich mit komplexen Cloud-Infrastrukturen konfrontiert, die sie schützen müssen. Der Mittelstand hält sich allerdings noch zurück, obwohl auch er auf dem Weg in die Cloud ist und einen signifikanten Anteil der Anwendungen aus den firmeneigenen Rechenzentren entfernt. SASE verlagert Sicherheits- und Netzwerkfunktionen in die Cloud und stellt so eine flexible, skalierbare und standortunabhängige Sicherheitslösung bereit. Ratsam ist es, sich frühzeitig damit zu beschäftigen: In Deutschland beispielsweise besteht eine starke Abhängigkeit von MPLS-Infrastrukturen, was den Umstieg kompliziert gestaltet. In solchen Fällen kann SD-WAN ein Weg in die Zukunft sein.

4. IoT-Infrastrukturen: Die vernachlässigte Seite der Vernetzung

Internet of Things (IoT) oder auch Operational Technology (OT) rückt erneut in das Zentrum der Diskussion: Besonders im Kontext politisch motivierter Angriffe zeigt sich, dass die Erpresser vermehrt versuchen, kri-

Indevis-Gründer Wolfgang Kurz
©Indevis

tische Infrastrukturen zu attackieren. Die Konvergenz von IT und IoT führt zu einer verstärkten Vernetzung von bisher isolierten Systemen. Traditionell abgeschlossene Netze wie Stromversorgung oder Produktionssteuerung öffnen sich zunehmend dadurch, dass Smart-Metering-Systeme, APIs in Autos und andere vernetzte Geräte integriert werden. Das eröffnet neue Möglichkeiten, in kritische Infrastrukturen einzudringen. Eine entgegenwirkende Sicherheitspraxis hat sich aber in diesem Bereich noch nicht etabliert. Dies liegt daran, dass IoT bisher isoliert agierte und nicht dieselben Sicherheitsstandards befolgt wie IT-Systeme. Mit der wachsenden Vernetzung von Devices entsteht jedoch ein weiterer Angriffsvektor, der nicht vernachlässigt werden darf. Ein besonderes Risiko ergibt sich auch aus den Lebenszyklen der IoT-Geräte: Produkte wie Waschmaschinen, Kühlschränke oder industrielle Maschinen können mehrere Jahrzehnte im Einsatz sein. Je länger die Betriebszeit jedoch dauert, desto seltener werden Softwareupdates und Patches.

5. Security kommt endgültig in der Geschäftsleitung an

Das Thema Sicherheit hat mittlerweile einen festen Platz in der Geschäftsleitung gefunden. Keiner glaubt mehr, dass sie ausschließlich in den Grenzen der IT-Abteilung verbleiben kann. Eine ernst zu nehmende Cybersecurity-Strategie muss als integraler Bestandteil in die ganzheitliche Unternehmensstrategie eingebettet sein. Sie schließt demnach nicht nur Produkte, sondern auch die Produktion und andere betriebliche Aspekte mit ein.

Es geht also nicht nur darum, finanzielle Mittel für Technologie bereitzustellen, sondern auch um die Resilienz; es ist eine stabile und widerstandsfähige Sicherheitsarchitektur mit modernen Security-Technologien zur Angriffserkennung zu schaf- fen, die Compliance-Anforderungen und Regularien wie NIS-2 erfüllt. Mitarbeiter zu sensibilisieren, gehört dazu – zum Beispiel sie zu schulen, wie sie Phishing-Angriffen wirkungsvoll entgegentreten.

Fazit

Wolfgang Kurz, Geschäftsführer und Gründer von indevis, fasst zusammen: „Die tiefgehenden Änderungen in der Bedrohungslandschaft zwingen Unternehmen dazu, ihre Sicherheitsstrategien anzupassen.

Sie umfassen KI-basierte Abwehr-Tools genauso wie Zugriffskontrollen und Maßnahmen, um IoT-Infrastrukturen abzusichern. Wer einen Partner an seiner Seite hat, der diese Trends für das kommende Jahr auf dem Schirm hat, fährt gut."

Mehr Zeit für Cyberangriffe

Im Schaltjahr hacken Cyberkriminelle 24 Stunden länger

2024 wird besonders gefährlich. Risiko für KI-gestützte Cyberangriffe und Lösegeldforderung steigt weiter an

Schneller als je zuvor und gestützt von KI entwickeln Cyberkriminelle ihre Lösungen und Angriffsmethoden weiter. Für Unternehmen und ihre Security-Teams wird 2024 ein erneuter Peak erreicht, erklärt Ontinue, der führende Experte für Managed Extended Detection and Response (MXDR). Grund genug, sich mit den fünf großen Trends des kommenden Jahres auseinanderzusetzen.

Selbstständige, Unternehmen jeder Größe, Behörden und Einrichtungen des öffentlichen Lebens rücken immer öfter in das Visier von kriminellen Banden. Ihre Interessen liegen im schnellen Geld und oft auch in der Beschädigung von Wirtschaftsstandorten. Weil die Täter kontinuierlich aufrüsten, wird der Schutz von Daten immer schwieriger. Zum Jahreswechsel gibt Ontinue einen Ausblick auf die fünf entscheidenden Trends 2024.

1. Ransomware:

Es ist das Hacker-Tool Nummer eins und wird IT-Verantwortlichen auch 2024 große Sorgen bereiten. Durch die Zahlungsoption Kryptowährung ist die Abwicklung für global agierende Kriminelle und ihre Netzwerke so einfach wie nie. Zudem verbessert sich die Qualität der infiltrierenden Schadsoftware durch den Einsatz von KI stetig und fordert Security-Teams heraus. Das Ransomware-Risiko für schlecht geschützte Unternehmen in Industriestandorten bleibt damit sehr hoch.

2. Phishing:

Für viele Entscheider ist Phishing gedanklich ein alter Hut – doch Vorsicht, es ist einer, der sich stetig weiterentwickelt. Während früher eine kryptisch anmutende E-Mail von ausländischen Absendern im Posteingang lag, präsentiert sich Social Engineering heute als realistische Budgetfreigabe des Vorgesetzten. Die Qualität von Phishing-Versuchen wird sich 2024 auch durch die Verwendung von KI-Modellen weiter verfeinern. Die gute Nachricht ist jedoch, dass es wirksame Gegenmaßnahmen gibt: Schulungen in Cybersicherheit, Zero-Trust-Strategie und Multi-Faktor-Authentifizierung können Kriminellen das Handwerk deutlich schwerer machen.

3. Passwordless:

Beim Passwortschutz galt die letzten Jahre die klare Devise: je länger und komplexer, umso besser. 2024 steht eine Revolution in den Startlöchern, die das Passwort nach über 50 Jahren in Rente schicken könnte. Passwordless ist das Schlagwort, hinter dem sich passwortlose und passive Sicherheitsschlüssel verbergen. US-amerikanische Hyperscaler haben die Transformation durch erste Ankündigungen bereits angestoßen: Google plant auf Passkeys umzustellen und auch Microsoft will persönliche Konten passwortlos machen. Das könnte der Anfang vom Ende des klassischen Passworts sein.

4. NIS2-Richtlinie:

Die Europäische Union ist ihrem Ziel, Europa stärker gegen Cyberkriminalität zu schützen, durch die 2023 in Kraft getreten NIS2-Richtlinie ein Stück näher gekommen. NIS2 setzt den Rechtsrahmen für ein gemeinsames Cybersicherheitsniveau in der EU und definiert die Anforderungen an die Mitgliedsstaaten. Nicht mehr nur KRITIS-relevante sondern auch die Anbieter wesentlicher Dienste in Wirtschaft und Gesellschaft werden sich im kommenden Jahr verstärkt damit auseinandersetzen müssen. Damit sind nahezu 30.000 Unternehmen alleine in Deutschland aufgefordert, geeignete Sicherheitsmaßnahmen zu ergreifen und nachzuweisen, um sich gegen Cyberkriminalität zu schützen.

5. Künstliche Intelligenz:

Reaktionsschnelligkeit ist einer der großen Trümpfe im Arsenal von Security-Teams, um Bedrohungen im Anfangsstadium zu neutralisieren oder diese sogar präventiv zu verhindern. Mit Technologien der Künstlichen Intelligenz lässt sich der Zeitbedarf bei der Erkennung, Analyse und dem Einleiten von Gegenmaßnahmen in akuten Bedrohungssituationen massiv senken. Viele Anbieter setzen schon heute auf Maschinelles Lernen, um verdächtige Verhaltensmuster zu erkennen und frühzeitige Warnmeldungen auszusprechen.

Um Teams nicht zu überschwemmen und Meldungen effektiver zu filtern und zu priorisieren, werden 2024 KI-gestützte Security Operations einen regelrechten Boom erfahren. Die Technologie lernt die spezifische Umgebung eines Unternehmens und die beteiligten Akteure kennen und kann so die Qualität von Warnmeldungen deutlich präziser beurteilen. Zudem ermöglicht sie eine Echtzeit-Interaktion zwischen beteiligten Teams und externen Dienstleistern. Das ist entscheidend, um die Barrieren für schnelles Handeln in Krisensituationen so niedrig wie möglich zu halten.

„Auch 2024 werden sich Hacker nicht entspannt zur Ruhe legen", erklärt Jochen Koehler, VP EMEA Sales bei Ontinue. „Verantwortliche müssen daher alle Hebel in Bewegung setzen, um eine Sicherheitsarchitektur aufzubauen, die Schutz vor Angriffen bietet."

Jeder vierte deutsche IT-Mitarbeiter fürchtet Arbeitsplatzverlust durch KI

Unternehmen arbeiten mit Hochdruck am praktischen Einsatz von generativer KI. Nur wenige beschäftigen sich damit, wie sich diese Entwicklung auf die Mitarbeitenden auswirken wird. Diese schwanken zwischen Optimismus und Sorge.

Ivanti, das Technologieunternehmen, das Everywhere Work ermöglicht und sichert, hat die Ergebnisse seiner Studie „Getting Employees on Board for the AI Revolution" veröffentlicht. Die Studie zeigt, dass Unternehmen die Einführung von KI vorantreiben, Arbeitnehmende aber noch skeptisch sind, was die Potenziale von KI betrifft. Allerdings: Nur wenn Mitarbeitende und Unternehmen auf einer Linie sind, entfaltet KI ihre Möglichkeiten.

Zentrale Ergebnisse im Überblick:

- 61 % der deutschen ITMitarbeitenden sind der Überzeugung, dass generative KI eher den Arbeitgebern nützt. Bei den Büroangestellten liegt dieser Wert bei 49 %. Anders der weltweite Durchschnitt: Hier sind es eher die Büroangestellten, die den Vorteil auf Unternehmensseite sehen.
- 42 % der ITMitarbeitenden hierzulande sind sehr besorgt, dass sie in den nächsten fünf Jahren von generativen KI-Tools ersetzt werden (weltweiter Durchschnitt: 36 %), nur 15 % sind es bei den Büroangestellten.
- Führungskräfte geben an, dass die wichtigsten Vorteile von KI im Unternehmen die Automatisierung alltäglicher Aufgaben (77 %) und eine höhere Mitarbeiterproduktivität (63 %) sind.
- Weniger als ein Viertel (21 %) der Büroangestellten glaubt jedoch, dass KI die Produktivität stark verbessern wird.
- 42 % der deutschen Büroangestellten stehen KI positiv gegenüber, jedoch fühlen sich nur 9 % befähigt, sie zu nutzen.

Zwischen Unternehmenslenkern und IT-Mitarbeitenden herrscht Uneinigkeit, wie KI dem Unternehmen nützen wird. Die Unternehmensleitung ist deutlich optimistischer, was das Potenzial von KI angeht. Die Tech-Profis dagegen sind weniger begeistert: Sie sind eher besorgt, dass KI ihnen ihre Arbeitsplätze streitig macht oder den Unternehmensgewinn auf Kosten ihres Stresslevels steigern wird.

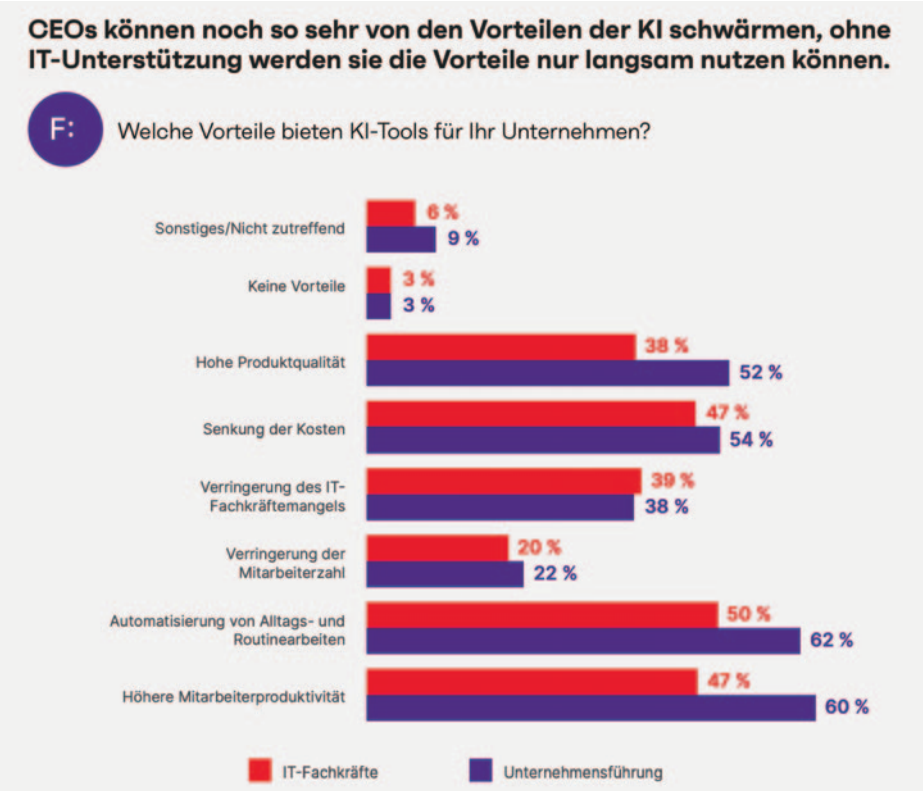
„Obwohl Unternehmen mit Hochdruck an Anwendungsfällen für KI arbeiten, sind ihre Mitarbeitenden uneins darüber, was dies für ihre berufliche Stellung bedeutet", sagt Dr. Srinivas Mukkamala, Chief Product Officer bei Ivanti. „Unternehmen können es sich nicht leisten, dieses Thema außer Acht zu lassen. Dabei reicht es nicht aus, alle Vorteile von KI darzulegen. Führungskräfte müssen ihre KI-Strategie klar kommunizieren und deutlich machen, wie sich diese auf die Zukunft der Mitarbeitererfahrung, die Produktivität und die Karriereentwicklung auswirkt. Ohne die Unterstützung der Mitarbeitenden und ohne menschliche Kontrolle über generative KI werden Unternehmen die Vorteile eventuell nur verzögert nutzen können."

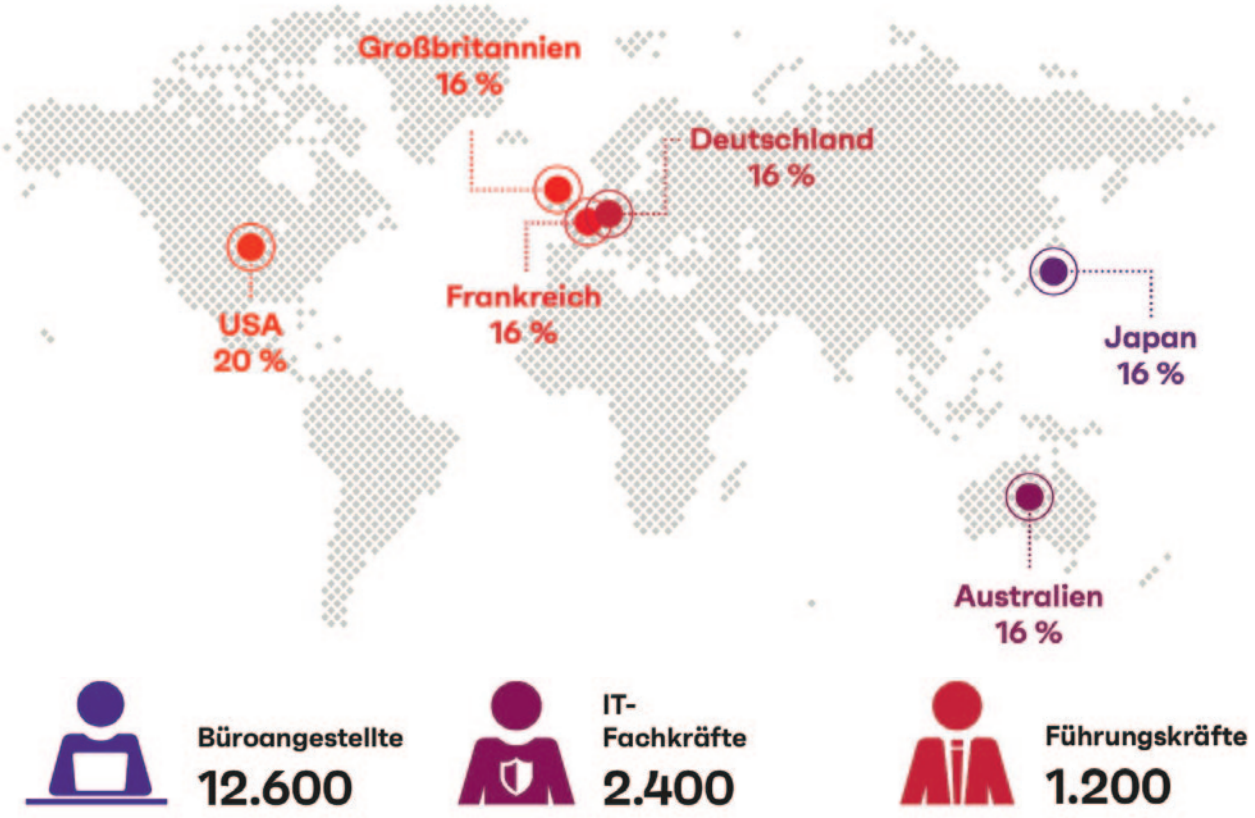
Da die IT-Teams die konkrete Umsetzung von KI- und Automatisierungsprojekten übernehmen, müssen sie auch aktiv einbezogen werden, wenn es um die Entwicklung einer KI-Strategie für das Unternehmen geht. Insbesondere dann, wenn diese sich auf den IT-Betrieb und die IT-Sicherheit auswirkt. Die Studie skizziert, wie Unternehmen generative KI nutzen und dabei die IT-Abteilung in die Definition ihrer KI-Strategie einbinden können.

Mukkamala fährt fort: „Alle Unternehmen müssen die Sicherheit der Daten und die Einhaltung der Datenschutzbedingungen

gewährleisten, wenn sie Daten sammeln und in KI-Systeme einspeisen. Der Schutz dieser Daten vor Missbrauch, Bedrohungsakteuren oder böswilligen Absichten ist ein elementares Thema und nicht verhandelbar. Bei den Rahmenbedingungen für KI-Modelle gilt es, Leitlinien so zu setzen, dass sie Verzerrungen vermeiden und keine Vorurteile replizieren – bei der KI als Ganzem, den Daten, den Modellen und Algorithmen. Unsere Studienergebnisse zeigen, dass die meisten Nutzer und Mitarbeiter KI skeptisch gegenüber stehen. Daher ist es wichtig, dass wir KI-Systeme sicher und widerstandsfähig gestalten und so weltweit Vertrauen schaffen."

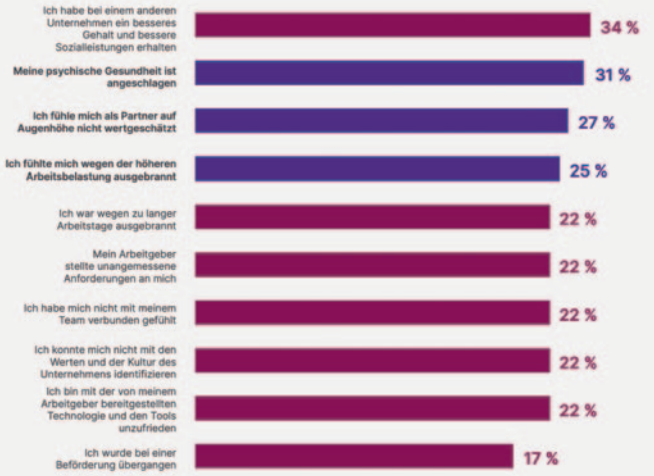
Diese Studie basiert auf zwei Befragungen, die Ivanti in der ersten Jahreshälfte 2023 durchgeführt hat, „Elevating the Future of Everywhere Work" und „New Imperatives for Digital Employee Experience". Insgesamt wurden 16.200 Führungskräfte, IT-Experten und Angestellte befragt.





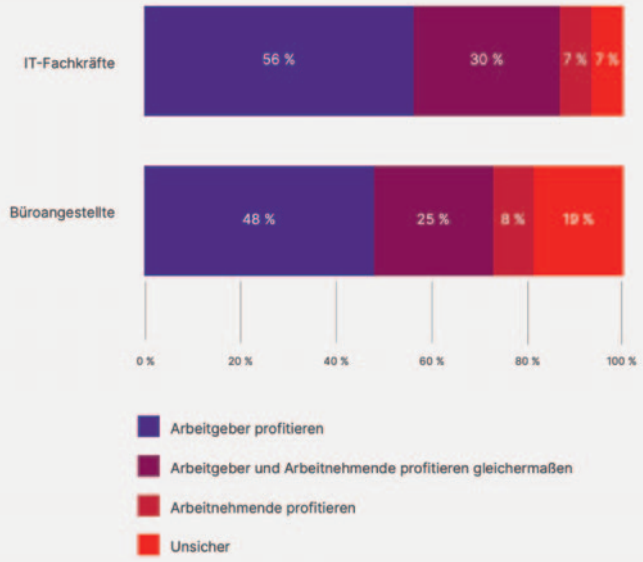
IT-Fachkräfte geben Burnout, eine hohe Arbeitsbelastung und eine Verschlechterung ihrer psychischen Gesundheit als die drei wichtigsten Gründe für die Suche nach einer neuen Arbeitsstelle an.

F: Warum haben Sie letztes Jahr Ihre Arbeitsstelle gewechselt? (Wählen Sie alle zutreffenden Antworten aus).



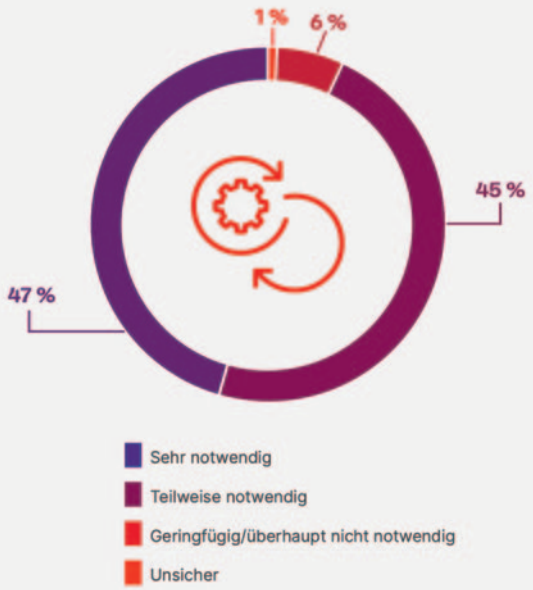
Wissensarbeiter sind 6x häufiger der Meinung, dass Arbeitgeber von KI profitieren und nicht Arbeitnehmende.

F: Glauben Sie, dass zukünftig vor allem Arbeitgeber oder Arbeitnehmende von KI-Tools profitieren?



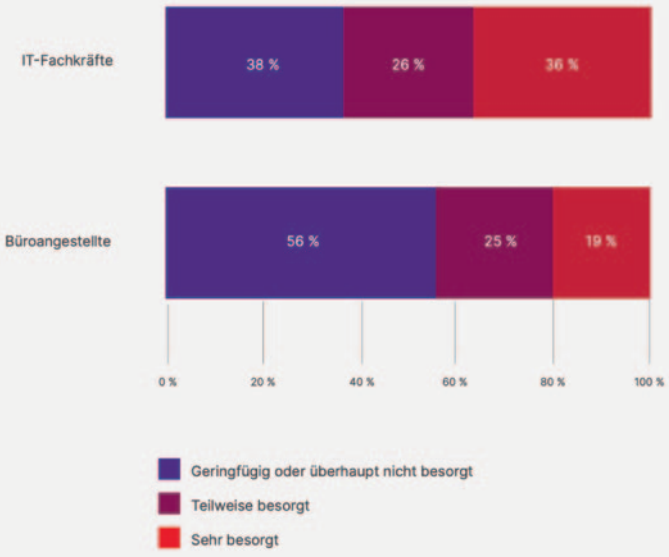
Mitarbeitende verstehen und unterstützen Automatisierung

F: Glauben Sie, dass Automatisierung notwendig ist, um Ihre Arbeit effizient zu erledigen?

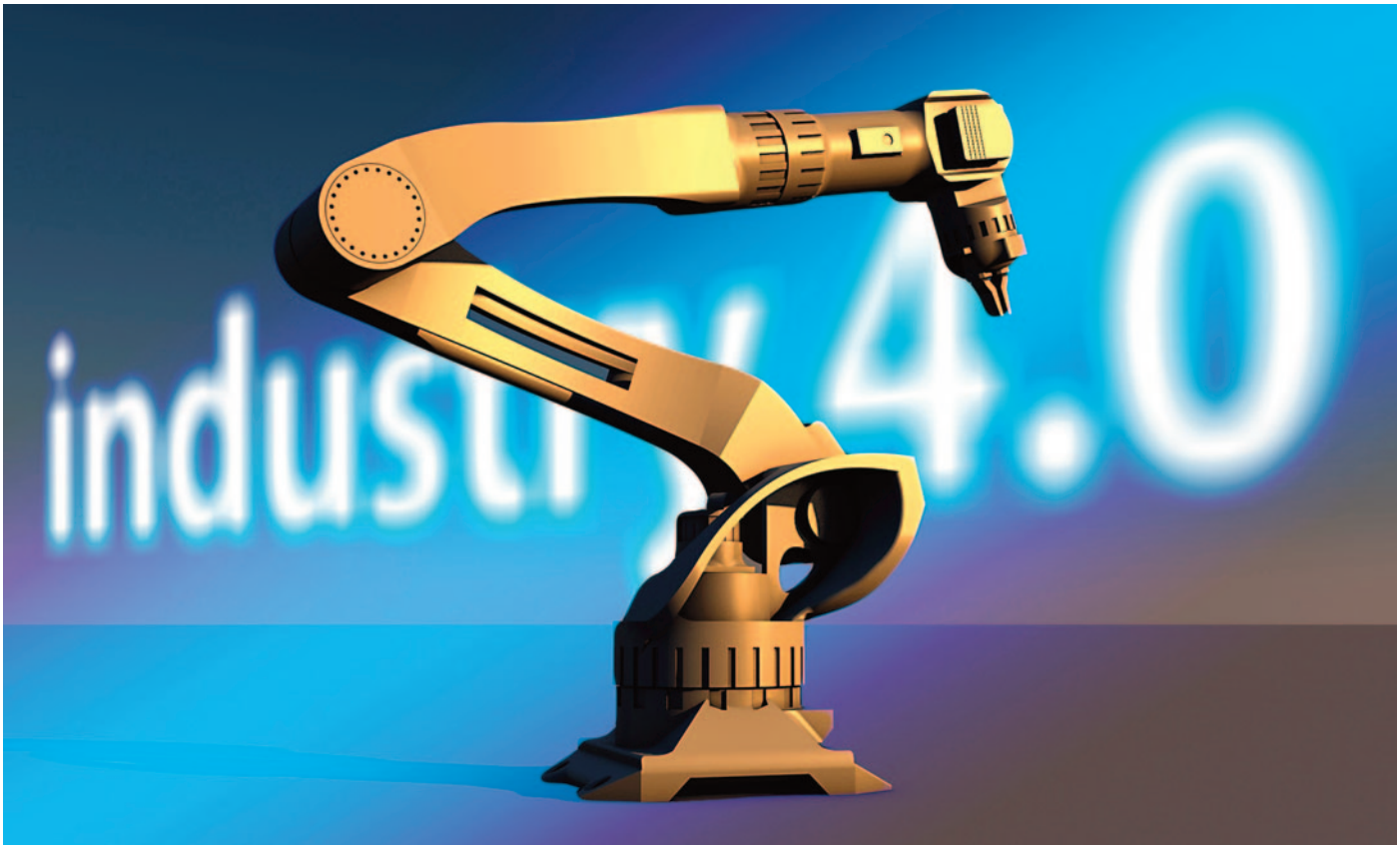


Die Angst vor KI ist bei IT-Fachkräften größer

F: Wie besorgt sind Sie darüber, dass KI-Tools wie ChatGPT, Bard und Bing Chat in den nächsten fünf Jahren Ihren Arbeitsplatz übernehmen könnten?



DOWNLOAD Möglichkeit für die Umfragen
Everywhere Work 2023 + Digital Employee Experience 2023
www.ivanti.com/de/lp/solutions/assets/s1/2023-dex-report-ai-revolution



Innovationen in der Fertigung – Die wichtigsten Trends für 2024

KI, Smart Factories und 4D-Druck: Björn Klaas, Vice President and Managing Director von Protolabs Europe, gibt seine zentralen Einschätzungen zu den Fertigungstrends für 2024 ab

Protolabs, globaler Fertigungsspezialist, gibt zum Jahresabschluss einen Ausblick auf die zentralen und bestimmenden Fertigungstrends, die die Fertigungsindustrie im kommenden Jahr erwarten werden. Geopolitische Spannungen, anhaltende Unterbrechungen der Lieferketten, steigende Kosten, neue Anforderungen an die Arbeitskräfte und Nachhaltigkeitsziele haben im vergangenen Jahr ein Gefühl der Dringlichkeit und Notwendigkeit von Innovationen in der Fertigung geschaffen und werden dementsprechend auch 2024 zentral für künftige Entwicklungen sein. Zugleich nehmen aber auch neue Technologien und Fertigungsmethoden einen entscheidenden Einfluss auf die Trends von 2024 – wie auch anhand der Trendprognose von Protolabs erkannt werden kann.

Mit KI & Smart Factories neue Ziele verwirklichen

Laut Protolabs wird 2024 der Übergang zu intelligenten Fabriken mit einer stärkeren Integration von KI, 5G, Internet der Dinge (IoT), Datenanalyse und Cloud Computing erfolgen. Dies wird unter anderem zahlreiche Vorteile wie Kosteneinsparungen, aber auch die Steigerung der Produktqualität, Sicherheit und Nachhaltigkeit mit sich bringen. Während 2023 ein Rekordjahr für die Implementierung von 3D-Druckern und additiver Fertigung innerhalb der Industrie darstellte, werden im kommenden Jahr die Effizienz, Geschwindigkeit und die vermehrt zu beobachtenden konkreten Anwendungsfälle von KI einen zusätzlichen Schub für die additive Fertigung auslösen. „Traditionell wurde die additive Fertigung besonders zur Herstellung von Prototypen benutzt", erklärt Björn Klaas, Vice President and Managing Director von Protolabs Europe. „Was wir derzeit beobachten können, ist allerdings, dass immer mehr Unternehmen auch reguläre Bauteile, die schlussendlich im fertigen Produkt verbaut werden, fertigen lassen. Eine besondere Rolle spielen dabei der Metall-3D-Druck und immer modernere Druckverfahren – aber eben auch die Anwendung von KI, die diese Entwicklung weiter vorantreiben wird."

Dezentralisierte Betriebe contra Lieferkettenschwierigkeiten

Eine weitere Prognose, die Protolabs und Björn Klaas für das kommende Jahr ausmachen, ist die stärkere Fokussierung der Industrie auf dezentralisierte Betriebe. Nicht

zuletzt dadurch, dass die Herstellung von Produkten so nah wie möglich an ihrem Verwendungsort zahlreiche Vorteile bietet, können hierbei lange Transportwege für Teile und Produkte vermieden werden. Unternehmen werden so dabei unterstützt, Unsicherheiten in Bezug auf die Lieferkette zu überwinden.

„Dadurch, dass die unterschiedliche Verfügbarkeit von Ressourcen, Spezialisierungen auf einzelne Fertigungsprozesse und bestehende gewachsene Lieferketten es nicht immer ermöglichen mit lokalen Einrichtungen oder Lieferanten zusammenzuarbeiten, erscheint diese Prognose zunächst kontrainduktiv", erklärtBjörn Klaas. „Dennoch ermöglicht eine engere Kooperation mit lokalen Partnern Unternehmen es, flexibler zu sein und schneller auf sich ändernde Kundenbedürfnisse und Markttrends zu reagieren. Hersteller werden daher 2024 zunehmend einen hybriden Ansatz verfolgen, bei dem sie je nach Bedarf sowohl eine zentrale Fabrik als auch ein Netz lokaler Einrichtungen nutzen können." Untermauert wird dieser Trend durch den 2023 erschienenen The Balancing Act Report von Protolabs, in dem rund 55 Prozent der Hersteller angaben, auch Alternativen wie „Friendly Shoring" in Betracht zu ziehen. Darunter versteht man das Verlagern von Lieferketten und Produktion in Länder, welche ähnliche Werte und eine ähnliche Kultur wie das eigene Heimatland aufweisen.

Seite an Seite mit Cobots – die Zukunft der Arbeitskraft?

Zweifellos verändern KI und andere Technologien wie Cobots die Art und Weise, wie Arbeit verstanden und gelebt wird – die Studie von Protolabs zeigt allerdings auch auf, dass die Befragten die menschliche Kreativität als entscheidendes Element für Innovationskraft ausmachen. Mehr als die Hälfte der Befragten (56 Prozent) glaubt, dass Cobots die Produktivität der Mitarbeiter steigern werden, und 57 Prozent sagen, dass sie eine bessere Ideenfindung unterstützen werden. Während Cobots repetitive und schwere Aufgaben übernehmen, können sich Mitarbeiter dementsprechend auf kreativere Aspekte ihrer Arbeit konzentrieren. „Der sich immer stärker verschärfende Fachkräftemangel zeigt klar auf, dass Mitarbeitende nach wie vor höchste Relevanz für Unternehmen haben", führt Björn Klaas aus. „Unternehmen müssen sich anpassen, um Talente anzuziehen und zu halten. Neben einer verstärkten Konzentration auf eine stärkere Unterstützung durch Cobots und Robotik in den Fabrikhallen sind auch andere moderne Revolutionen innerhalb der Arbeitswelt Ansätze, um hier die Produktion der Zukunft zu gestalten."

Neue Materialien – 3D bis 4D

Soft-Robotik und neue Materialien werden in den nächsten fünf Jahren den größten Einfluss auf die Entwicklung der Fertigung haben, wie der Statusbericht 2023 zur Roboterfertigung von Protolabs, zeigt. Für die Soft-Robotik, z. B. Greifer, die es Robotern ermöglichen, mehr logistische Aufgaben zu übernehmen, wird zwischen 2022 und 2027 eine jährliche Wachstumsrate von 35,1 Prozent erwartet, wobei vorrangig Biomedizin, Lebensmittel und Landwirtschaft davon profitieren werden. Zu Bedenken gilt dabei, dass der Einsatz neuer Materialien und Technologien zusätzliche Iterationen zur Prüfung und Verfeinerung erfordern wird, so dass die digitale Fertigung ein Schlüsselelement zur Beschleunigung dieses Entwicklungszyklus ist.

Neue Materialien werden auch in formverändernden Systemen, auch bekannt als 4D-Druck, eingesetzt werden. Durch die Verwendung reaktionsfähiger Materialien, die auf äußere Einflüsse wie Wärme, Licht, Feuchtigkeit, elektrischen Strom oder Druck reagieren, können 4D-gedruckte Objekte ihre Form oder Eigenschaften verändern.

„Bereits heute zeigen zahlreiche Beispiele aus der Forschung – aber auch tatsächlich Anwendungsgebiete – wie revolutionär diese Technologie ist", erklärt Björn Klaas, Vice President and Managing Director von Protolabs Europe. „Dass entsprechende Anwendungen in 2024 an Bedeutung gewinnen werden, ist dementsprechend ein Trend mit dem zu rechnen ist!"

Beispiele für die Entwicklung dieser Systeme sind:

- Luft- und Raumfahrt: 4D-gedruckte Drohnenflügel, die sich als Reaktion auf Stimuli um bis zu 20 Grad biegen können, was die Effizienz erheblich verbessert
- Medizintechnik: Implantate, die sich mit der Zeit an den Körper eines Patienten anpassen
- Intelligente Textilien, die ihre Atmungsaktivität an die Luftfeuchtigkeit anpassen
- Komponenten in einem Sanitärsystem, die sich als Reaktion auf Temperaturschwankungen ausdehnen oder zusammenziehen

Nachhaltigkeit als Motor der Innovation

„Nachhaltigkeit hat in der Fertigung nach wie vor oberste Priorität, sowohl bei den Verfahren der Unternehmen als auch bei den von ihnen hergestellten Produkten", erklärt Björn Klaas. „Branchen wie die Luft- und Raumfahrt, die Automobilindustrie und der Energiesektor haben gesetzliche Ziele zu erreichen, wie z. B. den Netto-Nullverbrauch bis 2050, so dass sich ein Großteil ihrer Produktentwicklung auf die Reduzierung von Kohlendioxid und die Integration hocheffizienter Technologien konzentriert." Protolabs eigene Studie mit 450 Führungskräften aus dem verarbeitenden Gewerbe zeigt, dass Nachhaltigkeit ein wichtiger Motor für Innovationen und ein Hauptgrund für Hersteller ist, neue Produkte zu entwickeln. Die digitale Fertigung spielt dabei eine wichtige Rolle, da sie eine lokalisierte Produktion ermöglicht und zu weniger Abfall führt.

„Dementsprechend – und das kann kaum genug unterstrichen werden – ist Nachhaltigkeit für die Industrie 2024 und auch in den folgenden Jahren eines der wichtigsten Themen. Für Protolabs ist klar, dass wir für unsere Partner und Kunden hier auch im kommenden Jahr als exzellenter und nachhaltiger Fertigungsdienstleiser zur Verfügung stehen werden", führt Björn Klaas abschließend aus.

Weitere Einblicke in die zentralen Prognosen für 2024, erhalten Sie in der aktuellen Studie von Protolabs.

5 Chancen, die Cyber Security Unternehmen bietet

Cyber Security wird in Unternehmen zunehmend zum Schlüsselthema. Das ist auch gut so, denn die Bedrohungslage verschärft sich weiterhin und macht einen guten Schutz vor Cyber-Angriffen immer wichtiger. Die neue Lünendonk Studie 2023 zeigt: 84 Prozent der befragten Betriebe schätzen die Bedrohungslage höher ein als noch 2022. 85 Prozent der Befragten sehen Cyber Security als festen Bestandteil der digitalen Transformation.

Einige Betriebe schrecken allerdings weiterhin vor Investitionen zurück und sehen Cyber Security als Bremsklotz. Dabei können sich durch eine durchdachte Cyber-Security-Strategie auch neue Chancen eröffnen.

1. Reputation stärken und Vertrauen erhöhen

Immer öfter berichten Medien über Datenlecks und Angriffe auf Unternehmen jedweder Größe. Dies führt dazu, dass die Awareness für Cyber Security steigt und wichtige Daten nur jenen Unternehmen anvertraut werden, die ein gutes, etabliertes Sicherheitskonzept vorweisen können. Ein ganzheitlicher Ansatz stärkt also die Reputation und erhöht das Vertrauen in Dienstleistungen und Produkte.

2. Rechtliche Anforderungen erfüllen

Die Sensibilität ist längst auch auf höherer Ebene angekommen. Immer mehr Cyber-Security-Regularien werden international oder europaweit erlassen. Unternehmen müssen sich vermehrt mit NIS2, Radio Equipment Directive (RED) oder dem europäischen Cyber Resilience Act (CRA) auseinandersetzen. Auch branchenspezifische Regularien wie das Rahmenwerk TIBER-EU für den Bankensektor werden fortlaufend verschärft. Datenschutz und digitale Sicherheit gewinnen dadurch zunehmend an Bedeutung. Setzen Betriebe bereits jetzt auf eine robuste Cyber Security und erfüllen die Anforderungen der Regularien direkt, vermeiden sie potenzielle Strafen und sparen sich zukünftig Aufwand.

3. Innovationen fördern

Auch für die digitale Transformation in Unternehmen sowie für das Entwickeln neuer Produkte und Services rückt das Thema Cyber Security immer stärker in den Fokus. Zentral ist sie von Beginn an in die Produkt- und Serviceentwicklung einzubeziehen. So gelingt es, neue und innovative Lösungen zu entwickeln, die sich ohne Gefahr betreiben und nutzen lassen. Ein robustes Cyber Security Framework kann zusätzlich Innovationen fördern, indem ein sicheres Umfeld zur Erprobung neuer Technologien geschaffen wird.

4. Von künstlicher Intelligenz und maschinellem Lernen profitieren

Cyber Security kann dazu beitragen, Daten im Unternehmen sicher zu sammeln, zu speichern und zu verarbeiten. Das bietet Betrieben die Chance, von künstlicher Intelligenz (KI) und maschinellem Lernen (ML) zu profitieren. Durch den sicheren Zugang zu den enormen Datenmengen eröffnen sich neue Innovationsbereiche, die Prozesse automatisieren und dadurch Tätigkeiten produktiver machen.

5. Weitere Geschäftsfelder erkunden

Der Einsatz von Cloud-Lösungen ermöglicht es Unternehmen, eine breite Masse an digitalen Dienstleistungen zu nutzen. Darüber hinaus bietet sie die Grundlage für neue und produktive Arten der Zusammenarbeit. Ohne den richtigen Schutz vor Angriffen ist die Cloud-Nutzung jedoch oft zu riskant. Unternehmen schrecken vor ihr zurück und Innovationspotenziale bleiben ungenutzt. Cyber Security hingegen bietet Unternehmen die Chance, durch die Cloud neue Geschäftsfelder zu erkunden.

Wie Unternehmen vorgehen sollten

Jedes Unternehmen wird früher oder später von einem Cyberangriff betroffen sein, daher sind verstärkte Cyber-Security-Maßnahmen unumgänglich. Risiken lassen sich minimieren, indem Firmen sich über neueste Angriffsmethoden informieren.
Zudem sollten Sicherheitsteams technische und organisatorische Schutzmaßnahmen fortlaufend überprüfen und aktualisieren. Prävention aufseiten der Mitarbeitenden ist für gute Cyber Security ebenso essenziell. Denn sollte die Technik versagen, sind diese besonders wichtig. Durch wachsame Mitarbeitende und eine robuste Sicherheitskultur lassen sich Angriffe teilweise frühzeitig erkennen und abwehren. Fehlen jedoch die notwendigen Fachkräfte oder Ressourcen, können Managed Security Services die Lösung sein.

Mit Anbietern wie Axians reduzieren sich die Aufwände in Unternehmen und IT-Abteilungen können ihre Kapazitäten nutzen, um das Tagesgeschäft aufrecht zu erhalten. Doch Investitionen in Cyber Security sind nicht nur passive Kostentreiber. Mit einer durchdachten Sicherheitsstrategie können Unternehmen auch Innovationen fördern, neue Technologien und Tools nutzen und weitere Geschäftsmodelle und -felder für sich erschließen – und so in einem volatilen Business-Umfeld für Stabilität und Zukunftssicherheit sorgen.

Marketsandmarkets.com

Große Wachstumschancen

Der globale Markt für Verkehrsmanagement wird bis 2028 auf 72 Milliarden Dollar anwachsen. Laut Marketsandmarkets wird erwartet, dass der Markt für Verkehrsmanagement bis 2028 72,5 Mrd. USD erreichen wird, ausgehend von 42,3 Mrd. USD im Jahr 2023, mit einer CAGR von 11,4 % zwischen 2023 und 2028.

Die Einführung von Verkehrsmanagement hat in den letzten Jahren einen bemerkenswerten Aufschwung erlebt, da Regierungsinitiativen auf der ganzen Welt die Bedeu- tung eines effektiven Verkehrsmanagements erkannt haben, was zu Investitionen in Technologien und zur Formulierung von Plänen für intelligente Stadtverkehre geführt hat. Diese Initiativen zielen darauf ab, den Verkehrsfluss zu verbessern, Staus zu reduzieren und öffentliche Verkehrsmittel als Teil eines ganzheitlichen Ansatzes zur Bewältigung der städtischen Mobilitätsprobleme zu fördern. Bei der Entwicklung von Smart Cities werden verschiedene Technologien wie Sensoren, Kameras, Datenanalyse und künstliche Intelligenz eingesetzt, um das Verkehrsmanagement zu revolutionieren.

Routenführung und -optimierung

Routenführungssysteme nutzen Echtzeitdaten, einschließlich Verkehrsbedingungen und Staumuster, um den Fahrern dynamische und personalisierte Navigationsanweisungen zu geben. Indem sie optimale Routen auf der Grundlage der aktuellen Verkehrssituation anbieten, tragen diese Systeme dazu bei, die Reisezeit zu minimieren, Staus zu reduzieren und die Gesamtauslastung des Straßennetzes zu verbessern.

Darüber hinaus spielen Algorithmen zur Routenoptimierung eine entscheidende Rolle bei der strategischen Verkehrsmanagementplanung, indem sie historische und Echtzeitdaten analysieren, um die effizientesten Routen für verschiedene Fahrzeugtypen zu ermitteln.

Durch die Berücksichtigung von Faktoren wie Verkehrsdichte, Straßenkapazität und Alternativrouten hilft die Routenoptimierung bei der proaktiven Steuerung des Verkehrsflusses, der Reduzierung von Engpässen und der Förderung eines reibungsloseren Verkehrsablaufs für Pendler. Zusammengenommen spielen die Technologien zur Routenführung und -optimierung eine zentrale Rolle bei der Entwicklung intelligenter und reaktionsschneller Verkehrsmanagementlösungen, die zu einer verbesserten Mobilität und einer nachhaltigeren städtischen Umwelt beitragen.

Adaptive Verkehrssteuerungssysteme

Ein adaptives Verkehrsleitsystem (ATCS) ist eine hochentwickelte Verkehrsmanagementlösung, die dynamisch auf Echtzeit-Verkehrsbedingungen reagiert und die Signalzeiten an Kreuzungen optimiert. Im Gegensatz zu herkömmlichen Verkehrssignalsystemen mit festen Zeiten nutzt ATCS ein Netzwerk von Sensoren, Kameras und Datenanalyse, um den Verkehrsfluss kontinuierlich zu überwachen. Dieses System passt die Signalzeiten in Echtzeit an, basierend auf Faktoren wie dem Verkehrsaufkommen, dem Grad der Verkehrsüberlastung und den sich im Laufe des Tages ändernden Mustern.

Durch die dynamische Anpassung an die aktuelle Nachfrage zielt ATCS darauf ab, Verkehrsverzögerungen zu reduzieren, Staus zu minimieren und die allgemeine Verkehrseffizienz zu verbessern. Das ATCS spielt eine zentrale Rolle im Verkehrsmanagement und bietet einen reaktionsschnellen und intelligenten Ansatz zur Bewältigung der komplexen Probleme der städtischen Mobilität. Es trägt dazu bei, einen reibungsloseren Verkehrsfluss zu schaffen, die Reisezeiten zu verkürzen, die Verkehrssicherheit zu erhöhen und letztlich die Leistung der Verkehrsnetze in städtischen Gebieten zu optimieren.

Staus als großes Problem in Asien

Im asiatisch-pazifischen Raum, in dem fast 40 % der Weltbevölkerung leben, werden verschiedene Verkehrsmanagementtechnologien eingesetzt.

Schnell wachsende Länder wie China, Indien und Südkorea haben mit Staus und Bevölkerungsexplosion zu kämpfen, während kleinere und hochtechnisierte Inseln wie Singapur und Japan ein anderes Szenario darstellen. In Thailand sind die schweren Verkehrsstaus darauf zurückzuführen, dass die Bürger für den städtischen Verkehr stark auf das Auto angewiesen sind.
In der Region befinden sich die am stärksten verstopften Städte der Welt, wobei sechs der zehn größten Städte in Asien liegen. Beispiele hierfür sind Bengaluru in Indien und Manila auf den Philippinen.

Die laufenden Verkehrsmanagementprojekte in Asien, wie das Gateway WA Perth Airport and Freight Access Project in Australien und das Smart City Kochi Projekt in Indien, sind ein Beispiel für die Bemühungen der Region, bestehende Verkehrssysteme zu ersetzen und zu verbessern.

Es wird erwartet, dass diese Initiativen den Verkehrsmanagementmarkt im asiatisch-pazifischen Raum, in dem verschiedene Technologiedienstleister bereits Lösungen anbieten, erheblich beeinflussen werden.

Datenexplosion, KI und Vorschriften

Prognosen für die Cybersicherheit

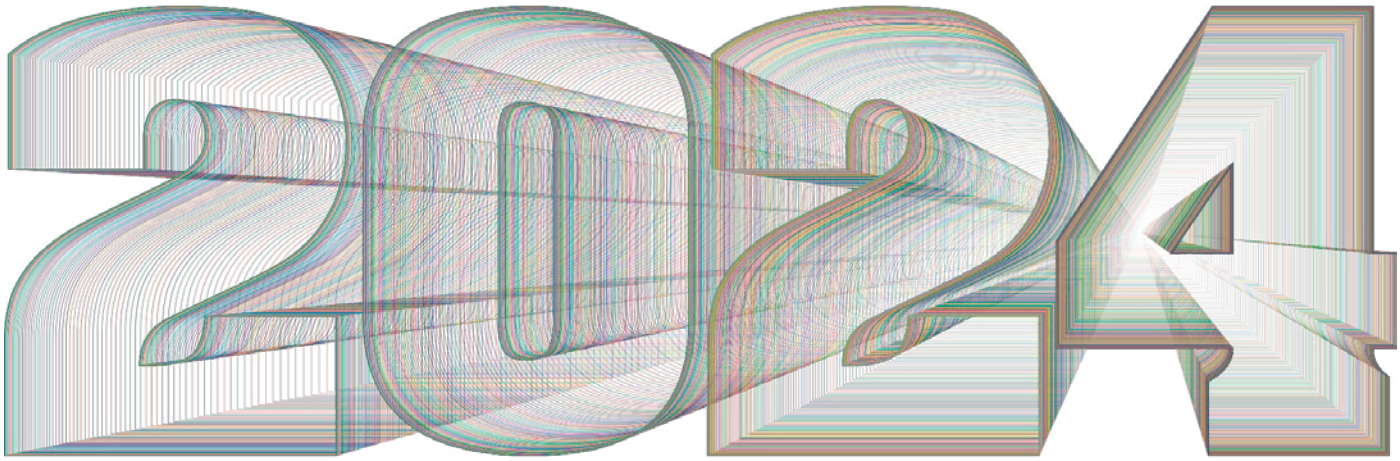
Das Jahr 2024 hält für die Cybersicherheit zahlreiche Herausforderungen bereit. Die Bedrohungslandschaft entwickelt sich weiter: Von der exponentiellen Zunahme von Daten und Angriffen auf virtualisierte Infrastrukturen über neue Regularien bis hin zur Rolle der künstlichen Intelligenz (KI). Nachfolgend fünf Entwicklungen, die dazu beitragen, dass sich die Cybersicherheitslandschaft im kommenden Jahr nachhaltig verändern könnte.

1 Neue Sicherheitsstrategie aufgrund der Datenexplosion

Prognosen des neuen Rubrik Zero Labs Reports gehen davon aus, dass die Menge an Daten, die ein Unternehmen sichern muss, im Jahr 2024 um 42 Prozent steigen und sich in den nächsten fünf Jahren sogar versiebenfachen wird. Das ist auf die zunehmende Verbreitung von datenerzeugenden Geräten und die Nutzung von künstlicher Intelligenz zurückzuführen.

Unternehmen stehen vor der Herausforderung, diese Daten in einer schnell wachsenden und sich stetig verändernden Umgebung zu sichern. Für viele Unternehmen wird der Schwerpunkt bei der Cybersicherheit im nächsten Jahr daher darauf liegen, in Cloud- und SaaS-Umgebungen dieselbe Transparenz und Übersicht über ihre Daten zu erlangen, die sie bereits in lokalen Umgebungen erzielen können. Denn: Bei der modernen Cybersicherheit geht es nicht mehr um den Schutz einzelner Schlösser, sondern um eine miteinander vernetzte Karawane.

Während die wertvollen Kronjuwelen, im heutigen Fall die Daten, früher in den



Schlössern versteckt waren, sind sie nun über die gesamte Karawane verteilt – was das gesamte Sicherheitskonstrukt verändert.

2 Angriffe auf virtualisierte Infrastrukturen

Da Unternehmen ihre traditionellen Ziele wie Computer und mobile Geräte immer besser schützen, verlagern einige böswillige Akteure ihre Angriffe bereits auf virtualisierte Infrastrukturen wie SaaS- und Linux-Anwendungen, APIs und Bare-Metal-Hypervisoren.

Ein Beispiel dafür ist die massive Angriffswelle auf die Virtualisierungsplattform VMware ESXi Anfang 2023, aufgrund der das Bundesamt für Sicherheit in der Informationstechnik sogar die zweithöchste Bedrohungslage „3 / Orange" ausgerufen hatte. Zum einen bieten diese Angriffe den Angreifern Vorteile hinsichtlich Geschwindigkeit und Umfang. Zum anderen ist die Cyberkriminalität eine „Mitläufer"-Wirtschaft, die schnell bekannte Er- folgsstrategien adaptiert. Deshalb werden wir im Jahr 2024 voraussichtlich noch mehr Vorfälle dieser Art sehen.

3 Edge-Geräte als Ziel staatlicher Hackergruppen

Von Regierungen unterstützte Hacker-Gruppierungen sehen in Edge-Geräten eine Möglichkeit, sich von gewöhnlichen Ransomware-Banden abzuheben. Ein bekannter Fall ist die mit China in Verbindung stehende Gruppierung BlackTech. Diese verwendete gestohlene oder schwache Anmeldeinformationen mit Administratorenrechten, um Cisco-Router zu kompromittieren und schwer zu entdeckende Hintertüren zur Aufrechterhaltung ihres Zugangs zu installieren.

Diese Art des Eindringens erfordert beträchtliche technologische Fähigkeiten und kann großen Schaden anrichten. Staatliche Gruppen könnten diesen Edge-Zugang sogar vor anderen cyberkriminellen Gruppen „verteidigen", um ihren heimlichen Zugriff nicht zu verlieren. Edge-Geräte werden damit auch im kommenden Jahr eine wichtige Front im Bereich der Cybersicherheit bilden.

4 Vormarsch der KI

Seit ChatGPT öffentlich verfügbar ist, hat die Menge an Phishing-Mails um 1.265 Prozent zugenommen. Künstliche Intelligenz wird im Jahr 2024 eine noch zentralere Rolle in der Cybersicherheit spielen – sowohl für die Angreifer als auch für die Verteidiger. Bösartige Akteure werden KI nutzen, um Angriffe zu automatisieren, schnell neue Malware zu generieren und die Effektivität von Social-Engineering-Kampagnen weiter zu steigern. Die „Guten" werden KI in ihre Cybersicherheitsstrategien integrieren, um Bedrohungen effektiver zu erkennen und abzuwehren. KI wird außerdem an Bedeutung gewinnen, um den Fachkräftemangel in der Cybersicherheit abzufedern.

5 Erhöhter Druck durch neue Regularien

Die Klage der US-Börsenaufsicht SEC gegen SolarWinds und seinen Chief Information Security Officer (CISO) wegen nicht gemeldeter Cyberrisiken zeigt: Sowohl CISOs als auch das gesamte C-Level werden aufgrund neuer Vorschriften und Meldepflichten im nächsten Jahr verstärkt unter Druck stehen. Mit Blick auf DORA, NIS2 und EHDS müssen CISOs ihre Organisation nicht nur gegen bösartige Akteure schützen, sondern auch die Einhaltung dieser strengeren Vorschriften sicherstellen.

Fazit

2024 wird die Welt der Cybersicherheit weiter in Atem halten. Wenn Unternehmen diese Entwicklungen auf ihrem Radar haben und die entsprechenden Vorbereitungen treffen, sind sie dem Aufbau einer echten Cyberresilienz fünf Schritte näher gekommen.

Über den Autor: Seit über 20 Jahren ist Frank Schwaak als Data Protection und Recovery Spezialist tätig. Der Schwerpunkt seiner Arbeiten bei verschiedenen Herstellern wie der SEP AG und Commvault lag in der Sicherung und Wiederherstellung von Relationalen Datenbanken. In seiner Karriere war er in den Abteilungen Technical Enablement/Training, Professional.

VicOne, Anbieter von Cybersicherheitslösungen für die Automobilindustrie, hat heute seinen VicOne Automotive Cyberthreat Landscape Report 2023 vorgestellt. Der umfassende jährliche VicOne Bericht über Cyberbedrohungen in der gesamten Automobilbranche basiert auf Daten von Automobil-Erstausrüstern (OEMs), Zulieferern und Händlern weltweit und enthält folgende Hauptpunkte:

- **Den Hinweis auf eine wachsende Nutzung und Monetarisierung von Automobildaten - und damit einhergehend die Gefahr der Ausnutzung durch Cyberkriminelle**
- **Eine Auflistung von cyberbasierten Trends und Vorfällen, die in diesem Jahr die Automobilindustrie bedroht haben**
- **Prognosen zu kommenden Gefahrenpotenzialen und wie eine effektive Cybersicherheitsstrategie für das nächste Jahr und darüber hinaus gewährleistet werden kann**

„Bei unserer Analyse der Bedrohungslandschaft haben wir festgestellt, dass die Verluste der Automobilbranche durch Cyberangriffe in der ersten Jahreshälfte mehr als 11 Milliarden US-Dollar betrugen, was einen noch nie dagewesenen Anstieg im Vergleich zu den letzten beiden Jahren darstellt", heißt es im VicOne Automotive Cyberthreat Landscape Report 2023. „Bei näherer Betrachtung zeigt sich, dass diese Cyberattacken vor allem auf Automobilzulieferer abzielten, was auf ein steigendes Gefährdungspotenzial in diesen Bereichen hindeutet. Alarmierend ist, dass über 90 % dieser Angriffe nicht auf die OEMs selbst, sondern auf andere Unternehmen in der Lieferkette abzielten. Für cyberkriminelle Angreifer ist es oft schwierig, in gut geschützte Unternehmen einzudringen, weshalb sie stattdessen weniger wachsame Firmen ins Visier nehmen. Die OEMs sind aufgrund der Unterbrechung ihrer Lieferkette aber trotzdem betroffen. Folglich geht es bei der Verteidigung von Systemen

Cyberbedrohungen für die Automobilindustrie

Neuer VicOne Sicherheitsbericht deckt Cyberbedrohungen für die Automobilindustrie auf und schlägt effektive Schutzstrategien vor

Der VicOne „Automotive Cyberthreat Landscape Report 2023" identifiziert die Lieferkette als Hauptziel der zunehmenden Cyberangriffe auf die Automobilindustrie

gegen Cyberangriffe nicht mehr nur um die Sicherung eines einzelnen Unternehmens, sondern um die Stärkung und den Schutz der gesamten Lieferkette."

Der neue VicOne-Bericht befasst sich demzufolge mit den Problemen der Cybersicherheit, die mit der zunehmenden Komplexität von Fahrzeugen aufgrund des Einsatzes verbesserter Konnektivität und Automatisierung sowie dem Aufkommen fortschrittlicher Fahrerassistenzsysteme (Advanced Driver Assistance Systems, ADAS) einhergehen. Er zeigt, dass die Verluste in der Branche durch Cyberangriffe mittels Ransomware und die Enthüllung sensibler Geschäftsdaten oder personenbezogener Informationen (PII) sowie durch Kosten im Zusammenhang mit Systemausfällen steigen. Die Berechnungen im VicOne Automotive Cyberthreat Landscape Report 2023 basieren nur auf den entstandenen materiellen Kosten im Zusammenhang mit beschädigter oder blockierter Technologie und Unterbrechungen des Produktionsbetriebs und nicht auf immateriellen Kosten der Cyberangriffe wie Markenpflege, Öffentlichkeitsarbeit, Vertriebs- und Marketingausgaben.

Der Bericht identifiziert die wichtigsten Sicherheitslücken, durch die Fahrzeugdaten kompromittiert werden können, und listet die Schwachstellen der sogenannten Common Weakness Enumeration (CWE) in Tabellen auf. Zu den häufigsten von VicOne dokumentierten Sicherheitslücken gehören Fehlfunktionen wie Out-Of-Bounds Write (OOBW), Out-Of-Bounds Read (OOBR), Buffer Overflow, Use after Free-Schwachstellen und falsche Eingabevalidierungen. Die meisten Sicherheitslücken wurden in Chipsätzen oder Systems-on-Chip (SoCs) Schaltkreisen gefunden, gefolgt von Schwachstellen in Managementanwendungen von Drittanbietern und Infotainment-Systemen in Fahrzeugen (In-Vehicle Infotainment, IVI). Drittanbieter wie Logistikunternehmen, Servicedienstleister und Komponenten-, Zubehör- oder Teilehersteller, sind zunehmend ins Visier von Hackern geraten.

Der VicOne-Bericht enthält Fallstudien zu einigen der wichtigsten Angriffsmuster des letzten Jahres. Zu nennen sind hier etwa die Zenbleed-Schwachstelle, die zum Abfluss sensibler Daten mit der bemerkenswert hohen Geschwindigkeit von 30 kB/s pro Computerkern führen kann, die sogenannte CAN-Bus-Injektion, die sich zu einer beliebten Technik unter Fahrzeugdieben entwickelt hat, und das Eindringen in die Backend-Cloud-Infrastruktur durch Ausnutzung von Schwachstellen in Telematiksystemen und Programmierschnittstellen (API - Application Programming Interface).

Der VicOne-Bericht stellt zwar fest, dass es derzeit an Regularien zum Schutz von Fahrzeug- und Fahrerdaten mangelt, weist aber darauf hin, dass die UN Regelung R155 bis Juli 2024 Vorschriften zur Cybersicherheit für neu hergestellte Fahrzeuge vorsieht.

„Es ist klar, dass die Automobilindustrie der Cybersicherheit eine höhere Priorität einräumen muss, was die Ressourcen und das Budget angeht.

Das ist etwas, das kontinuierlich geschehen muss und umfasst mit dem Aufbau der Prozesse, der Organisation und der Talente den Aufbau eines gesamten Systems - oder man wird nie in der Lage sein, Cybersicherheit effektiv zu implementieren", erklärt Max Cheng, Chief Executive Officer von VicOne. „Es ist höchste Zeit, dass sich Unternehmen in der gesamten globalen Automobilindustrie jetzt ernsthaft mit der Frage beschäftigen, wie sie ihre Fähigkeiten in den wichtigen Schwerpunktbereichen, die unser neuer Cybersecurity-Bericht abdeckt, ausbauen können."

Der gesamte VicOne Automotive Cyberthreat Landscape Report 2023 kann in Englisch unter https://vicone.com/reports/automotive-cybersecurity-report-2023 heruntergeladen werden.

Hier finden Sie die deutschen Landing Pages mit Zusammenfassungen: https://vicone.com/de-reports/automotive-cybersecurity-report-2023 sowie https://vicone.com/de-research/the-road-ahead-is-paved-with-risky-data

Digital-Wunschzettel 2024

76% der Deutschen unzufrieden mit Fortschritt der Digitalisierung

ExpertInnen wie Sascha Lobo, Corinna Enders und Aya Jaff äußern ihre Wünsche zu Vernetzung, Energie und KI

- **Eine neue Cisco-Umfrage zeigt, dass drei Viertel der deutschen Verbraucher mit dem Fortschritt der Digitalisierung in Deutschland unzufrieden sind.**
- **Die Befragten wünschen sich Verbesserungen bei Bildung & Verwaltung (62%), IT-Sicherheit (42%) und Gesundheitswesen (34%).**
- **Digital-ExpertInnen wie Sascha Lobo, Corinna Enders, Aya Jaff, Prof. Yasmin Weiß, Prof. Dr. Christian Dörr und Franziska Teubert verraten, worauf es ihrer Meinung nach ankommt.**

Ob Künstliche Intelligenz, Cybersecurity oder Homeoffice: Digitale Lösungen haben Deutschland und die Debatten im Land 2023 massiv geprägt. Dabei ist häufig zu hören, dass Deutschland unter seinen Möglichkeiten bleibt. Das bestätigt eine Umfrage von Civey im Auftrag von Cisco unter mehr als 5.000 Deutschen Verbrauchern. Passend zum Nikolaustag teilen deutsche Digital-ExpertInnen auch ihre Wünsche für ein digitales 2024.

Laut der Umfrage sind 76 Prozent der Befragten mit dem Fortschritt der Digitalisierung in Deutschland unzufrieden, weitere 77 Prozent sehen Deutschland im internationalen Vergleich im unteren Drittel oder auf dem letzten Platz der bei der Digitalisierung.
Weniger als 3 Prozent sehen Deutschland als führend in der Digitalisierung und 18

Prozent stufen Deutschland im Mittelfeld ein.

Zum Vergleich: Dieselbe Frage wurde vor fünf Jahren noch etwas positiver beatwortet. 2018 sahen immerhin noch etwas mehr als 7 Prozent Deutschland bei der Digitalisierung im globalen Vergleich im oberen Drittel, 25 Prozent im Mittelfeld und nur 62 Prozent im unteren Drittel. Das deutet auf einen negativen Trend in der Wahrnehmung des deutschen Digitalisierungsfortschritts hin.
„Die Digitalisierung bringt entscheidende Vorteile für Deutschland, aber wir müssen schneller und unkomplizierter werden, um den Fortschritt zu beschleunigen," sagt Uwe Peter, Chef von Cisco in Deutschland. „Technologie hat uns in den letzten Jahren angesichts des enormen Wandels erhebliche Vorteile gebracht. Ohne Videokonferenzen wäre Deutschland beispielsweise nicht durch die Pandemie gekommen. Die Erfahrungen, den Pragmatismus und die Investitionsbereitschaft aus dieser Zeit brauchen wir wieder. Sonst verlieren wir den Anschluss."

Der Digital-Wunschzettel für 2024

Aber was benötigt Deutschland 2024, um bei der Digitalisierung voll durchzustarten? Der Wunschzettel der befragten Deutschen für das neue Jahr zeigt deutlich den Wunsch nach Verbesserungen in den Bereichen Bildung und Verwaltung (62%), IT-Sicherheit (42%) und Gesundheitswesen (34%). Als größte Hindernisse für mehr Digitalisierung sehen die Deutschen Bürokratie (75%), den IT-Fachkräftemangel (44%), unklare politische Zuständigkeiten (44%) und schlechtes Breitbandinternet (42%).

Und was sagen Deutschlands Digital-ExpertInnen dazu? Cisco hat dafür bei führenden Persönlichkeiten nachgefragt, die sich mit der Digitalisierung auskennen: Was wünschen Sie sich für das neue Digital-Jahr 2024?

Vollständige Verglasfaserung Deutschlands

„Für 2024 wünsche ich mir in Sachen digitale Infrastruktur und Vernetzung die vollständige Verglasfaserung Deutschlands bis in die letzte Gebirgshütte hinein. Im Endeffekt also der Wunsch nach Normalität, sprich dass in Deutschland die normalen Durchschnittswerte führender Industrieländer erreicht werden, was digitale Infrastruktur von Glasfaser bis 5G angeht." – Sascha Lobo, Autor, SPIEGEL-Kolumnist, Digital-Experte

Intelligente Vernetzung, um erneuerbare Energien effizienter zu nutzen

„Für eine zukunftsweisende Digitalisierung im Bereich Energie und Nachhaltigkeit in Deutschland im Jahr 2024 wünsche ich mir eine intelligente Vernetzung und verstärkte Integration von Smart-Grid-Technologien, um erneuerbare Energien effizienter zu nutzen.
Es ist unabdingbar, dass wir innovative digitale Lösungen vorantreiben, um die Energiewende zu beschleunigen und nachhaltige Praktiken flächendeckend zu etablieren." – Corinna Enders, Vorsitzende der Geschäftsführung der Deutschen Energie-Agentur

Regulierungsrahmen, der KI fördert und nicht hemmt

„Mein Wunsch für 2024 ist ein Deutschland, das einen klaren und flexiblen rechtlichen Rahmen schafft, der die Entwicklung und Implementierung von Künstlicher Intelligenz fördert und nicht hemmt. Eine Umgebung, in der Regulierungen Innovationen unterstützen und beschleunigen, anstatt sie zu behindern, wäre ein entscheidender Schritt für Startups und Unternehmen." – Aya Jaff, Gründerin & Autorin

Cybersicherheit als gesamtgesellschaftliche Aufgabe

„Wir als Verteidiger können nur auf Dauer erfolgreich sein, wenn wir nicht alleine dastehen. Ich wünsche mir, dass wir Cybersicherheit als gesamtgesellschaftlicher Aufgabe begegnen, Akteure zusammenbringen, Voraussetzungen für den Austausch von Informationen und gegenseitige Unterstützung schaffen, um uns gemeinsam besser schützen zu können." – Prof. Dr. Christian Dörr, Leiter des Fachgebiets Cybersecurity - Enterprise Security am Hasso-Plattner-Institut

Mehr Selbstverantwortung in Sachen KI-Kompetenz

„Ich wünsche mir für das Jahr 2024, dass wir in der Breite der Bevölkerung lernen, wie wir verantwortungsvoll und sicher mit künstlicher Intelligenz in unserer Arbeitswelt umgehen.
Es gibt viele kostenfreie Bildungsangebote hierzu, die zu wenig genutzt werden. Hier wünsche ich mir mehr Selbstverantwortung und Drive von allen, KI-Anwendungskompetenz zu erlernen und sich dies selbst zum Geschenk zu machen." – Prof. Yasmin Weiß, Professorin für künstliche Intelligenz in der Arbeitswelt, Multi-Aufsichtsrätin

Schnellere und einheitlichere Visaprozesse für Startup-Talente

„Da Startups auf die besten Köpfe angewiesen sind, stellt der Fachkräftemangel eine besonders große Herausforderung dar. Ohne internationalen Fachkräftezuwachs können wir die Lücke an Arbeitskräften nicht schließen, die durch den demographischen Wandel entsteht.
Visaprozesse müssen schneller, einheitlicher und digitaler werden, sonst können wir im Wettbewerb um die besten Talente nicht bestehen!" – Franziska Teubert, Geschäftsführerin Startup Verband

„Es mangelt in Deutschland nicht an guten Ideen zur Digitalisierung. Wir müssen das Thema mit einer guten Mischung aus Erfindergeist, Digital-First-Einstellung und einer gesunden Portion Pragmatismus angehen," ergänzt Uwe Peter.
„Eine effiziente Digitalisierung Deutschlands ist ein wichtiger Dienst an unserer Gesellschaft, keine Kostenstelle, denn sie wird unsere globale Wettbewerbsfähigkeit und den Wohlstand in Deutschland fördern. Das wünsche ich mir für 2024."

Über die Umfrage: Die Umfrage unter 5.000 Deutschen ab 18 Jahren wurde von Civey im Auftrag von Cisco vom 15. bis 17. November 2023 online durchgeführt

messe frankfurt

light+building

3. – 8. 3. 2024
Frankfurt am Main

Intelligent. Vernetzt. Sicher!

Sicherheitstechnik im Gebäude: unverzichtbar! Erfahren Sie, wie wegweisende Innovationen die Gebäudesicherheit auf ein neues Level heben.

Weltleitmesse für Licht und Gebäudetechnik

Jetzt schnell Ticket sichern!