Governance für die sichere Nutzung generativer KI in der EMEA-Region

Von Chris Novak, Senior Director, Cybersecurity Consulting, Verizon

Einleitung

Unternehmen, die sich einen Wettbewerbsvorteil verschaffen möchten, kommen um eine effektive Nutzung künstlicher Intelligenz (KI) nicht herum. Dabei können sie mitunter schon innerhalb eines Jahres einen Return on Investment verzeichnen, der sich im Durchschnitt auf knapp vier Euro für jeden investierten Euro beläuft.[1]

Wirklich meistern lässt sich die Technologie jedoch nur mit der richtigen Governance – also mit angemessenen Sicherheitsmaßnahmen und ethischen Leitlinien für den „verantwortungsbewussten" Einsatz der KI. Außerdem müssen die spezifischen Bedrohungen und Sicherheitslücken abgedeckt werden, die mit der generativen KI (GenAI) einhergehen, einschließlich technischer Aspekte, Angriffsvektoren und zuverlässiger Sicherheitsmaßnahmen.

Der Prozentsatz der KI-basierten Angriffe ist bisher noch sehr gering, aber es ist dennoch ein wichtiges Thema, da er in Zukunft durchaus steigen kann.

KI könnte zur Bewältigung der größten Probleme weltweit in so diversen Bereichen wie Gesundheitswesen, Finanzwesen, Einzelhandel, Klimaschutz, Energieversorgung, Brandschutz, Industrie 4.0 und Produktivitätssteigerung beitragen. Wir bei Verizon sehen es als eine unserer wichtigsten Aufgaben, Unternehmen bei der Nutzung von KI zur Bewältigung dieser kritischen Herausforderungen zu unterstützen.

Die Kombination aus hohen Geschwindigkeiten, geringeren Latenzen und größeren Kapazitäten von 5G und KI, Edge und Cloud-Computing ermöglicht eine schnelle und reibungslose Datenübertragung in Unternehmensnetzwerken.[2] Doch der Schutz dieser innovativen Technologien ist eine echte Herausforderung, mit der sich sowohl Chief Information Security Officers (CISOs) als auch andere Führungskräfte befassen müssen.

Im Folgenden sehen wir uns die Vor- und Nachteile dieser innovativen Technologie für Europa, den Nahen Osten und Afrika (EMEA) an. In dieser Region leben 32,5 % der Weltbevölkerung[3] und erwirtschaften 38 % des Bruttoinlandsprodukts (BIP).[4] Daher sollten möglichst schnell effektive Governance- und Sicherheitsmaßnahmen umgesetzt werden, um diese Innovationen zu schützen und die ethische Nutzung sicherzustellen.

1. Schubmehl, D., Jyoti, R. und IDC (2023): „How leading organizations are using AI to drive impact across every industry and addressing barriers such as AI governance, upskilling, and cost", IDC, https://news.microsoft.com/source/wp-content/uploads/2023/11/US51315823-IG-ADA.pdf
2. Verizon Enterprise (18. September 2020): „5G and AI: creating a connected global business", https://www.verizon.com/business/resources/articles/s/5g-and-ai-creating-connected-global-business/
3. Worldometer. (o. D.): „World Population Clock: 8.2 billion people" (LIVE, 2024), https://www.worldometers.info/world-population/
4. Boshers, J. (5. März 2024): List of EMEA countries, IstiZada, https://istizada.com/list-of-emea-countries/

GenAI: die Lösung aller Probleme?

Im Gegensatz zur Prognose-KI kann generative KI neue Inhalte, Ideen und Datenmuster erzeugen, die nicht explizit für das System programmiert wurden.

1. Infrastrukturverbesserungen: Mit GenAI lassen sich die riesigen Datenmengen verarbeiten und übertragen, die für das Training komplexer KI-Modelle erforderlich sind. So werden Netzwerkleistung und -zuverlässigkeit verbessert.

2. Transformation der Betriebsabläufe: GenAI verändert auch die internen Betriebsabläufe, insbesondere im Vertrieb und im technischen Bereich. Chatbasierte GenAI-Tools können frühere Bereitstellungen, Designentscheidungen und Kundenlösungen abfragen und Auskunft über sie geben. Dadurch werden Informationen allgemein verfügbar, die bisher nur eingeschränkt zugänglich waren.

3. Produktentwicklung und Kundendienst: GenAI ermöglicht Datenanalysen nahezu in Echtzeit und bietet neue Möglichkeiten für Kundeninteraktionen wie die Transkription von Videostreams und unverzüglichen Kundensupport. Damit könnten zum Beispiel dynamischere und reaktionsschnellere Dienste angeboten werden.

Verizon Connect hat kürzlich seine neue KI-Dashcam in der EMEA-Region auf den Markt gebracht. Die Dashcam dient als zuverlässiger Co-Pilot für Fahrer von Fuhrparks.[5] Sie kann auf stark befahrenen Straßen in Echtzeit Tipps geben, zum Beispiel an den Sicherheitsabstand erinnern, wenn Sie zu nah an ein anderes Fahrzeug heranfahren.

Unternehmen auf der ganzen Welt nutzen unsere 5G-Plattformen, um die rasante Digitalisierung von Daten aus verteilten Netzwerken zu meistern. In Einrichtungen des Gesundheitswesens können Echtzeitdaten aus Monitoringgeräten eine fundierte medizinische Entscheidungsfindung unterstützen.

KI-gestützte Lösungen wie die intelligente Videoüberwachung[6] und die Asset-Ortung bieten Gesundheitsdienstleistern ganz neue Möglichkeiten, ihre Diagnoseverfahren, OP-Analysen und den Patientenschutz zu verbessern.

Wachsende Angriffsflächen

Die KI-Nutzung fördert jedoch nicht nur die Cloud-Migration und die Nachfrage nach verteilten 5G-Plattformen, sondern legt auch bislang unbeachtete Angriffsflächen frei.[7]

Die größeren Angriffsflächen und die auch für Angreifer verfügbare GenAI stellen ein erhebliches Risiko für Unternehmen dar, die KI-Lösungen schnell implementieren, ohne sich umfassend über die potenziellen Gefahren zu informieren.

Neben den immer komplexeren Bedrohungen kommt bei modernen Angriffen aber auch weiterhin eine eher primitive Technik zum Einsatz. Die Ausnutzung von Sicherheitslücken gehört immer noch zu den drei am häufigsten verwendeten Techniken, mit denen sich Angreifer Zugang zu Unternehmen verschaffen. Im Verizon Data Breach Investigation Report (DBIR) 2024 wurde auf die starke Zunahme an Zero-Day-Sicherheitslücken hingewiesen und betont, dass das Patch-Management unbedingt verbessert und beschleunigt werden muss.[8]

5. Verizon (18. Januar 2023): „New Verizon Connect AI Dashcam delivers enhanced fleet safety and management capability“, Pressemitteilung, https://www.verizon.com/about/news/new-verizon-connect-ai-dashcam-deliver
6. Verizon Business. (o. D.): „How 5G can Improve Patient Data Analytics in Healthcare“, Verizon Business, https://www.verizon.com/business/resources/5g/5g-business-use-cases/workforce-productivity/patient-data-analytics/#solution
7. Lowman, R. (21. Februar 2020): „How AI in edge computing drives 5G and the IoT“, Semiconductor Engineering. https://semiengineering.com/how-ai-in-edge-computing-drives-5g-and-the-iot/
8. Verizon Business: „DBIR 2024“, https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

Es empfiehlt sich daher, neue KI-Systeme genau unter die Lupe zu nehmen, um in Ihrer KI-Strategie Bereiche mit Verbesserungspotenzial aufzudecken und dadurch das Sicherheitsniveau langfristig zu optimieren. Das ist ein wichtiger Punkt für IT-Führungskräfte, da die Zahl der CVEs (Common Vulnerabilities and Exposures) weltweit Schätzungen zufolge bis Mitte des Jahres 2025 um 25 % steigen wird.[9]

Die Schattenseite von GenAI

GenAI bietet viele interessante Möglichkeiten, kann aber auch zur Gefahr für die Privatsphäre werden. Da GenAI-Technologien riesige Mengen potenziell sensibler Daten verarbeiten und analysieren, muss auf die ethische Nutzung dieser Daten und die Richtigkeit der KI-Ergebnisse geachtet werden.

Large Language Models (LLMs) geben oft falsche Ergebnisse aus, sogenannte Halluzinationen. Ihre Antworten klingen überzeugend,[10] stammen aber nicht immer aus sachlich richtigen Quellen. Aus diesem Grund gibt es Bedenken hinsichtlich ihrer Zuverlässigkeit und des Risikos von Fehlinformationen, insbesondere in Branchen wie dem Gesundheitswesen.

Zudem konnten Forscher das KI-Modell ChatGPT in einem Experiment zur Offenlegung seiner Trainingsdaten bewegen,[11] indem sie immer wieder dasselbe Wort eingaben. Dieses ungewöhnliche Vorgehen führte zur Preisgabe personenbezogener Daten. Das zeigt, wie schwierig es sein wird, zu verhindern, dass KI-Modelle versehentlich sensible Informationen ausgeben, die sie gespeichert haben.

Geben Mitarbeiter sensible Daten in dialogorientierte KI-Assistenten ein, riskieren sie versehentliche Datenlecks und Sicherheitsverstöße. Das bedeutet, dass das Trainieren von KI mit unternehmenseigenen Daten möglicherweise gegen Datenschutzgesetze verstößt und zur Weitergabe vertraulicher Details an nicht autorisierte Benutzer oder Server von Drittanbietern führen kann.

Unternehmen benötigen daher einen verantwortungsbewussten Ansatz für die KI-Implementierung, um die Vorteile dieser innovativen Technologie zu nutzen und gleichzeitig die Daten und die Privatsphäre von Benutzern zu schützen.

Neue KI-Sicherheitslücken

Die Datenbank ATLAS (Adversarial Threat Landscape for Artificial-Intelligence Systems)[12] beinhaltet Informationen aus realen Cyberangriffen und Sicherheitsübungen, die Hinweise auf die spezifischen Sicherheitslücken in KI-Systemen geben.

Diese werden kontinuierlich aktualisiert, aber es zeichnen sich bereits einige gefährliche neue Trends ab:

- Data Poisoning: Angreifer manipulieren KI-Trainingsdaten, um Fehler oder schädliche Trigger einzuschleusen. Dadurch wird das KI-Modell verändert; es werden zum Beispiel Sicherheitslücken oder Backdoors eingebettet, die unter bestimmten Bedingungen aktiviert werden und die Integrität und Zuverlässigkeit des Systems untergraben.

9. Staff, S. (21. Februar 2024): „CVEs expected to increase 25% in 2024“, Security Magazine, https://www.securitymagazine.com/articles/100426-cves-expected-to-increase-25-in-2024
10. University of Oxford (20. November 2023): „Large Language Models pose risk to science with false answers, says Oxford study“, https://www.ox.ac.uk/news/2023-11-20-large-language-models-pose-risk-science-false-answers-says-oxford-study
11. Nasr, M., Carlini, N., Hayase, J., Jagielski, M., Cooper, A.F., Ippolito, D., Choquette-Choo, C.A., Wallace, E., Tramèr, F. und Lee, K.: „Scalable Extraction of Training Data from (Production) Language Models“, arXiv preprint arXiv:2311.17035, Cornell University, 2023. https://arxiv.org/abs/2311.17035
12. MITRE ATLASTM. (o. D.), https://atlas.mitre.org/

- Umgehung durch Täuschung: Mit einer Technik namens LLM Prompt Injection[13] erstellen Angreifer Prompts, die KI-Modelle täuschen, und dann zu Fehlinterpretationen und falschen Antworten führen. Man kann sich das so vorstellen, dass die Täter KI-Sicherheitsmaßnahmen umgehen und Sicherheitslücken ausnutzen (sich also sozusagen am Sicherheitspersonal vorbeischleichen), um unbefugt Aktionen auszuführen.

- Ausspähen von Architekturen: Angreifer spähen die Architekturen von KI-Systemen mithilfe einer Technik namens Discover Machine Learning (ML) Model Ontology[14] aus, um Schwachstellen aufzudecken. Wenn sie das KI-Framework kennen, können sie ausnutzbare Sicherheitslücken identifizieren und gezielte Angriffe planen, die die Abwehrmaßnahmen des Systems äußerst präzise aushebeln.

Stärkere Fokussierung auf reale Bedrohungen

Laut dem Verizon Data Breach Investigations Report 2024 werden die meisten Cyberangriffe (68 %) nach wie vor durch menschliches Versagen begünstigt, zum Beispiel bei Social-Engineering-Angriffen oder durch menschliche Fehler. Der Missbrauch von Berechtigungen ist in dieser Zahl noch gar nicht inbegriffen.[15]

Bei Cybersicherheitskonferenzen werden als Beispiele für KI-Bedrohungen oft ungewöhnliche Fälle und Ausreißer beschrieben, die manchmal für unnötige Aufregung sorgen.

Auch Deepfake-Robocalls und die Gefahr, dass KI für neue und effizientere Social-Engineering-Angriffe zur Beeinflussung von Wahlen ausgenutzt wird, führen zu Beunruhigung.

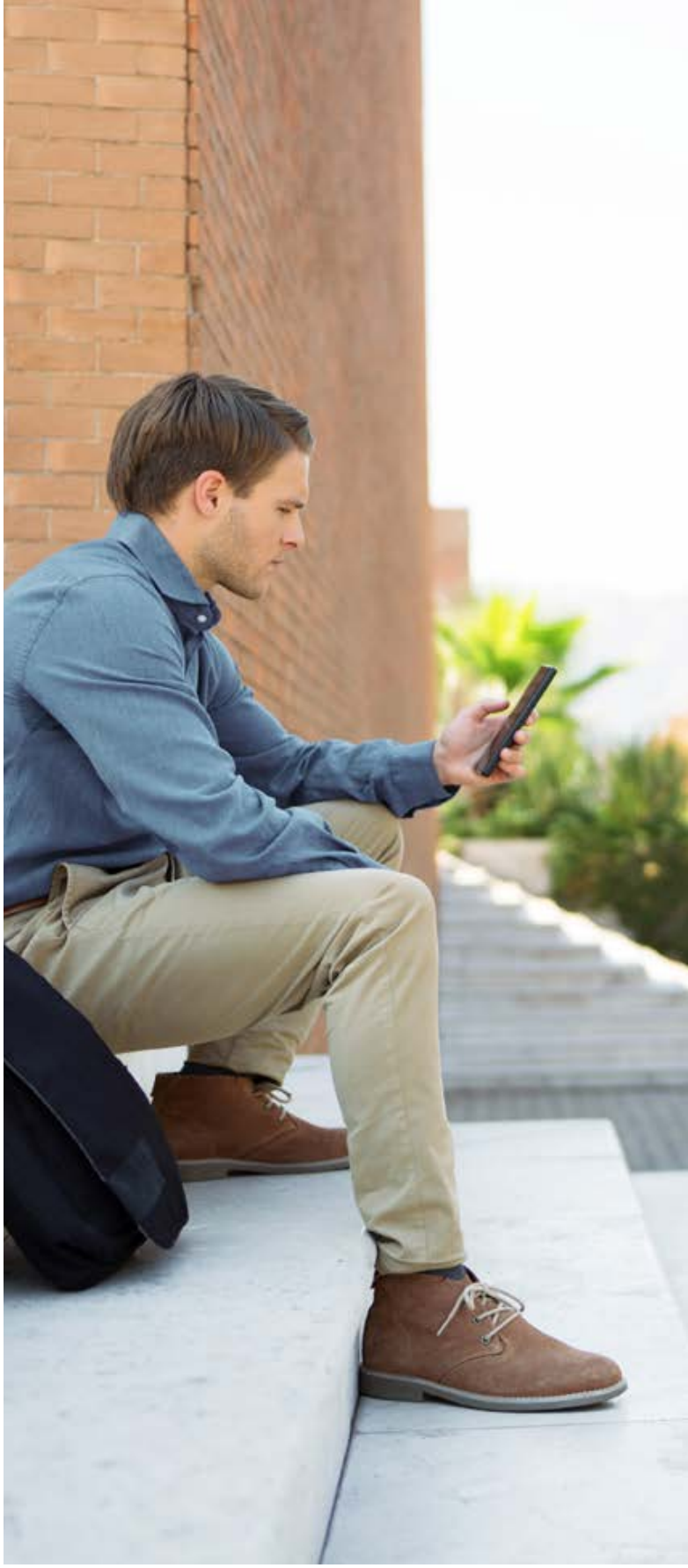
Sehen wir uns daher an, wie wahrscheinlich solche Angriffe sind:

- Die Wahrscheinlichkeit weitreichender Angriffe mithilfe von komplexen KI-Techniken ist derzeit äußerst gering.

- KI kann zwar für komplexere Angriffe missbraucht werden, doch diese sind noch relativ selten und zielen eher auf Prominente als auf die breite Öffentlichkeit ab.

- Die meisten Menschen fallen eher auf herkömmliche Phishing-Kampagnen, zum Beispiel in E-Mails oder Textnachrichten, herein als auf KI-gestützte Angriffe.

Diese Informationen helfen uns, die tatsächlichen Risiken und die Bedrohungslage besser einzuschätzen und unsere Abwehrmaßnahmen gezielt auf die wirklich relevanten Bereiche zu konzentrieren.



Die Rolle von KI-Governance

Unternehmen und Angreifer scheinen derzeit in einem Katz-und-Maus-Spiel gefangen, da die Angreifer ihre Techniken nur weiterentwickeln, wenn sie dazu gezwungen werden.

13. MITRE ATLASTM. (o. D.). https://atlas.mitre.org/techniques/AML.T0051
14. MITRE ATLASTM. (o. D.). https://atlas.mitre.org/techniques/AML.T0013
15. Verizon Business, „Data Breach Investigations Report 2024“, https://www.verizon.com/business/resources/reports/2024-dbir-data-breach-investigations-report.pdf

Wesentlich größer ist die Gefahr, dass neue KI-Modelle eingesetzt werden, um Innovationen voranzutreiben oder Unternehmen und Behörden zu schützen, dann aber selbst nur durch unzureichende oder unvollständige Sicherheitsmaßnahmen geschützt werden. KI mit KI zu bekämpfen ist kein Trend, sondern eine Notwendigkeit.

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat in seinem Leitfaden „Practical AI-Security Guide 2023" umfassende Informationen zu Sicherheitsbedenken in Zusammenhang mit KI-Systemen veröffentlicht.[16] In der Einleitung wird die Bedeutung von KI-Sicherheit unterstrichen, da KI-Systeme immer häufiger angegriffen werden. Es werden verschiedene Arten von Angriffen auf KI-Systeme vorgestellt und Sicherheits- und Abwehrmaßnahmen empfohlen.

Die britische Regierung befasst sich ebenfalls mit den potenziellen Bedrohungen und Risiken von KI. Das National Cyber Security Centre (NCSC) hat vor Kurzem den Bericht „The near-term impact of AI on the cyber threat" veröffentlicht, der eine Einschätzung der potenziellen Auswirkungen von KI auf die Effizienz von Cyberangriffen und der Konsequenzen für die Cyberbedrohungen in den nächsten zwei Jahren enthält. Darin heißt es: „Wir dürfen zwar die Risiken von KI nicht außer Acht lassen, sollten uns aber vor allem darauf konzentrieren, welche Möglichkeiten sie für die Cyberabwehr bietet."[17]

Viele Unternehmen können es kaum erwarten, ihre erste interne GenAI-Lösung zu entwickeln. Sie sollten sich allerdings immer zuerst fragen: Wie können wir die Lösung testen? Wenn Personen ohne KI-Spezialkenntnisse blind irgendwelche Tests durchführen, werden diese keine belastbaren Ergebnisse zur Sicherheit der GenAI-Lösungen liefern. Es ist immer ein maßgeschneiderter und angemessener Ansatz notwendig – es spielt ja auch bei der Auswahl von Sicherheitsmaßnahmen eine erhebliche Rolle, ob Sie Ihr Haus oder den Bundestag absichern wollen.

Wenn Sie einen allgemeinen Anbieter von Penetrationstests mit der Untersuchung einer komplexen KI-Umgebung betrauen, sind Schwachstellen geradezu vorprogrammiert – insbesondere, wenn deren Angriffsfläche auch IoT-Umgebungen und selbstoptimierende Produktionssysteme der Industrie 4.0 umfasst. Hacker halten sich nicht an Regeln. Sie versuchen, größtmögliches Chaos anzurichten. Daher müssen die Tester aufmerksam, fachkundig und den Angreifern immer einen Schritt voraus sein.

Anfällige Lieferketten

Unternehmen, die KI testen, werden eventuell als kritische Infrastrukturen eingestuft und geraten dadurch in das Visier staatlich gesponserter Hackergruppen, denen mehr Ressourcen zur Verfügung stehen. Aus diesem Grund sollte auch der Schutz ihrer Lieferketten höchste Priorität haben. 2022 gab es beispielsweise einen Cyberangriff auf drei europäische Unternehmen für den Transport und die Lagerung von Mineralöl, der Konsequenzen für Dutzende Ölterminals weltweit hatte. Die IT-Systeme von SEA-Invest in Belgien, Oiltanking in Deutschland und Evos in den Niederlanden wurden angegriffen und dadurch die Lieferketten in Häfen beeinträchtigt. Dieser Vorfall macht die Risiken von „Viert- und Fünftanbietern" deutlich, da Sicherheitslücken in der Lieferkette nicht nur die direkten Partner betreffen.

Globale Risiken führen weltweit zu Bedenken

Cyberkriminalität ist für Unternehmen in Europa, dem Nahen Osten und Afrika (EMEA) weiterhin ein großes Problem. Laut einer aktuellen Studie wurden mehr als ein Drittel der deutschen Unternehmen in den letzten zwei Jahren Opfer eines Cyberangriffs.[18] Für mehr als die Hälfte dieser Unternehmen sind die Gesamtschäden gestiegen, vor allem durch Phishing-Kampagnen, Angriffe auf Cloud-Dienste und die Ausnutzung von Datenschutzverletzungen. Die meisten Unternehmen schätzen ihr eigenes Risiko daher nachvollziehbar als hoch oder sehr hoch ein.

Das hat auch Konsequenzen für globale Sportveranstaltungen wie die Olympischen Winterspiele 2026 in Mailand und Cortina. Es ist sehr wahrscheinlich, dass KI-Angriffsvektoren für Cyberangriffe auf Großveranstaltungen wie diese missbraucht werden, was enorme finanzielle und Infrastrukturschäden verursachen könnte.

Während des Super Bowl LVIII 2024 arbeitete das Verizon Frontline Public Safety-Team mit Dutzenden Behörden zusammen, um für alle potenziellen Gefahren gerüstet zu sein – von Angriffen mit chemischen, biologischen, radiologischen und nuklearen Substanzen bis hin zu Cybersicherheitsangriffen. Das Team führte kontinuierlich Sicherheitsbewertungen für die Infrastruktur und den Veranstaltungsort durch, um potenziellen Angreifern einen Schritt voraus zu bleiben.

Schutz von GenAI

Laut einem Artikel in der Harvard Business Review, „4 Types of Gen AI Risk and How to Mitigate Them" von Mai 2024, „lassen sich die Risiken von GenAI anhand von zwei Faktoren klassifizieren: Absicht und Nutzung."[19] Zudem heißt es dort: „Viele Unternehmen zögern verständlicherweise, GenAI-Anwendungen einzuführen, und nennen als Gründe Datenschutz- und Sicherheitsbedenken, Urheberrechtsverletzungen, potenziellen Bias und Diskriminierung in den Ergebnissen sowie andere Gefahren."

Im öffentlichen und privaten Sektor in EMEA sollten diese Zweifel jedoch überwunden und angestrebt werden, bis 2030 für den Einsatz von KI bereit und durch robuste Cybersicherheitsmaßnahmen geschützt zu sein. Das kann

16. Ivezic, M. (14. September 2023): „German government publishes a practical AI-Security guide", Defence.AI. https://defence.ai/standards-frameworks-guidelines/german-ai-security-guide/
17. NCSC (o. D.): „The near-term impact of AI on the cyber threat", https://www.ncsc.gov.uk/report/impact-of-ai-on-cyber-threat#:~:text=Artificial%20intelligence%20(AI)%20will%20almost,techniques%20and%20procedures%20(TTPs).
18. Reisbeck, C. (27. Mai 2024): „Damage to German companies due to cyber attacks is increasing", KPMG, https://kpmg.com/de/en/home/media/press-releases/2024/05/cyber-attacks-damage-for-german-companies-increasing.html#:~:text=Cybercrime%20remains%20a%20real%20threat,in%20the%20past%20two%20years.
19. Isik, Ö. (31. Mai 2024): „4 Types of gen AI risk and how to mitigate them", Harvard Business Review, https://hbr.org/2024/05/4-types-of-gen-ai-risk-and-how-to-mitigate-them
20. DBIR Report 2024: Verizon. (o. D.): „Public Administration data breaches", Verizon Business, https://www.verizon.com/business/resources/reports/dbir/2024/industries-intro/public-administration-data-breaches/

gelingen, wenn bei der Entwicklung von Anwendungen auf „verantwortungsbewusste“ KI geachtet wird. Ohne zuverlässige Governance könnte KI mehr schaden als nutzen und zu unfairen Entscheidungen, voreingenommenen Modellen und Fehlinformationen führen. Laut dem Verizon Data Breach Investigations Report 2024 traten in der öffentlichen Verwaltung die meisten Vorfälle auf (12.217), davon 1.085 mit bestätigten Datenverlusten.[20]

Konkrete Maßnahmen zum Schutz von GenAI

KI-Prinzipien sollen dafür sorgen, dass die Gesellschaft in EMEA von dieser Technologie profitiert. Dazu müssen sie jedoch in den verschiedenen Ländern dieser Region durchgesetzt werden.

Die Europäische Union (EU) ist gemessen an den USA und China vielleicht kein Vorreiter bei der KI-Entwicklung, aber ihre Regulierungsbemühungen setzen weltweit Maßstäbe. Das EU-Gesetz zur künstlichen Intelligenz (EU AI Act) ist die weltweit erste umfassende Verordnung zu KI, die durch eine wichtige Regulierungsbehörde erlassen wurde. Das Gesetz soll dafür sorgen, dass KI-Technologien transparent und sicher sind und nicht gegen Grundrechte verstoßen. Es klassifiziert KI-Systeme nach Risikoniveau und macht striktere Vorgaben für Einsatzbereiche mit einem höheren Risiko, zum Beispiel im Zusammenhang mit Bewerbungsprozessen oder Inhalten für Kinder. [21]

Unternehmen in EMEA sollten ebenso zukunftsorientiert handeln und die Vorteile und Möglichkeiten von KI voll ausschöpfen. So können sie eine verantwortungsbewusste und sichere Transformation von Geschäftsmodellen, Marketing, Wissensmanagement und Softwareentwicklung vorantreiben.

Das Risikomanagement muss vollständig integriert und nicht erst nachträglich hinzugefügt werden. Ein Dienst zur Risikoeinschätzung kann helfen, potenzielle Schwachstellen in Plattformen und Lücken in der KI-Compliance aufzudecken.

Die Cybersecurity Assessments von Verizon umfassen beispielsweise Red Team Penetration Testing. Dabei werden Angriffe simuliert, um die Bedrohungen, einschließlich KI-Risiken, zu evaluieren. Bei Penetrationstests können automatisierte Tests durchgeführt werden, um die Systeme auf Angriffsvektoren und Sicherheitslücken zu überprüfen und potenzielle Ziele zu identifizieren.

Verizon hat zudem KI-Governance-Maßnahmen implementiert. So müssen Datenwissenschaftler KI-Modelle zur Überprüfung einreichen und Large Language Models (LLMs) werden genauer untersucht, um potenziellem Bias und Formulierungen, die zu Hass oder Gewalt anstacheln, entgegenzuwirken. Diese Maßnahmen tragen auch zu einem verantwortungsbewussten Umgang mit KI bei und sind in die GRC-Dienste (Governance, Risikomanagement und Compliance) integriert.

Diese taktischen Cybersicherheitsansätze müssen ebenfalls auf Governance, Risikomanagement und Compliance (drei Grundvoraussetzungen für Zero-Trust-Sicherheit) abgestimmt sein.

Alle Unternehmen sollten gemeinsam daran arbeiten, GenAI-Sicherheitslücken bis 2030 zu schließen. Diskrepanzen in der KI-Governance, von ethischen Richtlinien bis hin zu gesetzlichen Vorgaben, könnten zu uneinheitlichen Entwicklungen und Schwachstellen führen – und negative Folgen für diverse Bereiche haben, vom Wirtschaftswachstum bis zur Cybersicherheit.

Das Secure-by-Design-Framework[22] für KI und andere Technologien sorgt dafür, dass auch kleine Unternehmen ohne große IT-Teams einen sicheren Einstieg wagen können.

Insgesamt nutzen 21 internationale Gremien das Framework für KI-Systementwickler, damit die Cybersicherheit während des gesamten Entwicklungszyklus berücksichtigt wird.

21. AI Act (30. Juli 2024): „Shaping Europe's Digital Future“, https://digital-strategy.ec.europa.eu/en/policies/regulatory-framework-ai
22. CISA. (o. D.): „Secure by design“, Cybersecurity and Infrastructure Security Agency CISA, https://www.cisa.gov/securebydesign

Sichere GenAI für die Zukunft

Viele hoffen, dass sich mithilfe von GenAI in der Cybersicherheit gleiche Möglichkeiten für alle schaffen lassen,[23] doch die Realität sieht anders aus. In den meisten Behörden und Unternehmen fehlt es an Fachkenntnissen und Fachkräften, sodass die Sicherheit der Bürger in EMEA gefährdet wird.

Unternehmen sollten nicht länger warten, sondern sofort ihre KI-Risiken ermitteln.[24] Die Zielsetzung und Motivation dafür muss von der Führungsriege kommen, denn Sicherheit sollte als Chefsache und nicht als alleinige Aufgabe des Sicherheitsteams betrachtet werden.

Verizon kann Cyberteams helfen, ein abteilungsübergreifendes KI-Strategieteam zusammenzustellen. Das ist ein wichtiger Schritt, bevor ein Unternehmen seine erste GenAI-Anwendung entwickelt. Nur durch eine effektive Zusammenarbeit lassen sich KI-Risiken vermeiden und die Cybersicherheit stärken.

In den letzten Jahren hat Verizon stark in die Entwicklung spezialisierter und angewandter KI-Systeme investiert, mit denen sich Routineaufgaben bei der Optimierung der Netzwerkleistung, Identifizierung von Trends, Nachfragegenerierung und Verbesserung des Kundendienstes erledigen lassen.

Verizon trainiert KI-Modelle mit großen Datensätzen für bestimmte, genau definierte Aufgaben – und stimmt sie genau auf individuelle Geschäfts- oder Unternehmensanforderungen ab. Wir kennen die Vorteile und die Risiken.

Das Netzwerk von Verizon verarbeitet jeden Tag 70 Milliarden Datenpunkte und speist diese in komplexe KI-Systeme ein. Die Daten stammen aus 29.000 unterschiedlichen Quellen und repräsentieren damit ein riesiges und komplexes digitales Ökosystem.[25]

Wir passen unsere Empfehlungen stets an die individuellen Unternehmensanforderungen an, damit Sie aufgrund belastbarer Daten und Standards zuverlässige Abwehrmaßnahmen implementieren können. Außerdem erhalten Sie detaillierte Sicherheitsberichte und Vergleiche mit den Branchen-Benchmarks.

[23]Cosman, E. (o. D.): „Cybersecurity Risk is the Great Equalizer“, https://gca.isa.org/blog/cybersecurity-risk-is-the-great-equalizer
[24]Verizon Business (o. D.): Cybersecurity Assessment (CSA), https://www.verizon.com/business/products/security/cyber-risk-management/governance-risk-compliance/cybersecurity-assessments/
[25]Meyer, D. (8. Februar 2024): „Verizon's 70 billion network data points highlight genAI potential (and challenges)“, https://www.sdxcentral.com/articles/interview/verizons-70-billion-network-data-points-highlight-genai-potential-and-challenges/2024/02/

Sichere KI-basierte Bedrohungserkennung und -analyse

Mit diesem Framework können wir KI zur Weiterentwicklung unseres Sicherheitsansatzes nutzen:

- Kontinuierliches Monitoring: KI-Systeme überwachen die Netzwerkaktivitäten rund um die Uhr und decken Anomalien auf, die auf eine Bedrohung hinweisen könnten und von Menschen vermutlich übersehen würden.
- Automatisierte Penetrationstests: Diese Tests simulieren Cyberangriffe auf Computersysteme, Netzwerke oder Webanwendungen, um Sicherheitslücken aufzudecken, die ausgenutzt werden könnten.
- Datenverkehrsanalysen: KI unterscheidet zwischen normalem und verdächtigem Datenverkehr und erleichtert damit die Erkennung komplexer Cyberbedrohungen.
- Erkennung von Phishing-Angriffen: KI lernt, die Merkmale von Phishing-Angriffen und Spam zu erkennen und trägt damit zur proaktiven Blockierung schädlicher E-Mails bei.
- Identifizierung von Malware: KI-Tools analysieren Stichproben von bekannter Malware, um neue Varianten und Zero-Day-Bedrohungen (bisher unbekannte Malware) zu erkennen.
- Passwortschutz: KI kann komplexe Passwörter generieren und empfehlen, die schwer zu knacken sind.
- Aufgabenautomatisierung: Routineaufgaben im Cybersicherheitsbereich werden durch KI automatisiert, sodass die Experten mehr Zeit für strategisch wichtige Aufgaben haben.

GenAI ist eine leistungsstarke und effektive Lösung, die Unternehmen, Mitarbeiter und Kunden unterstützen kann. Damit verschaffen Sie sich nicht nur einen Wettbewerbsvorteil auf dem EMEA-Markt, sondern stärken auch die Sicherheit der Bevölkerung in dieser Region.

Wenn Sie mehr darüber erfahren möchten, wie Verizon Sie bei der KI-Sicherheit unterstützen kann, wenden Sie sich an Ihren Verizon Account Representative oder rufen Sie folgende Telefonnummer an: + 49 231 9720.