LOGICALIS
Architects of Change

Sicherheit neu denken im Zeitalter der KI

Maximieren Sie Chancen.
Minimieren Sie Risiken.

Inhalt

Sicherheit im Zeitalter der KI

Chancen durch KI nutzen, Risiken minimieren

Die Geschwindigkeit der Entwicklung im Bereich KI ist atemberaubend. Quanten-computer und GPTs (Generative Pre-trained Transformers) beschleunigen den digitalen Wandel. Diese Technologien haben ein enormes Potenzial für die Cybersicherheit und werden schnell zu unverzichtbaren Werkzeugen für alle Sicherheitsexperten.

Aber KI und generative KI schaffen auch neue Risiken. Aus einem aktuellen Bericht des Weltwirtschaftsforums geht hervor, dass die Fortschritte bei den Fähigkeiten von Angreifern (Phishing, Malware, Deepfakes) die besorgniserregendsten Auswirkungen der generativen KI für Unternehmen darstellen.

KI wird auch zu einem wichtigen Werkzeug für Cyberkriminelle und die Bedrohung wird durch geopolitische Instabilität und einen weltweiten Fachkräftemangel noch verstärkt.

Dieses Whitepaper geht darauf ein, wie Sie Ihr Unternehmen in die Lage versetzen können, die transformativen Chancen der KI zu maximieren und gleichzeitig die damit verbundenen Risiken zu minimieren. Wir untersuchen, wie innovative CISOs und CIOs die Technologie nutzen und gleichzeitig ihre Arbeitsplätze, Konnektivität und Cloud-Infrastruktur schützen.

Ein wichtiger Aspekt ist die Frage, ob Sie über die nötigen Sicherheitskompetenzen verfügen. Das ist nicht immer der Fall. Durch den Zugriff auf externes Know-How können Unternehmen von einem reaktiven zu einem proaktiven Ansatz wechseln. Intelligente, ständig verfügbare Managed Services nutzen modernste KI, um den Angreifern einen Schritt voraus zu sein. IT-Führungskräfte können ihre internen Teams so für Innovationen mit neuen Technologien freistellen und sich darauf verlassen, dass das Unternehmen geschützt ist.

KI verändert die Cybersicherheit

Angreifer und Angegriffene setzen auf KI

KI zum Angriff

Es ist oft davon die Rede, dass Hacker sogenannte FraudGPTs und WormGPTs erstellen, doch das auffälligste neue Risiko durch generative KI ist Social Engineering. Generative KI-Modelle in Chatbots oder Textgeneratoren können äußerst überzeugende Phishing-E-Mails, maßgeschneiderte Social-Media-Posts oder sogar Deepfakes erstellen, um Opfer zu täuschen.

Generative KI kann Angreifern dabei helfen, Zero-Day-Ransomware zu entwickeln, für die es keinen Patch gibt. Zudem birgt sie auch das Risiko, dass Mitarbeiter bei der Nutzung öffentlicher GPTs sensible Daten preisgeben.

Dank KI erzeugen Hacker polymorphe Malware, deren Signatur sich ständig ändert und dadurch schwerer erkennbar für Sicherheitslösungen wird. KI ermöglicht zudem automatische Angriffe auf weit mehr Schwachstellen als menschliche Angreifer.

KI zur Abwehr

Die Technologie wird bereits zur Abwehr bestehender Bedrohungen eingesetzt. KI analysiert riesige Datensätze von Netzwerkaktivitäten, erlernt normale Verhaltensmuster und zeigt Anomalien auf, die auf Angriffe hindeuten könnten. Generative KI verbessert dies, indem sie ausgefeiltere Modelle erstellt, die normale Aktivitäten besser imitieren können. KI-Modelle durchforsten historische Bedrohungsdaten und das aktuelle Netzwerkverhalten, um Muster zu erkennen und potenzielle künftige Angriffe vorherzusagen. Dies hilft Cybersicherheitsteams dabei, Schwachstellen proaktiv anzugehen. KI unterstützt auch die Analyse von Malware-Code und identifiziert automatisch Ähnlichkeiten, Varianten und mögliche Ursprünge.

KI scannt Systeme und Code nach potenziellen Schwachstellen. Generative KI kann weiterhin helfen, Schwachstellen vorherzusagen, sogar für Zero-Day-Angriffe. KI automatisiert Sicherheitsmaßnahmen wie die Isolierung infizierter Rechner oder die Blockierung verdächtigen Datenverkehrs, beschleunigt Reaktionszeiten und hilft, Angriffe frühzeitig einzudämmen.

Laut des Global Cybersecurity Outlook Surveys des Weltwirtschaftsforums glauben nur 10 % der IT-Führungskräfte, dass GenAI den Verteidigern in den nächsten zwei Jahren einen Vorteil gegenüber den Angreifern verschaffen wird.

Wir glauben jedoch, dass dieser Pessimismus unbegründet ist. Sicherheitsexperten haben mehr Zugang zu Quantencomputern und Daten, um KI für die Verteidigung zu trainieren, als Cyberkriminelle, um KI für Angriffe zu trainieren.

Wenn CIOs und CISOs sich das richtige Fachwissen zunutze machen, können sie das Gleichgewicht zu ihren Gunsten beeinflussen.

86 % aller CIOs glauben, dass GenAI die Qualifikationslücken und den Talentmangel lindert.

Logicalis CIO Report, 2024

Secure Workplace im Zeitalter der KI

Ein Großteil der Risiken am Arbeitsplatz drehen sich um Identitäts- und Gerätesicherheit. Generative KI kann realistische Deepfakes erstellen oder Text manipulieren, um Mitarbeiter zur Preisgabe sensibler Zugangsdaten zu verleiten.

Im August 2023 wurde ein Angestellter eines Softwareunternehmens dazu gebracht, den Code für die Multifaktor-Authentifizierung seines Unternehmens preiszugeben, weil der Angreifer ein Deepfake-Audio eines bekannten Kollegen verwendete.

KI kann jedoch Eindringlingen entgegenwirken, indem sie Nutzungsmuster lernt und unregelmäßige Zugriffsversuche erkennt. Es ist wichtig, Mitarbeiter über die neuen Risiken generativer KI aufzuklären, damit sie Social-Engineering-Angriffe erkennen und vermeiden können.

Rund 84 % der Arbeitnehmer, die generative KI verwenden, gaben an, dass sie in den letzten drei Monaten Daten ihres Unternehmens öffentlich gemacht haben. Dies geht aus einer neuen Studie des Oliver Wyman Forum hervor, für die mehr als 15.000 Angestellte in 16 Ländern befragt wurden.

Darktrace-Forscher stellten einen Anstieg von 135 % der neuartigen Social-Engineering-Angriffe von Januar bis Februar 2023 fest, was mit der weit verbreiteten Nutzung von ChatGPT zusammenfällt.

Secure Connectivity im Zeitalter der KI

Netzwerke sollten das Wachstum von IoT, 5G und Edge Computing unterstützen. Doch die zunehmende Angriffsfläche bietet auch mehr Möglichkeiten für Cyberkriminelle.

Edge-Geräte verfügen in der Regel über weniger Verarbeitungsleistung und Sicherheitsfunktionen als Cloud-Server, was sie anfälliger macht. Auch die Verarbeitung von Daten im Edge-Bereich birgt Risiken.

KI kann zur Sicherung von Netzwerken und Konnektivität eingesetzt werden, indem Datenströme am Netzwerkrand in Echtzeit analysiert werden. Sie kann ungewöhnliche Muster erkennen, die auf Malware, Eindringlinge und Denial-of-Service-Angriffe (DoS) hindeuten, und zwar schneller, als wenn die Daten zur Analyse in die Cloud gesendet werden.

Es ist jedoch unerlässlich, bei der Entwicklung von KI-Modellen für Edge-Geräte robuste Sicherheitsmaßnahmen zu implementieren. Dazu gehört die Härtung der Modelle gegen Manipulations- und Poisoning-Angriffe.

> Ich sehe in 5G neue Bedrohungen, da es mehr Edge-Daten geben wird.
>
> Paul Kurtz, Chef-Berater für Cybersicherheit, Splunk

Secure Hybrid Cloud im Zeitalter der KI

Die Sicherung einer hybriden Cloud-Umgebung ist ein komplexes Unterfangen. Oft setzen Unternehmen auf verschiedene Anbieter, die unterschiedliche Konfigurationen und Sprachen verwenden. Laut dem PWC Global Digital Trust Insights Report ist die Hybrid-Cloud für fast die Hälfte aller Unternehmen das größte Sicherheitsproblem.

Auch wenn KI nicht unfehlbar ist, spielt sie dennoch eine große Rolle. Sie kann riesige Datenmengen über hybride Clouds analysieren, Anomalien und Verstöße schneller erkennen als herkömmliche Methoden und sich wiederholende Aufgaben wie Schwachstellen-Scans automatisieren. Generative KI passt Sicherheitskontrollen anhand von Echtzeit-Bedrohungsdaten an.

Komplexe Hybrid-Cloud-Umgebungen können jedoch zu falsch konfigurierten Sicherheitsrichtlinien führen, die von der KI möglicherweise nicht immer erkannt werden. Außerdem können KI-Modelle wie Blackboxen sein, so dass es schwierig ist, zu verstehen, wie sie zu Sicherheitsentscheidungen kommen. Daher ist der Faktor Mensch unverzichtbar: So ist es Best Practice, KI-Modelle regelmäßig auf Schwachstellen zu testen und zu überwachen.

97 % der Unternehmen geben an, dass sie Lücken in ihren Cloud-Managementplänen haben.

PWC Global Digital Trust Insights Report

Mit Intelligent Security sicher ans Ziel

Viele Unternehmen konzentrieren sich nur auf einen Bereich der Sicherheitsstruktur. Wir bei Logicalis wissen, dass es in der heutigen Sicherheitslandschaft keine Silos mehr gibt. Unternehmen müssen Sicherheit ganzheitlich denken - von der sicheren Konnektivität über den Schutz der Cloud bis hin zur Absicherung hybrid tätiger Mitarbeiter und der Integration von Sicherheit in der gesamten Organisation.

Intelligent Security von Logicalis hilft Ihnen auf Ihrer Reise, damit Sie jeden Tag ohne Sorgen beginnen können.

Beratung

GRC-Beratung, um Organisationen dabei zu helfen, die sich schnell entwickelnde Welt von Governance, Risk & Compliance zu verstehen. Die Kenntnis Ihrer gesetzlichen und regularischen Verpflichtungen sowie Ihrer spezifischen Risikoschwelle ist der erste Schritt zur Bestimmung eines angemessenen Schutzniveaus, der benötigten Fähigkeiten und Prozesse.

Secure Workplace

Die Sicherung der Kommunikation von Mitarbeitern wie E-Mail und Chat, sowie der Geräte mit denen sie arbeiten und der Art und Weise, wie sie auf die Systeme zugreifen, sind entscheidende Sicherheits-komponenten.

Secure Connectivity

Das Netz ist die Grundlage für Konnektivität und Mitarbeiterzugriff auf Systeme. Bedrohungsakteure erkennen seine kritische Bedeutung und Anfälligkeit. Sichere Netze sind entscheidend für IoT, 5G und Edge Computing.

Secure Hybrid Cloud

Heutzutage sind Daten verteilt: manchmal on-premises, in der Cloud oder in SaaS-Diensten mit begrenzter Kontrolle. Unternehmen sollten einen „Zero-Trust“-Ansatz verfolgen, um den Zugriff, die Sicherheit und die Wiederherstellung von Daten zu gewährleisten.

Secure Operations

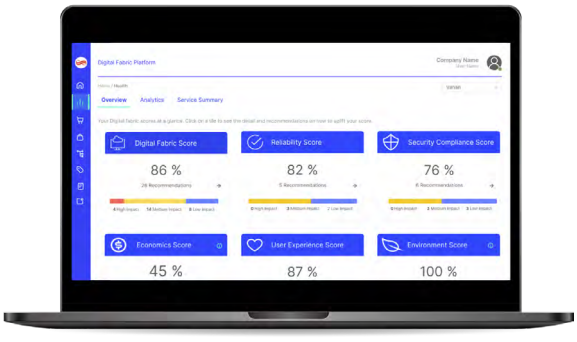
Das Logicalis Security Operation Centre (SOC) bietet hochqualifizierte Sicherheits-analysten, die in drei globalen Sicherheitsregionen tätig sind. Sie sind rund um die Uhr im Einsatz und bieten proaktive Schutz- und Reaktionsdienste. Das SOC entlastet Ihr Team und unterstützt beispielsweise auch bei der Schulung Ihrer Mitarbeiter.

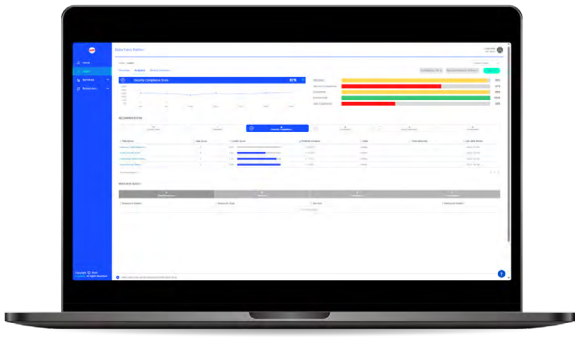
Intelligent Security auf Grundlage der ausgezeichneten Logicalis Digital Fabric Platform

Logicalis bietet seinen Kunden Zugang zu seiner preisgekrönten Digital Fabric Platform (DFP), die einen Echtzeit-Überblick über ihre verwaltete Umgebung in Schlüsselbereichen wie Zuverlässigkeit, Sicherheit, Compliance, Wirtschaftlichkeit, Benutzerfreundlichkeit und Umweltverträglichkeit bietet.

Mithilfe der Digital Fabric Platform können Sie schnell feststellen, ob Ihr Unternehmen vor Bedrohungen geschützt ist, Ihre Daten sicher sowie Systeme auf dem neuesten Stand sind und alle Komponenten unter Garantie stehen und den Vorschriften entsprechen.

Die DFP nutzt auch KI und Benchmarking, um hilfreiche Berichte und Empfehlungen zu erstellen, die zur weiteren Verbesserung Ihrer Sicherheitslage beitragen können.





Werfen Sie hier einen Blick auf unsere Sicherheits- und Compliance-Demo:

https://www.logicalis.com/managed-digital-fabric-demo-sign-up

Aus großer Kraft folgt große Verantwortung

KI bietet enorme Chancen für Wachstum und Fortschritt. Sie erfordert jedoch auch, dass Unternehmen die Sicherheit neu denken und proaktive Maßnahmen zum Schutz ihres Arbeitsplatzes, ihrer Konnektivität und ihrer Cloud-Infrastruktur ergreifen.

Durch einen intelligenten Sicherheitsansatz und die Nutzung der Möglichkeiten der KI können wir die Vorteile maximieren und gleichzeitig die damit verbundenen Risiken minimieren.

Mit Logicalis an Ihrer Seite sind Sie in der Lage, einen Großteil der Bedrohungen zu erkennen und auf sie zu reagieren. Bleiben Sie aufmerksam angesichts neuer Risiken und beginnen Sie dank eines durchdachten Sicherheitskonzepts jeden Tag mit Zuversicht.