schiffl

Cybersecurity im Fokus:

Traditionelle Abwehrmechanismen versus KI-gestützte Sicherheitslösungen

Ein Kommentar von Hermann Behnert, Geschäftsführer bei SCHIFFL IT und Leiter der Technik

01.10.2024

SCHIFFL IT Service GmbH
Leverkusenstraße 54
22761 Hamburg

Pressekontakt:
Katy Schlegel
040-42938-350
pr@schiffl.de
www.schiffl.de

In der aktuellen Cyberlandschaft sehen sich traditionelle Sicherheitsmechanismen wie Firewalls, Antivirensoftware und manuelle Überwachung zunehmend hochentwickelten Cyberbedrohungen gegenüber, die unter anderem auf KI basieren und konventionelle Abwehrstrategien geschickt umgehen. Dabei stoßen die herkömmlichen Methoden, die auf statischen Regeln und Signaturen basieren und einst als starke Verteidigung galten, immer häufiger an ihre Grenzen.

Gartners jüngste KI-Studie zeigt die wachsende Bereitschaft auf Seiten von Führungskräften, hierbei KI-Technologien einzubeziehen. In der Verteidigung analysieren diese den Netzwerkverkehr und Bedrohungsdaten in Echtzeit, ermöglichen proaktive Abwehr und passen sich dynamisch an. Im Gegensatz dazu sind traditionelle Methoden auf manuelle Updates angewiesen und erweisen sich als weitaus weniger adaptiv.

Um die Effektivität und Zukunftsfähigkeit von Cybersicherheitsstrategien aus Unternehmenssicht umfassend bewerten zu können, lohnt es sich, einen Blick auf die Verfahrensweisen der beiden Technologien zu werfen.

Im technischen Vergleich zwischen traditionellen Verteidigungsmechanismen und KI-gestützter Cybersecurity lassen sich signifikante Unterschiede identifizieren:

- **Signaturbasierte vs. Verhaltensbasierte Erkennung:**
  Traditionelle Systeme nutzen überwiegend signaturbasierte Erkennungsmethoden, die auf bekannten Malware-Mustern basieren. KI-Systeme hingegen setzen auf verhaltensbasierte Analysen, die nach einer Lernphase Anomalien in Echtzeit erkennen können, ohne auf vorher definierte Signaturen angewiesen zu sein.
- **Statische vs. Dynamische Anpassung:**
  Während traditionelle Systeme in der Regel manuelle Updates benötigen, erweitern KI-Systeme durch maschinelles Lernen kontinuierlich ihr Verständnis von Bedrohungsmustern und passen sich dynamisch an neue Angriffsvektoren an.
- **Reaktive vs. Prädiktive Abwehr:**
  Traditionelle Systeme reagieren meist auf bereits erkannte Bedrohungen. KI-gestützte Systeme können potenzielle Bedrohungen vorhersagen und präventive Maßnahmen einleiten, bevor ein Angriff erfolgt.

- **Skalierbarkeit der Datenverarbeitung:**
  KI-Systeme verarbeiten und analysieren enorme Datenmengen in Echtzeit, was bei der Erkennung komplexer, mehrstufiger Angriffe von entscheidender Bedeutung ist. Traditionelle Systeme stoßen bei der Auswertung oft an ihre Grenzen.
- **Kontextuelle Analyse:**
  KI-Systeme erfassen den Kontext von Aktivitäten automatisiert, was die Zahl falsch-positiver Meldungen reduziert. Traditionelle Systeme hingegen haben oft nicht die Möglichkeit, den Kontext vollständig zu erfassen.
- **Automatisierte Reaktion:**
  KI-gestützte Systeme können autonome Entscheidungen treffen und Gegenmaßnahmen einleiten, während traditionelle Systeme oft menschliches Eingreifen erfordern.
- **Tiefgreifende Netzwerkanalyse:**
  KI-Systeme analysieren komplexe Netzwerkstrukturen und -interaktionen und erkennen subtile Muster, die auf fortgeschrittene persistente Bedrohungen (APTs) hindeuten könnten.
- **Ressourceneffizienz:**
  Moderne KI-Systeme nutzen häufig Edge Computing und verteilte Architekturen, um Ressourcen effizienter zu nutzen, während traditionelle Systeme zentralisierter arbeiten.
- **Hybride Implementierung in der Cybersicherheit:**
  Unternehmen wie Darktrace setzen KI-Lösungen auf Appliances ein, die vor Ort beim Kunden installiert werden. Dies stellt einen Kompromiss zwischen Edge und zentralisierter Verarbeitung dar. Aus Sicht des Anbieters agiert die KI "am Edge", bleibt aber innerhalb des Kundennetzwerks ein zentrales Element. Dieser Ansatz ermöglicht schnellere Reaktionszeiten bei der Bedrohungserkennung im Vergleich zu reinen Cloud-Lösungen, ohne die KI auf einzelne Endgeräte zu verteilen.

Diese technischen Unterschiede verdeutlichen das Potenzial von KI in der Cybersecurity, zeigen aber auch die Herausforderungen bei der Integration solcher Systeme in bestehende Sicherheitsinfrastrukturen auf. Dazu gehören Veränderungen in der IT-Architektur, Kompatibilitätsprobleme mit bestehenden Systemen oder zeitintensive Implementierungsprozesse. Zudem erfordert die Bedrohung durch Adversarial AI, bei der Cyberkriminelle selbst KI-Techniken einsetzen, eine kontinuierliche Weiterentwicklung der Abwehrmechanismen.

Qualifizierte IT-Servicepartner als Schlüssel zur erfolgreichen KI-Integration

Ein tieferes Verständnis traditioneller und KI-gestützter Cybersecurity ermöglicht fundierte Entscheidungen hinsichtlich effizienter Ressourcennutzung und zukunftsorientierter Strategien, einschließlich der Erwägung, hybride Lösungen einzubeziehen.

Um die technischen Herausforderungen zu meistern, ziehen immer mehr Unternehmen Managed Service-Angebote qualifizierter IT-Partner in Betracht. Diese Experten verfügen über das notwendige Know-how, um KI-gestützte Sicherheitslösungen effektiv zu implementieren und zu verwalten. Darüber hinaus bieten sie auch strategische Beratung zur optimalen Integration von KI in die gesamte Sicherheitsarchitektur eines Unternehmens. Durch die Nutzung solcher Dienste können Unternehmen von den Vorteilen der KI in der Cybersicherheit profitieren, ohne selbst die komplexen technischen und personellen Anforderungen bewältigen zu müssen.

Über das Unternehmen

Die **SCHIFFL IT Service GmbH**, Teil einer international agierenden Unternehmensgruppe mit über 1.300 Mitarbeitenden in 23 Ländern, hat sich als kompetenter Anbieter von Managed-Multi-Service-Plattformen und Spezialist für End-User-Productivity in Deutschland und Europa fest etabliert. In zertifizierten Rechenzentren übernimmt SCHIFFL IT Aufgaben vom Design bis hin zum voll gemanagten Betrieb von Cloud-Umgebungen und baut dabei auf drei Jahrzehnten Erfahrung und einen maßgeschneiderten Fachservice, der die Betreuung komplexer IT-Infrastrukturen einschließt. Das ausgewählte Leistungsportfolio umfasst die Bereitstellung effizienter Plattform-Services, die Implementierung von Systemintegrationen, Lizenz- und Application Management sowie kontinuierlichen, zuverlässigen Support.
Weitere Informationen finden Sie unter www.schiffl.de