KEEPER

IT-Führungskräfte blicken einer Ära von KI-GESTÜTZTEN CYBERBEDROHUNGEN ENTGEGEN

Künstliche Intelligenz (KI) revolutioniert die Cyberbedrohungslandschaft und führt zu komplexen und fortschrittlichen Gefahrenpotenzialen, die traditionelle Abwehrmechanismen infrage stellen. Mit der Weiterentwicklung der KI-Technologie wird die Erkennung herkömmlicher Cyber-Bedrohungen wie Phishing und Smishing immer schwieriger. Dies unterstreicht den Bedarf an robusten, adaptiven Sicherheitsmaßnahmen.

HERAUSFORDERUNG DER KI-ERKENNUNG

84%

der IT-Führungskräfte sind davon überzeugt, dass KI-gestützte Phishing- und Smishing-Angriffe schwieriger zu erkennen sind

ANSTIEG DER RICHTLINIENIMPLEMENTIERUNG

81%

der Unternehmen haben KI-Nutzungsrichtlinien für Mitarbeitende eingeführt

WISSEN ÜBER KI-SICHERHEIT

77%

der IT-Führungskräfte sagen, dass sie mit Best Practices für die KI-Sicherheit äußerst oder sehr vertraut sind

Trotz der Zunahme der KI-Richtlinien und des Selbstvertrauens in die Fähigkeit, KI-gestützte Cyberangriffe zu bekämpfen, weist die Studie von Keeper Security eine erhebliche Lücke in der allgemeinen Vorsorge auf. KI-gestützte Angriffe, Supply-Chain-Angriffe und Deepfake-Technologie werden als wesentliche Problembereiche erkannt. Dennoch haben viele Unternehmen immer noch Schwierigkeiten, die Lücke im Hinblick auf die Vorsorge gegen diese ausgeklügelten Bedrohungen zu schließen.

Wichtige Bedrohungen und Lücken

Aufkommende Bedrohungen

51%

der IT-Führungskräfte betrachten KI-gestützte Angriffe als die schwerwiegendste Cyberbedrohung

36%

sind über Supply-Chain-Angriffe besorgt

36%

sehen in der Deepfake-Technologie ein erhebliches Risiko

Vorsorgelücken

35%

der IT-Führungskräfte fühlen sich auf KI-gestützte Angriffe unzureichend vorbereitet

30%

äußern sich besorgt über Deepfake-Technologie

Um diese Herausforderungen zu bewältigen, konzentrieren sich Unternehmen auf

Datenverschlüsselung	Schulung und Sensibilisierung der Mitarbeitenden	Erweiterte Systeme zur Bedrohungserkennung	Sichere KI-Modellentwicklung	Regelmäßige Sicherheitsaudits
51%	45%	41%	40%	36%

> "KI-gesteuerte Angriffe sind eine beeindruckende Herausforderung. Aber durch die Stärkung unserer Grundlagen der Cybersicherheit und die Einführung fortschrittlicher Sicherheitsmaßnahmen können wir eine widerstandsfähige Abwehr gegen diese sich entwickelnden Bedrohungen aufbauen."

Darren Guccione
CEO und Mitbegründer von Keeper Security

Die Zunahme von KI-gesteuerten Angriffen erfordert eine verbesserte Verteidigung. Wesentliche Praktiken wie Datenverschlüsselung, Schulung der Mitarbeitenden und erweiterte Bedrohungserkennung müssen konsequent aktualisiert und verbessert werden. Die Implementierung fortschrittlicher Frameworks wie Zero-Trust und Privileged Access Management (PAM) wird die Verteidigung weiter verstärken. Unternehmen sollten wachsam bleiben, ihre Sicherheitsrichtlinien kontinuierlich überprüfen und moderne Ansätze anwenden, um der sich entwickelnden KI-gestützten Bedrohungslandschaft einen Schritt voraus zu sein.