KEEPER

Die Zukunft der Verteidigung

IT-Führungskräfte bereiten sich auf beispiellose Cyberbedrohungen vor

Künstliche Intelligenz lässt die Zahl der Bedrohungen explosionsartig ansteigen, da Cyberkriminelle ihren Arsenalen raffinierte neue Waffen mit KI-Technologie hinzufügen.Da sich die Technologie ständig weiterentwickelt, ist eine ständige Anpassung durch IT- und Sicherheitsverantwortliche unerlässlich, um diese sich entwickelnden Bedrohungen zu bekämpfen. Keeper Security beauftragte ein unabhängiges Marktforschungsinstitut mit der Befragung von mehr als 800 Führungskräften rund um den Globus über die moderne digitale Landschaft.

ORGANISATIONEN UNTER BESCHUSS

92%

der IT-Führungskräfte sagen, dass Cyberangriffe heute häufiger vorkommen als noch vor einem Jahr

ZUNEHMENDE RAFFINESSE

95%

der IT-Führungskräfte geben an, dass Cyberangriffe raffinierter sind als je zuvor

FÜHRUNGSKRÄFTE BLEIBEN FOKUSSIERT

92%

der IT- und Sicherheitsverantwortlichen geben an, dass die Cybersicherheit für sie oberste Priorität hat

Cyberangriffe, die laut IT-Führungskräften zunehmen

1. **51%** Phishing
2. **49%** Malware
3. **44%** Ransomware
4. **31%** Passwortangriffe
5. **28%** DoS

Neue Angriffsvektoren, die IT-Verantwortliche beobachten

- **51%** KI-gestützte Angriffe
- **36%** Deepfake-Technologie
- **36%** Supply-Chain-Angriffe

Angriffsvektoren, gegen die sich IT-Verantwortliche schlecht gewappnet fühlen

- **35%** KI-gestützte Angriffe
- **30%** Deepfake-Technologie
- **29%** 5G-Netzwerkexploits

> Die Grundlagen der Cybersicherheit sind das Fundament unserer digitalen Stärke. Da sich die Bedrohungen weiterentwickeln, dienen diese Grundlagen als erste Verteidigungslinie. Sie bieten einen robusten und proaktiven Schutz gegen bestehende und neue Risiken. Die Priorisierung dieser Fundamente ist nicht nur eine Strategie, sie ist eine Notwendigkeit.

Darren Guccione
CEO und Mitbegründer, Keeper Security

IT-Führungskräfte navigieren durch Wellen von Angriffen

- Alle paar Monate: **31%**
- Monatlich: **22%**
- Wöchentlich: **18%**
- Jährlich oder weniger: **15%**
- Täglich: **11%**
- Stündlich: **3%**

Trotz der sich verändernden Bedrohungslandschaft bleiben die grundlegenden Regeln für den Schutz eines Unternehmens relevant. Unternehmen sollten vorrangig Passwort- und Privileged Access Management (PAM)-Lösungen einführen, die vor den gängigsten Cyberangriffen schützen. Ein Password Manager mindert das Risiko, indem er strikte Passwortpraktiken erzwingt, während PAM die lebenswichtigen Vermögenswerte eines Unternehmens schützt, indem es den Zugang auf hoher Ebene kontrolliert und überwacht. Dadurch werden die Verteidigungsmaßnahmen gestärkt und der potenzielle Schaden im Falle eines erfolgreichen Cyberangriffs minimiert.