KEEPER®

Die Zukunft der Verteidigung

IT-Führungskräfte bereiten sich auf beispiellose Cyberbedrohungen vor

March 2024

Cyberangriffe sind ausgeklügelter als je, und IT-Führungskräfte fühlen sich für den Umgang mit neuen Bedrohungen nicht ausreichend gerüstet

Eine weltweite Umfrage von Keeper Security in Zusammenarbeit mit TrendCandy Research unter mehr als 800 IT- und Sicherheitsverantwortlichen im Jahr 2024 zeigt, dass Cyberangriffe durch neuartige Bedrohungen durch künstliche Intelligenz (KI) und fortschrittliche, neuartige Angriffstechniken immer ausgefeilter werden. Neben diesen neuen Bedrohungen müssen IT-Führungskräfte auch mit einem erhöhten Aufkommen von Angriffen fertig werden. 92 % der Befragten gaben an, dass Cyberangriffe heute häufiger vorkommen als noch vor einem Jahr. Die Sicherheit im Jahr 2024 wird immer komplexer, und es steht mehr denn je auf dem Spiel.

Keeper Security, der führende Anbieter von Zero-Trust- und Zero-Knowledge-Cybersicherheitssoftware zum Schutz von Passwörtern, Passkeys, privilegiertem Zugriff, Geheimnissen und Remote-Verbindungen, wollte die Cybersicherheitslandschaft im Jahr 2024 abbilden. Keeper beauftragte ein unabhängiges Marktforschungsunternehmen, um von führenden Sicherheitsexperten aus der ganzen Welt Erkenntnisse über Trends in der Cybersicherheit und die Zukunft der Abwehr zu gewinnen.

Cyberangriffe werden immer häufiger und ausgeklügelter

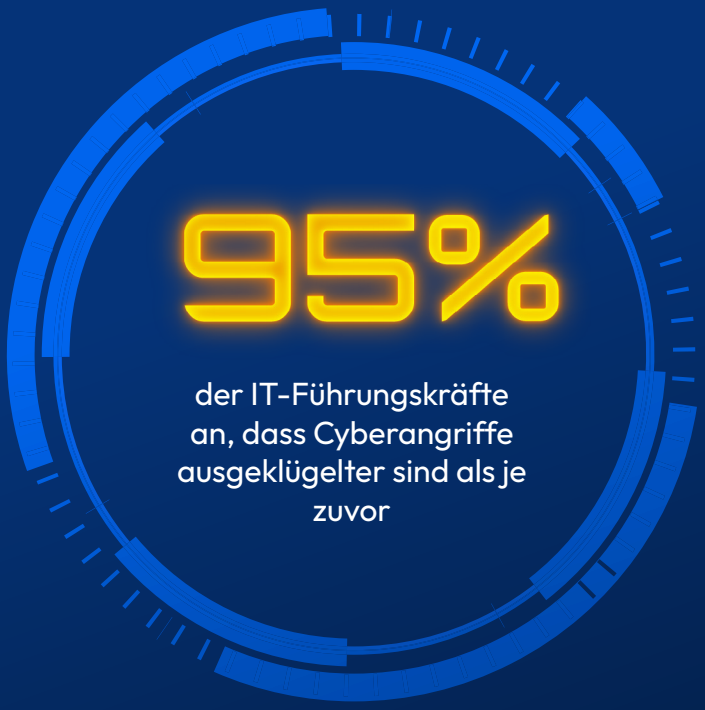
Angesichts der sich rasch entwickelnden Bedrohungen, neuer Vorschriften, Fortschritte wie Passkeys und einer Vielzahl von Geräten - von Desktops bis hin zu Space-Computing-Headsets - ist die Cybersicherheit wichtiger als je zuvor. Überwältigende 92 % der IT- und Sicherheitsverantwortlichen geben an, dass die Cybersicherheit ihre oberste Priorität ist. Diese Führungskräfte können es sich nicht leisten, den Fokus zu verlieren, denn 92 % der Befragten gaben an, dass die Zahl der Cyberangriffe im Vergleich zum Vorjahr zugenommen hat. Cyberkriminelle sind kreativ und unerbittlich in ihrem Bestreben, historisch sichere Lösungen zu knacken und anfälligen Unternehmen maximalen Schaden zuzufügen.

Mit dem zunehmenden Umfang von Cyberangriffen nehmen auch die Auswirkungen zu: 73 % der Befragten haben einen Cyberangriff erlebt, der zu einem finanziellen Verlust geführt hat. Direkte finanzielle Auswirkungen sind eine von vielen Folgen eines erfolgreichen Cyberangriffs, zusammen mit Geschäftsunterbrechungen, dauerhaften Umsatzeinbußen, Kunden- und Partnerverlusten und einem angeschlagenen Ruf.

Zu den fünf Geschäftsbereichen, die am stärksten von einem erfolgreichen Angriff betroffen sind, gehören

KEEPER

Da Vorfälle im Bereich der Cybersicherheit immer häufiger und kostspieliger werden, gaben 95 % der IT-Führungskräfte an, dass Cyberangriffe ausgeklügelter sind als je zuvor - und dass sie auf diese neue Welle von Bedrohungsvektoren nicht vorbereitet sind.



Nach Aussage der Befragten gehören zu den schwerwiegendsten neuen Angriffsarten

KI-gestützte Angriffe

Deepfake-Technologie

Supply-Chain-Angriffe

Cloud Jacking

IoT -Angriffe

5G-Netzwerkexploits

Dateilose Angriffe

Die fünf Techniken, gegen die sich IT-Führungskräfte am wenigsten gewappnet fühlen, sind

KI-gestützte Angriffe

Deepfake-Technologie

5G-Netzwerkexploits

Cloud Jacking

Dateilose Angriffe

KI-gestützte Angriffe werden als der ernsthafteste aufkommende Bedrohungsvektor angesehen, aber auch als die größte Herausforderung bei der Bekämpfung. Böswillige Akteure nutzen KI als Waffe, um gängige Angriffstechniken wie Phishing und das Knacken von Passwörtern zu beschleunigen und zu skalieren. Dies verdeutlicht die Notwendigkeit eines proaktiven Ansatzes für die Cybersicherheit, der fortschrittliche Abwehrmechanismen und grundlegende Best Practices zur Eindämmung und Bekämpfung sich entwickelnder Risiken kombiniert.

Weltweit planen IT-Verantwortliche, ihre KI-Sicherheit insgesamt zu erhöhen

Datenverschlüsselung

Mitarbeiterschulung und –bewusstsein

Erweiterte Bedrohungserkennungssysteme

Da die Cyberbedrohungen immer schlimmer werden und sich weiterentwickeln, müssen IT-Führungskräfte ihre Taktiken und Strategien anpassen und einen mehrschichtigen Sicherheitsansatz verfolgen, um den Anschluss nicht zu verlieren.

Häufige Gemeinsamkeiten bei Bedrohungen: Angriffsarten

Während neuartige Bedrohungen einen unheilbringenden Schatten werfen, müssen IT-Verantwortliche auch die gängigsten Angriffsvektoren bekämpfen, darunter:

61%
Phishing

59%
Malware

49%
Ransomware

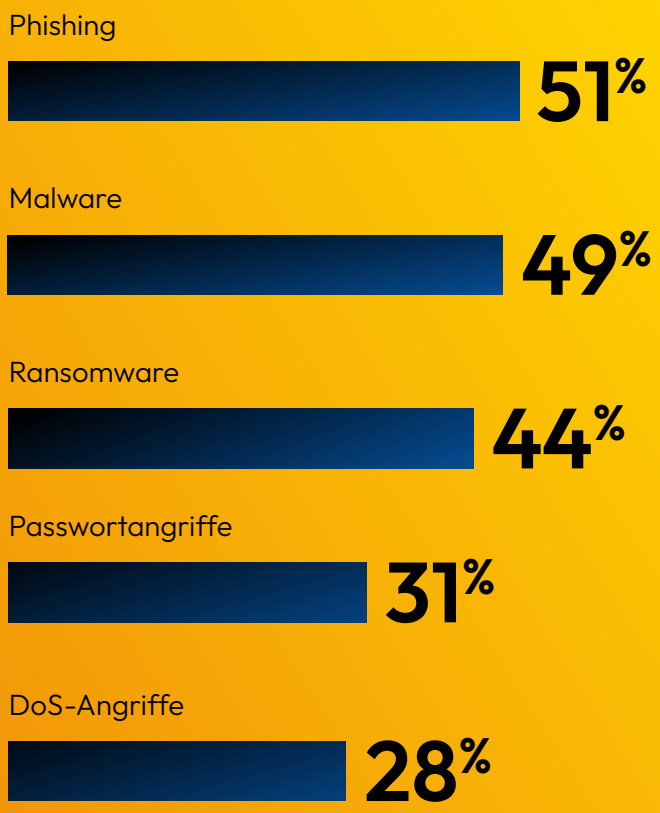
38%
Passwortangriffe

37%
DoS-Angriffe

Gestohlene oder schwache Passwörter und Anmeldeinformationen sind nach wie vor eine der Hauptursachen für Sicherheitsverletzungen. der Umfrageteilnehmer gaben an, dass das IT-Team ihres Unternehmens mit häufig gestohlenen Passwörtern zu kämpfen hat, was unterstreicht, wie wichtig es ist, starke, einzigartige Passwörter für jedes Konto zu erstellen und sicher zu speichern. Um zu verhindern, dass gehackte Anmeldeinformationen in die Hände von bösartigen Akteuren gelangen, überwachen 72 % der Unternehmen das Darknet auf gestohlene Anmeldeinformationen von Mitarbeitern. Die Nutzung eines Darknet-Überwachungsdienstes ermöglicht es Unternehmen, über die Kontoinformationen auf dem Laufenden zu bleiben und sofort Maßnahmen zu ergreifen, wenn festgestellt wird, dass die Anmeldeinformationen kompromittiert wurden. Die Verwendung eines dedizierten Password Managers kann dazu beitragen, beide Probleme direkt anzugehen, da er die höchste Verschlüsselungsstufe und Funktionen wie Darknet-Scans und Warnungen bietet.

KEEPER

Nach Ansicht von IT-Führungskräften nehmen die häufigsten Arten von Cyberangriffen auch am schnellsten zu



Heutzutage haben 67 % der Unternehmen Schwierigkeiten bei der Bekämpfung von Phishing-Angriffen. Die explosionsartige Entwicklung von KI-Tools hat dieses Problem noch verschärft, da sie Phishing-Betrügereien noch glaubwürdiger macht und es Cyberkriminellen ermöglicht, sie in großem Umfang einzusetzen. 84 % der Befragten gaben an, dass Phishing und Smishing aufgrund der zunehmenden Popularität von KI-gestützten Tools schwieriger zu erkennen sind. Sie erklärten außerdem, dass KI-gestütztes Phishing ihre größte Sorge ist (42 %), wenn es um KI-Sicherheit geht.

Wer steckt hinter den Angriffen, und wer ist am meisten gefährdet?

Zu den drei häufigsten Quellen von Cyberangriffen gehören heute:

Unabhängige Hacker

Hacktivistische Gruppen

Unternehmensspionage-Agenten

Zwar gehen viele Angriffe von unabhängigen Hackern oder Hacktivistengruppen aus, die Tausende von Kilometern entfernt sind, aber sie können auch im eigenen Umfeld eines Unternehmens stattfinden: 40 % der Umfrageteilnehmer gaben an, dass sie schon einmal einen Cyberangriff erlebt haben, der von einem Mitarbeiter ausging. Dies unterstreicht die Bedeutung des Einsatzes von Technologien, die sowohl beabsichtigte als auch unbeabsichtigte Insider-Bedrohungen verhindern. Eine Privileged Access Management (PAM)-Lösung unterstützt IT-Administratoren und Sicherheitspersonal bei der Verwaltung und Sicherung privilegierter Anmeldeinformationen und der Durchsetzung des Prinzips der geringsten Rechte. Wenn sich ein Cyberkrimineller Zugriff auf die Netzwerke eines Unternehmens verschafft, minimieren PAM-Plattformen den Explosionsradius, indem sie Seitwärtsbewegungen verhindern.

Wer sieht sich dem größten Risiko durch externe Bedrohungen ausgesetzt? Cyberkriminelle werden durch monetäre Transaktionen und sensible persönliche Informationen angelockt, die in bestimmten Branchen ausgenutzt werden können.

Die Flut von Angriffen, die IT-Führungskräfte heute abwehren müssen, verdeutlicht die Notwendigkeit proaktiver Cybersicherheitsstrategien, die sowohl bestehenden als auch neu aufkommenden Bedrohungsvektoren geschickt begegnen können.

Zu den drei am häufigsten gehackten Zweigen gehören:

Gastgewerbe/Reisen

Wöchentlich finden Angriffe statt, wobei Ransomware und Malware die häufigsten Arten von Cyberangriffen sind

Fertigung

Wöchentlich finden Angriffe statt, wobei Phishing und Malware die häufigsten Arten von Cyberangriffen sind

Finanzdienstleistungen

Monatlich finden Angriffe statt, wobei Phishing und Malware die häufigsten Arten von Cyberangriffen sind

Schlussfolgerung

Die Angriffe ändern sich, aber die grundlegenden bewährten Praktiken der Cybersicherheit nicht

Die Untersuchungen von Keeper beleuchten die neuen und neuartigen Methoden, mit denen Angreifer den Unternehmen, mittelständischen Organisationen und kleinen Betrieben Schaden zufügen. Mit KI-gesteuerten Angriffen an der Spitze werden die Tools im Arsenal der Cyberkriminellen immer ausgefeilter. Da die Technologie immer weiter fortschreitet, erfordert die Bekämpfung der sich entwickelnden Bedrohungen eine ständige Anpassung.

Trotz dieser sich ständig weiterentwickelnden Bedrohungslandschaft bleiben die grundlegenden Regeln für den Schutz eines Unternehmens in der digitalen Welt relevant. Unternehmen sollten vorrangig Lösungen einsetzen, die die häufigsten Cyberangriffe verhindern, einschließlich Passwort- und PAM-Lösungen. Ein Password Manager kann Risiken mindern, indem er strenge Passwortpraktiken durchsetzt, während PAM die vitalen Werte eines Unternehmens schützt, indem es den Zugriff auf hoher Ebene kontrolliert und überwacht. Auf diese Weise wird die Abwehr gestärkt und der potenzielle Schaden minimiert, falls ein erfolgreicher Cyberangriff stattfindet. Durch die Integration dieser Lösungen entsteht ein mehrschichtiger Sicherheitsansatz, der sich im Laufe der Zeit bewährt, den unbefugten Zugriff einschränkt und die allgemeine Widerstandsfähigkeit der Cybersicherheit verbessert – **jetzt und in Zukunft.**