Netzwerk- und Sicherheitstrends, die Sie im Jahr 2025 im Auge behalten sollten – und wie Sie sie für sich nutzen können

Aufgrund der Notwendigkeit überall verfügbarer Konnektivität, der Beschleunigung des Geschäftslebens und der unablässigen Cyberbedrohungen ist es für Unternehmen schwieriger denn je, Sicherheitslücken zu erkennen und zu schließen. Es ist an der Zeit, ein neues Tool zum Schutz von Benutzern, Geräten und Anwendungen zu nutzen: das Netzwerk.

Eine von Hewlett Packard Enterprise gesponserte und vom führenden Sicherheitsforschungsunternehmen Ponemon Institute unabhängig durchgeführte Studie liefert wichtige Erkenntnisse zur Sicherheit im Jahr 2025. Hier finden Sie eine Übersicht über die wichtigsten Trends, die Sie im Jahr 2025 im Auge behalten sollten – und wie Ihr Netzwerk Ihnen dabei helfen kann, darauf zu reagieren.

Ausbau von Zero-Trust-Sicherheitsinitiativen

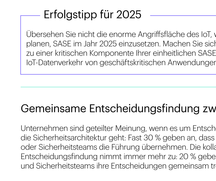
Viele Organisationen haben bereits Zero-Trust-Modelle eingeführt, um auf sich rasch entwickelnde Bedrohungslandschaften und wachsende Angriffsflächen zu reagieren. Fast zwei Drittel der Organisationen haben Zero-Trust-Sicherheit eingeführt oder planen, dies innerhalb des Jahres zu tun.

Erfolgstipp für 2025

Machen Sie Ihr Netzwerk an jedem Verbindungspunkt von einem Konnektivitätsermöglicher zu einem Verteidiger der Cybersicherheit. Wählen Sie ein Netzwerk, das auf den Zero-Trust-Prinzipien basiert – Zugriff nach dem Prinzip der geringsten Berechtigung, konsistente Durchsetzung, kontinuierliche Überwachung.

Anhaltende IoT-Risiken

Obwohl mehr als die Hälfte der Teilnehmer der Ponemon-Umfrage angab, dass die Identifizierung und Authentifizierung der IoT-Geräten, die auf ihr Netzwerk zugreifen, für die Sicherheitsstrategie ihres Unternehmens wesentlich sind, waren sich nur 16 % der Unternehmen sicher, dass sie alle mit ihrem Netzwerk verbundenen Benutzer und Geräte identifizieren können.



gaben an, dass die Identifizierung und Authentifizierung der IoT-Geräte, die auf ihr Netzwerk zugreifen, für die Sicherheitsstrategie ihres Unternehmens wesentlich sind

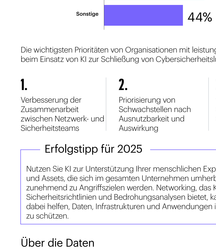
waren sich sicher, alle Benutzer und Geräte zu kennen, die ständig mit ihrem Netzwerk verbunden sind

Erfolgstipp für 2025

Vermeiden Sie blinde Flecken im IoT mithilfe von Tools der künstlichen Intelligenz (KI) und des maschinellen Lernens (ML). Suchen Sie nach Netzwerken, die KI und ML für umfassende Sichtbarkeit und genaues Profiling von Geräten verwenden. Mithilfe KI-basierter Verhaltens-Baselines auf Geräteebene können Sie anormales Verhalten von IoT-Geräten identifizieren und so besser auf frühe Signale potenzieller Bedrohungen reagieren.

Zunehmende Verbreitung von SASE

Die Secure Access Service Edge (SASE)-Architektur hat an Popularität gewonnen, da immer mehr Benutzer remote arbeiten und Anwendungen in die Cloud migriert werden. Der Anteil der Unternehmen, die SASE eingeführt haben oder dies planen, ist in den letzten Jahren stetig gestiegen und es gibt keine Anzeichen dafür, dass sich dieser Trend verlangsamt.

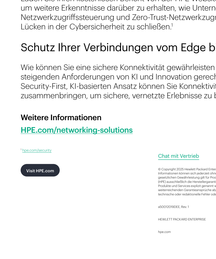


Erfolgstipp für 2025

Übersehen Sie nicht die enorme Angriffsfläche des IoT, wenn Sie planen. SASE im Jahr 2025 einzusetzen. Machen Sie sicheres SD-WAN zu einer kritischen Komponente Ihrer einheitlichen SASE-Strategie, um IoT-Datenverkehr von geschäftskritischen Anwendungen zu trennen.

Gemeinsame Entscheidungsfindung zwischen Teams

Unternehmen sind geteilter Meinung, wenn es um Entscheidungen über die Sicherheitsarchitektur geht: Fast 30 % geben an, dass Netzwerk- oder Sicherheitsteams die Führung übernehmen. Die kollaborative Entscheidungsfindung nimmt immer mehr zu: 20 % geben an, dass Netzwerk- und Sicherheitsteams ihre Entscheidungen gemeinsam treffen.



Erfolgstipp für 2025

Wählen Sie ein Netzwerk, das eine gemeinsame Toolbox bietet, um jedem Team zu helfen, seine spezifischen Ziele zu erreichen, ohne Kompromisse bei Leistung oder Schutz einzugehen. Sowohl Netzwerk- als auch Sicherheitsteams können von der Nutzung des Netzwerks als Sicherheitslösung profitieren.

Priorisierung des Einsatzes von KI für die Sicherheit

39 % der Organisationen geben an, KI zu nutzen, um Lücken in der Cybersicherheit zu schließen. Organisationen mit leistungsstarker Sicherheit – also Organisationen, die als besonders effizient im Schritt-Halten mit Bedrohungen und Schließen von Sicherheitslücken gelten – setzen KI häufiger ein als andere Organisationen.

Die wichtigsten Prioritäten von Organisationen mit leistungsstarker Sicherheit beim Einsatz von KI zur Schließung von Cybersicherheitslücken sind:

1.
Verbesserung der Zusammenarbeit zwischen Netzwerk- und Sicherheitsteams

2.
Priorisierung von Schwachstellen nach Ausnutzbarkeit und Auswirkung

3.
Verbesserung der Genauigkeit des IoT-Geräteprofilings

Erfolgstipp für 2025

Nutzen Sie KI zur Unterstützung Ihrer menschlichen Experten, da Benutzer und Assets, die sich im gesamten Unternehmen umherbewegen, zunehmend zu Angriffszielen werden. Networking, das KI-basiertes Profiling, Sicherheitsrichtlinien und Bedrohungsanalysen bietet, kann Ihrem Team dabei helfen, Daten, Infrastrukturen und Anwendungen im großen Maßstab zu schützen.

Über die Daten

Die 2025 Global Study on Closing the IT Security Gap befasst sich eingehend mit den wichtigen Maßnahmen, die erforderlich sind, um Sicherheitslücken zu schließen und wertvolle Daten im Zeitalter der KI zu schützen. Dieser Bericht trägt die Erkenntnisse von 2.120 IT-Fachleuten und IT-Sicherheitsexperten aus der ganzen Welt zusammen und bietet neue Einblicke in die IT-Sicherheits- und KI-Strategien von Unternehmen.

Laden Sie Ihren kostenlosen Bericht von der HPE-Website herunter, um weitere Erkenntnisse darüber zu erhalten, wie Unternehmen KI, Netzwerkzugriffssteuerung und Zero-Trust-Netzwerkzugriff nutzen, um Lücken in der Cybersicherheit zu schließen.[1]

Schutz Ihrer Verbindungen vom Edge bis zur Cloud

Wie können Sie eine sichere Konnektivität gewährleisten und gleichzeitig den steigenden Anforderungen von KI und Innovation gerecht werden? Mit einem Security-First, KI-basierten Ansatz können Sie Konnektivität und Sicherheit zusammenbringen, um sichere, vernetzte Erlebnisse zu bieten.

Weitere Informationen

HPE.com/networking-solutions

[1]ponemon.org

Visit HPE.com

Chat mit Vertrieb

a00133296ESE, Rev. 1

HEWLETT PACKARD ENTERPRISE

hpe.com