Gigamon

2019 CYBERTHREAT DEFENSE REPORT

Der fünfte jährliche Cyberthreat Defense Report der CyberEdge Group enthüllt, wie IT-Sicherheitsexperten die Sicherheitssituation ihrer Unternehmen, die Herausforderungen beim Schaffen effektiver Schutzmaßnahmen gegen Cyberbedrohungen und die Pläne für die Bewältigung dieser Herausforderungen einschätzen. Im Folgenden erfahren Sie einige der wichtigsten Ergebnisse des diesjährigen Berichts.

AKTUELLE BEDROHUNGSLAGE

Unternehmen fallen in alarmierendem Umfang erfolgreichen Cyberangriffen zum Opfer ... und erwarten mehr davon in der Zukunft.

IM JAHR 2018 MINDESTENS EINMAL BETROFFEN — 78,0%

IM JAHR 2018 SECHS MAL ODER ÖFTER BETROFFEN — 31,5%

WURDEN IM JAHR 2018 OPFER VON RANSOMWARE — 56,1%

ERWARTEN, IM JAHR 2019 BETROFFEN ZU SEIN — 65,2%

HAUPTHERAUSFORDERUNGEN

Trotz solider Budgets für die IT-Sicherheit haben die meisten Unternehmen in den letzten Jahren mit einer Handvoll bedeutender Herausforderungen zu kämpfen, die sie daran hindern, effektive Abwehrmaßnahmen gegen Cyberbedrohungen zu bewerkstelligen.

Nr. 1 Hindernis für Wirksamkeit

Zu viele zu analysierende Daten

Nr. 2 Hindernis für Wirksamkeit

84%

Unternehmen erfahren einen Mangel an qualifiziertem IT-Sicherheitspersonal

Das Nr. 1-Hindernis bei der JAGD GEGEN BEDROHUNGEN

ist die Schwierigkeit der Implementierung oder Integration von Tools für die Jagd gegen Bedrohungen

Eine weitere bedeutende Hürde

74%

Fast ein Viertel der Befragten geben an, dass die Entschlüsselung von SSL/TLS Datenverkehr zur Überprüfung ein Problem darstellt

ZUR HILFE BEREIT

Auch wenn ein paar neue Technologien vielversprechend sind und den IT-Sicherheitsteams helfen könnten, das durch die Sicherheitsdaten-Überlastung verursachte Chaos zu durchbrechen ...

Nr. 1

Sicherheitsanalytik ist die Nr. 1 unter den Sicherheitstechnologien, deren Anschaffung für das Jahr 2019 geplant ist (von 46,9 % der Befragten angegeben)

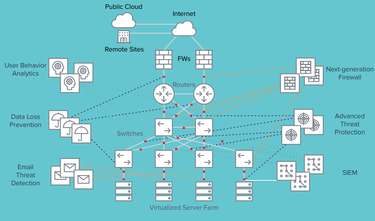
81%

81 % der Befragten stimmen darin überein, dass Technologien des maschinellen Lernens und künstlicher Intelligenz dabei helfen, hochentwickelte Cyberbedrohunge abzuwendenn

... Sie befassen sich leider nicht mit der Hauptursache.

EIN ZU GRUNDE LIEGENDES PROBLEM

Das Hinzufügen zahlreicher paralleler Schichten von Sicherheitstools im Laufe der Jahre hat zu einer Ad-hoc-Sicherheitsarchitektur geführt. Abgesehen davon, dass solche Konzepte zu der Flut an Sicherheitsdaten beitragen, leiden Sie unter folgenden Unzulänglichkeiten...



- unzuverlässiger Zugriff auf Netzwerkverkehr
- Unfähigkeit, verschlüsselten Datenverkehr effizient zu prüfen
- erhöhte Komplexität und Kosten des Security Stacks
- wiederkehrenden False Positives (Fehlalarme) und Warnungen
- schlechter Support beim Testen neuer Sicherheitstools

EINE LÖSUNG, DIE FUNKTIONIERT

Um diese Herausforderungen zu meistern, ist eine Lösung erforderlich, die eine durchgängige Sichtbarkeit bietet und zugleich die redundante Verteilung und Verarbeitung von Quelldaten sowie die daraus resultierenden Sicherheitsereignisse minimiert.
Es geht insgesamt darum, durch folgende Schritte die richtigen Informationen und Erkenntnisse für Ihre Tools und Teams zu erhalten, ohne diese zu überlasten:

1. Optimierter Datenverkehr für die Tools (aus physischen, virtuellen und cloudbasierten Umgebungen)
2. Zentralisierung und Auslagerung ressourcenintensiver Prozesse (z. B. Entschlüsselung)
3. Beschleunigung des Einsatzes und der Integration neuer Sicherheitstools
4. Aktivierung der Orchestrierung und Automatisierung (zur Verbesserung der Betriebseffizienz)

DOWNLOAD THE FULL REPORT AT
(LADEN SIE DEN VOLLSTÄNDIGEN
BERICHT HERUNTER UNTER):
www.gigamon.com/cdr2019

CYBEREDGE GROUP