Umfrage von ExtraHop- und SANS-Institut:
Netzwerksichtbarkeit leidet durch breit angelegte Remote-Arbeit massiv

- *Zwei Drittel der Organisationen haben in den vergangenen zwölf Monaten einen erfolgreichen Angriff auf ihre IT-Sicherheit erlitten*
- *Fast die Hälfte der Befragten identifiziert Desktop-Rechner von Mitarbeitern als das wahrscheinlichste Einfallstor für Cyberkriminelle*

Seattle/Berlin, 23. April 2020 – ExtraHop, der führende Anbieter für Cloud-native Network Detection und Response, veröffentlicht die Ergebnisse einer Umfrage des SANS-Instituts zum Thema Netzwerksichtbarkeit und Bedrohungserkennung, für die 213 Sicherheitsexperten aus weltweit agierenden Organisationen mit mindestens 1000 Mitarbeitern befragt wurden. Dem Bericht zufolge gaben mehr als 64 Prozent der Befragten an, innerhalb des letzten Jahres mindestens einen erfolgreichen Angriff auf die IT-Sicherheit erlebt zu haben, und 59 Prozent sind der Ansicht, dass eine mangelnde Netzwerksichtbarkeit ein hohes oder sehr hohes Risiko für ihren Betrieb darstellt. Da in letzter Zeit in großem Umfang auf Remote-Arbeit umgestiegen wurde, beunruhigt die Tatsache, dass 44 Prozent der Befragten die Desktops der Mitarbeiter als wahrscheinlichsten Angriffsvektor ansehen.

Unternehmen und Behörden müssen sich aktuell mit der Frage auseinandersetzen, wie sie die Arbeit der Belegschaft im Homeoffice ermöglichen, verwalten und sichern können. Bei der Anpassung an diese neue IT-Realität wird die Netzwerktransparenz daher wichtiger denn je. Die Umfrage deckt die wichtigsten Lücken in der Unternehmenssicherheit auf: 98 Prozent der Befragten sind besorgt darüber, dass sie den verschlüsselten Datenverkehr einsehen können, während über 80 Prozent den East-West Traffic sowie die mit dem Netzwerk verbundenen Geräte als undurchsichtige Bereiche identifizieren.

„Der Einblick in jedes Gerät und dessen Verhalten im eigenen Netzwerk ist entscheidend für das Verständnis, was normaler Datenverkehr ist und was als Abweichung betrachtet werden könnte", schreibt der Autor der Umfrage, Ian Reynolds.

Ronnen Brunner, Technology Evangelist EMEA bei ExtraHop, stimmt dem zu: „In einer Zeit, in der Unternehmen rasch auf Remote-Arbeit umstellen und die Cloud-Nutzung stark zunimmt, war die Sichtbarkeit des Netzwerks noch nie so wichtig wie heute. Unternehmen müssen in der Lage sein, den East-West Traffic zu überwachen, um Bedrohungen in der wachsenden Zahl von Cloud-Workloads zu erkennen und einen Überblick darüber zu erhalten, welche Geräte auf Unternehmensressourcen zugreifen. Je weniger Tools, Zeit und Anstrengungen erforderlich sind, um diesen Überblick zu erhalten, desto besser."

Neben der Identifizierung kritischer Lücken in der Netzwerksichtbarkeit gehören zu den wichtigsten Umfrage-Ergebnissen:

- **Zunehmende Komplexität innerhalb der Unternehmensumgebung:** Über 93 Prozent der Befragten gaben an, dass sie mehr als tausend Endpunkte verwalten. Fast 90 Prozent verwalten Hunderte bis Tausende von Servern.

- **Mangelnde Cloud-Sichtbarkeit beeinträchtigt die Sicherheitslage:** 40 Prozent der Befragten identifizierten Cloud-basierte Systeme als einen potenziellen Einstiegspunkt für böswillige Akteure. Gleichzeitig gaben nur 17 Prozent an, dass der Querverkehr innerhalb ihres Netzwerks (East-West Traffic) – einschließlich des gesamten Cloud-Verkehrs – gut sichtbar sei.

- **Tool-Reduktion immer dringlicher:** Die Mehrheit der Unternehmen verwendet Tools von mehr als 10 Anbietern, wobei fast ein Fünftel mehr als 20 verwendet. 68 Prozent der Befragten äußerten den Wunsch, die Komplexität ihrer Systeme zu verringern, indem sie die Gesamtzahl der für ihren Betrieb erforderlichen Tools reduzieren.

Die Umfrage ergab auch, dass sich Unternehmen zwar mehr Netzwerktransparenz wünschen, es jedoch betriebliche Hindernisse gibt. Personalmangel (62 Prozent), Zeitmangel (51 Prozent) – einschließlich dringlicherer Fragen – und der Mangel an geeigneten Qualifikationen bei der Belegschaft (46 Prozent) waren die größten Bedenken.

Laut Reynolds wird Maschinelles Lernen eine Schlüsselrolle bei der Bewältigung dieser Herausforderungen spielen: „Wählen Sie Werkzeuge, die Maschinelles Lernen nutzen, um bessere Analysen für den Zugang zu den richtigen Daten in kürzerer Zeit zu ermöglichen. Dies könnte dazu beitragen, Personalprobleme zu beheben und unerwartete Verhaltensweisen, Bedrohungen und Vorfälle schneller zu lösen."

Über ExtraHop

ExtraHop liefert Cloud-native Network Detection und Response (NDR), um das hybride Unternehmen zu sichern. Der innovative Ansatz wendet fortschrittliches Maschinelles Lernen auf den gesamten Cloud- und Netzwerkverkehr an, um vollständige Transparenz, die Erkennung von Bedrohungen in Echtzeit und die intelligente Reaktion darauf zu ermöglichen. Zu den Kunden von ExtraHop gehören weltweit führende Unternehmen wie The Home Depot, Credit Suisse, Liberty Global und Caesars Entertainment, die mit diesem Ansatz Bedrohungen erkennen, die Verfügbarkeit unternehmenskritischer Anwendungen gewährleisten und ihre Investition in die Cloud sichern.

Pressekontakt:
Mentha Benek
ExtraHop
206-787-8417
pr@extrahop.com