03.03.2020 – 10:00 Uhr

Forschung: IT-Manager betrachten verschlüsselten Datenverkehr als Quelle von Cyberbedrohungen und ihre Abwehr als unzureichend

Republik (ots/PRNewswire) -

Neue Untersuchungen von Flowmon und IDG Connect zeigen, dass 99 % der IT-Manager verschlüsselten Netzwerkverkehr als eine Quelle von Sicherheitsrisiken erkennen, dass aber zwei Drittel der Unternehmen scheitern, ihre Vermögenswerte vor internen und externen Bedrohungen, die SSL/TLS missbrauchen, zu schützen.

Flowmon Networks (https://www.flowmon.com/), ein Unternehmen für Netzwerkaufklärung, hat heute die Ergebnisse einer Umfrage veröffentlicht, die die Verteidigungsstrategien von Organisationen im Umgang mit den Bedrohungen bei verschlüsseltem Datenverkehr (https://www.flowmon.com/en/solutions/security-operations/encrypted-traffic-analysis) zusammenbringt. Die im Auftrag des Unternehmens von IDG Connect durchgeführte Umfrage unter mehr als 100 IT-Managern untersucht deren Erfahrungen mit diesem schnell wachsenden Angriffsvektor.

Im Laufe der gesamten IT-Geschichte wurden neue Technologien von schlechten Akteuren kooptiert und für böswillige Aktivitäten missbraucht. Und es kann keinen Zweifel daran geben, dass es bei der Verschlüsselung nicht anders ist. Obwohl die SecOps-Teams sie als standardmäßige Sicherheitsgegenmaßnahme einsetzen, eröffnet sie auch Raum für die Akteure der Bedrohung, um ihre Aktivitäten in einem als sicher geltenden Verkehr zu verstecken. Eine große Zahl von Unternehmen ist nicht nur Angriffen ausgesetzt, die SSL/TLS-Schwachstellen ausnutzen, sondern auch Angriffen, die SSL/TLS einsetzen, um Bewegungen im Netzwerk zu verschleiern und Anwendungen anzugreifen. Ohne ein geeignetes Toolset, das alle Angriffsvektoren abdeckt, ist der Umgang mit verschlüsselten Bedrohungen eine große Herausforderung.

"Die Studie zeigt, dass die überwiegende Mehrheit der Investitionen auf die Entschlüsselung des Datenverkehrs im Umkreis abzielt, wodurch die Organisation anfällig bleibt für viele gängige Angriffsformen wie Lösegeld, Botnets, die die Kommunikation mit Command- und Control-Servern verschleiern, oder Browser-Exploits. Nur 36 % der Befragten haben sowohl den Schutz für Umkreis und Netzwerk zusammen implementiert", so Mark Burton, Managing Director bei IDG Connect.

Die beiden größten Hindernisse bei der Entschlüsselung des Netzwerkverkehrs durch die Verwendung eines SSL-Proxys sind die Angst vor Datenschutzverletzungen (36 %) und die Sorge um Leistungsverschlechterung (29 %).

Netzwerkverteidiger müssen sich zusammenschließen, um alle verschlüsselten Bedrohungen des Datenverkehrs abzuwehren

Die Ergebnisse der Umfrage unterstreichen die Bedeutung der gemeinsamen Netzwerkverkehrsanalyse (https://www.flowmon.com/en/solutions/security-operations/encrypted-traffic-analysis) (NTA/Network Traffic Analysis) und der SSL-Entschlüsselung, um einen gleichwertigen Schutz vor externen und internen Bedrohungen zu gewährleisten.

Die Befragten erkennen NTA-Tools als eine Möglichkeit an, Netzwerk- und Sicherheitsbetriebsteams zusammenzubringen, eine einzige Version der Wahrheit zu teilen (49 % bewerten dies als die wichtigste Fähigkeit dieser Tools) und Prävention zu verbessern und die Erkennung und Reaktion zu beschleunigen.

"Die meisten Organisationen sind nicht in der Lage, den SSL/TLS-Verkehr in großem Umfang zu kontrollieren, und Cyberkriminelle wissen dies. Entschlüsselung ist leistungsstark, aber auch teuer und ressourcenintensiv. Daher ist es taktisch sinnvoll, eine verschlüsselte Verkehrsanalyse (ETA/Encrypted Traffic Analysis) zu verwenden, die leichtgewichtig ist und die die meisten Fälle abdeckt, um das Netzwerk ganzheitlich zu überwachen und die Entschlüsselung nur für kritische Dienste zu reservieren", so Artur Kane, Head of Product Marketing bei Flowmon Networks.

Den vollständigen Bericht finden Sie unter diesem Link: https://www.flowmon.com/en/idg-research-encrypted-traffic-threats

Umfrage-Methodik

IDG Connect führte die Umfrage im Auftrag von Flowmon Networks durch, um die Netzwerksicherheitslandschaft und die Netzwerkverschlüsselung in den USA, Kanada und Europa zu untersuchen. Ende 2019 befragte IDG Connect mehr als 100 Teilnehmer mittels eines Online-Fragebogens. Die Teilnehmer kamen aus verschiedenen Sektoren, darunter 27 % aus der vertikalen Technologiebranche. Alle Befragten hatten IT-Management-Titel und 40 % waren in C-Suite-Rollen tätig. Alle kamen aus Unternehmen mit mindestens 500 Mitarbeitern, wobei die höchste Anzahl (39 %) aus Unternehmen mit 1.000 bis 4.999 Mitarbeitern stammte.

Informationen zu Flowmon Networks

Flowmon (http://www.flowmon.com/) schafft eine sichere und transparente digitale Umgebung, in der Menschen das Netzwerk unabhängig von seiner Komplexität verwalten.

Informationen zu IDG Connect

IDG Connect ist die Demand Generation Division der International Data Group (IDG), dem weltweit größten Technologie-

Medienunternehmen. Sie wurde 2006 gegründet und nutzt den Zugang zu 44 Millionen Details von Geschäftsentscheidern, um Technologievermarkter mit relevanten Zielen aus allen Ländern der Welt zusammenzubringen. IDG hat es sich zum Ziel gesetzt, ein ungleiches, globales IT-Publikum mit wirklich lokalisierten Nachrichten zu erreichen, und veröffentlicht im Auftrag seiner Kunden auch marktspezifische Thought-Leadership-Dokumente und erstellt Studien für B2B-Vermarkter weltweit. Weitere Informationen finden Sie unter: www.idgconnect.com.

Foto - https://mma.prnewswire.com/media/1098125/Flowmon_Networks_Survey_Infographic.jpg

Logo - http://mma.prnewswire.com/media/590352/Flowmon_Networks_Logo.jpg

Kontakt:

Lukas Dolnicek, PR & Communications
T: +420-530-510-616
E: lukas.dolnicek@flowmon.com