12.09.2019 – 14:01 Uhr

Netzwerkbasierte Bedrohungen sind weiterhin auf dem Vormarsch

Threat Report von CenturyLink beschreibt die wichtigsten Angriffsarten und zeigt auf, wie sich das Netzwerk schützen lässt

Monroe, Louisiana (ots/PRNewswire) - Cyber-Bedrohungen eskalieren derart schnell, dass viele Unternehmen nicht Schritt halten können, wenn es darum geht, Bedrohungen zu identifizieren, abzublocken und zu entschärfen. Die sich ausweitende Bedrohungslandschaft sichtbar zu machen ist unerlässlich, aber Aktion ist wichtiger denn je, wie aus einem neuen Threat Report hervorgeht, der von CenturyLink, Inc. (NYSE: CTL) veröffentlicht wurde.

Die interaktive Multichannel-Version dieser Pressemitteilung finden Sie hier:

https://www.multivu.com/players/de/8524352-centurylink-2019-threat-report/

Den Threat Report 2019 können Sie unter folgendem Link abrufen:
https://www.centurylink.com/asset/business/enterprise/report/2019-threat-research-report.pdf

"Auf digitale Innovation fokussierte Unternehmen begeben sich zwangsläufig in eine Welt mit beispiellosen Bedrohungen und Risiken", sagt Mike Benjamin, Leiter von CenturyLinks Threat Research and Operations-Division Black Lotus Labs (https://c212.net/c/link/?t=0&l=de&o=2572935-1&h=1684333261&u=https%3A%2F%2Fc212.net%2Fc%2Flink%2F%3Ft%3D0%26l%3Dde%26o%3D2572935-1%26h%3D3837179863%26u%3Dhttps%253A%252F%252Fc212.net%252Fc%252Flink%252F%253Ft%253D0%2526l%253Den%2526o%253D2572935-2%2526h%253D195462112%2526u%253Dhttps%25253A%25252F%25252Fwww.centurylink.com%25252Fbusiness%25252Fsecurity%25252Fblack-lotus-labs.html%2526a%253DBlack%252BLotus%252BLabs%26a%3DBlack%2BLotus%2BLabs&a=Black+Lotus+Labs). "Die Bedrohungen entwickeln sich, genau wie die sogenannten Bad Actors, ständig weiter. Finanziell gut ausgestattete Akteure auf Staaten- oder Länderebene und auf Cybercrime fokussierte kriminelle Vereinigungen haben die Einzeltäter vom Typ einsamer Wolf und die weniger ausgefeilten Attacken von Angreifern abgelöst, die sich in Chatrooms profilieren wollen. Glücklicherweise können wir dank unserer umsetzbaren Erkenntnisse unser Netzwerk und das unserer Kunden gegen diese entwickelnden Bedrohungen schützen".

Beobachtungen:

- Botnetze: Diese aus infizierten Computern bestehenden Netzwerke sind nach wie vor erfolgreich, weil sie ihre Ziele leicht kompromittieren können und sich per Fernzugriff und verdeckt steuern lassen. Botnetze wie Necurs, Emotet und TheMoon haben sich sowohl in Bezug auf Komplexität als auch Resilienz weiterentwickelt. Malware-Familien wie Gafgyt und Mirai geben ebenfalls kontinuierlich Anlass zur Sorge, da sie auf IoT-Geräte abzielen.
- DNS: Der Domain Name Server (DNS) wird oft als potenzieller Angriffsvektor übersehen, doch wir konnten eine Anstieg der DNS-basierten Angriffe wie z.B. DNS Tunneling beobachten. Der Angriff über einen DNS-Tunnel kann dazu genutzt werden, Daten in den Sub-Domains einer DNS-Abfrage oder -Antwort zu kodieren, was einen ungebremsten Schleichweg ins Netzwerk ermöglicht, um Daten zu extrahieren, Sicherheitskontrollen zu untergraben oder beliebigen Daten-Traffic zu senden. Black Lotus Labs hat aktuell über einen mehrwöchigen Zeitraum hinweg feststellen können, dass durchschnittlich 250 Domains pro Tag auf diese Weise missbraucht wurden, mit mehr als 70.000 Lookups für jede Domain.
- DDoS: Distributed Denial of Service (DDoS) Attacken führen nach wie vor zu verzögert ausgelieferten Diensten und sorgen dafür, dass Unternehmen offline gehen müssen. Wir haben nicht nur eine kontinuierliche Progression bei der Größe der Angriffe beobachtet, sondern auch die Zunahme von sogenannten Burst-Attacken, die eine Minute oder weniger dauern. Die Security Operations Center (SOC) von CenturyLink haben in der ersten Hälfte dieses Jahres 14.000 DDoS-Angriffe auf Kunden abgewehrt. Interessant ist auch, dass 89 Prozent der 100 größten Angriffe in der ersten Jahreshälfte Multi-Vektor-Angriffe waren.
- Herkunftsländer: Regionen mit wachsenden IT-Netzwerken und -Infrastrukturen sind nach wie vor die Hauptquelle für cyberkriminelle Aktivitäten. Die fünf Top-Länder mit den meisten Angriffen in der ersten Jahreshälfte 2019 waren die Vereinigten Staaten, China, Indien, Russland und Vietnam. Während die Vereinigten Staaten, China und Russland hier bereits im Vorjahr geführt wurden, sind Indien und Vietnam neu in den Top 5. Die meisten C2-Angriffe in der ersten Jahreshälfte 2019 waren gegen die

Vereinigten Staaten, China, Russland, die Niederlande und Mexiko gerichtet. Die Niederlande und Mexiko sind Neuzugänge unter den Top 5.

Fakten:

Täglich werden 139 Milliarden NetFlow Sessions und 771 Millionen DNS-Abfragen über verschiedene, von Black Lots Labs entwickelte Threat Intelligence-Modelle mit maschinellem Lernen erfasst. Black Lotus Labs hat im Zeitraum von Januar bis Juni 2019:

- 1,2 Millionen einzelne Bedrohungen pro Tag erfasst, was für 15 Millionen verschiedene böswillige Hosts steht.
- 4.120 neue C2s validiert, was rund 686 C2s pro Monat entspricht.
- 3,8 Million einzelne Bedrohungen pro Monat nachverfolgt. Diese Bedrohungen werden mit CenturyLink NetFlow- und DNS-Metadaten korreliert, um die Kunden auf eine potenzielle Gefährdung hinzuweisen.

CenturyLink nimmt Sicherheit ernst und trägt proaktiv zum Schutz des Internets bei. Dazu gehört beispielsweise, die Arbeit der böswilligen Akteure zu unterbrechen und Erkenntnisse und Empfehlungen für Unternehmen zum Schutz ihrer Netzwerke bereitzustellen.Hier ist einiges zu beachten:

- Sicherheit sollte direkt in die Netzwerkschichten eingebettet sein, um eine agilere Abwehr und Entschärfung der Bedrohung zu ermöglichen.
- Die passende Lösung für das Unternehmen bestimmen - wo lassen sich Sicherheitskontrollen mit Kompetenz planen, wo wird ein externen Partner benötigt.
- Die Lücke schließen und von Anfang an zusammenarbeiten, um Schutz und Sicherheit in jedes Produkt und jede Lösung zu integrieren, damit in Sachen Sicherheit nicht aufwändig nachgebessert werden muss.
- Evaluieren, was eine vertrauenswürdige Netzwerkumgebung ausmacht, und gute Cyber-Hygiene praktizieren.

Informationen zu CenturyLink

CenturyLink (NYSE: CTL) ist ein Technologieführer, der Kunden weltweit hybride Netzwerk-, Cloud- und Sicherheitslösungen bereitstellt. Über sein umfassendes globales Glasfasernetz bietet CenturyLink sichere und zuverlässige Dienste, um die wachsenden digitalen Anforderungen von Unternehmen und Verbrauchern zu erfüllen. CenturyLink strebt danach die vertrauenswürdige Verbindung zur vernetzten Welt zu sein und konzentriert sich auf die Bereitstellung von Technologien, die das Kundenerlebnis verbessern. Erfahren Sie mehr unter http://news.centurylink.com/.

Logo - https://mma.prnewswire.com/media/134213/centurylink_logo.jpg

Kontakt:

Pressekontakt: D. Nikki Wheeler
Nikki.Wheeler@CenturyLink.com
+1 720-888-0560

Investoren-Kontakt: Mark Stoutenberg
Mark.Stoutenberg@CenturyLink.com
+1 720-888-1662