Sophos Studie zeigt weltweit höchste Gefahr für Cyberangriffe via RDP

Weltweit installierte Honeypots wurden von Cyberkriminellen alle sechs Sekunden angegriffen; „Widder", „Schwarm" und „Igel" sind die häufigsten Angriffsmuster der Cyberkriminellen

Wiesbaden, 22. Juli 2019 – Sophos hat seine knapp viermonatige Studie „RDP Exposed: The Threat That's Already at your Door" abgeschlossen und die Langzeitergebnisse veröffentlicht. Sie zeigt, wie Cyberkriminelle unerbittlich versuchen, Unternehmen via Remote Desktop Protocol (RDP) anzugreifen. Folgend sind die wichtigsten Ergebnisse zusammengefasst:

RDP ist nach wie vor ein valider Grund für schlaflose Nächte von Systemadministratoren. Im vergangenen Jahr haben sich Cyberkriminelle – neben den zwei großen Ransomware-Angriffen Matrix und SamSam – fast vollständig auf Netzwerkzugriffe mit RDP konzentriert und andere Methoden weitgehend aufgegeben.

Matt Boddy, Security-Spezialist bei Sophos und Leiter der Studie erklärt: „In jüngster Zeit hat ein Fehler bei der Ausführung des Remote-Code im RDP - genannt BlueKeep (CVE-2019-0708) - für Schlagzeilen gesorgt. Dies ist eine so schwerwiegende Schwachstelle, dass sie dazu genutzt werden kann, eine Ransomware-Welle auszulösen, die sich innerhalb von Stunden weltweit ausbreiten könnte. Die Absicherung gegen RDP-Bedrohungen geht weit über das Patchen von Systemen gegen BlueKeep hinaus, denn dies ist nur die Spitze des Eisbergs. Zudem müssen IT-Manager dem RDP deutlich mehr Aufmerksamkeit schenken. Denn wie unsere Studie zeigt, attackieren Cyberkriminelle alle potenziell gefährdeten Computer mit RDP indem sie versuchen die Passwörter herauszufinden.

Die neue RDP-Studie von Sophos zeigt, wie Angreifer RDP-fähige Geräte bereits kurz nach dem Erscheinen im Internet finden. Als Demonstration setzte Sophos zehn geografisch verteilte Honeypots ein, um RDP-basierte Risiken zu messen und zu quantifizieren.

Folgend eine Zusammenfassung der Untersuchungsergebnisse:

- Alle zehn Honeypots erhielten ihren ersten RDP-Login-Versuch innerhalb eines Tages.
- Das Remote Desktop Protocol exponiert PCs in nur 84 Sekunden.
- Die zehn RDP Honeypots protokollierten insgesamt 4.298.513 fehlgeschlagene Anmeldeversuche über einen Zeitraum von 30 Tagen. Dies entspricht einem Angriffsversuch alle sechs Sekunden.
- Im Allgemeinen wird angenommen, dass Cyberkriminelle Websites wie Shodan nutzen, um nach offenen RDP-Quellen zu suchen. Die Studie von Sophos zeigt jedoch, dass Cyberkriminelle ihre eigenen Werkzeuge und Techniken haben, um offene RDP-Quellen zu finden, und sich nicht unbedingt nur auf Websites von Drittanbietern verlassen.

Hackerverhalten aufgedeckt

Sophos hat auf der Grundlage der Studie unterschiedliche Angriffsmuster identifiziert. Dazu gehören drei Hauptprofile: der Widder, der Schwarm und der Igel:

- Der Widder ist eine Strategie, die darauf abzielt, ein Administrator-Passwort zu hacken. Ein Beispiel der Studie ist, dass ein Angreifer im Laufe von zehn Tagen 109.934

Anmeldeversuche am irischen Honeypot mit nur drei Benutzernamen machte, um Zugang zu erhalten.
- Der Schwarm ist eine Strategie, die sequentielle Benutzernamen und eine endliche Anzahl der schlechtesten Passwörter verwendet. Ein Beispiel aus der Studie: In Paris wurde ein Angreifer registriert, der den Benutzernamen ABrown neunmal innerhalb von 14 Minuten verwendete, gefolgt von neun weiteren Versuchen mit dem Benutzernamen BBrown, anschließend mit CBrown, gefolgt von DBrown und so weiter. Das Muster wurde mit A.Mohamed, AAli, ASmith und anderen wiederholt.
- Der Igel ist gekennzeichnet durch eine hohe Aktivität, gefolgt von längeren Inaktivitätsphasen. Ein Beispiel in Brasilien zeigt, dass jeder Spike, der von einer IP-Adresse erzeugt wird, etwa vier Stunden dauert und aus 3.369 bis 5.199 Passwortraten besteht.

Boddy erklärt, was der Umfang dieser RDP-Gefahr für Unternehmen bedeutet: „Derzeit gibt es weltweit mehr als drei Millionen Geräte, die über RDP zugänglich sind, und es ist heute ein bevorzugter Einstiegspunkt für Cyberkriminelle. Sophos hat darüber berichtet, wie Kriminelle, gezielt Ransomware wie BitPaymer, Ryuk, Matrix und SamSam einsetzen, und fast vollständig auf andere Methoden verzichtet haben, um in ein Unternehmen einzudringen. Alle Honeypots wurden innerhalb weniger Stunden entdeckt, nur weil sie per RDP im Internet sichtbar waren. Der grundlegende Lösungsansatz besteht darin, den Einsatz von RDP so weit wie möglich zu reduzieren und sicherzustellen, dass hervorragende Passwörter im Unternehmen angewendet werden. Unternehmen müssen handeln und die passende Security zum Schutz vor den unerbittlichen Angreifern nutzen.""

Eine Kopie der Studie steht zum Download bereit unter: www.sophos.com/RDP

Ein Kommentar zu den Ergebnissen findet sich auf Sophos Naked Security im Artikel „RDP Exposed: Die Wölfe stehen bereits vor deiner Tür“: https://nakedsecurity.sophos.com/wolf

Die Sophos Security-Experten stehen zudem gerne für Fragen zur Verfügung. Bitte kontaktieren Sie uns bei Bedarf.

Über Sophos
Als ein weltweit führender Anbieter von Next-Generation-Cybersicherheit schützt Sophos fast 400.000 Unternehmen jeder Größe in mehr als 150 Ländern vor den neuesten Cyberbedrohungen. Mit den SophosLabs und seinem globalen Team für Bedrohungs- und Datenanalyse schützen die Cloud- und KI-gestützten Sophos-Lösungen Endpoints (Laptops, Server und mobile Geräte) sowie Netzwerke vor kontinuierlich neu entwickelten Cybertaktiken und -techniken, einschließlich automatisierter Attacken, Ransomware, Malware, Exploits, Datenexfiltration, Phishing und mehr. Die preisgekrönte, Cloud-basierte Plattform Sophos Central integriert das gesamte Sophos-Produktportfolio, von der Intercept X Endpoint-Lösung bis zur XG Firewall, in einem einzigen Synchronized Security System. Die Lösungen von Sophos sind exklusiv über den globalen Channel mit mehr als 47.000 Partnern und Managed Service Providern (MSPs) erhältlich. Sophos stellt seine Technologien für Unternehmen auch Privatanwendern mit Sophos Home zur Verfügung. Das Unternehmen hat seinen Hauptsitz in Oxford, Großbritannien, und ist an der Londoner Börse unter dem Symbol "SOPH" notiert. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617

Ulrike Masztalerz, +49-30-55248198
Ariane Wendt +49-172-4536839
sophos@tc-communications.de