Sophos Active Adversary Report: Häufigster Weg von Cyberkriminellen in Netzwerke führt über Remote-Dienste

In 90 Prozent der Angriffe wird das Remote Desktop Protocol (RDP) genutzt
Kompromittierte Anmeldedaten und das Ausnutzen von Schwachstellen sind nach wie vor die beiden häufigsten Angriffsursachen

Wiesbaden, 5. April 2024 – Sophos hat seinen Active Adversary Report It's Oh So Quiet (?): The Sophos Active Adversary Report for 1H 2024 veröffentlicht. Im Rahmen dieser Untersuchung analysiert Sophos X-Ops mehr als 150 Incident Response (IR)-Fälle, die es im Jahr 2023 bearbeitet hat. Die Experten stellen fest, dass Cyberkriminelle in 90 Prozent der Angriffe das Remote Desktop Protocol (RDP) missbraucht haben – eine gängige Methode, um Remote-Zugriff auf Windows-Systeme herzustellen. Dies ist die höchste Häufigkeit von RDP-Missbrauch seit Sophos im Jahr 2021 mit der Veröffentlichung seiner Active Adversary Reports begann.

Weiterhin waren externe Remote-Dienste wie RDP der häufigste Weg der Angreifenden, initial in Netzwerke einzudringen: in 65 Prozent der IR-Fälle erhielten Cyberkriminelle 2023 so einen Erstzugang. Externe Remote-Dienste waren seit der Einführung der Active Adversary-Berichte im Jahr 2020 durchgehend die häufigste Quelle für den Erstzugriff von Cyberkriminellen. Unternehmen und Organisationen sollten dies als klares Zeichen dafür betrachten, der Verwaltung dieser Dienste bei der Risikobewertung Priorität einzuräumen.

„Externe Remote-Dienste sind für viele Unternehmen notwendig, aber riskant und Angreifer sind sich dieses gefährlichen Spagats zwischen Workflow und Sicherheit durchaus bewusst. Sie versuchen aktiv, diese Lücken zu nutzen, Netzwerke zu unterwandern und damit an die wertvollen Daten von Unternehmen zu kommen. Die Freigabe von Diensten ohne sorgfältige Abwägung und Minderung ihrer Risiken führt unweigerlich zu einer Gefährdung. Es dauert heutzutage in der Regel nicht lange, bis Cyberkriminelle einen ungeschützten RDP-Server finden und infiltrieren - und ohne zusätzliche Kontrollen ist es dann auch ein Leichtes, den Active Directory Server zu finden, der auf der anderen Seite wartet", sagt John Shier, Field CTO bei Sophos.

Kompromittierte Daten sind häufigstes Einfallstor
Kompromittierte Anmeldedaten und das Ausnutzen von Schwachstellen sind nach wie vor die beiden häufigsten Ursachen für Angriffe. Im 2023 Active Adversary Report for Tech Leaders, der im August des vergangenen Jahres veröffentlicht wurde, stellten die Sophos-Experten jedoch fest, dass in der ersten Jahreshälfte 2023 kompromittierte Zugangsdaten zum ersten Mal als häufigste Ursache für Angriffe eintreten. Dieser Trend setzte sich bis zum Ende des Jahres fort, wobei kompromittierte Anmeldeinformationen die Ursache für mehr als 50 Prozent der IR-Fälle im gesamten Jahr waren. Betrachtet man die Daten von Active Adversary kumulativ über die Jahre 2020 bis 2023, so waren kompromittierte Anmeldedaten auch die häufigste Ursache für Angriffe, die in fast einem Drittel aller IR-Fälle auftraten. Trotz der historisch hohen Zahl der Fälle von kompromittierten Anmeldeinformationen bei Cyberangriffen, hatten 43 Prozent der IR-Fälle im Jahr 2023 keine Multi-Faktor-Authentifizierung konfiguriert. Das Ausnutzen von Schwachstellen war die zweithäufigste Ursache für Angriffe, sowohl im Jahr 2023 als auch bei

der kumulativen Analyse der Daten von 2020 bis 2023, die in 16 Prozent bzw. 30 Prozent der IR-Fälle die Hauptursache war

„Risikomanagement ist ein aktiver Prozess und Unternehmen, die diese Aufgabe ernst nehmen, haben angesichts der ständigen Bedrohungen eine bessere Sicherheitslage als solche, die dies nicht tun“, erklärt Shier. „Ein wichtiger Aspekt des Managements von Sicherheitsrisiken ist neben der Identifizierung und Priorisierung der Risiken auch, aus den erlangten Informationen Handlungen abzuleiten. Dennoch werden bestimmte Risiken, wie zum Beispiel ein offenes RDP, schon viel zu lange von Unternehmen vernachlässigt – zur Freude der Cyberkriminellen, die direkt durch die Eingangstür eines Unternehmens spazieren können. Die Sicherung des Netzwerks durch die Verringerung ungeschützter und anfälliger Dienste und die Härtung der Authentifizierung versetzt Organisationen insgesamt besser in die Lage, Cyberangriffe abzuwehren.“

Über den Report
Der Sophos Active Adversary Report für das erste Halbjahr 2024 basiert auf mehr als 150 Incident Response (IR)-Untersuchungen, die sich weltweit über 26 Branchen erstrecken. Die untersuchten Unternehmen befinden sich in 23 verschiedenen Ländern, darunter die USA, Kanada, Mexiko, Kolumbien, Großbritannien, Schweden, die Schweiz, Spanien, Deutschland, Polen, Italien, Österreich, Belgien, die Philippinen, Singapur, Malaysia, Indien, Australien, Kuwait, die Vereinigten Arabischen Emirate, Saudi-Arabien, Südafrika und Botswana.

Weitere Informationen zu aktuellen Herangehensweisen der Cyberkriminellen unter It’s Oh So Quiet (?): The Sophos Active Adversary Report for 1H 2024

Social Media von Sophos für die Presse
Wir haben speziell für Sie als Journalist*in unsere Social-Media-Kanäle angepasst und aufgebaut. Hier tauschen wir uns gerne mit Ihnen aus. Wir bieten Ihnen Statements, Beiträge und Meinungen zu aktuellen Themen und natürlich den direkten Kontakt zu den Sophos Security-Spezialisten.

Folgen Sie uns auf und

LinkedIn: https://www.linkedin.com/groups/9054356/
X/Twitter: @sophos_info

Über Sophos
Sophos ist ein weltweit führender und innovativer Anbieter von fortschrittlichen Cybersecurity-Lösungen, darunter Managed Detection and Response (MDR)- und Incident-Response-Dienste. Das Unternehmen bietet ein breites Portfolio an Endpoint-, Netzwerk-, E-Mail- und Cloud-Sicherheitstechnologien, das bei der Abwehr von Cyberangriffen unterstützt. Als einer der größten auf Cybersecurity spezialisierten Anbieter schützt Sophos mehr als 500.000 Unternehmen und mehr als 100 Millionen Anwender weltweit vor aktiven Angriffen, Ransomware, Phishing, Malware und vielem mehr.

Die Dienste und Produkte von Sophos werden über die cloudbasierte Management-Konsole Sophos Central verbunden und vom bereichsübergreifenden Threat-Intelligence-Expertenteam Sophos X-Ops unterstützt. Die Erkenntnisse von Sophos X-Ops erweitern das gesamte Sophos Adaptive Cybersecurity Ecosystem. Dazu gehört auch ein zentraler Datenspeicher, der eine Vielzahl offener APIs nutzt, die Kunden, Partnern, Entwicklern und anderen Anbietern von Cybersecurity und Informationstechnologie zur Verfügung stehen. Sophos bietet Cybersecurity-as-a-Service für Unternehmen an, die vollständig verwaltete, schlüsselfertige Sicherheitslösungen benötigen. Kunden können ihre Cybersecurity auch direkt mit der Security Operations Platform von Sophos verwalten oder einen hybriden Ansatz verfolgen, indem sie ihre internen Teams mit Sophos Services ergänzen, einschließlich Threat Hunting und Systemwiederherstellung.

Sophos vertreibt seine Produkte über Reseller und Managed Service Provider (MSPs) weltweit. Der Hauptsitz von Sophos befindet sich in Oxford, U.K.

Weitere Informationen unter: www.sophos.de

Pressekontakt:

Sophos
Jörg Schindler, PR-Manager Central & Eastern Europe
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