Ransomware-Ära: Neue Bedrohungen und Strategien für lokale Unternehmen

Erfahren Sie, wie sich Ransomware-Taktiken verändern und welche Auswirkungen dies auf die Branchen hat, insbesondere auf Ingenieurwesen und Fertigung.

In der heutigen Zeit sind Cyberangriffe und insbesondere Ransomware-Bedrohungen eine ständige Herausforderung für Unternehmen. Tim West, Direktor für Bedrohungsanalysen und Outreach bei WithSecure, beleuchtet die aktuellen Trends im Ransomware-as-a-Service (RaaS)-Sektor und die zunehmende Komplexität dieser Bedrohungen. Besonders bemerkenswert ist der dynamische Wandel in der Struktur und den Zielstrategien der Ransomware-Operationen.

West hebt hervor, dass die Konkurrenz im RaaS-Bereich zunimmt. Mit der Schließung bedeutender Gruppen wie LockBit und ALPHV haben sich viele der ehemaligen Mitglieder nach neuen Kollektionen umsehen müssen. Diese „nomadischen“ Affiliates suchen nach attraktiveren Angeboten von anderen Ransomware-Marken, die bessere Bedingungen, zuverlässige Auszahlungen und fortschrittliche Tools offerieren. Kleinere Gruppen wie Medusa und Cloak dienen als Anziehungspunkt, indem sie attraktive Anreize wie hohe Gewinnbeteiligungen anbieten.

Strukturwandel in Ransomware-Operationen

Die Struktur vieler Ransomware-Operationen hat sich in den letzten Jahren erheblich verändert. Anstatt dass eine einzelne,

zentral organisierte Gruppe den gesamten Angriffsprozess steuert, arbeiten jetzt viele erfolgreiche RaaS-Modelle mehrheitlich als lose verbundene Netzwerke. Unterschiedliche Gruppen sind auf spezielle Phasen des Angriffs spezialisiert, was die Komplexität der Attribution erweitert und gleichzeitig die Widerstandsfähigkeit des gesamten Systems gegenüber Störungen erhöht.

Ein weiterer entscheidender Faktor sind die Initial Access Brokers (IABs), die eine Schlüsselrolle in diesem Ökosystem übernommen haben. Sie sind in der Lage, hochentwickelte und skalierbare Zugänge zu Bibliotheken anzubieten, wodurch es anderen böswilligen Akteuren erleichtert wird, auf anfällige Systeme zuzugreifen. Diese IABs haben den Prozess der Ausnutzung von Schwachstellen industrialisiert, was die Einstiegshürden für neue Ransomware-Betreiber erheblich gesenkt hat.

Besonders gefährdet sind Branchen wie die Ingenieur- und Fertigungsindustrie, die laut aktueller Forschung in der ersten Hälfte des Jahres 2024 die am stärksten betroffene Branche war, mit über 20% aller beobachteten Opfer. Die damit verbundenen finanziellen Verluste und Vertragsstrafen bei Produktionsunterbrechungen machen dieses Sektor zu einem attraktiven Ziel.

Die Interaktion zwischen den verschiedenen Akteuren in diesen komplexen Lieferketten bringt zusätzliche Gefahren mit sich. Ein erfolgreicher Ransomware-Angriff auf eine einzige Einheit kann weitreichende Auswirkungen auf die gesamte Lieferkette haben, wodurch Ransomware-Gruppen einen größeren Verhandlungsspielraum gewinnen.

Erosion des Vertrauens unter Cyberkriminellen

Ein auffälliger Trend ist die Erosion des Vertrauens unter Ransomware-Akteuren. Vorfälle wie der Exit-Scam der ALPHV-

Gruppe, in dem Affiliates angeblich um ihre Einnahmen betrogen wurden, deuten auf wachsende Spannungen innerhalb der Community hin. Der Zwang, ständig neuen Affiliationen zu suchen, wird dadurch verstärkt, dass loyale Affiliates sich von etablierten Marken abspalten und potenziell eigene Gruppen gründen.

Diese Fragmentierung könnte zu weniger vorhersehbaren Ransomware-Gruppen führen, die ihre Angriffe schwerer zuzuordnen machen. Aus der Perspektive der Verteidigung jedoch könnte diese interne Misstrauensdynamik Vorteile bringen, da sie die Effektivität und Effizienz der Angriffe beeinträchtigt.

Die Nutzung von sogenannten Dual-Use-Tools, also Software, die sowohl für legitime als auch kriminelle Zwecke eingesetzt werden kann, wird immer ausgeklügelter. Programme wie TeamViewer oder rclone erlauben Cyberkriminellen, sich in Systeme einzuschleichen, ohne auf Anti-Malware-Anwendungen zu stoßen. Dabei ist es entscheidend, dass Sicherheitsteams ihre Strategien anpassen, um verdächtige Verhaltensmuster in der Nutzung dieser Tools schnell zu identifizieren und anzugehen.

Um diesen Bedrohungen zu begegnen, sollten Unternehmen sich auf datenschutztechnische Maßnahmen konzentrieren. Dazu gehört die Identifizierung sensibler Daten, strenge Zugangskontrollen und fortlaufende Überwachung verdächtiger Aktivitäten im Datenverkehr. Kritische Maßnahmen wie die Verschlüsselung von Daten können den Wert gestohlen Daten im Falle eines Angriffs erheblich mindern.

Die Tendenz der Akteure, sich verstärkt auf Datendiebstahl zu konzentrieren und nicht ausschließlich auf die traditionelle Verschlüsselung, hat weitreichende Auswirkungen auf die Risikolandschaft für Organisationen. Cyberkriminelle können dadurch ihre Angriffe schneller durchführen und Ressourcen effektiver nutzen.

Details