Sicherheit in der Retrospektive.
Warum Endpoint-Schutz auch bei Offline-Systemen notwendig ist

Was können wir aus den Fallbeispielen, in denen Unternehmen Opfer von Cyberangriffen werden, lernen? In einer mehrteiligen Artikelserie reisen die Sophos-Experten zurück in die Zukunft und widmen sich verschiedenen spezifischen Aspekten der IT-Sicherheit, um Empfehlungen abzuleiten, die für jeden umsetzbar sind.

In Teilen der IT-Welt dominiert die Meinung, dass einige Systeme keinen Endpoint-Schutz benötigen. Diese Einschätzung ist häufig für solche Geräte anzutreffen, die isoliert und nicht mit dem Internet verbunden sind oder keine wichtigen Daten oder Programme erhalten, wie etwa Entwicklungssysteme. So manches Unternehmen lässt sogar seine Endpoint-Schutz-Lizenzen auslaufen, in dem Glauben, dass diese ohnehin keinen zusätzlichen Nutzen bringen. Diese Denkweise rührt daher, dass der Endpoint-Schutz (in der IT-Welt jedenfalls) darauf ausgelegt ist, Malware zu stoppen. Einige Unternehmen halten den Schutz von Endpoints nicht für erforderlich, wenn das System isoliert und leicht wiederherzustellen ist oder keine wichtigen Daten enthält. Auch werden Nutzer-Workstations/Laptops oftmals für weniger wichtig erachtet als Server und daher nur letztere geschützt. Tatsächlich trafen laut Sophos 2021 Active Adversary Playbook 54 Prozent der Angriffe ungeschützte Systeme.

Sowohl der Endpoint-Schutz als auch die Art und Weise von Angriffen haben sich in letzter Zeit drastisch verändert. Cyberkriminelle gehen mit ausgeklügelten Taktiken vor, bei denen sie selbst auf häufig verwendet Verwaltungstools (z. B. PowerShell), Skriptumgebungen (z.B. JavaScript), Systemeinstellungen (z.B. geplante Aufgaben und Gruppenrichtlinien), Netzwerkdienste (z.B. SMB und Admin Shares und WMI) und gängige Anwendungen (wie TeamViewer, AnyDesk oder ScreenConnect) zurückgreifen. So vermeiden sie, dass sie Malware einsetzen müssen, um ihre Ziele zu erreichen. Techniken, die früher als „Nation State“ und „Advanced Persistent Threat“ (APT) galten, könne heute selbst von technisch unversierten Angreifern eingesetzt werden.

Es geht ums Geld

Das Ziel der Attacken ist jedoch immer noch weitgehend dasselbe: Geld zu verdienen. Dies kann durch den Einsatz von Ransomware (oft mit anschließender Datenexfiltration und Löschung von Sicherungskopien, um die Zahlung des Lösegelds dringlicher zu machen), das Schürfen von Kryptowährungen, die Beschaffung von personenbezogenen Daten zum Verkauf oder Industriespionage geschehen. Als Reaktion darauf hat sich auch der Endpoint-Schutz weiterentwickelt. Er erkennt und verhindert nun auch bösartiges Verhalten und bietet gleichzeitig detaillierte Transparenz, Kontext und Tools zur Bedrohungssuche.

Auch Systeme ohne direkten Internetzugang müssen geschützt werden

In der Regel starten Cyberkriminelle ihren Angriff von einem System aus, das über einen Command-and-Control-Kanal auf Port 443 (schwer zu identifizierender, anomaler, verschlüsselter Datenverkehr) mit einem Trojaner oder Stager als Vermittler verbunden ist. Dabei ist es nicht wichtig, ob es sich um einen Server oder ein Benutzersystem handelt. Alle verfügen über ähnliche Kernfunktionen und der Angreifer kann auf die gleiche Weise wie der Anwender selbst auf diese Systeme zugreifen. Für einen Angriff auf das System über das LAN stehen dem Angreifer gleich mehrere Techniken zur Verfügung, wie zum Beispiel Remote Desktop Protocol (RDP), Secure Shell (SHH) oder Windows Remote Management (WinRM). Angesichts der vielen zur Verfügung stehenden Optionen ist es erforderlich, auch Systeme

ohne Internetzugang mit Endpoint-Schutz auszustatten. Wenn die blinden Flecken durch den Einsatz von Endpoint Security überall beseitigt sind, haben Angreifer weniger Möglichkeiten, sich zu verstecken. Das ist wichtig, denn wenn sich Angreifer auf einem Systemen verstecken, können sie tage-, wochen- oder sogar monatelang unentdeckt bleiben und im Stillen Informationen über die Umgebung, Benutzer, Netzwerke, Anwendungen und Daten sammeln.

Neu: 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/
Twitter: @sophos_info

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