Cyberangriffe auf Lieferketten – wenn die eigene Sicherheit nicht ausreicht

Partnerschaften, Dienstleistungen, Kundenbeziehungen – keine Organisation agiert autark. Verträge, Compliances und Gesetze regeln die Zusammenarbeit, doch wie steht es um Sicherheitskriterien? Cyberangriffe auf Lieferketten treffen besonders kleine und mittelständische Unternehmen zeigt der neueste Threat Report von Sophos.

Im neuesten Sophos Threat Report: Cybercrime on Main Street berichten die Security-Experten, dass das Sophos MDR Team in 2023 vermehrt auf Fälle reagierte, in denen Unternehmen über die sogenannte Supply Chain, sprich die Lieferkette im Business und in der IT-Infrastruktur, attackiert wurden. In mehreren Fällen lagen die Schwachstellen in der Remote-Monitoring- und Management-Software (RMM) eines Dienstanbieters. Die Angreifer nutzen dafür den RMM-Agent, der auf den Rechnern des anvisierten Opfers lief, um neue administrative Konten in dem angegriffenen Netzwerk zu erstellen und setzten dann kommerzielle Tools für Remote-Desktop, Netzwerkerkundung und Software-Einrichtung ein. Im Folgenden installierten sie erfolgreich die LockBit-Ransomware.

Wie reagiert man auf Angriffe des Dienstleisters?
Für KMUs ist es oft schon nicht leicht, die eigene Cybersicherheit aus wirtschaftlicher Perspektive und personell unter Dach und Fach zu bringen. Ist das einmal geschafft, bleiben externe Risiken bestehen. Angriffe, die vertrauenswürdige Software ausnutzen und die Option der Endpointschutz-Deaktivierung geben, sind besonders perfide, und gern im kriminellen Einsatz. Hier heißt es: besonders sorgfältig und aufmerksam auf Warnungen der Systeme achten, dass der Endpointschutz manipuliert oder deaktiviert wurde!

Der gerade veröffentlichte Threat Report: Cybercrime on Main Street dokumentiert für das letzte Jahr neben RMM-Software eine Reihe von Fällen, in denen Angreifer anfällige Kernel-Treiber von älterer Software nutzten, die noch über gültige digitale Signaturen verfügten. Zudem registrierten die Experten immer wieder Einsätze von speziell erstellter Software, die betrügerisch erlangte digitale Signaturen verwendete – einschließlich bösartiger Kernel-Treiber, die über das Windows Hardware Compatibility Publisher (WHCP)-Programm von Microsoft digital signiert wurden – um die Erkennung durch Sicherheitstools zu umgehen und Code auszuführen, der den Malware-Schutz deaktiviert.

Manipulation von Kernel-Treibern sind ein Problem
Da Kernel-Treiber auf einer sehr niedrigen Ebene innerhalb des Betriebssystems arbeiten und normalerweise vor anderer Software beim Starten des PCs geladen werden, heißt das: sie werden in vielen Fällen ausgeführt, bevor die Sicherheitssoftware überhaupt starten kann. Die digitalen Signaturen fungieren sozusagen als Eintrittskarte. In allen Windows-Versionen seit Windows 10 Version 1607 müssen Kernel-Treiber eine gültige digitale Signatur haben, sonst werden sie von Windows-Betriebssystemen mit aktiviertem Secure Boot nicht geladen.
Nachdem Sophos Microsoft über die Entdeckung der schädlichen Kernel-Treiber im Dezember 2022 informiert hatte und Microsoft einen Sicherheitshinweis herausgab, widerrief das Unternehmen im Juli 2023 eine Reihe von Zertifikaten bösartiger Treiber, die über WHCP bezogen wurden.

Treiber müssen allerdings nicht zwangsläufig bösartig sein, um ausgenutzt zu werden. Die Sophos Security-Spezialisten haben mehrere Fälle gesehen, in denen Treiber und andere

Bibliotheken aus älteren und sogar aktuellen Versionen von Softwareprodukten von Angreifern genutzt wurden, um Malware in den Systemspeicher einzuschleusen.

Ebenso waren Microsoft-eigene Treiber bei Angriffen im Einsatz. Eine anfällige Version eines Treibers für das Microsoft-Dienstprogramm Process Explorer wurde mehrfach von Ransomware-Betreibern verwendet, um Endpunktschutzprodukte zu deaktivieren. Im April 2023 berichtete Sophos über ein Tool namens „AuKill", das diesen Treiber in mehreren Angriffen verwendete, um die Ransomware Medusa Locker und LockBit zu installieren.

Manchmal gelingt es, anfällige Treiber zu identifizieren, bevor sie ausgenutzt werden können. Im Juli wurden die Verhaltensregeln von Sophos durch die Aktivität eines Treibers für ein Sicherheitsprodukt eines anderen Unternehmens ausgelöst. Der Alarm wurde durch einen kundeneigene Angriffssimulationstest ausgelöst. Die Untersuchung des Vorfalls deckte drei Schwachstellen auf, die an den Softwarehersteller gemeldet und daraufhin gepatcht wurden.

KMUs können sich gegen Cyberbedrohungen wehren
Kleiner und mittlere Betriebe sind genauso Cyberbedrohungen ausgesetzt wie weltweit agierende Unternehmen und Konzerne, verfügen aber nicht über die finanziellen und personellen Mittel wie diese. Sie können sich aber wappnen:

- konsequente Schulungen der Mitarbeiter
- Nutzung von Multi-Faktor-Authentifizierung auf allen nach außen gerichteten Anlagen
- konstante Server-und Netzwerkhygiene (regelmäßiges Patchen und Updaten)
- Migration schwer zu verwaltender Ressourcen wie Microsoft Exchange-Server auf SaaS-E-Mail-Plattformen
- Regelmäßige Schwachstellenbewertungen und Penetrationstests

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

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