Mit diesen Tricks verbreitete sich die neue Ransomware-Attacke

Wiesbaden, 28. Juni 2017. SophosLabs hat die in der neuesten Cyberattacke verwendeten Technologien untersucht und festgestellt, dass höchstwahrscheinlich eine neue Variante der Ransomware Petya, auch bekannt als GoldenEye oder PetrWrap, hinter dem massiven Ausbruch in Europa steckt. Allerdings unterscheidet sich der aktuelle Angriff durch eine gefährliche Ergänzung: Die neue Variante enthält zusätzlich den Exploit EternalBlue, um sich noch schneller in einem infiltrierten Netzwerk auszubreiten. Der Exploit greift gezielt den Windows Server Message Block (SMB) Service an, der dazu dient, Dateien oder Drucker ohne große Umstände innerhalb lokaler Netzwerke zu nutzen. Dieses Problem wurde zwar von Microsoft mit Bulletin MS17-010 im März angegangen, ist aber aufgrund fehlender Updates in vielen Systemen noch immer präsent, und der Exploit wurde bereits von WannaCry im letzten Monat genutzt.

Die neue Attacke auf Basis von Petya scheint außerdem zu versuchen, sich innerhalb eines Netzwerks weiter zu verbreiten, in dem es Admin-Passwörter knackt und andere Netzwerk-PCS durch die Nutzung von Remote Admin Tools infiziert. Last but not least dehnt sich die Ransomware durch die Infektion von Netzlaufwerken auf anderen Computern aus. Das geschieht durch die Ausführung eines Codes, der Zugangsdaten stiehlt und die Passwörter von Nutzer-Konten knackt, um Ransomware zu implementieren. Die Malware ist sogar in der Lage Remote-Geräte zu infizieren, indem sie ein legitimes Remote Admin Tool namens PsExec von der Microsoft SysInternals Suite nutzt.

Was sollten Unternehmen jetzt tun?

- Stellen Sie sicher, dass alle Systeme auf dem aktuellen Stand sind – inklusive Microsoft Bulletin MS17-010.
- Evtl. macht es Sinn, das Microsoft-Tool PsExec auf Standard-PCs mit einer Endpoint-Protection-Lösung zu blockieren und so einen Verbreitungsweg einzudämmen.
- Erstellen Sie regelmäßig Back-ups und speichern Sie die letzte Kopie außerhalb des Netzwerks. Eine Verschlüsselung sorgt außerdem dafür, dass Sie keine Angst haben müssen, falls die Datei einmal in die falschen Hände gerät.
- Schulen Sie Mitarbeiter dahingehend, dass Sie Emails mit Anhängen immer mit einer gewissen Vorsicht handhaben, vor allem wenn die Absender nicht bekannt sind.
- Erwägen Sie den Einsatz von Anti-Ransomware-Technologie wie zum Beispiel Intercept X. Eine kostenlose Testversion dieser Lösung, die u.a. WannaCry und die neue Petya-Attacke gestoppt hat, finden Sie hier.

Über Sophos
Sophos ist führender Anbieter von Endpoint- und Network-Security-Lösungen der nächsten Generation. Als Pionier der Synchronized Security entwickelt Sophos sein innovatives Portfolio an Endpoint-, Netzwerk-, Verschlüsselungs-, Web-, E-Mail- und mobilen Security-Lösungen, die miteinander kommunizieren. Mehr als 100 Millionen Anwender in 150 Ländern verlassen sich auf Lösungen von Sophos mit hervorragendem Schutz vor anspruchsvollen Bedrohungen und Datenverlust. Sophos Produkte sind exklusiv über den weltweiten Channel mit mehr als 26.000 registrierten Partnern erhältlich. Sophos hat seinen Hauptsitz in Oxford, Großbritannien, und wird an der Londoner Börse unter dem Symbol "SOPH" öffentlich gehandelt. 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 +172 4536839
sophos@tc-communications.de