SONICWALL

KURZDARSTELLUNG: DIE FOLGEN VON WANNACRY

Anatomie eines Ransomware-Angriffs

Zusammenfassung

Mangelnde Entschlossenheit bei der Einführung von Best Practices kann schwerwiegende Folgen haben — speziell wenn es sich dabei um einen kritischen Bereich wie die Netzwerksicherheit handelt. Jüngstes Beispiel ist eine Ransomware-Attacke, die vor kurzem Schlagzeilen machte und globale Auswirkungen hatte. In dieser Kurzdarstellung erfahren Sie, wie Cyberkriminelle diesen Angriff durchgeführt haben, warum diese Art von Bedrohung nach wie vor eine Gefahr für die IT darstellt und was wir daraus gelernt haben, um zukünftige Angriffe zu vermeiden.

Eine wahre Geschichte

Vor kurzem hackten Cyberkriminelle über eine mit WannaCry-Ransomware präparierte Phishingmail das Netzwerk eines Unternehmens. Einer der Mitarbeiter hatte den E-Mail-Anhang auf einem ungepatchten Computer geöffnet und so den Angreifern Tür und Tor geöffnet. Auf das ungepatchte System angesprochen, meinte der betroffene Unternehmer: „Ich dachte nicht, dass der Patch so wichtig war.“ Kaum zu glauben, aber wahr.

Anatomie eines Angriffs

Bedenkt man, wie einfach diese Panne hätte vermieden werden können, könnte man wirklich weinen – wie der Name *WannaCry* schon sagt. Dieser besonders massive Ransomware-Angriff infizierte über 250.000 Systeme in mehr als 150 Ländern, darunter einige große Healthcare-Einrichtungen im Vereinigten Königreich und sogar eine Reihe größerer Telekommunikationsunternehmen in Spanien.

WannaCry ist lediglich ein Beispiel für einen Typ von Bedrohung, die sich aus einer Ransomware und einem Wurm zusammensetzt, der eine Schwachstelle im SMB-File-Sharing-Protokoll nutzt. Laut unbestätigten Quellen begann alles damit, dass eine US-amerikanische Behörde ein Exploit-Kit (in diesem Fall EternalBlue) entwickelte. Einige Zeit später fiel die Schadsoftware in die Hände von Cyberkriminellen.

Obwohl Ransomware-Angriffe immer öfter in den Medien auftauchen, sind sie nichts Neues. Sie sind ein alltägliches Problem, das jeden treffen kann. Die Ausrede „ich wusste das nicht“ bringt Sie nicht wirklich weiter.

Im April 2017 machte die Hackergruppe Shadow Brokers EternalBlue im Rahmen eines größeren Dumps von Exploits öffentlich, die von der NSA entwickelt worden waren. Teile dieses Exploit-Kits wurden anschließend von Cyberkriminellen in einer neuen, extrem aggressiven Form von Ransomware wiederverwendet. Diese führt einen wurmähnlichen Angriff gegen vernetzte Netzwerkgeräte mittels verschiedener Lese-/Schreibfunktionen des Windows-Betriebssystems durch. Dieser Exploit wirkt bei verschiedenen Versionen der Microsoft-Windows-Betriebssysteme, einschließlich einer Reihe von Versionen, die sich in der End-of-Life-Phase befinden. Obwohl Microsoft zahlreiche Patches veröffentlicht hat, um diese Schwachstelle zu beseitigen, ist dieser Angriff nach wie vor gefährlich, da viele Organisationen den Patch nicht heruntergeladen haben.

Die erste Version des Wurm-/Ransomware-Pakets hatte einen Notausschalter, der aus Versehen getätigt wurde, um den Wurm zu deaktivieren. Somit breitete er sich langsamer aus. Allerdings verfügen die über 20 Versionen, die danach folgten, nicht über diese Schwachstelle. Das Wichtigste ist es, Sicherheitslösungen einzusetzen, die einerseits alle bekannten Versionen von Ransomware stoppen und gleichzeitig neue Ransomware-Angriffe erkennen können.

Fazit

Alle 60 Sekunden werden weltweit über 114 neue Viren und Varianten entwickelt. *WannaCry* ist bestimmt nicht der erste Exploit dieser Art, noch wird er der letzte sein. Unternehmen und Organisationen tun gut daran, sich mit diesen neuen Cybergefahren zu beschäftigen, statt die Augen davor zu verschließen.

Erfahren Sie mehr. Lesen Sie unsere Lösungsübersicht „7 Best Practices zur Bekämpfung von Ransomware“.

Über SonicWall

Seit über 25 Jahren schützt SonicWall kleine, mittlere und große Unternehmen weltweit vor Cyberkriminalität. Mit unseren Produkten und Partnerschaften können wir eine Echtzeit-Cyberabwehrlösung für die individuellen Anforderungen von über 500.000 globalen Organisationen in über 150 Ländern bereitstellen, damit sie sich voll und ganz auf ihr Geschäft konzentrieren können.

Wenn Sie Fragen zur Nutzung dieser Unterlagen haben, wenden Sie sich an:

SonicWall Inc.
5455 Great America Parkway
Santa Clara, Kalifornien 95054, USA

Weitere Informationen finden Sie auf unserer Website.
www.sonicwall.com

ExecBrief-InTheWakeOfWannaCry-US-VG-29362