2017/21 Thema

https://www.jungle.world/artikel/2017/21/das-erfolgsvirus

Wannacry ist gestoppt, aber nicht beseitigt

Das Erfolgsvirus

Von **Elke Wittich Boris Mayer**

Die Ransomware Wannacry, mit der einer der bisher größten Hacker-Angriffe weltweit ausgeführt wurde, ist nicht die erste Schadsoftware, die von der NSA entdeckte Sicherheitslücken ausnutzt. Trotz der großen Reichweite hat sich die Attacke für die Hacker allerdings kaum gelohnt.

Nur die wenigsten Schadprogramme sind erfolgreich genug, um es an prominenter Stelle in die Nachrichten zu schaffen. Die meisten verenden still und von Computernutzern unerkannt in Spamfiltern oder ungeöffneten E-Mail-Attachments.

Wannacry – auch bekannt als Wcrypt, WCRY, Wannacrypt oder Wana Decrypt0r 2.0 – ist dagegen ein echtes Erfolgsvirus; nicht nur Privatanwender, sondern weltweit zahlreiche Institutionen und Firmen wie Krankenhäuser, Autohersteller, Telekommunikationsunternehmen und auch die Deutsche Bahn traf die Cyberattacke.

Besonders innovativ war Wannacry eigentlich nicht, lediglich die Kombination aus verschiedenen Techniken machte den Angriff so erfolgreich. Bei Wannacry handelt es sich nämlich nicht nur um ein Trojanisches Pferd, sondern um ein richtiges Computervirus.

> Die NSA stufte die Gefahr als nachrangig im Vergleich zu den eigenen Interessen ein – und schwieg.

Trojanische Pferde, wie der Name es schon andeutet, tarnen sich als etwas Nützliches oder Schönes – zum Beispiel eine E-Mail –, während sie heimlich Computerviren transportieren. Genau das führte zur schnellen Verbreitung vom Wannacry. Das Verschlüsseln von Dateien und die anschließende Aufforderung an die betroffenen Nutzer, Lösegeld zu zahlen, ist auch nicht gerade neu, sondern hat schon seit Jahren einen eigenen Namen: Ransomware, ein Begriff, der Mitte Mai weltbekannt geworden ist.

Vor Trojanischen Pferden wird eigentlich jeder Computernutzer immer wieder gewarnt: Man soll nicht auf Links oder angehängte Dokumente in E-Mails mit unbekanntem Absender klicken. Die entsprechenden, mehr oder weniger anschaulich gestalteten

Hinweise und Alarmmeldungen kennt man zur Genüge. Weil viele Anwender das inzwischen gelernt haben, hat diese Verbreitungsart es inzwischen sehr schwer und beschränkt sich meistens auf sehr wenige Rechner, bevor Antivirenprogramme die Schädlinge erkennen und ausfiltern – nicht nur auf dem heimischen Computer, sondern oft auch gleich auf dem Mailserver, noch bevor eine solche E-Mail zugestellt wird.

Doch da Wannacry sich als Computervirus selbständig verbreitete, genügten eben diese wenigen anfänglich infizierten Computer. War ein Computer erst einmal befallen, verschlüsselte Wannacry etwa 100 verschiedene Dateitypen und zeigte die Forderung nach Lösegeld an. Zugleich nutzte er einen Systemfehler im Zusammenhang mit der Datei- und Druckerfreigabe im lokalen Netzwerk aus, um weitere Computer zu infizieren. Zusätzlich suchte der Wurm über IP-Anfragen im Netz nach anfälligen fremden Computern.

Aufgehalten wurde der Angriff erst einmal dadurch, dass Analytiker eine Internetadresse im Code entdeckten, die Wannacry zu kontaktieren versuchte. Weil einer der Experten sich weitere Erkenntnisse erhoffte, registrierte er diese Domain, woraufhin sich die Verbreitung des Virus fast bis zum Stillstand reduzierte. Die Entwickler des Virus hatten ihm offenbar eine Abschaltfunktion einprogrammiert, die ausgelöst wird, wenn unter der Webadresse irgend etwas erreichbar ist. Ganz beendet wurde der Angriff durch die Registrierung jedoch nicht, und daran waren ausgerechnet einige Antivirenprogramme Schuld. Sie stuften den Kontaktversuch von Wannacry zu dieser Domain als verdächtig ein und unterbanden ihn – woraufhin sich das Virus weiterverbreitete, statt abgeschaltet zu werden.

Der Virenstopp bedeutete nicht, dass die bereits verschlüsselten Computer wieder funktionierten. Aber immerhin war die Verbreitung so stark gebremst, dass die technische Aufarbeitung beginnen konnte.
Die Virusfunktion von Wannacry bediente sich einer Sicherheitslücke, die Microsoft bereits im März geschlossen hatte. Die Mehrzahl der infizierten Computer hatten diese Updates jedoch nicht eingespielt, sonst hätte sich das Virus auch nicht verbreiten können – eine Ausnahme stellen jene Systeme dar, die sich über eine E-Mail infizierten.

Die Sicherheitslücke existierte jedoch schon viel länger. Öffentlich bekannt wurde sie erst dadurch, dass die National Security Agency (NSA) Microsoft auf die Lücke aufmerksam machte. Das geschah nach einem Einbruch in die Computersysteme der NSA, bei dem mehrere interne Hackertools gestohlen wurden, die die NSA für Ermittlungen nutzte. Eines dieser Programme verwendete die Lücke schon seit mehr als fünf Jahren, erst dann trat Wannacry auf den Plan.

Obwohl die NSA nicht wissen konnte, ob die Schwachstelle nicht auch Hackern bereits aufgefallen war, stufte sie die Gefahr als nachrangig im Vergleich zu den eigenen Interessen ein – und schwieg.

Microsoft kritisierte denn auch vehement, von der Behörde nicht schon lange informiert worden zu sein. Wäre Wannacry nur ein paar Monate früher in dieser Version erschienen, wären die Auswirkungen in der Tat weit schlimmer gewesen. Für Windows 7 und aufwärts stand der Patch zum tatsächlichen Angriffszeitpunkt allerdings schon bereit und war auf vielen Systemen eingespielt. Microsoft stellte schnellstmöglich auch Patches für

Betriebssysteme zur Verfügung, die eigentlich gar nicht mehr mit Updates versorgt werden.

Costin Raiu, Director of Global Research and Analysis bei Kaspersky Lab – ein weltweit anerkanntes Softwareunternehmen für Computersicherheit –, veröffentlichte vorige Woche eine Statistik, dass 98 Prozent der infizierten Computer Windows 7 verwendeten. Von Microsoft nicht mehr unterstützte Windows-Versionen hatten also nur einen sehr kleinen Anteil an der Verbreitung – wie auch das aktuelle Windows 10. Letzteres dürfte vor allem daran liegen, das Windows 10 dem Nutzer nicht mehr die Wahl lässt, ob Updates installiert werden oder nicht – zur Not wird der Anwender einfach darüber informiert, dass das System in drei Minuten neu gestartet wird, weil Updates fertig installiert werden müssen. Beliebter macht dieses Vorgehen das Installieren von solchen Updates zwar nicht, aber der Wannacry-Angriff zeigt, dass automatische Updates ein entscheidender Sicherheitvorteil sind. Gleichwohl bleibt die Frage, warum in wichtigen Infrastrukturbereichen wie Krankenhäusern nicht auf Sicherheitsupdates geachtet wird. Es ist schließlich sehr fahrlässig, wichtige Systeme, deren Funktionieren durchaus über Leben und Tod entscheiden kann, nicht entsprechend zu warten und zu administrieren.

Bis es eine neue Schadsoftware als Aufmacher in die Fernsehnachrichten schafft, wird es vielleicht Monate oder sogar Jahre dauern. Gleichwohl bleiben diese Programme eine ständige Gefahr. G DATA, ein Hersteller von IT-Sicherheitslösungen bezifferte die Anzahl der allein im Jahr 2016 neu entdeckten Schadprogrammtypen auf 6,83 Millionen. Dabei enthält ein Schadprogrammtyp eben nicht nur ein einziges Programm, sondern in den meisten Fällen gleich eine ganze Familie von Programmen, also mehrere Versionen, die auf dem gleichen Programmcode beruhen und dieselben Angriffswege wählen. Die Tendenz für 2017 ist steigend.

Wannacry ist übrigens nicht die erste Schadsoftware, die diese bei der NSA gestohlenen Lücken ausnutzte. Ein Trojanisches Pferd mit dem Namen Adylkuzz verbreitete sich auf demselben Weg, machte sich aber nicht durch spektakuläre Lösegeldforderungen bekannt, sondern rechnete einfach nur still im Hintergrund. Das Programm schürfte nach Geld in der Kryptowährung Monero. Dem Nutzer eines Computers konnte dabei nur auffallen, dass der Computer langsamer lief als normal – und das ist ja gefühlt eigentlich immer der Fall. (Bei Kryptowährungen muss Rechenzeit investiert werden, um Aufgaben zu lösen, die dann weiteres Geld freischalten, um die verfügbare Geldmenge in dieser Währung langsam, aber ständig zu erhöhen. Wer bei diesen Berechnungen einen Treffer landet, darf das neu entstandene Geld behalten, deshalb spricht man hier auch von »Mining«.)

Die Attacke mit Adylkuzz war deutlich profitabler als die mit Wannacry – eine Million Dollar sollen die Hacker umgerechnet erzeugt haben.
Wannacry hingegen war Experten zufolge, die den Bitcoin-Account der Wanncry-Programmierer beobachten (etwa auf **cnet.com**), ein ziemlicher Flop: Die Einnahmen lagen bei lediglich rund 100 000 Dollar.

© Jungle World Verlags GmbH