

« vorige | nächste »

Kommentar zu WannaCry: Staatliche Dienste müssen Erkenntnisse teilen

14.05.2017 08:30 Uhr – Michael Link

vorlesen



(Bild: dpa, Jim Lo Scalzo)

Der Krypto-Trojaner WannaCry wird nicht der letzte sein. Aber es ist beschämend, dass Anwender und die Software-Anbieter daraus nicht lernen – und auch die Geheimdienste tragen Verantwortung, meint Michael Link

Es ist also schon wieder passiert: Ein Krypto-Trojaner namens [WannaCry kapert Rechner](#), blockiert [Anzeigetafeln der Bahn](#) und sorgt dafür, dass [britische Patienten von Krankenhäusern abgewiesen](#) werden. Klar, die Schuldigen sind die Erpresser, die Summen zwischen 300 und 600 US-Dollar von ihren Opfern fordern. Aber damit macht man es sich zu einfach, denn dies war nur "dank" fahrlässiger Mithilfe vieler möglich.

Danke, Microsoft! Echt?

Der Krypto-Trojaner nutzt [längst bekannte Einfallstore](#). Microsoft hat mit der Behäbigkeit eines Flugzeugträgers auf Sicherheitslücken reagiert und erst im März einen Sicherheitspatch geliefert. Wird schon gutgehen? Diesmal nicht. Denn hier kommen die Nutzer ins Spiel: Viele Menschen ignorieren die aktuellen Sicherheitspatches. Wie bei Impfgegnern schadet das nicht nur ihnen selbst, sondern sie erhalten damit die Fortpflanzungsfähigkeit der Ransomware und helfen bei der Verbreitung der digitalen Erpresser.

Sind also die Nutzer schuld? Nein, auch damit macht man es sich zu einfach. Denn viele sind zu Recht genervt von dem, was bei Sicherheitspatches noch so mit ihren Rechnern passiert. So muss man oft Datenschutzfreigaben und mühsam gefundene Voreinstellungen wieder zurückstellen. Aber auch die schiere Größe der Updates macht Probleme für jene Nutzer, die nicht mit einem potenten Breitbandanschluss gesegnet sind.

Immerhin: Wenigstens hat Microsoft außer der Reihe einen Patch für das nicht mehr gepflegte, aber weltweit noch millionenfach eingesetzte Windows XP geliefert. Da muss man sich schon fragen: Wieso sind diese Systeme noch so verbreitet? Auch dafür gibt es viele mögliche Antworten. nicht zuletzt: "Never change a running system!". Warum auswechseln.

Ein Kommentar von Michael Link



Michael Link, c't-Redakteur, gebürtiger Rheinländer, testet gern, was mit Funk und Wearables zu tun hat. Leidenschaftlicher Taucher (Tauchlehrer), Funkamateurl, Rennrad- und Mountainbike-Fahrer.

Ähnliche Artikel

Weltweiter Erpressungstrojaner-Angriff auf Computernetzwerke

"WannaCry": Das Bundeskriminalamt (BKA) hat die strafrechtlichen Ermittlungen übernommen. Global sollen 99 Länder betroffen sein



74

Analysiert: Ransomware meets Info-Stealer - RAA und das diebische Pony

Im Rahmen unserer Analysiert-Serie geht es diesmal einem Erpressungstrojaner an den Code: Olivia von Westernhagen untersucht den in JavaScript...



6

BKA bis Goldeneye: Geschichte der Erpressungs-Trojaner

Mit Goldeneye und Locky erlebt Ransomware im Jahr 2016 Hochkunjunktur. Das Geschäft mit gekaperten Rechnern und verschlüsselten Daten gab es schon...



Anzeige

TÜVRheinland®
Genau. Richtig.

Zielgerichtet weiterentwickeln.
Werden Sie Cloud Administrator, Cloud Developer oder Cloud Architect

[Zu den Lempfaden](#)

Anzeige

Schöpfen Sie das Potenzial von Flash-Arrays aus? Erfüllt Ihre Lösung die Erwartungen der Nutzer? Kostenlos: Nützliche eBooks für Bildung und Beruf! Über 5.000 Gutscheine für heise online User Mehr IT-Sicherheit – durch Mitarbeiterschulungen! IBM Maas360 und Watson entlasten den Admin Schwachstelle Drucker – Einfallstor für Hacker Unternehmensdaten in der Cloud – ein Risiko? heise jobs, dein Stellenmarkt für den IT-Sektor

...möglichst funktionieren, nicht zuletzt: "never change a running system". Warum ausgerechnet, was funktioniert? Besonders, wenn ein Umstieg auf neuere Betriebssysteme Geld kostet oder dringend benötigte Hardware nur mit Uralt-Betriebssystemen läuft, so wie in vielen Krankenhäusern, wo die Betreiber durch diese Wurschtigkeit nun sogar Menschenleben riskiert.

Die so genannten Sicherheitsdienste

Was an diesem Fall besonders pikant ist: Den Angriffsweg des Krypto-Trojaners hat sich kein Klischee-Hacker mit Kapuzenpullover im Keller ausgedacht, sondern eine NSA-nahe Gruppe, wenn man den immer weiter präzisierten [Enthüllungen der Shadow Brokers](#) glauben darf. Die Geheimdienste ließen also nicht nur dieses Angriffsszenario entwickeln, sie hielten auch die ihnen zugrunde liegenden Sicherheitslücken geheim.

Wenn ein Geheimdienst, der sich die "Sicherheit" des Landes und seiner Bürger auf die Fahnen schreibt, mit solchen Unterlassungen die Sicherheit von Internetnutzern gefährdet, muss man da nicht protestieren? Muss man nicht verlangen, dass Sicherheitslücken, auf die staatliche Stellen stoßen, umgehend öffentlich gemacht werden? Oder zählen die sogenannten Sicherheitsinteressen der Regierungen mehr als echte Computersicherheit für Millionen Bürger?

Am ehesten sollten die Regierenden das Interesse ihrer Bürger (und damit ihrer Wähler) im Auge haben. Wie sehr die Demokratie in Gefahr gerät, wenn die Allgemeinheit das Gefühl bekommt, dass der Staat unter dem Vorwand des Terrorschutzes sogar massive Verbrechen an den Bürgern in Kauf nimmt, das sieht man an Wahlergebnissen in vielen Ländern.

[\(mil\)](#)

[Kommentare lesen \(48 Beiträge\)](#)

[« vorige | nächste »](#)

Forum bei heise Security: [heise Security](#)

[zur Startseite](#)



<https://heise.de/-3713450>

[Drucken](#)

Mehr zum Thema [#saukontrovers](#) [Ransomware](#) [Malware](#)

Weitere News zum Thema

WannaCry: Microsoft liefert Sicherheits-Patches für veraltete Windows-Versionen

Selbst das 16 Jahre alte Windows XP, das Microsoft seit 2014 nicht mehr pflegt, bekam nun einen Sicherheits-Patch. Die dramatischen Folgen der...

13. Mai 2017, 11:52 Uhr 180

WannaCry: Was wir bisher über die Ransomware-Attacke wissen

Es begann am Freitagabend mit Schreckensmeldungen aus Großbritannien: Computer des nationalen Gesundheitssystem waren von einer Ransomware infiziert.

13. Mai 2017, 16:20 Uhr 435

WannaCry: Angriff mit Ransomware legt weltweit Zehntausende Rechner lahm

In ganz England hat ein Kryptotrojaner am Freitag zahlreiche Krankenhäuser lahmgelegt. Und das ist offenbar nur die Spitze des Eisbergs einer...

12. Mai 2017, 17:59 Uhr 1209

Geleakte NSA-Hackersoftware: Erkennungstool kann Malware nun auch entfernen

Gegenwärtig infizieren Unbekannte mit einer geleakten Malware der NSA unzählige ungepatchte Windows-Computer in aller Welt. Das Tool, das diese...

26. April 2017, 11:00 Uhr 20

Themen im Trend

[Schnelles Internet: 1000 Gigabit/s per Telefonkabel](#)

[WannaCry: Was wir bisher über die Ransomware-Attacke wissen](#)

[Naidoo und Gerüchte über das System](#)

[WannaCry: Angriff mit Ransomware legt weltweit Zehntausende Rechner lahm](#)

Gegenwind für Glasfaser und TV-Kabel: Der DSL-Erfinder John Cioffi will mit extrem hochfrequenter Übertragung ein Terabit pro Sekunde über 100 Meter...

13. Mai 2017, 18:33 Uhr 101

Es begann am Freitagabend mit Schreckensmeldungen aus Großbritannien: Computer des nationalen Gesundheitssystem waren von einer Ransomware infiziert.

13. Mai 2017, 16:20 Uhr 435

Xavier Naidoo ist kein "Systemkritiker". Wer das Unverzeihliche an seinen Texten verteidigt, läuft Gefahr, zur Marionette seiner Medienstrategie zu...

315

In ganz England hat ein Kryptotrojaner am Freitag zahlreiche Krankenhäuser lahmgelegt. Und das ist offenbar nur die Spitze des Eisbergs einer...

12. Mai 2017, 17:59 Uhr 1209

WannaCry
Was wir bisher über die Ransomware-Angriffe wissen



Es begann am Freitagabend mit Meldungen aus Großbritannien: Computer des nationalen Gesundheitssystems waren mit Ransomware...

Schnelle Reaktion
Microsoft liefert Patches für alte Windows-Versionen



Selbst das 16 Jahre alte Windows XP, das Microsoft seit 2014 nicht mehr pflegt, bekam nun einen Sicherheits-Patch.

WannaCry
Ransomware legt weltweit Rechner lahm



So fing es an: In ganz England hat der Kryptotrojaner am Freitag zahlreiche Krankenhäuser lahmgelegt.

WannaCry
Sicherheitsexperte findet "Kill-Switch"



Durch Zufall hat ein Security-Experte eine Funktion im Code entdeckt, der die Verbreitung offenbar stoppt.

- | | | | | | | |
|-------------------|-----------------|-------------------|----------------|----------------|----------------|----------------|
| heise online | Telepolis | heise Netze | heise Video | heise Events | Artikel-Archiv | Leserforum |
| c't Magazin | Make | Open Source | TechStage | IT-Markt | Abo | Newsletter |
| iX Magazin | heise Autos | heise Security | Download | heise Business | Loseblattwerke | Suche |
| Technology Review | heise Developer | heise Produkte | Preisvergleich | Services | RSS | iMonitor |
| Mac & i | | Spielen bei Heise | Stellenmarkt | Tarifrechner | | Netzwerk-Tools |
| c't Fotografie | | | | Shop | | |