Der monatliche Security Awareness Newsletter für Jedermann

OUCH!

IN DIESER AUSGABE...

Was lernen wir aus WannaCry

Überblick

Sie haben kürzlich sicher auch die unüberseh- und –hörbaren Medienberichte zum Cyberangriff namens „WannaCry“ mitbekommen. “WannaCry” infizierte binnen weniger Tage mehr als 200.000 Computer, und entzog einer Vielzahl von Unternehmen den Zugriff auf ihre Daten, darunter Krankenhäuser in Großbritannien. Dieser Angriff erlangte aus verschiedenen Gründen so große Aufmerksamkeit: Er griff eine bekannte Schwachstelle in Microsoft Windows an und verbreitete sich dadurch in Windeseile von Computer zu Computer. Zudem handelte es sich um einen Angriff mit sogenannter “Ransomware”, d.h. einem Schadprogramm das die Dokumente auf Ihrem Computer verschlüsselt und Ihnen so den Zugriff auf Ihre Daten verwehrt. Der einzige Weg, wieder Zugriff auf Ihre Daten zu erhalten, besteht in einer Zahlung von 300 USD an die Erpresser. Der gewichtigste Grund ist jedoch, dass ein solcher Angriff nie möglich gewesen sein sollte. Die Windows-Schwachstelle, die “WannaCry” nutzte, war bei Microsoft seit einiger Zeit bekannt, ja sogar 2 Monate vorher durch einen Patch geschlossen. In vielen Unternehmen war der Patch jedoch noch nicht eingespielt, oder sie nutzten noch Betriebssysteme wie Windows XP, die so alt sind, daß kein Patch mehr dafür erschien. Hier sind drei Schritte die Sie unternehmen können um sicherzugehen, dass Angriffe wie „WannaCry“ Ihnen nicht schaden können.

Gastautor

Dr. Johannes Ullrich ist Leiter des Forschungsbereichs des SANS Technology Institute und Gründer von DShield.org. Er verantwortet das **SANS Internet Storm Center**, welches aktuelle Bedrohungen im Bereich Cybersicherheit beobachtet. Darüber hinaus lehrt er die SANS Kurse Web Application Security (**DEV522**), Intrusion Detection (**SEC503**) und IPv6 (**SEC546**).

Patchen

Der wichtigste Schritt besteht darin, für Computer, Mobilgeräte, Apps und alles was mit dem Internet verbunden ist sicherzustellen, dass es aktuell ist. Cyberkriminelle suchen fortwährend nach Schwachstellen im Code von Apps und Geräten. Wenn sie eine solche Schwachstelle entdecken, nutzen sie spezielle Programme um sich damit Zugriff auf die Geräte zu verschaffen. Die Hersteller der Geräte und Programme arbeiten zeitgleich mit Hochdruck daran, Updates zum Schließen dieser Schwachstellen zu veröffentlichen. In dem Sie sicherstellen, dass Ihre Geräte solche Updates zeitnah installieren, machen Sie es Angreifern viel schwerer, Sie zu hacken. Genau das ist das Frustrierende an der Verbreitung von WannaCry. Die Aktualisierungen, die den Angriff verhindern, wurden fast zwei Monate vorher von Microsoft veröffentlicht. Hätten Unternehmen ihre Computer aktuell gehalten, wäre dieser Angriff nie von Erfolg gekrönt gewesen. Aktivieren Sie

© SANS Institute 2017

Was lernen wir aus WannaCry

daher auf Ihren Geräten wann immer möglich die Funktion für „Automatische Updates“. Das betrifft nahezu jede Technologie die mit dem Internet verbunden ist, nicht nur Ihre Computer und Mobilgeräte, sondern auch Fernseher mit Netzwerkanbindung, WLAN-Router, Spielekonsolen und vielleicht sogar Ihr Auto. Wenn Betriebssystem oder Geräte selbst so alt sind, dass sie vom Hersteller nicht mehr mit Sicherheitsaktualisierungen versorgt werden, wie beispielsweise Windows XP, ersetzen Sie sie mit einer neuen, aktuellen Version die wieder Unterstützung bietet.

Wichtig zum Schutz vor Angriffen wie WannaCry sind drei einfache Schritte; Aktuellhalten Ihrer Computer, Sicherung Ihrer Daten und Vorsicht vor Phishing Angriffen.

Datensicherung

In einigen Fällen infizieren Angriffe mit Erpresser-Schadsoftware („Ransomware“) sogar Geräte, die auf dem aktuellen Stand sind. Ein weiterer Baustein zur Sicherung Ihrer Daten ist daher die regelmäßige Datensicherung. Unter Datensicherung versteht man eine Kopie Ihrer Daten, die an einem anderen Ort als auf Ihrem Computer oder Mobilgerät gespeichert ist. Wenn Sie wertvolle Daten verlieren, können Sie diese aus einer Datensicherung wiederherstellen. Leider erstellen viel zu wenige Menschen regelmäßige Datensicherungen, obwohl sie sehr einfach und kostengünstig wären. Es gibt zwei Wege zum Sichern Ihrer Daten: auf physische Medien oder cloud-basierten Speicher. Jeder Ansatz hat seine Vor- und Nachteile, sie können jedoch auch beide Verfahren kombinieren wenn Sie sich nicht sicher sind, welches Verfahren für Sie das geeignetere ist.

Unter “Medien” verstehen wir Datenträger oder Geräte unter Ihrer Kontrolle, wie z.B. externe USB Laufwerke oder via WLAN zugreifbare Netzwerkgeräte. Der Vorteil, ein eigenes physisches Medium zu benutzen, besteht darin, dass man sehr schnell große Datenmengen sichern und wiederherstellen kann. Der Nachteil eines solchen Vorgehens ist, dass wenn Sie z.B. mit einer Erpresser-Schadsoftware infiziert werden, sich diese auch auf Ihre Datensicherung ausbreiten kann. Auch wenn ein Unglück wie z.B. ein Brand oder Diebstahl eintritt kann dies zu einem totalen Datenverlust, einschließlich der Datensicherung, führen. Wenn Sie externe Geräte für Datensicherungen nutzen, sollten Sie daher einen Prozess haben um die Datenträger an einem anderen, entfernten Ort zu lagern. Stellen Sie aber sicher, alle Datensicherungen eindeutig zu kennzeichnen. Cloud-basierte Lösungen sind Onlinedienste, die Ihre Dateien im Internet speichern. Sie zeichnen sich vor allem durch ihre einfache Nutzung aus. Außerdem kann eine Infektion mit Ransomware den in der Cloud gesicherten Daten nichts anhaben. Nachteilig ist die lange Dauer zur Sicherung und Wiederherstellung größerer Datenmengen. Sehen Sie sich

Was lernen wir aus WannaCry

unbedingt die AGB hinsichtlich Datenschutz bzw. Datensicherheit und Vertraulichkeit an. Bietet der Datensicherungsdienst Funktionen zur Verschlüsselung und sichere Anmeldeverfahren?

Phishing

Die Angreifer verändern ihre Angriffsmethoden ständig und passen sie an aktuelle Gegebenheiten an. Cyberkriminelle nutzen häufig eine Methode namens „Phishing“, um ihre Opfer anzugreifen. Dabei senden sie Ihnen eine E-Mail, mit der sie versuchen Sie zum Öffnen eines infizierten Anhangs oder zum Aufruf einer präparierten Webseite zu verleiten. Wenn Sie eines davon tun, wird Ihr Computer möglicherweise infiziert. “WannaCry” hat diese Methode nicht genutzt, doch sie ist sehr gängig bei vielen anderen Angriffsformen, darunter bei nahezu allen Ransomware-Angriffen. Die Cyberkriminellen, die WannaCry entwickelt haben, können zweifelsfrei ihre Angriffsmethoden in den kommenden Monaten anpassen und z.B. über Phishing noch viel mehr Computer infizieren. Der Schlüssel zu Ihrem Schutz ist gesunder Menschenverstand beim Erhalt verdächtiger E-Mails. Wenn eine E-Mail komisch oder verdächtig aussieht oder klingt, oder einfach zu gut um wahr zu sein, handelt es sich sehr wahrscheinlich um einen Angriff.

Weiterführende Informationen

Schadprogramme:	https://securingthehuman.sans.org/ouch/2016#march2016
Ransomware:	https://securingthehuman.sans.org/ouch/2016#august2016
Datensicherung:	https://securingthehuman.sans.org/ouch/2015#august2015
Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Sichere Nutzung der Cloud:	https://securingthehuman.sans.org/ouch/2016#november2016

Informieren Sie Sich

Abonnieren Sie den monatlichen OUCH! Security Awareness Newsletter, greifen Sie auf die OUCH! Archive zu und lernen Sie mehr über SANS Security Awareness Angebote unter securingthehuman.sans.org/ouch/archives.

Deutsche Ausgabe

Diese OUCH! Ausgabe wurde von Marek Kreul und René Wiedewilt aus dem Englischen übersetzt. Beide arbeiten für das CERT eines DAX-Konzerns und haben sich auf IT-Forensik spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

OUCH! wird durch das SANS Securing The Human Programm herausgegeben und unter der Creative Commons BY-NC-ND 4.0 Lizenz vertrieben. Die Erlaubnis zur Weitergabe dieses Newsletters oder Verwendung in einem Weiterbildungsprogramm wird gewährt, solange der Newsletter unverändert bleibt. Für Übersetzungen und weitere Informationen kontaktieren Sie bitte ouch@securingthehuman.org.

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley