Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Überblick
- Anzeichen einer Kompromittierung
- Richtige Verhaltensweisen

Ich wurde “gehackt”, was nun?

Überblick

Natürlich sind Sie besorgt über die Sicherheit Ihres Computers und Ihrer Daten, und überlegen was Sie unternehmen können um diese zu schützen. Vergleichbar dem Autofahren, wo Sie früher oder später Teil eines Unfalls sein werden, egal wie umsichtig Sie fahren, kann dies auch auf Ihre PC-Nutzung zutreffen. In diesem Newsletter werden wir Ihnen erläutern, woran Sie erkennen können ob Ihr Computer kompromittert (“gehackt”) wurde, und was Sie in einem solchen Fall unternehmen sollten. Letztendlich ist es so, dass Sie Schaden um so besser abwenden können, je schneller Sie einen Angriff erkennen und je besser und kompetenter Sie darauf reagieren.

Gastautor

Jake Williams (**@MalwareJake**; **malwarejake.blogspot.com**) ist wissenschaftlicher Leiter bei CSRgroup, einem auf Beratung im Kontext IT-Sicherheit spezialisierten Unternehmen. Er ist zudem der Co-Autor der Kurse Memory Forensics (FOR526) und Malware Reverse Engineering (FOR610) des SANS Institute.

Anzeichen einer Kompromittierung

Zunächst sollten Sie verstehen, dass in den meisten Fällen nicht ein einziger Blick auf einen einzigen Aspekt genügt, um zu erkennen ob Ihr Computer kompromittiert ist. Es sind meist mehrere Indikatoren die zusammengenommen einen solchen Schluss zulassen. Hier sind einige Beispiele:

- Ihr Antivirus-Programm hat einen Alarm bezüglich. einer infizierten Datei angezeigt und meldet vielleicht sogar, diese nicht löschen oder in “Quarantäne” verschieben zu können.
- Die Startseite Ihres Internetbrowsers hat sich plötzlich ohne Ihr Zutun verändert oder Sie werden auf Webseiten umgeleitet, die Sie nicht aufgerufen haben
- Auf Ihrem Computer existieren neue Benutzerkonten, die Sie nicht angelegt haben
- Es laufen neue Dienste oder Programme, die Sie nicht installiert haben
- Ihr Computer stürzt gehäuft ab oder läuft sehr langsam
- Ein Programm auf Ihrem Computer fordert Ihre Zustimmung an, um Veränderungen am System vorzunehmen; Sie selbst haben jedoch keine Installation oder Aktualisierung aktiv gestartet
- Ihre Firewall alarmiert Sie weil ein Programm, dass Sie nicht gestartet haben, Zugriff auf das Internet anfordert.

Ich wurde “gehackt”, was nun?

Richtige Verhaltensweisen

Wenn Sie den begründeten Verdacht haben, dass Ihr Computer kompromittiert wurde, gilt es schnell und kompetent zu handeln. Wenn Ihnen der Computer von Ihrem Arbeitgeber bereitgestellt wurde, sollten Sie nicht versuchen selbst zu reparieren und den Computer auch nicht ohne Rücksprache mit Experten ausschalten. Sie würden damit eventuell mehr schaden als nutzen und möglicherweise sogar wertvolle Beweise zerstören die in einer Untersuchung entscheidend sein können. Melden Sie stattdessen den Vorfall an die zuständigen Stellen Ihres Arbeitgebers, meist die IT Hotline, das Sicherheitsteam oder Ihre Vorgesetzten. Wenn eine Kontaktaufnahme zeitnah nicht erfolgreich sein sollte, trennen Sie den Computer vom Netzwerk und aktivieren den Standby- oder Ruhezustands-Modus. Auch wenn Sie sich mit Ihrem Verdacht einer Kompromittierung nicht sicher sind ist es wichtig, diesen Verdacht zu melden. Wenn Ihr Unternehmen über Prozesse und ein Spezialistenteam für derartige Situationen verfügt, lassen dieses alles Weitere übernehmen.

Früher oder später besteht die Gefahr, dass Ihr Computer einem Angriff zum Opfer fällt. Je früher Sie einen Vorfall erkennen und je vorbereiteter Sie sind, um so geringer fallen die Konsequenzen aus.

Wenn der Computer nur Ihnen selbst gehört bzw. privat genutzt wird, sollten Sie die folgenden Schritte befolgen:

- **Backups**: Der wichtigste vorbereitende Schritt ist die regelmäßige Erstellung von Sicherungskopien, sog. Backups. Stellen Sie dabei aber auch sicher, dass die gesicherten Daten im Falle eines Falles auf einem anderen Gerät lesbar sind. Oft ist bei kompromittierten Computern die einzige Möglichkeit der Bereinigung, das System komplett zu löschen und von Grund auf neu zu installieren oder gar einen neuen Computer zu kaufen. In jedem Fall benötigen Sie ein funktionierendes Backup, um Ihre Daten wiederherstellen zu können.
- **Ändern Ihrer Passwörter**: Stellen Sie sicher alle Ihre Passwörter zu ändern. Nutzen Sie hierfür einen anderen, vertrauenswürdigen Computer, und ändern Sie alle Passwörter bei allen Onlinediensten die sie nutzen.
- **Antivirus**: Wenn Sie Ihr Antivirenprogramm über eine infizierte Datei informiert, können Sie gewöhnlich die vorgeschlagenen Aktionen befolgen. Gängig sind hier ein Verschieben in Quarantäne, das Bereinigen oder vollständige Löschen der Datei. Viele Antivirenprogramme bieten auch noch die Möglichkeit, weitere Informationen zur erkannten Bedrohung auf den Internetseiten des Herstellers nachzulesen.
- **Neuinstallation**: Wenn es nicht möglich ist den Computer mittels Antivirensoftware zu säubern, ist einer der sichersten Wege, den Computer von Grund auf neu zu installieren. Trennen Sie dafür zunächst die

Ich wurde “gehackt”, was nun?

Netzwerkverbindung und folgen Sie dann der Anleitung des Herstellers des Computers. In den meisten Fällen bedeutet das, das System von der eingebauten Wiederherstellungspartition zu starten, um das Betriebssystem neu zu installieren. Sollte diese fehlen, kontaktieren Sie den Hersteller um Unterstützung oder ein Installationsmedium anzufordern. Stellen Sie das System nicht aus dem Backup wieder her, dieses enthält wahrscheinlich die Schwachstellen, über die der Angreifer Zugriff auf Ihren Computer erhielt. Aus dem Backup sollten Sie nur Ihre benötigten Benutzerdaten wiederherstellen. Falls Ihr Computer bereits betagt ist, wird es einfacher (und vielleicht sogar günstiger) sein, einen neuen zu kaufen statt mühsam den alten neu zu installieren.

- **Professionelle Unterstützung**: Wenn Sie befürchten gehackt worden zu sein, aber der Meinung sind nicht über ausreichende Kenntnisse zu verfügen um dem zu entgegnen, sollten Sie Ihren Computer in professionelle Hände geben. Sollten Sie z.B. feststellen, dass Ihr Computer kompromittiert ist und Sie nicht über ein aktuelles Backup verfügen, könnten Sie versucht sein kritische Daten vom infizierten System auf ein neues zu übertragen. Dabei können Sie jedoch unabsichtlich auch Schadprogramme wieder auf das neue System aufbringen, und das Spiel beginnt von neuem. Ein viel besserer Weg ist es dann, den infizierten Computer einem qualifizierten Spezialisten zu übergeben, der die benötigten Daten sichern kann ohne das Risiko einer Infektion des neuen Systems eingehen zu müssen.

Weiterführende Informationen

OUCH! Backups:	http://www.securingthehuman.org/ouch/2013#september2013
OUCH! Passwörter:	http://www.securingthehuman.org/ouch/2013#may2013
OUCH! Was ist Malware:	http://www.securingthehuman.org/ouch/2014#february2014
Detecting Evil Poster:	https://digital-forensics.sans.org/media/poster_2014_find_evil.pdf

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 http://www.securingthehuman.org.

Deutsche Ausgabe

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

Redaktionsleitung: Bill Wyman, Walt Scrivens, Phil Hoffman, Bob Rudis