Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

Ich wurde gehackt, was nun?

Überblick

Wir gehen davon aus, dass Sie als Leser des OUCH! Newsletters sich um die Sicherheit Ihres Computers und Ihrer Mobilgeräte kümmern und Maßnahmen zu deren Schutz getroffen haben. Ganz gleich wie vorsichtig Sie bei der Nutzung dieser Technologie sind – früher oder später werden sie möglicherweise 'gehackt' oder 'kompromittiert'. In diesem Newsletter lernen Sie, wie Sie die Anzeichen dafür erkennen und wie Sie richtig darauf reagieren. Je schneller Sie erkennen, dass etwas nicht stimmt und je schneller und besser Sie reagieren, desto weniger Schaden werden die Cyberangreifer anrichten können.

Gastautor

Samantha Davison (**@sam_e_davison**) ist bei Uber für die IT Sicherheitstrainings der weltweit auf 350 Städte verteilten Mitarbeiter zuständig.

Anzeichen, dass Sie gehackt wurden

Es ist schwer festzustellen, ob man gehackt wurde, da es keinen bestimmten Weg gibt, das herauszufinden. Hacker hinterlassen aber oft verschiedene Spuren, auch Indikatoren genannt. Je mehr dieser Indikatoren Ihr System aufweist, desto wahrscheinlicher ist, dass es gehackt wurde.

- Ihr Antivirus-Programm hat Sie alarmiert, dass Ihr System infiziert ist. Besonders kritisch ist ein Alarm der besagt, dass die betroffene(n) Datei(en) nicht entfernt oder in Quarantäne verschoben werden konnte(n).
- Die Startseite Ihres Browsers wurde unerwartet geändert, oder Ihr Browser leitet Sie auf Webseiten, die Sie nicht aufgerufen haben.
- Es gibt neue Benutzerkonten auf Ihrem Computer oder Mobilgerät, die Sie nicht angelegt haben, oder neue Programme, die Sie nicht installiert haben.
- Ihr Computer oder manche Anwendungen stürzen fortwährend ab, es gibt Symbole für unbekannte Anwendungen oder komische Fenster erscheinen unerwartet.
- Ein Programm erfordert Ihre Zustimmung um Änderungen am System vorzunehmen, Sie haben jedoch keine Installation oder Aktualisierung angestoßen.
- Beim Versuch, sich am System oder einem Online Benutzerkonto anzumelden wird Ihr Passwort nicht mehr akzeptiert, obwohl Sie sich sicher sind es korrekt eingegeben zu haben.
- Freunde fragen Sie, warum Sie sie mit E-Mails bombardieren obwohl Sie diese nie abgeschickt haben.

Ich wurde gehackt, was nun?

- Ihr Mobilgerät verursacht unberechtigt Gebühren für die Nutzung von Premium SMS Nummern.
- Ihr Mobilgerät verbraucht überraschend sehr viel Datenvolumen oder Akkuladung.

Je schneller Sie eine Kompromittierung Ihres Computers oder Mobilgeräts feststellen und darauf reagieren, desto besser.

Richtig reagieren

Wenn Sie den Verdacht haben, Ihr Computer oder Mobilgerät sei gehackt worden, sollten Sie so schnell wie möglich reagieren. Versuchen Sie nicht das Problem auf eigene Faust zu lösen, wenn das Gerät von Ihrem Arbeitgeber bereitgestellt oder für die Arbeit genutzt wird. Sie können dadurch nicht nur mehr Schaden als Nutzen verursachen, sondern sogar wichtige Beweismittel vernichten die für eine Untersuchung essentiell sind. Melden Sie stattdessen den Vorfall sofort an Ihren Arbeitgeber, üblicherweise an den Helpdesk, an das Sicherheitsteam oder Ihren Vorgesetzten. Wenn Sie Ihr Unternehmen aus irgendwelchen Gründen nicht kontaktieren können oder einen zeitlichen Verzug fürchten, trennen Sie das Gerät vom Netzwerk und schalten Sie es in den Schlaf- oder Flugzeugmodus. Auch wenn Sie sich nicht sicher sind, gehackt worden zu sein, ist es weitaus besser schon den Verdacht zu melden. Wenn das Gerät rein privat genutzt wird, sollten Sie die nachfolgenden Schritte durchführen:

- **Ändern Sie Ihre Passwörter**: Das sollte sich nicht nur auf Ihre betroffenen Geräte beschränken, sondern auch all Ihre Benutzerkonten im Internet einbeziehen. Nutzen Sie dafür aber nicht das möglicherweise gehackte Gerät, sondern eines von dem Sie annehmen können, dass es sicher ist.
- **Antivirus**: Wenn Ihr Antiviren-Programm Sie über eine infizierte Datei informiert, befolgen Sie die von ihm vorgeschlagenen Aktionen. Das beinhaltet üblicherweise das Verschieben der fraglichen Datei in einen Quarantäne Bereich, ein Säubern der Datei von Schadcode oder gar das Löschen der Datei. Die meisten Antiviren-Programme verweisen dabei auf Dokumente, die Ihnen detaillierte Informationen über die erkannte Infektion liefern. Wenn Sie Zweifel haben, schieben Sie die Datei sofort in den Quarantäne Bereich und oder löschen Sie sie.
- **Neuinstallation**: Wenn Sie die Infektion nicht beheben können bzw. wenn Sie absolut sicher sein wollen, dass Ihr System wieder sauber ist, sollten Sie es neu installieren. Befolgen Sie bei dabei die Anweisungen des Herstellers. Meist bedeutet das bei Computern, eingebaute Mechanismen zur Neuinstallation des Betriebssystems zu nutzen. Wenn diese Mechanismen fehlen, defekt oder infiziert sind, kontaktieren Sie den Hersteller des Geräts oder besuchen Sie dessen Webseite für weitere Hilfestellungen. Vermeiden Sie eine Wiederherstellung des Betriebssystems von einer Datensicherung, diese ist eventuell bereits infiziert oder hat bereits die Verwundbarkeiten, die es den

Ich wurde gehackt, was nun?

Angreifern ermöglichte Zugriff auf Ihr System zu erlangen. Datensicherungen sollten nur zur Wiederherstellung Ihrer Daten genutzt werden. Für Mobilgeräte befolgen Sie die Anweisungen des Herstellers oder Diensteanbieters, die meist auf deren Webseiten zu finden sind. In vielen Fällen ist nichts weiter zu tun, als das Gerät auf die Werkseinstellungen zurückzusetzen. Wenn Sie sich nicht wohl dabei fühlen, diese Schritte selbst durchzuführen, wenden Sie sich an einen professionellen Dienstleister der Sie unterstützt. Wenn Ihr Computer oder Gerät schon recht alt ist, kann es oft auch sinnvoller und sogar günstiger sein, ein neues Gerät zu kaufen. Stellen Sie nach einer Neuinstallation oder einem Zurücksetzen unbedingt sicher, dass das Gerät komplett aktualisiert ist und aktivieren Sie die automatische Aktualisierung sofern diese Option verfügbar ist.

- **Datensicherung**: Die wichtigste proaktive Maßnahme, die Sie zu Ihrer Sicherheit durchführen können, ist eine regelmäßige Datensicherung, die Sie an einem sicheren Ort lagern. Einige Lösungen sichern neue oder veränderte Daten automatisch in stündlichen Intervallen. Prüfen Sie in regelmäßigen Abständen, ob Sie auf die gesicherten Daten zugreifen können. Oft ist das Wiederherstellen Ihrer Daten aus einer Datensicherung der einzige Weg, eine Kompromittierung zu beheben.
- **Rechtliche Schritte**: Wenn Sie sich in irgendeiner Weise bedroht fühlen, melden Sie den Vorfall an die örtliche Polizeidienststelle.

Weiterführende Informationen

Backup & Wiederherstellung:	https://securingthehuman.sans.org/ouch/2015#august2015
Starke Passwörter:	https://securingthehuman.sans.org/ouch/2015#april2015
Schadprogramme:	https://securingthehuman.sans.org/ouch/2016#march2016
Absicherung Ihres neuen Tablets:	https://securingthehuman.sans.org/ouch/2016#january2016

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

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.

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