SANS SECURITY AWARENESS

Der monatliche Security Awareness Newsletter für Jedermann

Wurde ich gehackt?

Übersicht

Egal wie sicher Sie sind, genau wie beim Autofahren ist es kaum zu vermeiden, früher oder später einen Unfall zu haben. Nachfolgend finden Sie Hinweise, um herauszufinden, ob Sie gehackt wurden und wenn ja, was zu tun ist. Je früher Sie feststellen, dass etwas Schlimmes passiert ist, desto wahrscheinlicher ist es, dass Sie das Problem beheben können.

Hinweise, dass Sie gehackt wurden

Ihr Antivirenprogramm generiert eine Warnung, dass Ihr System infiziert ist. Stellen Sie sicher, dass wirklich Ihre Antivirensoftware den Alarm generiert und nicht ein Popup-Fenster von einer Website, das Sie täuschen will, eine Nummer anzurufen oder etwas anderes zu installieren. Nicht sicher? Öffnen Sie Ihr Antivirenprogramm.

Sie erhalten ein Popup-Fenster, in dem steht, dass Ihr Computer verschlüsselt wurde und Sie ein Lösegeld zahlen müssen, um Ihre Dateien zurückzubekommen.

Ihr Browser führt Sie zu allen möglichen Websites, die Sie nicht besuchen wollten.

Ihr Computer oder Ihre Anwendungen stürzen ständig ab, es gibt Symbole für unbekannte Anwendungen auf dem Desktop oder seltsame Fenster tauchen auf.

Ihr Passwort funktioniert nicht mehr, obwohl Sie wissen, dass Sie es korrekt eingegeben haben.

Freunde fragen Sie, warum Sie sie mit E-Mails zumüllen, von denen Sie wissen, dass Sie sie nie gesendet haben.

Auf Ihrer Kreditkarte oder Ihrem Bankkonto gibt es Belastungen, die Sie nie getätigt haben.

Wie man reagiert

Wenn Sie vermuten, dass Sie gehackt wurden, sollten Sie so schnell wie möglich reagieren. Wenn der Hack einen Bezug zu Ihrer Arbeit hat, versuchen Sie nicht, das Problem selbst zu beheben, sondern melden Sie es sofort der zuständigen Sicherheitsabteilung Ihrer Firma. Wenn es sich um ein privates System oder Benutzerkonto handelt, das gehackt wurde, finden Sie nachfolgend einige Schritte, die Sie durchführen können.

Ändern Sie Ihre Passwörter: Dazu gehören nicht nur diejenigen auf Ihren Computern und mobilen Geräten, sondern auch für Ihre Online-Konten. Verwenden Sie nicht den gehackten Computer, sondern ein anderes System, von dem Sie dafür wissen, dass es sicher ist. Wenn Sie viele Benutzerkonten haben, beginnen Sie mit den wichtigsten zuerst. Wenn Sie nicht alle Ihre Passwörter im Kopf behalten können, verwenden Sie einen Passwortmanager.

Finanziell: Bei Problemen mit Ihrer Kreditkarte oder einem Bankkonto rufen Sie sofort Ihre Bank oder Ihr Kreditkartenunternehmen an. Verwenden Sie eine vertrauenswürdige Telefonnummer, um sie anzurufen, z.B. von der Rückseite Ihrer Bankkarte, Ihrer Jahresrechnung oder besuchen Sie deren Website von einem vertrauenswürdigen Computer aus. Zudem sollten Sie erwägen, Ihre Bank- oder Kreditkarten zu sperren.

Virenschutz. Wenn Ihre Antivirensoftware Sie über eine infizierte Datei informiert, befolgen Sie die von ihr empfohlenen Maßnahmen. Die meisten Antivirenprogramme haben Links, denen Sie folgen können, um mehr über die jeweilige Infektion zu erfahren.

Neuinstallation. Wenn Sie einen infizierten Computer nicht reparieren können oder wenn Sie Gewissheit möchten, dass Ihr System sicher ist, installieren Sie das Betriebssystem neu. Stellen Sie nicht das komplette System aus einem Backup wieder her, sondern verwenden Sie Backups nur zur Wiederherstellung Ihrer persönlichen Dateien. Wenn Sie sich beim Wiederaufbau unwohl fühlen, sollten Sie einen professionellen Service in Anspruch nehmen. Wenn Ihr Computer oder Gerät alt ist, kann ein Neukauf die einfachere Möglichkeit sein. Sobald Sie Ihr System umgebaut oder ein neues gekauft haben, stellen Sie sicher, dass es auf dem aktuellen Stand ist und aktivieren Sie nach Möglichkeit automatische Updates.

Backups. Ein wichtiger Schritt zu Ihrem Schutz ist die frühzeitige Vorbereitung mit regelmäßigen Backups. Viele Lösungen sichern Ihre Dateien automatisch täglich oder sogar stündlich. Überprüfen Sie regelmäßig, ob Sie diese Dateien wiederherstellen können. Nicht selten ist die Wiederherstellung von Datensicherungen die einzige Möglichkeit, sich von einem Hackerangriff zu erholen.

Strafverfolgung: Wenn Sie sich in irgendeiner Weise bedroht fühlen, melden Sie den Vorfall der örtlichen Polizei. Wenn Sie das Opfer von Identitätsdiebstahl sind besuchen Sie die Seiten von bsi-fuer-buerger.de.

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 Sicherheit spezialisiert. Sie haben langjährige Erfahrung im Bereich IT-Sicherheit und sind mehrfach GIAC zertifiziert.

Gast-Autor

Dr. Johannes Ullrich *(@johullrich) ist Forschungsdekan des SANS Technology Institute, Direktor des SANS Internet Storm Center und SANS Fellow. Er schuf das kollaborative Sensornetzwerk DShield und veröffentlicht den täglichen Podcast "Network Security News" des Internet Storm Center.*

Ressourcen

Datensicherung:	https://www.sans.org/u/JGP
Passphrasen:	https://www.sans.org/u/JGU
Passwortverwaltung:	https://www.sans.org/u/JGZ
Was ist Malware:	https://www.sans.org/u/JH4
Kreditsperre:	https://krebsonsecurity.com/2018/09/credit-freezes-are-free-let-the-ice-age-begin/