Der monatliche Security Awareness Newsletter für Sie

Vier einfache Schritte, um sicher zu bleiben

Übersicht

Wenn man Technologie optimal nutzen möchte, gleichzeitig aber auch sicher, kann einem das einiges an Kopfzerbrechen bereiten. Unabhängig davon, welche Technologie Sie verwenden oder wie Sie sie verwenden, finden Sie nachfolgend vier einfache Schritte, die Ihnen bei der sicheren Verwendung helfen.

1. Sie selbst: In erster Linie kann die Technologie allein Sie nicht vollständig schützen; Sie persönlich sind Ihre beste Verteidigung. Angreifer haben gelernt, dass der einfachste Weg, das zu bekommen, was sie wollen, darin besteht, Sie ins Visier zu nehmen, anstatt Ihren Computer oder andere Geräte anzugreifen. Wenn Angreifer Ihr Passwort, Ihre Kreditkartennummer oder die Kontrolle über Ihren Computer wollen, werden sie versuchen, Sie dazu zu bringen es ihnen zu geben, oft indem sie ein Gefühl der Dringlichkeit schaffen. Beispielsweise können sie Sie anrufen, indem sie vorgeben, ein Mitarbeiter des technischen Microsoft Supports zu sein und behaupten, dass Ihr Computer infiziert ist. In Wirklichkeit sind es aber nur Cyberkriminelle, die wollen, dass Sie ihnen Zugang zu Ihrem Computer gewähren. Möglicherweise senden sie Ihnen aber auch eine E-Mail-Warnung, dass Ihr Paket nicht zugestellt werden konnte, und nötigen Sie dazu, auf einen Link zu klicken, um Ihre Postanschrift zu bestätigen, während sie Sie in Wirklichkeit dazu bringen, eine bösartige Website zu besuchen, die sich in Ihren Computer hackt. Letztendlich sind Sie die größte Verteidigung gegen Angreifer. Mit gesundem Menschenverstand können Sie viele Angriffe erkennen und stoppen.

2. Passphrasen: Moderne Rechengeschwindigkeiten haben das alte, achtstellige Passwort verwundbar gemacht. Wenn eine Website Sie auffordert, ein Passwort zu erstellen, erstellen Sie stattdessen eine starke und eindeutige Passphrase. Eine Passphrase ist eine Art von Passwort, das eine Reihe von Wörtern verwendet, die leicht zu merken sind, wie z.B. "Biene Honig, Whiskey Regen". Je länger Ihre Passphrase ist, desto stärker ist sie. Eine einzigartige Passphrase bedeutet, dass für jedes Gerät oder Online-Konto eine andere verwendet wird. Wenn Sie dies beherzigen und eine Passphrase kompromittiert wird, sind alle Ihre anderen Konten und Geräte immer noch sicher. Sie können sich all diese Passphrasen nicht merken? Verwenden Sie einen Passwortmanager, das ist ein spezielles Programm, das alle Ihre Passphrasen sicher in einem verschlüsselten Format speichert (und auch viele andere großartige Funktionen bietet).

Aktivieren Sie außerdem die zweistufige Verifizierung (auch Zwei-Faktor- oder Mehr-Faktor-Authentifizierung genannt). Damit verwenden Sie Ihr Passwort, fügen aber einen zweiten Schritt hinzu, wie z.B. die Eingabe eines Codes, der an Ihr Smartphone gesendet wird oder einen Code, der von einer App für Sie generiert wird. Die

Aktivierung der zweistufigen Überprüfung ist wahrscheinlich der wichtigste Schritt, den Sie zum Schutz Ihrer Online-Konten unternehmen können, und es ist viel einfacher, als Sie vielleicht denken.

3. Updates: Stellen Sie sicher, dass das Betriebssystem auf jedem Ihrer Computer und mobilen Geräte, sowie all Ihre Programme und Apps, auf dem aktuellsten Versionsstand sind. Cyber-Angreifer sind ständig auf der Suche nach neuen Schwachstellen in der Software, die Ihre Geräte verwenden Wenn sie Schwachstellen entdecken, verwenden sie spezielle Programme, um sie auszunutzen und sich in die von Ihnen genutzten Geräte zu hacken. In der Zwischenzeit arbeiten die Unternehmen, die die Software für diese Geräte entwickelt haben, hart daran, diese Schwachstellen durch die Veröffentlichung von Updates zu beheben. Indem Sie sicherstellen, dass Ihre Computer und mobilen Geräte diese Updates umgehend installieren, machen Sie es den Angreifern viel schwerer, Sie zu hacken. Um auf dem aktuellsten Stand zu bleiben, aktivieren Sie einfach die automatische Aktualisierung, wann immer möglich. Diese Regel gilt für fast jede Technologie, die mit einem Netzwerk verbunden ist, einschließlich Fernseher, Baby-Monitore, Sicherheitskameras, Heimrouter, Spielekonsolen und sogar Ihr Auto.

4. Datensicherung und -wiederherstellung: Ganz gleich, wie vorsichtig Sie sind, Sie können immer noch gehackt werden. Wenn dieser Fall eintritt, können Sie Ihre persönlichen Daten nur noch aus einem Backup wiederherstellen. Stellen Sie sicher, dass Sie regelmäßig Backups aller wichtigen Daten erstellen und prüfen Sie, dass Sie Ihre Daten auch wiederherstellen können. Die meisten Betriebssysteme und mobilen Geräte unterstützen automatische Backups, entweder auf externe Laufwerke oder in die Cloud.

Gastredakteur

*SANS Certified Instructor **Steve Anson** bietet IT-Sicherheitsteams und Regierungen auf der ganzen Welt Anleitung zur Verbesserung ihrer Sicherheitslage. Steve ist Autor des bald erscheinenden Buches "Applied Incident Response" und stellt kostenlos Informationen für IT-Sicherheitsexperten unter AppliedIncidentResponse.com zur Verfügung.*

Weiterführende Informationen

Social Engineering:	https://www.sans.org/u/W3G
Angriffe & Betrügereien mittels Telefon:	https://www.sans.org/u/W3Q
Einfache Passwörter erzeugen:	https://www.sans.org/u/W3V
Haben Sie Backups?:	https://www.sans.org/u/Uzl