Der monatliche Security Awareness Newsletter für Jedermann

OUCH!

IN DIESER AUSGABE...

- Sie selbst
- Passwörter
- Aktualisierungen
- Datensicherungen

Vier Schritte zur Sicherheit

Überblick

Während Technologie eine immer wichtigere Rolle in unsere Leben spielt, nimmt auch ihre Komplexität stetig zu. So schnell wie sich die Technologie verändert kann es sehr schwierig sein mit den sich verändernden Sicherheitsempfehlungen Schritt zu halten. Es scheint ständig neue Ratschläge zu geben, was Sie tun oder lassen sollten. Während sich die Details zum sicheren Umgang mit Technologie mit der Zeit verändern, bleiben die Grundlagen zu Ihrem eigenen Schutz meist die gleichen. Unabhängig davon, welche Technologien Sie nutzen oder wo Sie sie nutzen, sollten Sie die vier folgenden Maßnahmen befolgen. Um mehr über die einzelnen Schritte zu erfahren folgen Sie einfach den Links im Abschnitt „Weiterführende Informationen“ am Ende dieses Newsletters.

Gastautor

Ryan Johnson hilft Organisationen sich vorzubereiten, um im unvermeidbaren Fall eines Hacker-Einbruchs richtig reagieren zu können. Darüber hinaus lehrt er den Kurs „Advanced Network Forensics“ des SANS Institute. Ryan ist auf Twitter als **@ForensicRJ** aktiv.

1. **Sie selbst**: Seien Sie sich gewahr, dass Ihnen Technologie allein nie vollständigen Schutz bieten wird. Angreifer haben längst gelernt, dass der einfachste Weg zur Umgehung selbst der fortschrittlichsten Technologie im Angriff auf die Nutzer besteht. Wenn sie Ihr Passwort, Ihre Kreditkarteninformationen oder persönlichen Daten wollen, ist es für sie am Einfachsten, Sie dazu zu verleiten, das Sie ihnen die Informationen zu geben. Die Kriminellen könnten Sie z.B. anrufen und vorgeben, vom Microsoft Serviceteam zu sein, das Ihren infizierten Computer bereinigen soll – in Wahrheit handelt es sich aber nur um Cyberkriminelle, die Zugriff auf Ihren Computer erlangen wollen. Oder sie schicken Ihnen vielleicht eine E-Mail, in der steht das Ihr Paket nicht zugestellt werden konnte und das Sie einen Link anklicken sollen um Ihre Adresse zu bestätigen. Dahinter steht jedoch eine schadhafte Webseite, die Ihren Computer infiziert. So beginnen beispielsweise die als „Ransomware“ oder “CEO Fraud” bezeichneten Angriffe gewöhnlich. Die absolut beste Verteidigung dagegen sind letztendlich Sie selbst. Seien Sie wachsam und misstrauisch. Indem Sie Ihren gesunden Menschenverstand einsetzen, können Sie die meisten Angriffe erkennen und verhindern.

2. **Passwörter**: Der nächste Schritt zu Ihrem Schutz umfasst starke, einzigartige Passwörter für jedes Ihrer Geräte und Online-Benutzerkonten. Wichtig sind hier die Begriffe stark und einzigartig. Ein starkes Passwort ist eines, das nicht einfach von Angreifern oder ihren automatisierten Programmen erraten werden kann. Sie haben keine Lust mehr auf

Vier Schritte zur Sicherheit

komplexe Passwörter die schwer zu merken und noch schwerer zu tippen sind? Versuchen Sie es stattdessen doch einfach einmal mit einem Passwortsatz. Statt eines einzigen PassWORTes nehmen Sie eine Aneinanderreihung von Wörtern, die leicht zu merken ist, wie z.B. “Wo ist mein Kaffee?”. Je länger Ihr Passwortsatz ist, desto stärker ist er auch. Einzigartig ist ein Passwort, wenn Sie für jedes Gerät und jedes Benutzerkonto ein anderes Passwort verwenden. Auf diese Art sind all Ihre anderen Benutzerkonten immer noch sicher, wenn das Passwort eines Kontos kompromittiert wird. Sie können sich all diese starken, einzigartigen Passwörter nicht merken? Keine Sorge, das kann niemand. Wir empfehlen daher die Nutzung eines Passwortmanager-Programms. Mit diesem speziellen Programm für Ihren Computer oder Ihr Smartphone können Sie all Ihre Passwörter sicher und verschlüsselt abspeichern.

Durch das Befolgen dieser vier Grundprinzipien haben Sie bereits den wichtigsten Schritt zu Ihrem Schutz bei der Nutzung neuester Technologien getan.

Noch mehr Schutz bietet die Aktivierung der “Anmeldung in zwei Schritten”, auch “Zwei-Wege-Authentisierung” genannt. Meist reichen gute Passwörter allein nicht aus, um wichtige Benutzerkonten zu sichern. Zwei-Wege-Anmeldung ist ein viel stärkeres Verfahren. Es beinhaltet die Nutzung Ihres Passworts, fügt jedoch noch einen zweiten Schritt hinzu, entweder etwas das Sie sind (Biometrie), oder etwas das Sie haben (Besitz, z.B. ein Code der auf Ihr Smartphone gesendet wird oder eine App, die einen speziellen Code für die Anmeldung generiert). Aktivieren Sie dieses Verfahren wann immer möglich, insbesondere auch bei Ihrem Programm zur Passwort-Verwaltung. Die “Anmeldung in zwei Schritten” ist wahrscheinlich die eine, wichtigste Methode um sich zu schützen, und viel leichter zu nutzen als sie vielleicht denken.

3. **Aktualisierungen**: Vergewissern Sie sich, dass Ihre Computer, Mobilgeräte, Apps und alles weitere, das mit dem Internet verbunden ist mit der neuesten verfügbaren Softwareversion läuft. Cyberkriminelle suchen fortwährend nach Schwachstellen in den eingesetzten Programmen auf Ihren Geräten. Wenn sie solche Schwachstellen finden, nutzen sie spezielle Programme die die Schwachstelle angreifen, und können somit Ihre Geräte hacken. Gleichzeitig arbeiten die Unternehmen, die die Software für Ihre Geräte herstellen, mit Hochdruck an der Behebung dieser Schwachstellen durch Aktualisierungen (Updates). Indem Sie sicherstellen, dass Ihre Computer und Mobilgeräte diese Aktualisierungen installieren, erschweren Sie jegliche Hacking-Versuche gegen sich. Um aktuell zu bleiben, aktivieren Sie wann immer möglich “Automatische Updates”. Diese Regel bezieht sich auf nahezu jede Technologie die mit einem Netzwerk verbunden ist, sei es ein moderner Fernseher, Babyphones, Heimrouter, Spielekonsolen, oder vielleicht sogar Ihr neuer

Vier Schritte zur Sicherheit

PKW. Wenn ein Programm, Betriebssystem oder Gerät alt ist und nicht mehr vom Hersteller unterstützt wird, empfehlen wir Ihnen es mit einem aktuellen, vom Hersteller mit Updates versorgten, Gerät zu ersetzen.

4. **Datensicherungen**: Ganz gleich wie vorsichtig Sie sind, eines Tages kann es dennoch passieren, dass einer der Angriffe gegen Sie erfolgreich ist. In einem solchen Fall ist Ihre einzige Möglichkeit um sicherzustellen, dass Ihr Computer oder Mobilgerät wirklich wieder frei von Schadsoftware ist, ein komplettes Löschen und von Grund auf neu Installieren. Die Angreifer verhindern möglicherweise sogar Ihren Zugriff auf Ihre persönlichen Dateien, Fotos und anderen auf dem Gerät gespeicherten Informationen. Oft können Sie all diese Daten nur von einer Datensicherung wiederherstellen. Stellen Sie sicher, dass all Ihre Geräte eine regelmäßige Datensicherung durchführen und prüfen Sie gelegentlich, ob Sie diese Daten auch wirklich wiederherstellen können. Die meisten Betriebssysteme und Mobilgeräte unterstützen automatische Datensicherungen. Zusätzlich sollten Sie Ihre Daten auch auf externe Datenträger oder, falls nicht vorhanden, mittels Cloud-Diensten speichern, um sie gegen Cyberangreifer zu schützen.

Weiterführende Informationen

Phishing:	https://securingthehuman.sans.org/ouch/2015#december2015
Passwortverwaltung:	https://securingthehuman.sans.org/ouch/2015#october2015
Authentifizierung in zwei Schritten:	https://securingthehuman.sans.org/ouch/2015#september2015
Sichere Passwörter:	https://securingthehuman.sans.org/ouch/2015#april2015
Datensicherung:	https://securingthehuman.sans.org/ouch/2015#august2015

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.

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