Der monatliche Security Awareness Newsletter für Jedermann

OUCH!

IN DIESER AUSGABE...

Hilfe zur Selbsthilfe

Überblick

Für viele von uns stellt die Nutzung von Technologie kein Problem dar, auch ihre sichere Nutzung. Bei Freunden oder Familienmitgliedern sieht das möglicherweise anders aus. Sie sind eventuell unsicher oder haben sogar Angst davor. Dies macht sie sehr anfällig für heutige Cyberangreifer. Cybersicherheit muss aber nicht unheimlich sein, sie ist eigentlich ziemlich leicht, wenn man die Grundlagen verstanden hat. Freunde und Familie brauchen wahrscheinlich nur einen Ratgeber wie Sie, der ihnen hierbei hilft.

Gastautor

Randy Marchany (Twitter: **@randymarchany**) ist CISO von Virginia Tech und zertifizierter SANS Institute Kursleiter.

Fünf einfache Schritte

Hier folgen fünf einfache Schritte, die Sie befolgen können um anderen zu helfen ihre Scheu und Angst abzulegen und Technologie sicher zu verwenden. Weitergehende Informationen zu jedem dieser Punkte finden Sie am Ende dieses Newsletters.

1. **Social Engineering**: Social Engineering ist eine gängige Technik von Cyberangreifern, um ihre Opfer dazu zu verleiten etwas zu tun, das sie besser nicht tun würden, wie z.B. ihr Passwort weiterzugeben, den Computer unabsichtlich zu infizieren oder sensible Informationen weiterzugeben. Dabei handelt es sich um keine neue Idee, Betrüger und Hochstapler gibt es schon seit tausenden Jahren. Der einzige Unterschied besteht heute darin, dass die bösen Jungs diese Konzepte auf Internettechnologien übertragen. Sie können anderen helfen, indem Sie ihnen die gängigsten Anzeichen von Social Engineering Angriffe erläutern, wie z.B. wenn jemand eine hohe Dringlichkeit suggeriert, wenn etwas zu gut um wahr zu sein klingt, oder wenn ein Cyberangreifer vorgibt jemand zu sein, aber die Nachrichten nicht wie die ihrer Bekannten klingen. Zeigen Sie ihnen Beispiele solcher gängigen Angriffe, wie z.B. Phishing E-Mails oder die berühmten Microsoft Hotline-Anrufe. Das Mindeste ist, dass Familienmitglieder verstehen, dass sie ihr Passwort nie an jemanden weitergeben oder jemandem Fernzugriff auf ihren Computer geben dürfen.
2. **Passwörter**: Starke Passwörter sind der wichtigste Aspekt zum Schutz von Geräten und wichtigen Online-Benutzerkonten. Zeigen Sie Ihren Familienmitgliedern, wie sie starke Passwörter erstellen können. Wir empfehlen Passwortsätze, weil diese leicht zu merken und zu tippen sind. Passwortsätze sind nichts anderes als Passwörter, die aus mehreren Worten bestehen. Helfen Sie ihnen zudem bei der Installation und Nutzung eines Passwortmanagers. Es ist wichtig, ein einzigartiges Passwort für jedes einzelne Benutzerkonto und jedes Gerät zu

Hilfe zur Selbsthilfe

verwenden. Wenn ein Passwortmanager zu viel des Guten ist, sollten die Passwörter zumindest aufgeschrieben und an einem sicheren Ort abgelegt werden. Für wichtige Online-Benutzerkonten sollte unbedingt die Zwei-Faktor-Authentisierung aktiviert werden. Dies ist eine der effektivsten Methoden um ein Nutzerkonto abzusichern.

3. **Aktualisieren**: Systeme jederzeit auf dem aktuellen Stand zu halten ist ein entscheidender Schritt, den jeder zur Absicherung seiner Geräte unternehmen kann. Das betrifft nicht nur Computer und Mobilgeräte, sondern alles was mit einem Netzwerk verbunden wird, darunter Spielekonsolen, Thermometer, ja sogar Lampen und Lautsprecher. Der einfachste Weg dies sicherzustellen ist, sofern möglich, die "automatischen Updates" auf allen Geräten zu aktivieren.
4. **Anti-Virus**: Menschen machen Fehler, und manchmal klickt man auf etwas oder installiert etwas was man besser gelassen hätte – und was dann unsere Systeme infiziert. Antivirenprodukte sollen uns bei solchen Fehlern schützen. Sie können zwar nicht vor jeglichem Schadprogramm schützen, aber gängige Angriffe zuverlässig erkennen und abwehren. Stellen Sie daher sicher, dass ein Antivirenprodukt auf allen Geräten installiert, aktiv und aktuell ist. Manche Antivirenprodukte bringen heute auch noch weitere empfehlenswerte Komponenten, wie Firewalls und Browserschutz, mit.
5. **Datensicherung**: Wenn alle anderen Maßnahmen ihren Zweck verfehlen, sind Datensicherungen oft der einzige Weg, sich von Fehlern wie dem versehentlichen Löschen von Dateien oder Cyberattacken wie der sogenannten Ransomware zu erholen. Stellen Sie sicher, dass Freunde und Familie eine automatische Datensicherung nutzen. Die einfachste Lösung hierfür sind oft Cloud-basierte Dienste, zu denen ein Gerät stündlich oder bei jeder Änderung einer Datei eine Sicherung anfertigt. Diese Lösungen erleichtern nicht nur die Datensicherung, sondern auch die Wiederherstellung.

Helfen Sie anderen bei der sicheren Nutzung von Technologie, indem Sie diese fünf Schritte mit ihnen teilen.

Schutz der Kinder außerhalb der eigenen vier Wände

Wenn Sie keine Probleme im Umgang mit Technologie haben, haben Sie wahrscheinlich nicht nur für Ihre eigene Sicherheit, sondern auch für die Ihrer Kinder gesorgt. Wenn Kinder jedoch einen Verwandten besuchen, der im Umgang mit Technologie nicht so firm ist, beispielsweise die Großeltern, können diese sich nicht auf die gleiche Weise um die Online-Sicherheit Ihrer Kinder kümmern, vielleicht weil sie sich der Gefahren selbst nicht bewusst sind. Hier sind einige Dinge die Sie unternehmen können um Ihre Kinder beim Besuch von Familienmitgliedern zu schützen.

- **Regeln**: Stellen Sie sicher, dass Andere Ihre Regeln und Erwartungen an Ihre Kinder kennen. Reglementieren Sie z.B. die Online-Zeit Ihrer Kinder, mit wem sie sich online unterhalten dürfen oder welche Spiele sie spielen können?

Hilfe zur Selbsthilfe

Glauben Sie uns, vertrauen Sie nicht darauf, dass Ihre Kinder diese Regeln anderen Familienmitgliedern erklären. Eine Möglichkeit ist das Erstellen einer Übersicht der Regeln, die Sie an alle Familienmitglieder weitergeben die öfter von Ihren Kindern besucht werden.

- **Kontrolle**: Wenn Kinder ein besseres Verständnis für Technologie haben als ihre Aufpasser, werden sie das zu ihrem Vorteil ausnutzen. Kinder könnten beispielsweise die Großeltern um Administratorrechte bitten und dann machen was immer sie wollen, wie z.B. ein Spiel installieren von dem Sie nicht wollen, dass sie es spielen. Familienmitglieder sollten wissen, dass sie den Kindern keine weitergehenden Rechte auf Systemen geben als die, über die sie bisher verfügen.

Schlagen Sie Ihren Freunden und Verwandten schlussendlich vielleicht auch vor, sich Informationsquellen wie die OUCH! Newsletter zu bestellen, um sich weiterzubilden. Dieser Newsletter wird monatlich in über 20 Sprachen veröffentlicht – kostenlos. Das Abonnieren geht ganz leicht unter https://securingthehuman.sans.org/ouch.

Weiterführende Informationen

Social Engineering:	https://securingthehuman.sans.org/ouch/2017#january2017
Passwortsätze:	https://securingthehuman.sans.org/ouch/2017#april2017
Passwortmanager:	https://securingthehuman.sans.org/ouch/2017#september2017
Zwei-Faktor-Authorisierung:	https://securingthehuman.sans.org/ouch/2015#september2015
Datensicherung und Wiederherstellung:	https://securingthehuman.sans.org/ouch/2017#august2017
Absicherung heutiger Online-Kinder:	https://securingthehuman.sans.org/ouch/2017#may2017

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: Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley