OUCH! | Mai 2015

Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

Generationenübergreifende Sicherheit

Überblick

Viele von uns fühlen sich im Umgang mit Technologie wohl, einschließlich ihrer sicheren Nutzung. Anderen Familienmitgliedern geht es möglicherweise nicht so, insbesondere wenn sie nicht mit Computern oder dem Internet groß geworden sind. Hier sind einige Schritte die Sie unternehmen können, um die Kluft zwischen den Generationen zu verkleinern. Mit den hier genannten Ratschlägen ist es Ihnen zwar möglich, Ihre Kinder zuhause, während der Nutzung von Computer und Internet zu schützen. Es besteht jedoch die Möglichkeit, dass vergleichbare Maßnahmen bei Ihren Verwandten nicht existieren und Ihre Kinder bei Besuchen nicht entsprechend geschützt sind. Daher gehen wir in dieser OUCH auch darauf ein, wie Sie Ihre Verwandten unterstützen können, eine sichere Umgebung zu schaffen.

Gastautor

Brian Honan (Twitteraccount **@brianhonan**) ist unabhängiger Sicherheitsberater in Dublin, Irland; Gründer und Leiter des IRISSCERT, Irlands erstem CERT, Sonderberater des Europol Cybercrime Centre (EC3), und hält Vorlesungen über Informationssicherheit an der Universität Dublin. Er hat mehrere Bücher verfasst und veröffentlicht in verschiedenen fachbezogenen Publikationen.

Die Grundlagen

Oft können bereits einige grundlegende Schritte viel zur Absicherung des digitalen Lebens beitragen. Nachfolgend finden Sie einige dieser Grundlagen, deren Umsetzung wir für alle Familienmitglieder empfehlen. Wenn Sie bemerken, dass jemand diese Schritte nicht versteht, sollten Sie demjenigen bei der Umsetzung helfen oder dies selbst in die Hand nehmen.

- **Social Engineering**: Erklären Sie das Konzept hinter Social Engineering. Schwindler und Hochstapler gibt es schon seit Tausenden von Jahren. Heutzutage wenden die Gauner einfach die gleichen Konzepte auf das Internet an. Bringen Sie Ihren Familienmitgliedern das Thema anhand von Beispielen für die gängigsten Angriffe näher, wie zum Beispiel alltägliche Phishing E-Mails oder den berühmt-berüchtigten Microsoft Hotline Telefonbetrug. Stellen Sie auf alle Fälle sicher, dass alle Familienmitglieder verstehen, dass sie unter keinen Umständen ihr Passwort an jemanden herausgeben oder jemandem Fernzugriff auf ihren Computer gewähren dürfen. Auch sollten Sie ihnen die Sicherheit geben, Sie jederzeit per E-Mail oder Anruf kontaktieren zu dürfen, wenn sie sich unsicher fühlen oder Fragen zu einer verdächtigen E-Mail oder einem Anruf haben, bevor sie irgendwelche Informationen herausgeben.
- **Heimisches WLAN**: Nehmen Sie sich die Zeit um sicherzustellen, dass Ihr heimisches WLAN wirklich sicher konfiguriert ist. Es sollte zumindest das Administrator Passwort geändert werden, ein starkes WLAN Passwort vergeben und der Verschlüsselungsmechanismus auf dem aktuellsten Stand der Technik sein. Überlegen Sie sich, ob Sie ihr

Generationenübergreifende Sicherheit

WLAN nicht so konfigurieren wollen, dass es einen sicheren DNS Dienst wie www.opendns.org nutzt. Diese Dienste schützen Nutzer nicht nur davor, infizierte Webseiten aufzurufen, sondern können Ihnen auch die Kontrolle darüber ermöglichen welche Webseiten jemand besuchen darf, z.B. wenn Kinder im Internet surfen.

Ältere Generationen benötigen wahrscheinlich Hilfe bei der Absicherung der von ihnen genutzten Technik und bei der Schaffung einer sicheren Umgebung für besuchende Kinder.

- **Patchen**: Systeme auf dem aktuellsten Stand zu halten ist einer der grundlegendsten Schritte um sie abzusichern. Stellen Sie also sicher, dass alle heimischen Geräte, einschließlich den Mobilgeräten, mit den aktuellsten Patches für Betriebssystem und Anwendungen versehen sind. Das geht am Einfachsten, wenn Sie (wo immer möglich) die Funktionen zum automatischen Update aktivieren.
- **Virenschutz**: Menschen machen Fehler, wir klicken manchmal auf Dinge oder installieren Sachen, die wir besser gelassen hätten. Virenschutzprodukte können zwar nicht jede Schadsoftware aufhalten, helfen aber die gängisten Angriffe zu erkennen und zu unterbinden. Stellen Sie daher sicher, dass alle heimischen Computer ein Virenschutzprogramm installiert haben, und dass es aktiv und auf dem aktuellsten Stand ist.
- **Passworte**: Starke Passworte sind der Schlüssel, um sowohl Geräte als auch Benutzerkonten abzusichern. Erklären Sie Ihren Familienmitgliedern die notwendigen Schritte zur Erstellung sicherer Passwörter. Passwortsätze sind für sie wahrscheinlich am einfachsten zu merken und zu benutzen. Sie können ihnen auch einen Passwortmanager installieren und ihnen beibringen, wie er zu benutzen ist. Wenn das nicht funktioniert, halten Sie sie dazu an ihre Passworte aufzuschreiben und an einem sicheren Platz zu verwahren auf den nur sie Zugriff haben. Für besonders kritische Benutzerkonten sollten Sie zudem, wenn möglich, die Zwei-Faktor-Authentisierung aktivieren.
- **Backups**: Wenn alles andere versagt, werden Backups die letzte Rettung sein. Stellen Sie sicher, dass alle Familienmitglieder ein einfaches und zuverlässiges Datei-Backupsystem nutzen.

Vielleicht können Sie es einrichten, einmal im Monat oder quartalsweise zu prüfen, ob all diese Schritte umgesetzt sind. Als Notfallplan könnten Sie Software zum Fernzugriff auf den Geräten installieren, stellen Sie in diesem Fall aber sicher, dass eine gute Verschlüsselung und ein starkes, einzigartiges Passwort verwendet wird.

Kinder zu Besuch

Wenn Kinder zu Besuch bei Verwandten sind(z.B. bei ihren Großeltern) existieren die Regeln, die sie aus dem elterlichen

Generationenübergreifende Sicherheit

Haushalt gewohnt sind, oft nicht. Das schließt natürlich auch Regeln zum Schutz der Kinder im Internet ein. Mit den folgenden Schritten können Sie dazu beitragen, dennoch einen gewissen Schutz zu gewährleisten.

- **Regeln**. Stellen Sie sicher, dass Ihre Verwandten die von Ihnen aufgestellten Regeln und Ihre Erwartungen an die Sicherheit Ihrer Kinder kennen. Gibt es z.B. Regeln, wie lange die Kinder Onlinespiele spielen dürfen oder wann sie ihre Mobilgeräte nutzen dürfen? Glauben Sie uns, es ist keine gute Idee darauf zu vertrauen, dass Ihre Kinder den Großeltern die von Ihnen vorgegeben Regeln erklären und sie selbständig befolgen. Sie werden die Regeln den Großeltern selbst erklären müssen. Eine Möglichkeit wäre, die Regeln auf einem Blatt zusammenzuschreiben und dieses im Haus Ihrer Verwandten aufzuhängen.
- **Kontrolle**: Vorsicht, Ihre Kinder verstehen die Technik oft besser als ihre älteren Aufpasser, sie werden diesen Fakt wahrscheinlich auszunutzen wissen. Kinder könnten z.B. nach administrativen Rechten für den Computer der Großeltern fragen und damit machen was immer sie wollen, wie z.B. das Spiel installieren von dem Sie nicht wollen, dass die Kinder es spielen. Gehen Sie sicher, dass die Verwandten den Kindern keine Zugriffe über das bestehende, abgesprochene Maß hinaus gewähren.

Weiterführende Informationen

Social Engineering:	http://www.securingthehuman.org/ouch/2014#november2014
So sichern Sie Ihr Heimnetzwerk:	http://www.securingthehuman.org/ouch/2014#january2014
Sicher in 5 Schritten:	http://www.securingthehuman.org/ouch/2014#october2014
Starke Passwörter:	http://www.securingthehuman.org/ouch/2015#april2015
Virenschutz:	http://www.securingthehuman.org/ouch/2014#december2014
Technik-Hotline Betrug:	http://www.securingthehuman.org/ouch/2012#july2012

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