Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Überblick
- Fünf Schlüsselpunkte

Sicher in 5 Schritten

Überblick

Technologie wird in unserem Leben immer wichtiger – sie wird aber auch immer komplexer. Je schneller sie sich weiterentwickelt, umso schwerer wird es aus Sicht der Sicherheit, Schritt zu halten. Ständig gibt es neue Empfehlungen, was Sie tun oder lassen sollten. Während sich diese Empfehlungen im Detail kontinuierlich ändern, gibt es aber grundlegende Prinzipien, denen Sie immer folgen können um sich zu schützen. Unabhängig davon, welche Technologie sie nutzen oder wo Sie sie nutzen, empfehlen wir Ihnen daher die folgenden fünf Punkte zu beachten.

Gastautor

Lenny Zeltser arbeitet bei NCR Corporation, seine zentrale Aufgabe ist die Sicherheit des IT-Betriebs der Kunden sicherzustellen. Er lehrt außerdem die Abwehr von Schadsoftware beim SANS Institute. Lenny ist auf Twitter als **@lennyzeltser** aktiv und schreibt ein IT-Sicherheits-Blog unter **blog.zeltser.com**.

Fünf Schlüsselpunkte

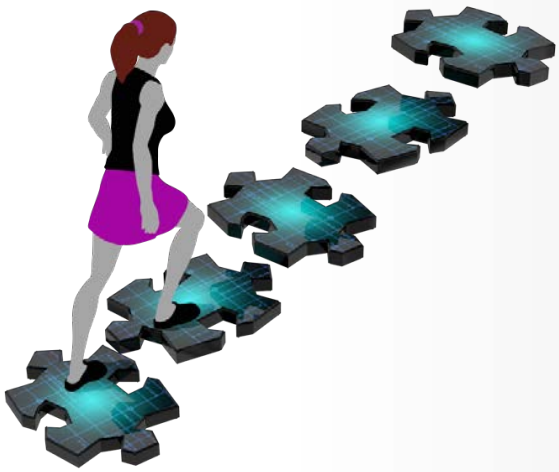
Jeder der fünf nachfolgenden Punkte ist ein einfacher Überblick über ein Thema. Weitergehende Informationen erhalten Sie im entsprechenden Kapitel am Ende dieses Newsletters.

1. **Sie selbst**: In erster Linie sollten Sie sich im Klaren sein, dass Technologie allein Sie nicht schützen kann. Angreifer haben schon lange realisiert, dass der einfachste Angriffsweg auf den Benutzer abzielt. Wenn ein Angreifer es auf Ihr Passwort oder Ihre Kreditkartendaten abgesehen hat, ist es doch das Einfachste, wenn er Sie überlistet und dazu bringt, ihm die Informationen freiwillig zu geben. Der Angreifer könnte zum Beispiel anrufen und sich als Computertechniker von Microsoft ausgeben, der helfen will Ihren Computer von Infektionen zu befreien – in Wirklichkeit handelt es sich aber nur um einen Kriminellen, der Zugang zu Ihrem PC erlangen will. Oder vielleicht sendet er Ihnen auch eine E-Mail, die Sie informiert, dass ein Paket nicht zugestellt werden konnte, und die Sie bittet einen Link anzuklicken um Ihre Adresse zu bestätigen. Dies dient jedoch nur dazu, Sie auf eine bösartige Webseite zu locken die Ihren Computer infiziert. Letztendlich sind Sie selbst die wirksamste Verteidigung gegen derartige Angriffe. Seien Sie vorsichtig, nutzen Sie Ihren gesunden Menschenverstand, und Sie werden die gängigsten Angriffe erkennen und abwehren können.

2. **Updates**: Stellen Sie sicher, dass Ihre Computer, Ihre Mobilgeräte, und alle weiteren IT-Geräte die mit einem Netzwerk verbunden sind jederzeit mit der neuesten verfügbaren Software betrieben werden. Cyberkriminelle suchen ständig nach Schwachstellen in den komplexen Produkten die wir nutzen. Sobald sie eine solche identifiziert haben, erstellen sie spezielle Programme um die Schwachstelle auszunutzen und die Kontrolle über jed-

Sicher in 5 Schritten

wedes Produkt, das Sie als Endanwender nutzen, zu übernehmen. Gleichzeitig arbeiten die Hersteller der Produkte mit Hochdruck daran, diese auf dem neuesten Stand zu halten. Sobald eine Schwachstelle bekannt wird, erstellen Sie einen kleinen Flicken dafür und veröffentlichen diesen. Indem Sie derartige Sicherheitsaktualisierungen immer zeitnah installieren, reduzieren Sie die Anzahl bekannter Schwächen in von Ihnen genutzten Produkten und erschweren damit den Angreifern das Leben. Um aktuell zu bleiben, sollten Sie wo immer möglich die Funktionen zum automatischen Update aktivieren. Diese Regel betrifft nahezu alle mit einem Netz werk verbundenen Geräte, darunter Ihre Fernseher mit WLAN, DSL Endgeräte, Kabelmodems, WLAN Router, Babyphones, Spielekonsolen – in naher Zukunft wahrscheinlich sogar Ihr Auto. Sollte für Produkte und deren Komponenten durch den Hersteller kein Support oder keine Updates mehr zur Verfügung gestellt werden, empfehlen wir Ihnen die Anschaffung eines durch den Hersteller unterstützten Produkts.



Das Befolgen dieser fünf Punkte bietet Ihnen einen grundlegenden Schutz für die Nutzung der neuesten Technologien.

3. **Passwörter**: Der nächste Schritt sich selbst zu schützen betrifft die Nutzung von starken, einzigartigen Passwörtern für all Ihre Geräte, Online-Benutzerkonten und Anwendungen. Der Schwerpunkt liegt auf stark und einzigartig. Ein starkes Passwort ist eines, das nicht ohne weiteres von Angreifern und Ihren Automatismen erraten werden kann. Statt eines einzelnen Wortes sollten Sie hier einen Passwortsatz aus mehreren Worten, gemischt mit Zahlen und Zeichen, verwenden. Einzigartig bedeutet, für jedes Gerät und jedes Benutzerkonto ein anderes Passwort zu verwenden. So stellen Sie sicher, dass alle anderen Zugänge geschützt bleiben, wenn eines Ihrer Passwörter Angreifern in die Hände fällt. Sie können sich all diese langen Passwörter nicht merken? Keine Sorge, so geht es uns allen. Daher empfehlen wir die Nutzung eines Passwortmanager-Programms, also einer Anwendung für Ihren Computer oder Ihr Smartphone, die auf das sichere, verschlüsselte Speichern all Ihrer Passwörter spezialisiert ist. Schlussendlich sollten Sie wann immer die sog. Zwei-Faktor-Anmeldung bei einem Benutzerkonto verfügbar ist, diese auch aktivieren, da dies eine der besten Varianten zum Schutz von Benutzerkonten ist.

4. **Verschlüsselung**: Der vierte empfehlenswerte Schritt ist die Benutzung von Verschlüsselung. Diese stellt sicher, dass nur Sie und Personen denen Sie vertrauen auf Daten zugreifen können. Daten müssen sowohl auf Speichermedien wie Festplatten, USB Sticks oder Speicher in Smartphones (ruhende Daten), als auch während des Transfers über Netze verschlüsselt werden. Heutige Betriebssysteme beinhalten meist eine Funktion, automatisch alle Daten z.B. durch eine Festplattenverschlüsselung zu schützen. Wir empfehlen,

Sicher in 5 Schritten

diese Funktion wann immer möglich zu aktivieren. Daten während des Transfers über ein Netzwerk zu sichern, bedeutet, sie zu sichern während sie von Ihrem Computer oder Mobilgerät zu anderen Geräten übertragen werden, z.B. beim Online-Banking. Sie können eine aktive Verschlüsselung leicht im Browser erkennen, wenn die Adresse der Webseite mit https:// beginnt und das Symbol eines geschlossenen Vorhängeschlosses daneben zu sehen ist.

5. **Backups**: Ganz egal wie vorsichtig Sie mit Ihren Geräten und Benutzerkonten umgehen, die Wahrscheinlichkeit ist hoch, dass eines davon irgendwann doch einem Angreifer zum Opfer fällt. In diesem Fall ist die einzig wirksame Möglichkeit zur Bereinigung des Geräts eine vollständige Löschung und Neuinstallation. Angreifer können Ihnen sogar den Zugriff auf Ihre eigenen persönlichen Daten, wie Dateien, Fotos und anderen auf dem lokalen Gerät gespeicherten Dokumenten, entziehen. Ihre einzige Möglichkeit besteht dann in der Wiederherstellung dieser Daten von einer Sicherheitskopie (Backup). Stellen Sie sicher, dass wichtige Daten regelmäßig (z.B. auf eine externe Festplatte) gesichert werden und, in regelmäßigen Zyklen, dass die Daten dort auch lesbar und wiederherstellbar sind. Die meisten Betriebssysteme auf Computern und Mobilgeräten haben bereits standardmäßig Funktionen dafür implementiert.

Weiterführende Informationen

Email Phishing Angriffe:	http://www.securingthehuman.org/ouch/2013#february2013
Absicherung Ihres (neuen) Tablet-Computers:	http://www.securingthehuman.org/ouch/2013#december2013
Starke Passwörter:	http://www.securingthehuman.org/ouch/2013#may2013
Passwortverwaltung:	http://www.securingthehuman.org/ouch/2013#october2013
2-Wege Authentifizierung:	http://www.securingthehuman.org/ouch/2013#august2013
Verschlüsselung:	http://www.securingthehuman.org/ouch/2014#august2014
Backups:	http://www.securingthehuman.org/ouch/2013#september2013

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

OUCH! wurde aus dem Englischen übersetzt von Marek Kreul und René Wiedewilt. Beide arbeiten für das CERT eines deutschen IT-Dienstleisters 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