Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Überblick
- Warum gerade Sie?
- Wie kann man sich schützen?

Ja, Sie sind tatsächlich ein Angriffsziel

Überblick

Viele Menschen leben mit dem Missverständnis, dass sie kein Ziel für Cyber-Kriminelle wären; dass Sie oder ihre Computer keinen Wert haben. Nichts könnte weiter von der Wahrheit entfernt sein. Wenn Sie einen Computer, ein Mobilgerät, ein Online-Konto, eine E-Mail-Adresse, eine Kreditkarte besitzen oder sich mit irgendeiner anderen Art von Online-Aktivitäten beschäftigen, sind Sie für Cyber-Kriminelle bares Geld wert. In diesem Newsletter erklären wir, warum Sie ein Ziel sind, wie Sie angegriffen werden und was Sie tun können um sich selbst zu schützen.

Gastautor

Eric Conrad ist Präsident und CTO der Firma Backshore Communications und ist der Hauptautor der Bücher „CISSP Study Guide, Second Edition“ und „Eleventh Hour CISSP, Second Edition“. Außerdem ist er Co-Autor des 6-tägigen SANS Kurses „Continuous Monitoring and Security Operations” (SEC511).

Warum gerade Sie?

Verbrechen wie Betrug, Identitätsdiebstahl oder Erpressung sind, seit zivilisierte Gesellschaften existieren, ein Teil unseres täglichen Lebens. Ziel eines Verbrechers ist immer das Gleiche: so viel Geld wie möglich, so einfach wie möglich und mit so wenig Risiko wie möglich erbeuten. Traditionell war dies schwierig, weil Kriminelle oft auf Ihren Standort beschränkt waren und sich körperlich mit ihren Opfern auseinandersetzen mussten. Dies hat nicht nur den Opferkreis begrenzt, sondern auch die Kriminellen einem höheren Risiko ausgesetzt. Allerdings hat sich das Verbrechen mit dem Aufkommen des Internet und der Online-Technologie radikal verändert. Heutzutage können Cyber-Kriminelle ganz einfach fast jeden in der Welt mit wenig oder gar keinen Kosten und einem sehr geringem Risiko angreifen. Zusätzlich organisieren sich die Cyber-Kriminellen immer besser und werden dadurch effizienter und effektiver als je zuvor.

Letztlich wissen Cyber-Kriminelle dass sie, je mehr Kreditkarten sie stehlen, je mehr Bankkonten sie hacken, oder je mehr Passwörter sie ausspähen, um so mehr Geld erbeuten können. Sie werden buchstäblich versuchen jeden der mit dem Internet verbunden ist zu hacken. Millionen von Menschen auf der ganzen Welt online anzugreifen klingt wie eine Menge Arbeit, aber es ist überraschend einfach wenn automatische Werkzeuge zur Verfügung stehen die die ganze Arbeit verrichten. Zum Beispiel können die Cyber-Kriminellen eine Datenbank mit Millionen von E-Mail -Adressen erstellen und dann ein automatisiertes Programm verwenden, um eine Phishing- Nachricht an jede dieser Adressen zu senden. Das Senden der E-Mails kostet die Kriminellen fast nichts: Sie verwenden einfach andere, bereits gehackte Computer und nutzen deren Internet-Bandbreite. Oft werden ganze Netze gekaperter Heim-PCs auch anderen Kriminellen vermietet,

Ja, Sie sind tatsächlich ein Angriffsziel

um deren schmutzige Arbeit zu verrichten. Dies ist auch ein weiteres Beispiel dafür, warum selbst Ihre Geräte einen nicht zu vernachlässigenden Wert haben. Wenn keine wichtigen Daten darauf abgreifbar sind, können sie immer noch verwendet werden, um weitere Systeme zu hacken oder zu schädigen. Letztlich wissen diese Kriminellen meist nicht wer Opfer ihrer E-Mail- Angriffe wird, aber sie haben die Gewissheit, dass sie um so mehr Opfer haben je mehr E-Mails sie versenden. Es gibt auch andere Möglichkeiten bereits gekaperte Computer zu benutzen. Zum Beispiel können Kriminelle mit Hilfe dieser jeden einzelnen Computer im Internet auf Schwachstellen überprüfen und diese dann ausnutzen. Denken Sie daran: Sie werden nicht angegriffen weil Sie etwas Besonderes sind, sondern weil die Kriminellen auf die breite Masse zielen, darunter auch auf Sie.

Sie haben es möglicherweise noch nicht bemerkt, aber Ihre Geräte und Ihre Informationen haben einen erheblichen Wert für Cyber-Kriminelle auf der ganzen Welt.

Wie kann man sich schützen?

Wenn Cyber-Kriminelle versuchen Internetnutzer auf der ganzen Welt anzugreifen benutzen sie gewöhnlich relativ einfache Methoden. Glücklicherweise reicht es daher aus, einige ähnlich einfache Schritte zu befolgen um sich dagegen bestmöglich zu schützen. Wir empfehlen ihnen die folgenden Aspekte zu beachten:

- **Sie selbst**: Sie stehen an vorderster Front bei der Verteidigung gegen Cyber-Angreifer. Viele Angriffe beginnen damit, dass ein Krimineller versucht Sie zu überlisten, Ihnen einen manipulierten E-Mail-Anhang unterzuschieben oder Ihnen per Telefon ein Passwort zu entlocken. Gesunder Menschenverstand ist die beste Verteidigung: Wenn etwas eigenartig, verdächtig oder zu gut um wahr zu sein aussieht, ist es mit hoher Wahrscheinlichkeit ein solcher Angriff.

- **Aktualisierungen**: Stellen Sie sicher, dass alle Computer, Mobilgeräte, Smartphones oder sonstige Geräte die sie nutzen, zu jeder Zeit auf dem aktuellsten Stand seitens Sicherheitsupdates und Programmaktualisierungen sind. Davon betroffen ist nicht nur das Betriebssystem, auch alle Anwendungen und Erweiterungen die Sie nutzen müssen aktuell gehalten werden. Sie vermeiden es so den einfachsten Angriffen zum Opfer zu werden.

- **Passwörter**: Benutzen Sie für jede Anwendung bzw. jedes Benutzerkonto ein separates starkes Passwort. Auf diesem Weg verhindern Sie eine Gefährdung all Ihrer Benutzerkonten, wenn einer der von Ihnen genutzten Dienste angegriffen und Zugriff auf alle Passwörter erlangt wurde (darunter auch Ihres). Auch alle Ihre Geräte sollten eine

Ja, Sie sind tatsächlich ein Angriffsziel

starke PIN, ein Passwort oder eine andere Art von Zugangsschutz besitzen. Um den Überblick über die vielen Anmeldeinformationen nicht zu verlieren empfehlen wir die Nutzung eines Passwortverwaltungsprogramms, die es für PCs ebenso wie für Mobilgeräte gibt.

- **Kreditkarten**: Prüfen Sie Ihre Kontobewegungen häufig, wir empfehlen mindestens wöchentliche Intervalle. Sobald Sie eine unautorisierte Transaktion finden, melden Sie diese dem zuständigen Kreditinstitut. Viele Banken bieten auch die Möglichkeit, sich per SMS oder E-Mail über Buchungsvorgänge informieren zu lassen; so können Sie verdächtige Buchungen noch schneller feststellen.

- **Ihr Netzwerk**: Sichern Sie Ihr heimisches WLAN Netz mit einem starken Passwort und stellen Sie sicher, dass eine aktuelle Verschlüsselungstechnologie (WPA2) genutzt wird.

- **Soziale Medien**: Je mehr Informationen Sie online veröffentlichen, desto höher ist das Risiko dem Sie sich aussetzen. Die über Sie verfügbaren Informationen machen es Cyber-Kriminellen leichter sie gezielt auszutricksen, können aber zudem auch dazu führen, dass man Sie als wertvolles Ziel identifiziert.

Weiterführende Informationen

OUCH! Passwortverwaltungsprogramme:	http://www.securingthehuman.org/ouch/2013#october2013
OUCH! Sichern Ihres Heimnetzwerks:	http://www.securingthehuman.org/ouch/2014#january2014
OUCH! Phishing Angriffe:	http://www.securingthehuman.org/ouch/2013#february2013
Poster: Sie sind ein Ziel:	http://www.securingthehuman.org/resources/posters

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