SANS SECURITY AWARENESS

OUCH! | Januar 2018

Der monatliche Security Awareness Newsletter für Jedermann

OUCH!

IN DIESER AUSGABE...

- **Ihr drahtloses Netzwerk**
- **Ihre Geräte**
- **Passwörter**
- **Backups**

Ein Cybersicheres Zuhause

Überblick

Vor einigen Jahren war das Absichern der häuslichen Computer noch einfach; in den meisten Wohnungen gab es nicht viel mehr als ein drahtloses Netzwerk und einige wenige Computer. Heute ist die Technologie weitaus komplexer und in jeden Aspekt unseres Lebens integriert, von Mobilgeräten über Spielekonsolen bis hin zum Heizungsthermostat und vielleicht sogar dem Kühlschrank. Nachfolgend sind vier einfache Schritte aufgeführt, wie Sie Ihr Zuhause „cybersicher“ machen können.

Gastautor

Matt Bromiley unterstützt tagsüber Kunden jeder Größe bei der Aufarbeitung von IT-Sicherheitsvorfällen (vor allem mit Datenabfluss). Er ist darüber hinaus auch Lehrer am SANS Institut, wo er den Kurs FOR508, Advanced Digital Forensics and Incident Response, hält. Folgen Sie Matt Bromiley unter **@mbromileyDFIR**.

Ihr drahtloses Netzwerk

Nahezu jedes Heimnetzwerk besteht zunächst einmal aus einem drahtlosen Netzwerk, auch WLAN oder Wi-Fi genannt. Darüber erhalten all Ihre Geräte Zugang zum Internet. Die meisten Drahtlosnetzwerke werden vom Internetrouter oder einem separaten, dedizierten WLAN-Zugangspunkt aufgespannt. Beide basieren auf der gleichen Technologie: Sie senden Funksignale aus und die Geräte in Ihrem Haushalt verbinden sich mittels dieser Signale. Der Schutz Ihres WLANs ist daher ein zentraler Punkt bei der Absicherung Ihres Heims. Wir empfehlen hierzu die folgenden Schritte.

- Ändern Sie das werksseitig gesetzte Administratorpasswort auf Ihrem Internetrouter oder WLAN-Zugangspunkt, je nachdem worüber Ihr WLAN gesteuert wird. Dieser Administratorzugang erlaubt es, die Einstellungen für das WLAN vorzunehmen.
- Stellen Sie sicher, dass nur Personen denen Sie vertrauen sich mit Ihrem WLAN verbinden können. Dies erreichen Sie durch die Nutzung starker Verschlüsselungsmechanismen. Ideal hierfür ist ein Mechanismus namens WPA2. Dadurch muss zum Zugriff auf das WLAN ein Passwort eingegeben werden, und sobald man verbunden ist sind alle Übertragungen im Funknetz verschlüsselt.
- Nutzen Sie ein starkes Passwort zum Schutz Ihres WLANs, das zwingend ein anderes als das Administratorpasswort ist. Sie müssen dieses Passwort schließlich auf jedem Gerät nur ein einziges Mal eingeben, da die Geräte sich das Passwort merken.
- Viele Drahtlosnetzwerke unterstützen auch ein sogenanntes Gastnetzwerk. Damit können Besucher auf das Internet zugreifen, aber es schützt alle anderen Geräte in Ihrem Netzwerk vor Zugriffen durch Besucher. Wenn Sie

Ein Cybersicheres Zuhause

ein Gastnetzwerk aktivieren, vergeben Sie auch hierfür ein einzigartiges, starkes WPA2 Passwort.

Sie wissen nicht, wie Sie sie diese Schritte ausführen sollen? Fragen Sie Ihren Internetanbieter oder schauen Sie sich auf dessen Webseite um, gehen Sie die Bedienungsanleitungen Ihres Internetrouters oder WLAN-Zugangspunkts durch, oder sehen Sie auf den entsprechenden Herstellerwebseiten nach.

Befolgen Sie diese vier einfachen Schritte für ein cybersicheres Zuhause; sichern Sie Ihr WLAN Netzwerk, aktivieren Sie automatische Updates, nutzen Sie einzigartige Passphrasen und aktivieren Sie Backups.

Ihre Geräte

Der nächste Schritt besteht darin, zu wissen, welche Geräte mit Ihrem Heimnetz verbunden sind und sicherzustellen, dass alle diese Geräte sicher sind. Das war noch einfach, als es sich nur um ein oder zwei Computer handelte. Heute verbindet sich nahezu jedes Gerät mit Ihrem Heimnetz, darunter Smartphones, Fernseher, Spielekonsolen, Babyphones, Lautsprecher, ja vielleicht sogar Ihr Auto. Sobald Sie alle Geräte in Ihrem Heimnetz identifiziert haben, stellen Sie sicher, dass jedes einzelne sicher ist. Das ist am einfachsten, indem man, wo immer das möglich ist, automatische Aktualisierung aktiviert. Cyberangreifer finden ständig neue Schwachstellen in den verschiedenen Geräten und Betriebssystemen. Durch das Aktivieren automatischer Updates nutzen Ihre Computer und Ihre sonstigen Geräte immer die aktuellste Software, was sie viel schwerer angreifbar macht.

Passwörter

Der nächste Schritt besteht darin, für jedes Gerät und für jedes Online-Benutzerkonto ein einzigartiges, starkes Passwort zu nutzen. Die Schlüsselwörter sind hier *einzigartig* und *stark*. Sie sind es müde, sich Unmengen komplexer Passwörter zu merken, die auch noch mühsam zu tippen sind? Das geht uns ähnlich. Nutzen Sie stattdessen sog. Passphrasen. Bei diesen nutzen Sie eine leicht zu merkende Abfolge von Worten, wie z.B. “Wo ist mein Kaffee?” oder “Sonnenschein-Kuchen-glücklich-verloren”. Je länger eine solche Passphrase ist, desto stärker ist sie. Einzigartig bedeutet, für jedes Gerät und jedes Benutzerkonto ein anderes Passwort zu verwenden. Wenn eines Ihrer Passwörter gestohlen wird, sind all Ihre anderen Benutzerkonten und Geräte dadurch noch sicher. Sie können sich all diese starken, einzigartigen Passwörter nicht merken? Machen Sie sich nichts draus – das kann wahrscheinlich niemand. Wir empfehlen daher sog. Passwortmanager, spezielle Programme, die auf eine sichere Art und Weise all Ihre Passwörter für Sie in einem verschlüsselten, virtuellen Safe speichern.

Ein Cybersicheres Zuhause

Aktivieren Sie darüber hinaus, wo immer möglich, die sogenannte 2-Faktor-Anmeldung, insbesondere für Online-Benutzerkonten. Diese Technik ist viel sicherer als Passwörter allein. Sie benötigen weiterhin Ihr Passwort, aber darüber hinaus noch einen zweiten Schritt zur Anmeldung, z.B. einen Code der auf Ihr Handy gesendet wird oder von einer Smartphone-App erzeugt wird. 2-Faktor-Anmeldung ist wahrscheinlich der eine, wichtigste Schritt den Sie zur Absicherung Ihrer Onlinekonten unternehmen können, und zudem noch viel einfacher als Sie vielleicht annehmen.

Backups

Manchmal wird man doch gehackt, und wenn man noch so umsichtig war. Wenn dies der Fall sein sollte, können Sie Ihre persönlichen Daten oft nur noch von einer Datensicherung wiederherstellen. Machen Sie daher regelmäßige Sicherungen aller für Sie wichtigen Daten und prüfen Sie auch, ob Sie die Daten wirklich wiederherstellen können. Die meisten Mobilgeräte unterstützen automatische Backups in die Cloud. Für die meisten Computer müssen Sie eine Backup-Software oder Zugang zu einem Backupdienst kaufen, die recht preisgünstig und leicht zu nutzen sind.

Weiterführende Informationen

Passphrasen:	https://securingthehuman.sans.org/ouch/2017#april2017
Passwortmanager:	https://securingthehuman.sans.org/ouch/2017#september2017
2-Faktor Authentisierung:	https://securingthehuman.sans.org/ouch/2017#december2017
Datensicherung:	https://securingthehuman.sans.org/ouch/2017#august2017

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