Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Absicherung Ihres neuen Tablets
- Halten Sie es sicher

Absicherung Ihres neuen Tablets

Überblick

Glückwunsch zu Ihrem neuen Tablet! Dieses Gerät ermöglicht Ihnen eine bequeme Art der Kommunikation mit anderen Personen, im Internet einzukaufen, Filme anzuschauen, Spiele zu spielen oder eine Vielzahl anderer Aktivitäten. Höchstwahrscheinlich wird Ihr Tablet ein wichtiger Teil Ihres Lebens werden und eventuell sogar Ihren Computer ersetzen. Daher möchten wir Ihnen in den folgenden Absätzen erklären, wie Sie sicher mit Ihrem Tablet und den darauf gespeicherten Informationen umgehen.

Gastautor

Lori Rosenberg hat umfangreiche Erfahrungen in der Erstellung von Schulungsunterlagen im Bereich Informationssicherheit für Mitarbeiter und Kunden, und sucht beständig nach neuen, besseren Methoden zur Wissensvermittlung. Sie können Sie auf Twitter unter **@InfoSecLori** finden.

Absicherung Ihres neuen Tablets

Es wird Sie überraschen, aber das größte Risiko für Ihr Tablet stellen nicht die Hacker, sondern in erster Linie Sie dar. Es ist wahrscheinlicher, dass Sie Ihr Tablet verlieren, irgendwo vergessen oder gestohlen bekommen, als dass jemand sich unberechtigt Zugriff darauf verschafft. Eine Schutzmaßnahme sollte die Aktivierung der automatischen Bildschirmsperre sein. Das heißt, vor jeder Benutzung Ihres Tablets müssen Sie dieses mit einem starken Passwort, einer komplexen Wischgeste oder Ihrem Fingerabdruck entsperren. Dies stellt sicher, dass auf Ihr Tablet bei Verlust oder Diebstahl nicht zugegriffen werden kann und somit Ihre persönlichen Informationen, mobilen Apps und sonstigen Daten geschützt sind. Sobald Sie die automatische Bildschirmsperre aktiviert haben, empfehlen wir Ihnen, die nachfolgenden Vorschläge zum Schutz Ihres Tablets umzusetzen:

1. Installieren oder Aktivieren Sie eine Software um Ihr Tablet via Internet orten zu können. Mit dieser Methode können Sie im Falle eines Verlustes oder Diebstahls darauf zugreifen und es somit orten oder, im schlimmsten Falle, auf Werkszustand zurücksetzen und somit Ihre kompletten persönlichen Informationen löschen.
2. Bringen Sie Ihr Gerät auf den aktuellsten Softwarestand und aktivieren Sie die automatische Aktualisierung, somit stellen Sie sicher, dass Ihr Tablet immer mit der aktuellsten Betriebssystemversion läuft. Angreifer suchen immer nach neuen Schwachstellen in Software und deshalb veröffentlichen die Hersteller ständig neue Aktualisierungen oder Patches um diese zu schließen. Wenn Sie also immer die aktuellste Betriebssystemversion und Version Ihrer mobilen Apps installiert haben,

Absicherung Ihres neuen Tablets

machen Sie es den Angreifern schwer sich unberechtigten Zugriff auf Ihr Tablet zu verschaffen.

3. Bei der Inbetriebnahme Ihres Tablets sollten Sie besonders achtgeben, vor allem bei den Einstellungen welche die Privatsphäre betreffen. Eines der größten Probleme in Sachen Privatsphäre ist die Möglichkeit für andere Personen Sie zu orten und somit Ihren Standort zu bestimmen. Wir empfehlen Ihnen daher den Ortungsdienst komplett zu deaktivieren und nur für einzelne Apps zu aktivieren, für die Sie es für wichtig erachten. Einige Apps, wie Navigationssoftware oder Apps die Ihnen das nächstgelegene Restaurant anzeigen, funktionieren ohne Standortinformationen nicht, aber die meisten Apps müssen nicht wissen, wo genau Sie sich aufhalten.
4. Ein Großteil der Tablets und Apps speichern Ihre Informationen in der Cloud. Es ist daher wichtig zu verstehen, wo sich Ihre Daten befinden und wie sie gesichert sind. So gilt es beispielsweise zu vermeiden, dass Ihre privaten Fotos (inkl. Standortinformationen) für jedermann einsehbar im Internet abgelegt sind. Deaktivieren Sie daher grundsätzlich das Speichern von Daten in der Cloud, und aktivieren Sie es nur ganz gezielt für einzelne Inhalte.
5. Tablets synchronisieren Ihre Apps zunehmend mit anderen Geräten wie Laptops oder Smartphones. Diese Synchronisierung ist ein wunderbares Hilfsmittel, Sie sollten jedoch achtgeben was und womit Sie synchronisieren lassen. So kann es Ihnen z.B. passieren, dass die auf Ihrem Tablet besuchten Webseiten und geöffneten Browser-Tabs im Browser Ihres Arbeits-PCs erscheinen.

Zur Absicherung Ihres Tablets aktivieren Sie die Bildschirmsperre, überprüfen Sie die Privatsphäreeinstellungen und halten Sie dessen Software immer aktuell.

Halten Sie es sicher

Sobald Sie Ihr Tablet abgesichert haben, sollten Sie sicherstellen, dass es auch so sicher bleibt. Dabei helfen Ihnen die folgenden Schritte:

- Führen Sie nie einen “Jailbreak” auf dem Gerät durch oder “hacken” Sie es. Dadurch werden viele Sicherheitsmaßnahmen des Herstellers umgangen oder deaktiviert, was Ihr Tablet bedeutend anfälliger für Angriffe macht.
- Laden Sie nur wirklich benötigte Apps und diese nur aus vertrauenswürdigen Quellen herunter. Für iPads ist das der Apple AppStore, die dort enthaltenen Apps werden von Apple vor der Bereitstellung überprüft. Für Android empfehlen wir Downloads nur von Google Play und bei einem Amazon Tablet sollten Sie beim Amazon App Store bleiben. Sie

Absicherung Ihres neuen Tablets

können natürlich auch Apps von anderen Seiten herunterladen, doch diese sind gewöhnlich nicht sicherheitsüberprüft und könnten infiziert sein. Abschließend sollten Sie noch darauf achten Apps auch wieder vom Tablet zu entfernen, wenn Sie sie nicht mehr nutzen.

- Wenn Sie eine neue App installieren, überprüfen Sie deren Privatsphäreeinstellungen und setzen Sie sie auf sinnvolle Werte, genau wie bei der erstmaligen Inbetriebnahme Ihres Tablets. Achten Sie genau darauf, was Sie jeder einzelnen App erlauben. Benötigt die gerade heruntergeladene App wirklich Zugriff auf alle Inhalte Ihres Adressbuch? Wenn Sie sich mit den Berechtigungsanforderungen einer App nicht wohl fühlen, suchen Sie sich einfach eine andere App die Ihre Anforderungen erfüllt. Prüfen Sie die vergebenen Berechtigungen regelmäßig, um sicherzugehen dass sie sich nicht verändert haben.

Ihr Tablet ist ein mächtiges Werkzeug, bei dessen Nutzung wir Ihnen viel Freude wünschen. Merken Sie sich einfach diese grundlegenden Schritte, denn sie leisten bereits einen großen Beitrag zur Absicherung des Geräts und Ihrer Daten.

Weiterführende Informationen

Sichere Nutzung von mobilen Apps:	https://www.securingthehuman.org/ouch/2015#january2015
Starke Passwörter:	https://www.securingthehuman.org/ouch/2015#april2015
Sichere Nutzung der Cloud:	https://www.securingthehuman.org/ouch/2014#september2014
Entsorgung von mobilen Endgeräten:	https://www.securingthehuman.org/ouch/2014#june2014
SANS Sicherheitstip des Tages (engl.):	https://www.sans.org/tip_of_the_day.php

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