Der monatliche Security Awareness Newsletter für Computeranwender

OUCH!

IN DIESER AUSGABE...

- Überblick
- Privatsphäre
- Sicherheit

Soziale Medien

Überblick

Soziale Medien wie Facebook, Twitter, Instagram und Xing sind unheimlich nützliche Dienste, die es Ihnen erlauben Menschen auf der ganzen Welt kennen zu lernen, mit ihnen zu interagieren und Inhalte mit ihnen zu teilen. Mit all diesen Möglichkeiten gehen aber auch Risiken einher, nicht nur für Sie, sondern auch für Ihre Familie, Freunde und Ihren Arbeitgeber. In diesem Newsletter erläutern wir diese Gefahren und wie Sie diese Dienste sicher nutzen können.

Gastautor

Tanya Baccam ist seit vielen Jahren als Sicherheits-Consultant tätig. Sie ist zudem SANS Kurs-Autor und lehrt seit über 10 Jahren unter anderem die Kurse SEC502, SEC542, SEC401, MGT414, AUD507 und viele weitere. Folgen Sie ihr auf Twitter unter **@tbaccam**.

Privatsphäre

Eine der häufigsten Sorgen bei der Nutzung von sozialen Medien ist der Schutz der persönlichen Daten. Mögliche Gefahren wären:

- **Einfluss auf Ihre Zukunft**: Einige Organisationen führen eine Art Background-Check in sozialen Netzwerken durch. Peinliche oder belastende Fotos bzw. Beiträge, ganz gleich wie alt, können Ihre Einstellung oder eine Beförderung möglicherweise verhindern. Auch manche Universitäten führen vergleichbare Überprüfungen durch, wenn sich neue Studenten bewerben. Privatsphäreeinstellungen schützen Sie hiervor meist nicht, da die Organisationen Sie bitten könnten, sie zu "liken" bzw. ihren Seiten beizutreten oder weil manche Posts auf mehreren Seiten archiviert wurden.
- **Angriffe gegen Sie**: Cyberkriminelle können Ihre Beiträge analysieren und nutzen, um z.B. Zugriff auf Informationen Ihres Unternehmens zu erlangen. Sie könnten die von Ihnen geteilten Informationen beispielsweise verwenden, um die "Geheimfragen" zum Zurücksetzen eines Ihrer Online-Passwörter zu beantworten, um gezielte E-Mail-Angriffe zu entwickeln ("Spearfishing") oder jemanden in Ihrer Organisation anrufen, sich für Sie ausgeben oder vorgeben in Ihrem Auftrag zu handeln. Die Angriffe haben auch Auswirkungen in der realen Welt, indem z.B. herausgefunden wird wo Sie arbeiten oder Ihren Wohnsitz haben.
- **Zufällige Schäden für Ihren Arbeitgeber**: Kriminelle oder Wettbewerber können sensible Informationen, die Sie über Ihr Unternehmen veröffentlichen, gegen dieses verwenden. Ihre Beiträge können zudem einen Reputationsschaden für Ihr Unternehmen nach sich ziehen. Beherzigen Sie die von Ihrem Unternehmen herausgegebenen Regeln zum Umgang mit sozialen Medien, bevor Sie Informationen über Ihren Job veröffentlichen. Bedenken Sie, dass Ihre Aktivitäten auf Plattformen sozialer Netzwerke möglicherweise von Ihrem Arbeitgeber kontrolliert werden.

Der beste Schutz besteht darin, die Menge der veröffentlichten Informationen möglichst gering zu halten. Natürlich können Privatsphäreoptionen einen gewissen Schutz bieten, sie sind aber oft auch verwirrend und werden häufig ohne Ihr Wissen geändert. Was Ihrer Meinung nach zunächst auf "privat" gesetzt war, kann somit aus verschiedenen Gründen schnell öffentlich

Soziale Medien

werden. Die von Ihnen geteilten Informationen sind zudem nur so sicher, wie die Personen mit denen Sie sie teilten. Mit je mehr Freunden oder Kontakten Sie Informationen teilen, um so wahrscheinlicher ist es, dass diese Informationen öffentlich werden. Sie sollten immer davon ausgehen, dass alles was Sie online stellen irgendwann öffentlich und damit ein permanenter Teil des Internet werden könnte.

Geben Sie auch acht, was Freunde über Sie veröffentlichen. Wenn Ihre Freunde etwas online stellen, bei dem Sie kein gutes Gefühl haben, fordern Sie sie auf es zu entfernen. Wenn sie es ablehnen oder Sie ignorieren, kontaktieren Sie die zuständigen Verantwortlichen des sozialen Netzwerks und bitten Sie um Entfernung des Beitrags. Entsprechend fair und respektvoll sollten Sie aber auch vorgehen, wenn Sie Informationen über andere veröffentlichen.



Soziale Medien machen Spaß und sind sehr vielseitig, passen Sie aber auf was und mit wem Sie dort Inhalte teilen.

Sicherheit

Neben den Hinweisen zum Thema Datenschutz, haben wir auch ein paar Tipps zum sicheren Umgang mit sozialen Medien inkl. dem Schutz Ihrer Benutzerkonten.

- **Login**: Sichern Sie jedes Ihrer Benutzerkonten mit einem starken und jeweils unterschiedlichen Passwort. Teilen Sie Ihre Passwörter mit niemandem. Viele soziale Medien unterstützen zudem einen stärkeren Schutz beim Anmelden, wie z.B. eine Zwei-Wege-Authentifizierung. Nutzen Sie diese Möglichkeit so oft es geht. Nutzen Sie Ihre Benutzerkonten sozialer Netzwerke niemals, um sich auf anderen Webdiensten anzumelden. Falls diese Benutzerkonten kompromitiert wurden, hat der Angreifer Zugriff auf alle Webdienste die Sie darüber nutzen.
- **Privatsphäreeinstellungen**: Falls Sie die Privatsphäreeinstellungen nutzen, überprüfen und testen Sie diese regelmäßig. Die Anbieter sozialer Medien ändern die Privatsphäreeinstellungen häufig und es besteht die Gefahr, dass man bei der Konfiguration Fehler begeht. Viele Apps und Dienste ermöglichen Ihnen beim Posten Ihrer Nachrichten auch Ihren Standort anzugeben (auch Geotagging genannt). Prüfen Sie Ihre Einstellungen regelmäßig, falls Sie Ihren Standort nicht preisgeben wollen.
- **Verschlüsselung**: Die Betreiber von Webseiten der sozialen Medien verschlüsseln den Zugriff via HTTPS. Twitter oder Google+ haben dies standardmäßig aktiviert, während andere Dienste dies nur als Option anbieten, die separat eingerichtet werden muss. Prüfen Sie die von Ihnen genutzten Dienste dahingehend und aktivieren Sie HTTPS als Standard, wo immer dies möglich ist.
- **E-Mail**: Seien Sie misstrauisch gegenüber E-Mails, die scheinbar von sozialen Netzwerken verschickt worden sind. Solche E-Mails werden gerne von Cyberkriminellen genutzt, um Sie anzugreifen. Der sicherste Weg um auf solche E-Mails zu reagieren ist, sich in Ihrem Profil des jeweiligen Dienstes anzumelden und diese von dort direkt zu beantworten. Greifen Sie auf den Dienst aber nur über ein von Ihnen angelegtes Lesezeichen zu oder geben Sie die URL direkt in den Browser ein. Klicken Sie niemals auf einen Link in der E-Mail.

Soziale Medien

- **Bösartige Links/Betrügerische Beiträge**: Seien Sie misstrauisch gegenüber verdächtig aussehenden Links oder möglicherweise betrügerischen Beiträgen auf Webseiten sozialer Netzwerke. Cyberkriminelle nutzen soziale Medien um ihre Angriffe durchzuführen. Nur weil eine Nachricht von einem Freund veröffentlicht wurde bedeutet das nicht, dass die Nachricht wirklich von ihm stammt, denn sein Benutzerkonto könnte kompromittiert sein. Wenn ein Familienmitglied oder ein Freund eine ungewöhnliche Nachricht veröffentlicht hat, die Sie nicht überprüfen können (wie z.B. dass er ausgeraubt wurde und Sie ihm Geld senden sollen), rufen Sie ihn an oder kontaktieren Sie ihn auf einem anderen Weg um zu bestätigen, dass die Nachricht wirklich von ihm stammt.
- **Mobile Apps**: Die meisten sozialen Netzwerke bieten auch mobile Apps, mit denen Sie auf Ihren Account zugreifen können. Stellen Sie sicher diese Apps nur von einer vertrauenswürdigen Quelle zu laden und Ihr Smartphone mit einem starken Passwort zu schützen. Wenn Ihr Smartphone entsperrt ist und Sie es verlieren, kann jedermann auf Ihr Profil zugreifen und in Ihrem Namen Beiträge veröffentlichen.

Soziale Medien sind eine wunderbare Möglichkeit, mit anderen zu kommunizieren und in Kontakt mit der ganzen Welt zu bleiben. Wenn Sie die hier beschriebenen Ratschläge befolgen, sollten Sie eine bedeutend sicherere Onlinenutzung genießen können. Um mehr über die Möglichkeiten zur sicheren Konfiguration und zur Meldung unautorisierter Vorgänge zu erfahren, besuchen Sie die Sicherheitsseiten der von Ihnen genutzten sozialen Netzwerke.

Weiterführende Informationen

Passwortsätze:	http://www.securingthehuman.org/ouch/2015#april2015
2-Wege Authentifizierung:	http://www.securingthehuman.org/ouch/2013#august2013
Sichere Nutzung von Mobilen Apps:	http://www.securingthehuman.org/ouch/2015#january2015
Cyber-Sicherheit für Kinder:	http://www.securingthehuman.org/ouch/2015#june2015
Facebook Sicherheitsseite:	https://www.facebook.com/safety

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