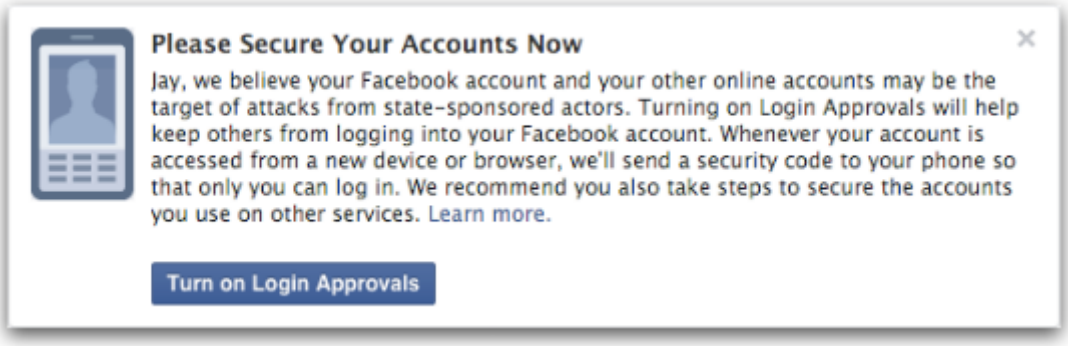
Facebook warnt User vor Überwachung

Kürzlich verkündete Facebook, seine User von jetzt an zu informieren, falls der Verdacht bestehe, diese würden von Staaten oder Regierungen gezielt ausgespäht. Sophos erklärt, wie es dazu kommt und was sich dahinter verbirgt.

Wiesbaden, 8. September 2015 – In seinem Blog Post vom 16. Oktober beschreibt Alex Stamos, Chief Security Officer bei Facebook die neue Regelung. Nutzer, so heißt es dort, erhalten von nun ab Warnungen, wenn Facebook Hinweise darauf vorliegen, dass diese von nationalstaatlich gesponserten Angreifern ausgespäht werden. Ist das soziale Netzwerk also der Ansicht, ein User würde von staatlich geförderten Hackern ins Visier genommen, weist eine Pop-up-Nachricht im Feed ihn darauf hin und legt nahe, besondere Sicherheitsvorkehrungen zu ergreifen.

Bei den vorgeschlagenen Maßnahmen handelt es sich um Login-Berechtigungen.
Facebook, so Stamos, ergreift grundsätzlich Schritte, um Konten zu sichern von denen das Unternehmen annimmt, sie wären kompromittiert worden. Nun geht man jedoch noch einen Schritt weiter und weist die Nutzer darauf hin. Einige Angriffe, so die Erklärung, wären "weiter fortgeschritten und gefährlicher" als andere. Die Meldung in der Desktop-Version sieht dann so aus:



(„Jay, wir glauben, dein Facebook und anderen Online-Konten könnten zum Ziel von Angriffen staatlich geförderter Akteure geworden sein. Login-Bestätigungen können helfen, dies zu verhindern. Wann immer von einem neuen Gerät oder Browser auf dein Konto zugegriffen wird, senden wir einen Sicherheitscode an dein Telefon, so dass nur du eingeloggt sein kannst. Wir raten außerdem dazu, auch Konten bei anderen Diensten besonders zu schützen.“)

Aufgrund der anhaltenden Angriffe durch staatlich unterstützte Angreifer ist davon auszugehen, dass jeder User, dessen Facebook-Konto unter Beschuss geraten ist, auch um die Sicherheit seiner anderen Konten fürchten muss. Facebook empfiehlt daher, die Sicherheitsvorkehrungen auf alle digitalen Konten auszuweiten. Ähnliche Warnungen sprach schon Google im Jahr 2012 aus. Genau wie Google verrät auch Facebook nicht, welche Quellen ihren Vermutungen zugrunde liegen. Das Unternehmen gibt an, den Angreifern keine wertvollen Hinweise über die Sicherheitsmechanismen liefern zu wollen.

Staaten können Personen aus politischen oder aus Gründen der nationalen Sicherheit ausspähen. Sie können einzelne Individuen angreifen, um Zugang zu ihren Arbeitgebern, zu

geistigem Eigentum oder Kundendaten zu erhalten. Länder wie Nordkorea und China stehen schon seit längerem im Verdacht, solche Angriffe zu sponsern.
Hacker mit Verbindungen zum chinesischen Militär wurden von den USA vor zwei Jahren wegen des angeblichen Eindringens in mehrere US-Stahlunternehmen angeklagt. Die USA behaupten, die chinesischen Hacker hätten via Phishing-Mails und Malware den Zugang zu E-Mail-Konten der Unternehmensvertreter gewonnen, um Informationen zu entwenden, die den staatlichen chinesischen Betrieben nützen konnten.

Attackiert oder nicht – Sicherheit ist immer gut
Auch wenn Regierungen sich nicht für die Angelegenheiten von Verbrauchern interessieren, so sollten diese ihre bequeme Komfortzone "Niemand interessiert sich für meine Wenigkeit" schleunigst verlassen. Paul Ducklin, Sicherheitsexperte bei Sophos, beschrieb es kürzlich in seinem Blog: "Wir alle sind interessant und potenzielle Opfer für Internetbetrüger irgendwo in der Welt. Wir schulden es uns selbst, uns so gut wie möglich vor ihnen zu schützen."
Die heutigen Cyberkriminellen sind hauptsächlich darauf aus, Geld zu verdienen. Die Nutzung von Malware ist hier noch immer der beste Schuss aufs Tor. Diese gelangt auf verschiedenen Wegen auf die Rechner der User, beispielsweise über schadhafte Email-Anhänge oder durch den Besuch einer Website, die Drive-by-Downloads installiert. Diese Form von Schadsoftware installiert sich komplett ohne Wissen und zutun der Besitzer. Um sich zu infizieren, muss der User lediglich eine verseuchte Webseite besucht haben.

Kürzlich hörten wir von einem Hacker, der mit einer "Facebook Spreader" genannten Malware Konten über bösartige Links in Facebook Chat-Nachrichten kompromittierte. Im August wurde ein US-amerikanischer Hacker namens Eric Crocker für schuldig befunden, Malware an Tausende Facebook Accounts gesendet zu haben, um über diese Spam zu versenden. Facebooks Empfehlung, zusätzliche Sicherheitsebenen in Form von Login-Überprüfung oder einer Zwei-Faktor-Authentifizierung zu nutzen, ist sinnvoll und sollte befolgt werden. Auch wenn man nicht im Fokus eines Staates ist, muss man es Verbrechern nicht unnötig leicht machen.

Wie man auf Facebook Login-Berechtigungen aktiviert
Facebook Login Berechtigungen funktionieren mit einem Einmal-Code. Dieser muss eingegeben werden, wenn man sich von einem nicht erkannten Gerät oder Browser anmeldet. Man erhält ihn als Text-Nachricht auf das Telefon, Facebook benötigt allerdings die Telefonnummer des Users. Login-Bestätigungen sind sicherer als Login-Benachrichtigungen. Bei diesen wird der User zwar darüber informiert, dass sein Konto soeben verwendet wurde, Missbrauch wird jedoch nicht verhindert.

So wird's gemacht
1. Klicken Sie auf den nach unten zeigenden Pfeil in der rechten oberen Ecke der Facebook-Seite
2. Wählen Sie „Einstellungen", dann „Sicherheit"
3. Unter „Anmeldebestätigungen" setzen Sie Ihr Häkchen und bestätigen die Änderunge. wählen Sie die Option Aktivieren Sie das Feld und speichern Sie die Änderung.
4. Prüfen Sie abschließend unter „Privatsphäre-Einstellungen", dass man auf Facebook nicht über ihre Telefonnummer nach Ihnen suchen kann.

Sophos hat seinen Hauptsitz in Boston, USA, und Oxford, Großbritannien. In Deutschland hat das Unternehmen seinen Hauptsitz in Wiesbaden und ist in Österreich und der Schweiz je an einem Standort vertreten. Weitere Informationen unter www.sophos.de.

Pressekontakt:

Sophos
Jörg Schindler, PR Manager CEEMEA
joerg.schindler@sophos.com, +49-721-25516-263

TC Communications
Arno Lücht, +49-8081-954619
Thilo Christ, +49-8081-954617
Christiane Capps, +49-174-3335550
Ulrike Masztalerz, +49-30-55248198
sophos@tc-communications.de