tronische Identitäts-funktion (eID) des neuen Personalausweises (nPA). Bürgerinnen und Bürgern, aber auch Mitarbeiterinnen und Mitarbeiter von Unternehmen können ihre Daten sowohl von stationären als auch von mobilen Endgeräten vertraulich in der nPA-Box ablegen und rund um den Globus mobil darauf zugreifen. Mobile Endgeräte werden dabei ohne Lesegerät aber dennoch sicher an die elektronische Identität des Nutzers gebunden.

Die nPA-Box wird vom IT-Beauftragten der Bayerischen Staatsregierung, der Anstalt für Kommunale Datenverarbeitung in Bayern und der Unternehmensberatung H&D GmbH für eine Konzeptstudie im Rahmen eines Bürgerkontos prototypisch implementiert. Ziel ist es, die Eignung der nPA-Box als konkreten Mehrwertdienst eines Bayerischen Bürgerkontos zu untersuchen und weitere Anwendungsfälle zu identifizieren.

Weitere Informationen: *http://www.it-planungsrat.de/SharedDocs/Downloads/DE/Entscheidungen/10._Sitzung/nPA-Box.pdf*

Kaspersky-Analyse: Spam-Rückgang in I/2013

Kaspersky Lab teilte am 08.05.2013 mit, dass derzeit ein signifikanter Rückgang des Spam-Aufkommens am gesamten E-Mail-Verkehr zu verzeichnen ist. Allerdings erhalten deutsche Nutzer im weltweiten Vergleich nach den USA nach wie vor den gefährlichsten Spam. Während Cyberkriminelle generell häufiger auf Soziale Netzwerke zur Spam-Verbreitung ausweichen, treiben auf Twitter zunehmend Spam-Bots ihr Unwesen.

Der Spam-Anteil am weltweiten E-Mail-Aufkommen ist derzeit stark rückläufig. Laut Kaspersky-Spam-Report betrug der Spam-Anteil im ersten Quartal dieses Jahres 66,5 Prozent[3]. Das entspricht einem Rückgang von über zehn Prozentpunkten im Vergleich zum selben Zeitraum des Vorjahres, als der Spam-Anteil am gesamten Mail-Traffic bei 76,6 Prozent lag. Auch im Vergleich zum Jahresdurchschnitt 2012 sank der Spam-Anteil im Zeitraum Januar bis März 2013 immerhin um 5,6 Prozentpunkte. Der Anteil an E-Mails, die einen infizierten Anhang enthielten, blieb im Vergleich zum Vorjahr mit 3,3 Prozent identisch.

Die Spam-Analysen für das erste Quartal 2013 festigen einen weiteren Trend: Nach den USA (13,2 Prozent) schlägt die Anti-Virus-Engine von Kaspersky Lab – aufgrund schädlicher Anhänge oder gefährlicher Links auf infizierte Webseiten – bei den deutschen Nutzern am häufigsten Alarm. Deutschland liegt in dieser Kategorie mit 11,2 Prozent weltweit auf dem zweiten Platz – vor Italien, Indien und Australien. Dieser Wert entspricht im Vergleich zum ersten Quartal des Vorjahres (5,79 Prozent) fast einer Verdoppelung.

Spam und Soziale Netzwerke

Um die Glaubwürdigkeit ihrer Nachrichten zu erhöhen, setzen Spammer nach wie vor darauf, gefälschte E-Mails im Namen von bekannten Diensten zu versenden. Beliebt waren in diesem Jahr bisher vor allem Soziale Netzwerke wie Facebook, Twitter oder seit neuestem auch Foursquare. Das Vorgehen: Beim so genannten Spoofing täuschen Cyberkriminelle eine glaubwürdige E-Mail-Adresse vor. In den betrügerischen E-Mails im Namen von Facebook und Co. verlinken sie dann auf eine infizierte Webseite mit einer Vielzahl an Exploits, die bestehende Sicherheitslücken auf dem Computer oder in einem genutzten Programm (zum Beispiel im Adobe Flash Player) finden und zur Installation verschiedener Schadprogramme ausnutzen können. Dafür wird derzeit die Exploit-Sammlung „Blackhole" am häufigsten verwendet.

Spam findet aktuell nicht mehr nur im E-Mail-Verkehr, sondern zunehmend auch in Sozialen Netzwerken statt. So laufen Social-Media-Nutzer Gefahr, dass ihr Account von Spammern gehackt und anschließend gekapert wird. Wenn anschließend über diese Facebook- und Twitter-Accounts Nachrichten an Freunde versendet werden, erhöht sich die Reputation des Spams. Ein Link, der angeblich von einem Freund kommt, wird eher angeklickt. Eine Cyberkriminellen-Kampagne machte sich diesen Social-Engineering-Trick vor kurzem zu Nutze und versendete von einem gekaperten Twitter-Account Nachrichten mit dem Inhalt „LOL, funny pic of you". Der in der Nachricht enthaltenen Link führte auf eine schädliche Webseite.

Spam-Bot via Twitter

Kaspersky Lab ermittelt immer mehr Spam-Bots, die auf Twitter aktiv sind. Diese Bots können sowohl willkürlich als auch direkt unerwünschte Nachrichten versenden. Diese Bots werden zwar leicht erkannt und von Twitter wieder entfernt, allerdings sind sie auch leicht wieder neu erstellt. Twitter-Bots sind sehr dynamisch. Eine von Kaspersky Lab auf Twitter entdeckte Porno-Spam-Kampagne operierte mit mehr als 5.000 aktiven Bots, wobei täglich 250 neue Bots erstellt wurden. Die für die Bots genutzten gefälschten Twitter-Profile haben oft nur eine Halbwertszeit von weniger als 45 Minuten. Einige dieser Social-Spam-Kampagnen verbreiten sich auch über Facebook. So spielte sich die Kampagne „job-deals.com", die seit Anfang April aktiv ist, zwar im Wesentlichen auf Twitter ab, hatte aber auch Facebook-Nutzer im Visier.

Bots in Sozialen Netzwerken belästigen Anwender mit unerwünschten Nachrichten. Zudem missbrauchen Cyberkriminelle Twitter und Facebook als Kanäle zur Verbreitung von Schadprogrammen, indem die Nachrichten gefährliche Links auf infizierten Seiten enthalten. Kommt diese Nachricht von einem gekaperten Account ist die Wahrscheinlichkeit, dass der Nutzer auf den Link klickt ungleich höher.

Neben dem Einsatz einer Anti-Spam-Lösung und dem regelmäßigen Aktualisieren aller genutzten Programme rät Kaspersky Lab sowohl E-Mail-Anwendern als auch der Social-Media-Gemeinde, sich immer davon zu überzeugen, dass die Nachricht, der Tweet oder das Posting von einer vertrauenswürdigen Quelle stammt, wenn man auf einen Link klickt oder einen Anhang öffnet. Zudem sollten alle Accounts mit sehr starken und individuellen Passwörtern abgesichert werden, damit dieser nicht gehackt und als Malware-Schleuder missbraucht werden kann.

Fraunhofer AISEC: Tech Report zur Effektivität von Antiviren-Apps

Der Großteil der frei verfügbaren Antiviren-Apps für Android-Geräte ist wirkungslos und lässt sich mit einfachen Mitteln umgehen. Zu diesem Ergebnis kommen Sicherheitsforscher des Fraunhofer AISEC (Angewandte und Integrierte Sicherheit) München, die 11 der populärsten kostenlosen Antiviren-Apps für Android-Geräte untersucht haben. Dabei stellten sie fest, dass keine der Antiviren-Apps einen ausreichenden Schutz gegen aktuelle Schad-Software bietet. Bereits einfache Änderungen an bekannten Viren führen dazu, dass diese, noch immer schädlichen Varianten von den

3 http://www.securelist.com/en/analysis/204792291/Spam_in_Q1_2013