Die aktualisierte Karte und das Verzeichnis können online auf der folgenden Website und ihren Unterseiten eingesehen werden: *https://www.enisa.europa.eu/activities/cert/background/inv*

Angriffsziel Android

Ein G Data Redpaper vom 22.05.2012 zeigt, warum das mobile Betriebssystem ein optimales Angriffsziel für Cyber-Verbrecher ist .

Android-Smartphones und Tablet-PCs sind nicht nur bei Anwendern sehr beliebt, auch Cyber-Kriminelle setzen auf die mobilen Alleskönner mit dem Google-Betriebssystem, um Nutzer zu schädigen. Doch warum attackieren die Täter insbesondere Android und nicht Symbian oder iOS? Im Redpaper „Android im Visier – eine Analyse der Ursachen" geht G Data Security Evangelist Eddy Willems dieser Frage auf den Grund. Dabei kommt er zu dem Ergebnis, dass Googles mobiles Betriebssystem ein nahezu ideales und lohnendes Angriffsziel für Kriminelle ist, da hier die drei entscheidenden Faktoren für kriminelle Handlungen gegeben sind: das Motiv, das Mittel und die Gelegenheit: Die große Popularität von Android-Geräten ist ein starkes Motiv für die Täter, um mit Hilfe von Schadcode-Apps (Mittel) Daten zu stehlen oder Geld zu ergaunern. Da Apps vor der Veröffentlichung in Google Play nicht geprüft werden, ergibt sich für die Verbrecher die ideale Gelegenheit zum Angriff.

Drei Faktoren für Cyber-Kriminelle bei Android-Mobilgeräten

Motiv

Als mobiles Betriebssystem ist Android inzwischen flächendeckend verbreitet, so hatten nach einer Analyse von IDC im dritten Quartal 2011 rund 53 Prozent aller verkaufen Smartphones eine Version des von Google entwickelten Programms installiert. Erst an zweiter folgte Symbian, Apple erreichte Platz drei. Für Cyber-Kriminelle ergibt sich daher ein starkes Motiv, mobile Schädlinge für Android-Geräte zu schreiben, da sie so eine sehr große Zielgruppe erreichen, um Nutzer anzugreifen und Geld oder persönliche Daten zu stehlen.

Vergleichbar ist dies mit der Situation bei Windows: Die meisten Schadprogramme sind für Windows-Systeme programmiert, da die Täter aufgrund der enormen Verbreitung der Microsoft-Betriebsprogramme die größte Wirkung erreichen.

Apps als Mittel der Täter

Bei Android haben die Kriminellen ein sehr einfaches Mittel, um mobilen Schadcode zu verbreiten: Apps. Hierzu werden u.a. erfolgreiche Apps in einer neuen und manipulierten Version oder vermeintlich harmlose und nützliche Applikationen in den Android-Marktplätzen, u.a. Google Play verbreitet. Dabei wurde u.a. die mobile Anwendung, die den Trojaner DoridDream enthielt, in wenigen Tagen weltweit über 250.000 Mal herunter geladen. Dank Social Engineering lassen sich die Programme zudem sehr attraktiv präsentieren, so dass die Anwender diese bereitwillig herunter laden und installieren.

Anders als Android bot der frühere aussichtsreiche Spitzenkandidat Symbian den Verbrechern kein ausreichendes Mittel. Angriffe über Bluetooth waren zwar möglich, erforderten aber eine räumliche Nähe zum Zielgerät und die Aktivierung der Schnittstelle. Der angreifbare Personenkreis wurde so stark reduziert, so dass diese Methode unattraktiv wurde.

Gelegenheit

Ähnlich wie bei Android steht auch Apple-Nutzern eine Vielzahl verschiedenster Apps zur Verfügung. In der Zwischenzeit war iOS bei Anwendern zwar das favorisierte mobile Betriebssystem. Die Plattform wurde allerdings genauso wie Symbian kein bevorzugtes Angriffsziel von Kriminellen, da Apple alle Anwendungen vor der Veröffentlichung im App-Store umfangreich prüft. Hinzu kommt, dass iOS ist im Gegenteil zu Android kein Semi-Open Source Betriebssystem ist. Ein Großteil des Programmcodes des Google-Betriebssystems ist öffentlich zugänglich, wodurch die Täter Sicherheitslücken wesentlich einfacher herausfinden und ausnutzen können.

Für die Kriminellen ist das das Nutzen von Schad-Apps auch deswegen so einfach, weil sie diese mit beliebigen Berechtigungen ausstatten können, so kann z.B. eine vermeintlich harmlose Taschenlampen-Applikation auch Anrufe initiieren und GPS-Ortungsdaten auslesen. Wenn der Anwender diese Anwendung auf seinem Smartphone oder Tablet-PC installieren möchte, muss er neben den anderen angeforderten Berechtigungen auch diese bestätigen. Android bietet keine Möglichkeit, nur bestimmte Befugnisse zu erteilen. Nach der Installation der App haben die Kriminellen so leichtes Spiel, denn auch Android-Schädlinge können je nach Funktionsweise beliebigen Schadcode nachladen, wenn das Zielgerät gerootet wurde.

Das G Data Redpaper „Android im Visier – eine Analyse der Ursachen" ist hier erhältlich: *http://public.gdatasoftware.com/*

eIDEE – Wettbewerb für den digitalen Handschlag

Die Bundesdruckerei und ihre Partner Ageto und Procilon haben am 05.06.2012 zu einem Wettbewerb für Anwendungsideen für den neuen Personalausweis aufgerufen.

Egal ob im Bereich eCommerce, eGovernment oder bei anderen Online-Services, die Online-Ausweisfunktion des Personalausweises ermöglicht es künftig rund 80 Millionen potenziellen Kunden sich in der digitalen Welt ohne Medienbruch auszuweisen.

Unternehmen aus allen Branchen können mit der Online-Ausweisfunktion ihre Geschäftsprozesse im Netz abbilden und sich dadurch einen Wettbewerbsvorteil verschaffen. Komplexe Geschäfte können so effizient und medienbruchfrei in Sekunden über das Internet abgeschlossen werden. Auch PINs, TANs, Passwörter und andere Zugangsdaten entfallen dank der Online-Ausweisfunktion, die zum Login genutzt werden kann.

Wie kann ein Unternehmen durch den Einsatz des neuen Personalausweises Geld und Zeit sparen, wie effizienter und kundenfreundlicher arbeiten?

Innovationsdenken und Kreativität sind keine Grenzen gesetzt – allein die Idee zählt. Eine unabhängige Jury kürt die beste eIDEE.

Den Gewinnern des Wettbewerbs winken attraktive Preise. Hauptgewinn sind Beratungs- und Sachleistungen zur Umsetzung der besten eIDEE im Gegenwert von 10.000 Euro. Weitere eIDEEN dürfen sich über Sachpreise wie iPads, MacBooks und allerlei Zubehör freuen.