SMARTPHONES

Direktzugang für Datendiebe

Wie sich Smartphone-Nutzer vor Viren und Datenlecks schützen können, verrät der Informatiker Peter Leppelt, Geschäftsführer des hannoverschen Unternehmens Praemandatum (auf Deutsch: Steckbrief), im Interview. Das Unternehmen berät Firmen, Institutionen und Privatleute im Hinblick auf Datenschutz und IT-Sicherheit.

Wie können Smartphones von Viren oder Schadsoftware befallen werden?

Leppelt: Smartphones sind Computer wie Desktoprechner auch, das heißt, sie können von allen Viren befallen werden, die Kriminelle durch Methoden wie Phishing oder durch Sicherheitslücken verbreiten. Hinzu kommt, dass Smartphones oft nicht nur permanent mit dem Internet, sondern auch mit dem Netz der Mobilfunkanbieter verbunden sind. So bieten sie auch Angriffsfläche über SMS-, MMS-, Social-Media-Anwendungen oder Bluetooth. Derzeit überwiegen allerdings (noch) Viren, die der Nutzer freiwillig über „Apps" auf sein Gerät einspielt. Sehr viele dieser Programme tun nicht nur das, wofür man sie installiert hat. Statistiken zeigen, dass 60 Prozent der Applikationen für Smartphones sehr viel mehr Rechte von dem Betriebssystem anfordern, als sie sie für ihre eigentliche Funktion benötigen. Wiederum sehr viele Programme wurden weiterhin „überführt", persönliche Daten des Geräteeigentümers direkt ins Ausland geschickt zu haben. Ein schönes Beispiel ist auch die erste Version der Facebook-Anwendung für das iPhone: Diese hat sämtliche Kontakte des Mobilgeräts mit denen bei Facebook synchronisiert – und zwar in beide Richtungen. Das heißt, dass im schlimmsten Fall alle Geschäfts- und Privatkontakte ohne Wissen des Handybesitzers plötzlich bei Facebook gespeichert waren. Insbesondere das iOS-Betriebssystem von Apple bietet den Nutzern in seiner Grundform relativ wenig Funktionalität. Für die meisten Funktionen gibt und braucht es eine zusätzliche App.

Sehr viele Apps haben persönliche Daten direkt ins Ausland geschickt

Im Gegensatz zur de-fakto-Monokultur von Betriebssystemen auf Desktoprechnern gibt es für Smartphones mit iOS, Android, Windows Mobile, Windows Phone 7, Symbian, Bada und anderen jedoch zurzeit noch mehrere, sehr unterschiedliche Plattformen am Markt. Diese Heterogenität ist ein Vorteil des Smartphone-Markts, wenngleich sich aktuell herauskristallisiert, dass es schlussendlich auf Apples iOS, Googles Android und vielleicht noch auch RIMs BlackBerry hinauslaufen wird. Was es noch schlimmer macht: Funktioniert ein Schädling auf praktisch allen Endgeräten, sind mit einem Schlag eben auch alle angreifbar. Damit würden Smartphones sofort sehr viel attraktiver für Virenprogrammierer werden, als sie es ohnehin schon sind. Ein weiteres großes Einfallstor sind Spionageprogramme, die schlicht auf einem unbeaufsichtigten Smartphone installiert werden und damit Unbefugten die volle Kontrolle über das Gerät ermöglichen.

Zum Schutz der Daten auf dem Smartphone sollten Nutzer einiges beachten - damit es nicht zu bösen Überraschungen kommt.

Welche Schäden können Viren oder andere Schadsoftware verursachen?

Leppelt: Alles ist möglich. Dem Nutzer muss klar sein, dass bei den meisten Betriebssystemen für Smartphones eine installierte Anwendung praktisch das gesamte Gerät steuern kann. Sie kann alles nach Belieben tun, was der Nutzer selbst auch damit tun kann. So könnte ein Programm zum Beispiel jeden Anruf von Ihnen unbemerkt als Konferenzschaltung mit einem dritten, unbekannten Teilnehmer gestalten. Ein anderes Beispiel sind Botnetze, mit denen Angreifer das Gerät im Verborgenen für ihre kriminellen Machenschaften einsetzen. Es ist absehbar, dass Daten-Flatrates in Kürze zum festen Bestandteil von Mobilfunkverträgen werden, was Smartphones als Angriffsziel für solche Zwecke noch attraktiver machen würde. Aktuell sieht es eher so aus, dass die Schädlinge entweder einfach zeigen, dass es möglich wäre, das Gerät zu übernehmen (Proof-of-Concepts) oder aber persönliche Daten – durchaus auch kritischer Natur – an fremde Server schicken. Besonders gefährlich ist das natürlich bei Firmen-Smartphones.

Wie bemerke ich, dass mein Gerät infiziert ist?

Leppelt: Wenn der Schädling gut ist: gar nicht. Ansonsten existieren inzwischen einige Sicherheitsscanner für Smartphones; aber ein plattformunabhängiger Tipp existiert derzeit leider nicht.

Wie kann ich mich dagegen schützen?

Leppelt: Sie sollten grundsätzlich sehr viel Sorgsamkeit bei der Installation von Anwendungen walten lassen – auch und insbesondere aus App-Stores gleich welcher Plattform. Hilfreich ist hierbei das App-Genome-Project, das Anwendungen auf ihre Sicherheit und unautorisierte Funkfreudigkeit hin überprüft. Dennoch kann man sich

unter anderem wegen der Vielfalt der verfügbaren Anwendungen nicht darauf verlassen. Wenn Ihre Plattform es zulässt – bei BlackBerry wurde dies beispielsweise sehr sauber gelöst - sollten Sie unbedingt die Rechte jeder Anwendung auf das Notwendigste beschränken. Ein Kartenspiel benötigt zum Beispiel sicher keinen Zugriff auf Ihre Kontakte oder Termine – also unterbinden Sie dies. Auf jeden Fall sinnvoll ist auch das Einrichten eines Passworts am Endgerät, das beim Entsperren eingegeben werden muss. So unterbindet man das schnelle Installieren eines Schädlings oder Spionageprogramms, wenn das Telefon kurzzeitig unbeaufsichtigt ist.

Peter Leppelt gründete Praemandatum vor drei Jahren.

Damit Ihre Daten bei Verlust oder Diebstahl nicht in falsche Hände geraten, sollten sie verschlüsselt im Speicher abgelegt werden. Leider ist diese Möglichkeit bei den meisten Betriebssystemen entweder gar nicht vorhanden oder unsicher gelöst, sodass man oft selbst Hand anlegen muss.

Sollte ich bestimmte Funktionen meines Geräts besser deaktivieren?

Leppelt: Bluetooth sollte nur dann aktiv sein, wenn man es benötigt. Gleiches gilt für das WLAN-Modul und für zahlreiche, gerätespezifische Funktionen. Hier lautet die Devise wie so oft: Beschäftigen Sie sich mit dem Gerät und spielen Sie damit herum. Alles, was Sie nicht benötigen, schalten Sie ab oder nur dann an, wenn Sie es brauchen.

Und was bieten die verschiedenen Handy-Betriebssysteme von Apple, Google oder Microsoft, um ihre Nutzer zu schützen?

Leppelt: Die drei hier aufgezählten bieten tragischerweise relativ wenig. Apple wacht ganz allmählich auf und investiert etwas mehr in Sicherheitskonzepte, steht aber noch ganz am Anfang. Googles Android arbeitet häufig mit veralteten Betriebssystemkernen mit möglichen Sicherheitslücken und Microsofts neue Plattform Windows Phone 7 ist einfach eher unerforscht – schlicht, weil sie kaum genutzt wird. Das derzeit einzige, sauber gelöste Sicherheitskonzept bei den großen Plattformen bietet RIM bei seinen BlackBerrys. Sie sind zudem sehr gut zentral von einer Firmen-IT administrier- und somit abdichtbar. Freie, auf Linux basierende Systeme wie MeeGo sind ebenfalls sicherheitstechnisch gut konzipiert, MeeGo wurde aber leider von seinem Hauptanwender Nokia in eine Nische geschoben. Es ist aber gut möglich – und ich würde mir das allein schon zugunsten der bereits erwähnten Heterogenität wünschen – dass sie aufgrund ihrer freien Architektur von anderen Herstellern aufgegriffen werden.

Was muss ich beim Surfen mit Laptop, Smartphone oder Tablet-PC über sogenannte Hotspots in Cafes, Restaurants oder im ICE beachten?

Leppelt: Ganz generell sollten Sie auf eine Ende-zu-Ende-Verschlüsselung achten. Viele denken, wenn das WLAN passwortgeschützt ist, seien sie sicher vor Abhörmaßnahmen. Das ist natürlich falsch, insbesondere, wenn alle Nutzer des Drahtlos-Netzes das gleiche Passwort haben. Beispiele für Ende-zu-Ende-Verschlüsselungen sind bei Websites SSL - andeutungsweise erkennbar am https:// in der Adresszeile - oder bei Firmennetzwerken VPNs (Virtual Private Networks). Eine solche Verschlüsselung nutzt Ihnen natürlich nur dann etwas, wenn Sie nicht bereits einen Spion auf Ihrem mobilen Endgerät installiert haben.

Wenn ich alle ihre Ratschläge befolge und mich nun sehr umsichtig im Netz bewege, bin ich dann sicher vor kriminellen Angriffen?

Leppelt: Sollte Ihnen jemand irgendetwas Digitales anbieten, das vollkommen sicher ist, so suchen Sie sich dringend einen anderen Anbieter. Jeder Informatikstudent lernt in seiner ersten Vorlesung, dass nichts Digitales sicher ist, sobald es online geht. Die Kunst ist es, den Aufwand, der nötig wäre, ein System zu knacken, höher als den Wert der Daten werden zu lassen. Und ja, dieses Hochschrauben des Aufwands funktioniert normalerweise – allerdings nicht mit den hier angebrachten Tipps. Dafür sind ein Artikel und sogar ein ganzes Buch zu kurz. Für alle technischen Entwicklungen gilt: Sie müssen sich damit beschäftigen. Die Einfachheit, mit der die Dinge in der Werbung angepriesen werden, kann es nicht geben. Es ist mit hochkomplexen Konfigurationsmöglichkeiten ausgestattete Technologie. Davon abgesehen: Es lohnt sich. Ich bin begeisterter Technik- und Smartphone-Nutzer; unter anderem auch deswegen, weil ich weiß, was das Ding tut und wie ich es steuern kann.

Die Fragen stellte Christian Heegardt.

IHK-SERVICE

Seminar: Datenschutz und -sicherheit in einer vernetzten Welt

Daten-Lecks bergen ein extrem hohes geschäftliches Risiko. Zumeist sind in Unternehmen nicht die einzelnen IT-Systeme das Problem, sondern – vor allem bei gewachsenen Systemen – viel mehr das Zusammenspiel der Systeme sowie der Umgang damit. Um Unternehmen adäquat auf diese Herausforderungen vorzubereiten, zeigt dieses Seminar Hintergründe und Lösungsmöglichkeiten auf – auf kurzweilige Art und Weise. Zielgruppe sind Datenschutz-/IT-Sicherheitsbeauftragte, IT-Verantwortliche, Geschäftsführer sowie Mitarbeiter von IT- und Rechtsabteilungen.

Programm:

- Einführung und Sensibilisierung für Sicherheits-Belange
- Datenschutz vs. IT-Sicherheit – Grundlagen für kleine und mittlere Unternehmen
- Viren, Phishing & Co. – Was genau passiert da?
- Schutz wichtiger Daten auf mobilen Geräten bei Verlust und Diebstahl
- Social-Media – Vor- und Nachteile
- Industriespionage – Was jeder tun kann und sollte

Das Seminar „Datenschutz und sicherheit in einer vernetzten Welt" findet am 19. Mai von 14 bis 18 Uhr in der IHK Hannover statt. Die Teilnahmegebühr beträgt 130 Euro zzgl. 19% USt. (brutto 154,70 Euro).

Anmeldung und Informationen zu diesem und weiteren Seminaren rund um die Themen Datenschutz und IT-Sicherheit:

www.begin.de/seminar