Mission Impossible: Dieses Handy zerstört sich nach 15 Sekunden….

In wirtschaftlich schwierigen Zeiten nimmt die Kriminalitätsrate beständig zu. Dabei geht es nicht nur um die Kleinkriminalität auf den Straßen, sondern vor allem um Identitäts- und Datendiebstähle. Seit 2006, so munkeln die Anti-Viren-Software-Hersteller, wird weltweit mehr Geld mit Viren und Spams umgesetzt, als im Drogenhandel. Alle 2 Sekunden werde eine neue Schadsoftware auf den Markt gebracht, so berichtet TrendMicro. Der Trend gehe dabei eindeutig in Richtung gezielte Angriffe auf elektronisch gespeicherte Daten, wobei Highpotentials, VIPs und andere leitende Personen, bei denen wichtige oder geheime Daten vermutet werden besonders betroffen sind.
Leichte Beute sind dabei mobile Endgeräte wie Handy, Smartphone, PDA und Blackberry, die nicht nur häufig vergessen oder verlegt werden, sondern auch leicht zu entwenden sind.

Nach einer Umfrage von F-Secure ist das Unrechtsbewusstsein beim Fund eines Handys drastisch gesunken. F-Secure hat anlässlich der letzten Weihnachtsfeiern rund 300 Personen im Alter zwischen 20 und 49 Jahren zum Thema „Wie gehen Sie mit einem herrenlosen Handy um?" befragt. Nur 32% würden es unangetastet abgeben. Über zwei Drittel würden zumindest nach Hinweisen auf die Identität des Besitzers suchen. Dieses vielleicht noch entschuldbare, wenn auch rechtswidrige Verhalten wird noch übertroffen, indem 40% die SMS-Nachrichten lesen würden, 23,3% sich die Kontakte näher ansehen und 10% sogar private Ordner nach Informationen durchsuchen würden. Noch einen Schritt weiter gehen einige der Befragten, die dem Besitzer Schaden zufügen würden. Dabei würden 6,6% Freunde im Ausland anrufen, 3,3% würden Bilder herunterladen und ins Internet stellen und 2,1% wären sogar so dreist und würden Daten verändern oder löschen. [1]
Die meisten Benutzer von mobilen Endgräten machen sich darüber wenig Gedanken. Noch immer seien die meisten mobilen Geräte nicht vor Viren oder Spams geschützt, geschweige denn verschlüsselt oder gegen Diebstahl abgesichert.

Dass der Virenschutz auf Handys so stiefmütterlich behandelt wird mag daran liegen, dass zurzeit „nur" ca. 250 Viren bekannt sind, die explizit für Handys geschrieben wurden. Bekannter sind schon die Angriffe über Bluetooth. Besonders auf Messen, wenn Besucher per Bluetooth-Nachricht aufgefordert werden, bestimmte Stände zu besuchen. Dabei wird Schadsoftware auf vor allem auf geschäftlich genutzte Handys und PDAs übertragen.
Ein weiterer Aspekt ist auch, dass einige Hersteller von Betriebssystemen sich weigern die Schnittstellen preis zu geben, weil die Existenz eines Virenscanners für ein bestimmtes Betriebssystem oder Handy impliziert, dass es Probleme mit Schadsoftware oder Crimeware gibt.
Es ist sträflich, diese Gefahr außer Acht zu lassen. Schaut man sich die Entwicklung der PC-Viren der letzten 4 Jahre an, so hat sich die Anzahl der neuen Viren pro Jahr verzehnfacht. „Im Jahr 2008", so Rüdiger Trost von der Firma F-Secure, „wurden 1,6 Mio. neue Viren und Schadsoftware auf den Markt gebracht."

Warum ist es so wichtig auch das Handy zu schützen? Abgesehen davon, dass es mehr als ärgerlich ist, wenn nach Verlust oder Diebstahl eines Handys die Telefonrechnung ins unermessliche steigt, weil mit dem Gerät ins Ausland telefoniert wird oder die im Adressbuch gespeicherten Kontakte belästigt werden, so grenzt es schon an Rufschädigung, wenn Bilder und Videos im Internet auftauchen. Viel schlimmer allerdings ist, wenn Daten, die achtlos auf dem Handy abgelegt wurden (durch Synchronisation von Emails, VPN-Verbindungen ins Firmennetzwerk, o. ä.) in falsche Hände geraten. So

[1] Quelle: www.f-secure.de, „F-Secure Umfrage: „40 Prozent der Befragten würden private Nachrichten in gefundenen Handys lesen" vom 09.12.2008

werden Passwörter von Internet-Shops, Benutzerbereichen oder anderen geschlossenen Webseiten oftmals per Email versendet. Hin und wieder kommt es sogar vor, dass Dienste wie Online-Banking von unterwegs über den PDA genutzt werden. Diese Daten gilt es zu schützen. Immer moderner werden die Bezahldienste über das Handy oder das digitale Bahnticket, bei dem das Handy-Display als Fahrkarte gilt.

Als erste Maßnahme sollten bei einem Handy die Funktionen wie Bluetooth, etc. nur dann benutzt werden, wenn es explizit erforderlich ist. Ansonsten sollten diese Funktionen abgeschaltet bleiben. Idealerweise sollte das Handy auch nur dann angeschaltet sein, wenn es benötigt wird und zur ersten Absicherung mit einer Handysperre versehen werden.

Im zweiten Schritt sollte dann eine weitere Absicherung der Daten gegen Diebstahl, Viren oder Verlust stattfinden. Die großen Antiviren-Software-Hersteller liefern hierfür Produkte, die meist mit Virenschutz, Spamschutz und einer Firewall ausgestattet sind. Meist ist die Software vom eigenen PC aus verwaltbar. Zu den geschützten Betriebssystemen gehören derzeit Windows Mobile und Symbian, sowie kompatible Handy- und Smartphone-Modelle der gängigsten Hersteller.
Beim Einsatz sollte darauf geachtet werden, dass folgende Punkte im Leistungsumfang des Antiviren-Produkts enthalten sind:

- Die Software muss im Hintergrund laufen, damit der Benutzer bei seinen eigentlichen Aufgaben nicht gestört wird
- Der Scannvorgang sollte sowohl beim Dateizugriff erfolgen, als auch manuell steuerbar sein
- Die Updates der Virenpattern sollte automatisch erfolgen, eine Online-Verbindung zu einer entsprechenden Datenbank haben oder einem Algorithmus gehorchen, der verdächtige Software in Quarantäne stellt
- Es sollte die Möglichkeit bestehen, eine Firewall einzuschalten, um unberechtigte Zugriffe blockieren zu können
- Für Personen, die ihre Emails mit Windows Mobile und Outlook auf das Handy oder den PDA herunterladen, ist ein Mail-Scanner unerlässlich
- Mit einer der wichtigsten Punkte ist der Diebstahl-Schutz. Dabei ist darauf zu achten, dass man das Handy oder Smartphone im Falle eines Diebstahls per SMS sperren kann, auch wenn die SIM-Karte gewechselt wird, damit die Daten entweder gelöscht oder unbrauchbar sind

Ein besonderes Plus wäre die SMS, die den Bestohlenen über den Verbleib seines Handys informiert.

Doch bei all dem Software-Schutz ist die Umsicht und das Bewusstsein des einzelnen noch immer der beste Schutz. Bei unsachgemäßem Einsatz nützen die ganzen Sicherheitsvorkehrungen nichts. Deshalb ist es wichtig, die Daten nicht auf der SIM-Karte zu speichern und den vorgesehenen Passwortschutz auch zu verwenden. Leider sind wir noch nicht so weit, dass sobald ein Handy-Dieb seine Beute in Betrieb nimmt ein lautes Piepsen ertönt und eine Computerstimme warnt: „Sie haben das Handy gestohlen, das Gerät zerstört sich in Sekunden…"

PS: Seit Sie diesen Artikel lesen, sind 95 neue Viren programmiert worden….