Angriff aufs Smartphone ? Gefahr für Android-Nutzer
20.01.2013

Auf dem Windows-PC ist es heuet ganz selbstverständlich, eine Sicherheitssoftware installiert zu haben, die vor Viren und Trojanern, Malware und Hackerangriffen schützt. Aber auf dem Smartphone? iPhone-Nutzer sind sicher, weil Apple ein in sich geschlossenes System erschaffen hat, und Nutzer von Windows-Phone-8-Geräten sind aufgrund der geringen Reichweite für Cyberkriminelle kaum interessant. Problematisch ist jedoch Android. Welche Gefahren lauern und wie sich Nutzer können, der Beitrag verrät´s.

Leadin
Auf dem Windows-PC ist es heuet ganz selbstverständlich, eine Sicherheitssoftware installiert zu haben, die vor Viren und Trojanern, Malware und Hackerangriffen schützt. Aber auf dem Smartphone? iPhone-Nutzer sind sicher, weil Apple ein in sich geschlossenes System erschaffen hat, und Nutzer von Windows-Phone-8-Geräten sind aufgrund der geringen Reichweite für Cyberkriminelle kaum interessant. Problematisch ist jedoch Android. Welche Gefahren lauern und wie sich Nutzer können, hat Björn Czieslik bei der CeBIT-Preview in München erfahren.

An und für sich ist Android ein sicheres System. Apps können nur aufs Telefonbuch zugreifen, Daten übermitteln oder den Standort weitergeben, wenn der Nutzer dies bei der Installation erlaubt hat, erklärt Udo Schneider vom Sicherheitssoftware-Anbieter Trend Micro.

O-Ton 1 (0:13)

Angriff aufs Smartphone ? Gefahr für Android-Nutzer

Auf dem Windows-PC ist es heuet ganz selbstverständlich, eine Sicherheitssoftware installiert zu haben, die vor Viren und Trojanern, Malware und Hackerangriffen schützt. Aber auf dem Smartphone? iPhone-Nutzer sind sicher, weil Apple ein in sich geschlossenes System erschaffen hat, und Nutzer von Windows-Phone-8-Geräten sind aufgrund der geringen Reichweite für Cyberkriminelle kaum interessant. Problematisch ist jedoch Android. Welche Gefahren lauern und wie sich Nutzer können, hat Björn Czieslik bei der CeBIT-Preview in München erfahren.

An und für sich ist Android ein sicheres System, erklärt Udo Schneider vom Sicherheitssoftware-Anbieter Trend Micro. Apps können nur aufs Telefonbuch zugreifen, Daten übermitteln oder den Standort weitergeben, wenn der Nutzer dies bei der Installation erlaubt hat.

O-Ton 1 (0:13)

Das kann zum Beispiel ein beliebtes Spiel sein, das verändert und um Schadsoftware erweitert wurde und dann zu einem günstigeren Preis in einem anderen App-Store wieder angeboten wird.

O-Ton 2 (0:16)

Das Problem: Einmal erteilte Zugriffsrechte kann man Android-Apps nur entziehen, indem man sie wieder deinstalliert. Doch dann könnte es bereits zu spät sein.

Wer Apps nur aus dem Google-Play-Store oder den offiziellen App-Stores der Gerätehersteller und Netzbetreiber herunter lädt, ist zwar sicherer, doch Experte Udo Schneider empfiehlt:

O-Ton 3 (0:22)

Daneben hilft der gesunde Menschenverstand: Angebote, die zu gut klingen, um wahr zu sein, sind oft alles andere als gut und sollten hellhörig machen. Und da die Verbreitung von Android stetig wächst, wird das System auch für Angreifer zunehmend interessanter.