

Gibt es ein App für Sicherheit? Die EU-IT-Sicherheitsagentur hebt die Risiken und Vorzüge von Smartphones hervor

Ein neuer Bericht der ENISA ermittelt die wichtigsten Sicherheitsrisiken und Vorzüge beim Einsatz von Smartphones hin und gibt Unternehmen, Verbrauchern und Regierungen praktische Hinweise. Zu den wichtigsten Risiken gehören Spyware, die unzureichende Löschung von Daten bei der Entsorgung von Mobiltelefonen, versehentlicher Datenverlust und unberechtigte Anrufe oder SMS über Mehrwertdienste.

Der Verkauf von Smartphones hat sich im letzten Jahr weltweit verdoppelt (Gartner); allein im 3.Quartal 2010 wurden weltweit 80 Millionen Stück verkauft. Der Bericht der ENISA über die Sicherheitsrisiken und Vorzüge von Smartphones kommt daher genau zur rechten Zeit. Wenn Sie zu den weltweit Abermillionen Smartphone-Nutzern gehören, verbringen Sie wahrscheinlich mehr Zeit mit Ihrem Telefon als mit Ihrem Ehepartner. Mit der Vielzahl von Applikationen und Sensoren kann es sein, dass Ihr Telefon Sie sogar besser kennt. Die neuen „Lebenspartner“ sind heute bei Mitgliedern aller Gesellschaftsbereiche zu einem unverzichtbaren Instrument geworden – von führenden Regierungsbeamten über Geschäftsleute bis hin zu Verbrauchern. Sie werden wegen der Vielzahl ihrer Funktionen geschätzt, denn ein Smartphone kann als kontaktlose Brieftasche dienen, als Kamera- oder Videotelefon, als Barcode-Reader, als E-Mail-Client oder als Zugangsweg zu sozialen Netzwerken.

„Angesichts der zunehmenden Bedeutung von Smartphones für Unternehmen, Regierungen und Bürger in der EU ist es unserer Meinung nach entscheidend, ihre Sicherheits- und Datenschutzimplikationen zu ermitteln“, meint Prof. Dr. Udo Helmbrecht, Geschäftsführender Direktor der ENISA. Die ENISA analysiert in ihrem neuen Bericht die wichtigsten Sicherheitsvorzüge und -risiken. Zu den Risiken gehören:

- Zufällige Weitergabe vertraulicher Informationen beispielsweise durch GPS-Daten auf Bildern.
- Datendiebstahl durch Schadprogramme und von entwendeten, verlorenen oder stillgelegten Telefonen.
- „Dialer“ - Einwahlprogramme, die mittels unberechtigter Telefonanrufe Geld entwenden.
- Überlastung der Netzwerkinfrastruktur durch Smartphone-Apps.

Bezüglich der Vorzüge ist zu sagen, dass Sicherungsspeicherungen häufig sehr gut in Smartphone-Plattformen integriert sind, wodurch es sehr einfach wird, Daten im Falle des Verlusts oder Diebstahls des Telefons wiederherzustellen. Ein weiterer Vorteil besteht in der Nutzung von App-Stores: *„Die meisten Nutzer von Smartphones installieren Software von Drittanbietern über kontrollierte Software-Vertriebskanäle“*, erklärt Dr. Marnix Dekker, Ko-Autor des Berichts.

10/12/2010

www.enisa.europa.eu

Das wichtigste Ergebnis des Berichts ist eine umfassende Liste mit Strategien zur Sicherung von Smartphones. *„Smartphones sind eine Goldmine für sensible und persönliche Daten. Daher ist es entscheidend zu wissen, wie man die Kontrolle über diese Daten behält. Wir haben unsere Empfehlungen so gestaltet, dass sie in typische Sicherheitskonzepte integriert werden können“*, so Dr. Giles Hogben, Ko-Autor des Berichts. Der Bericht verfügt über Empfehlungen für Unternehmen, leitende Beamte und Verbraucher – und für den Umgang mit Sicherheitsrisiken, die aus einer Vermischung dieser Rollen entstehen.

Lesen Sie den [vollständigen Bericht](#).

[Video](#)

Zusatzmaterial: [FAQs zur Sicherheit bei Smartphones](#)

Für Interviews wenden Sie sich an: Ulf Bergstrom, Pressesprecher, ENISA, press@enisa.europa.eu, Handy: +30-6948-460143, oder für weitere Informationen an: Dr. Marnix Dekker, marnix.dekker@enisa.europa.eu.

Übersetzung. Das Englische Original bleibt die maßgebliche Fassung.