

08/02/2010

www.enisa.europa.eu

Instantly Online - 17 Goldene Regeln zur Bekämpfung von Online-Risiken und für sichereres Surfen mobiler sozialer Netzwerke

Die EU-„Cyber Security“-Agentur - ENISA (European Network and Information Security Agency, Europäische Agentur für Netz- und Informationssicherheit), stellt heute einen neuen Bericht über den Zugang zu sozialen Netzwerken per Mobiltelefon vor: „[Online as soon as it happens](#)“. In dem Bericht werden die Risiken und Gefahren mobiler sozialer Netzwerke dargelegt, z. B. Identitätsdiebstahl, Datenverlust von Unternehmen und Reputationsrisiko. Die Verfasser stellen auch 17 „Goldene Regeln“ auf, wie diese Gefahren zu bekämpfen sind.

Online Social Networking Sites (SNSs) haben im Internet einen außergewöhnlichen Wachstumstrend verzeichnet. 211 Millionen Nutzer (von 283 Millionen) in Europa benutzen SNS und in 11 von 17 untersuchten Ländern vorzugsweise Facebook. Der moderne Weg, mit Geschäftspartnern oder im persönlichen Umfeld Kontakt zu halten, läuft über SNS und andere digitale Tools. Folglich ändert sich die Art und Weise, auf die sich Leute treffen, ihre Meinungen austauschen, Informationen und Ideen kommunizieren. Mit dem wachsenden Beliebtheitsgrad von SNS ist die Nachfrage nach sofortigem, kontinuierlichem Zugang über das Mobiltelefon gestiegen – dem mobilen sozialen Netzwerk (MSN). Mehr als 65 Millionen Nutzer haben über ihr Mobilgerät Zugang zum sozialen Netzwerk Facebook. MSN-Nutzer sind 50 % aktiver als Nicht-Mobilnutzer und diese Zahl wird in Europa bis 2012 voraussichtlich auf 134 Millionen steigt.

Viele MSN-Nutzer benutzen ihr Telefon auch als Backup-Gerät für Geschäftsmails, persönliche Daten, Kontaktangaben, Bilder und Zugangscodes. Folglich kann ein verlorenes Mobiltelefon ernsthaften Schaden anrichten, wenn es illegalerweise benutzt wird, um auf MSNs zuzugreifen. Viele Mobiltelefone werden als Kompaktpaket verkauft und verfügen über eingebaute MSN-Anwendungen, sogenannte ‚On-Deck‘-Anwendungen.

Mehreren Berichten aus Italien, Frankreich, Spanien, Griechenland und Großbritannien zufolge sind viele SNS/MSN-Nutzer sich der Sicherheitsrisiken, der Gefahr des Eindringens in die Privatsphäre und der Gefahren, die mit dem Missbrauch der per SNS ins Internet gestellten Information einhergehen, sowie der Notwendigkeit eines angemessenen Datenschutzes im Internet kaum bewusst. Einige der besonderen MSN-Risiken/Gefahren werden in dem Bericht aufgezeigt. Der ENISA-Bericht (<http://www.enisa.europa.eu/act/ar/deliverables/2010/onlineasithappens>) gibt einen Überblick über die Lage und betont, dass besonders MSN-Nutzer sich über Möglichkeiten klar sein sollen, wie man MSN auf einem Mobiltelefon sicherer benutzen kann, um unerwartete und schädigende Konsequenzen zu vermeiden. Risiken beinhalten Identitätsverlust, ernsthafte Schäden bezüglich der Reputation von Einzelpersonen oder Unternehmen sowie Datenverlust. Zwei Fallbeispiele:

08/02/2010

www.enisa.europa.eu

- **Falsches Profil auf Facebook.** Ein Professor der Universität Turin entdeckte, dass jemand für ihn ein Profil mit beleidigenden Merkmalen auf Facebook geschaffen und somit seinen Ruf geschädigt hatte.

- **Datenverlust/Reputation eines Unternehmens.** Nach einer Begebenheit in 2008 kündigte die Virgin Atlantic Airlines später 13 Mitarbeitern, die Kommentare auf Facebook veröffentlicht hatten, *mit denen sie z.B. die Sauberkeit der Firmenflotte und die Passagiere kritisiert hatten*. Ebenso haben Mitarbeiter des Check-in-Personals von British Airlines in Gatwick Mitteilungen auf Facebook veröffentlicht und von „stinkenden“ Passagieren gesprochen und den „chaotischen“ Ablauf in Heathrow kritisiert.

Der Bericht gibt auch einen umfassenden Einblick in die SNS-Welt aus der Sicht der EU Datenschutz-Richtlinie (95/46/EG). Der geschäftsführende Direktor von ENISA Udo Helmbrecht kommentiert:

„Dieser Bericht bietet nützliche und praktische Hinweise, wie man sich online, überall und jederzeit, beim Benutzen mobiler sozialer Netzwerke sicherer verhalten kann.“

Der Bericht beinhaltet 17 praktische „Goldene Regeln“. Hier einige Beispiele:

- Denken Sie daran, sich nach der Session immer aus dem sozialen Netzwerk abzumelden.
- Erlauben Sie dem sozialen Netzwerk nicht, sich an Ihr Passwort zu erinnern (diese Funktion heißt „Auto-complete“, automatische Vervollständigung).
- Mischen Sie Ihre geschäftlichen Kontakte nicht mit den persönlichen Kontaktangaben Ihrer Freunde.
- Erstaten Sie sofort Bericht über gestohlene/verlorene Mobiltelefone mit gespeicherten Kontaktangaben, Bildern oder persönlichen Daten.
- Stellen Sie das Niveau der Privatsphäre Ihres Profils sachgemäß ein.

Alle Empfehlungen sind in dem vollständigen Bericht zu finden, der hier zum [Download zur Verfügung](#) steht:

Interviews: Ulf Bergstrom, Pressesprecher, ENISA, press@enisa.europa.eu, Mobiltelefon: +30-6948-460143, oder Isabella Santa, Senior Expert Awareness Raising, ENISA, awareness@enisa.europa.eu