27/08/2012
EPR010/2012

www.enisa.europa.eu

EU Behörde ENISA analysiert die Gesetzgebung zur Sicherheit im Internet und macht Lücken in der Umsetzung ausfindig; Vorfälle bleiben unerkannt oder werden nicht angezeigt

In einem kürzlich veröffentlichten Bericht macht sich die EU „Sicherheit im Netz" Behörde ENISA ein Bild der bestehenden und künftigen EU Gesetzgebung zu den Sicherheitsmaßnahmen im Netz und dem Berichten von Vorfällen. Die Analyse hebt wichtige Fortschritte hervor, macht aber auch Lücken in der nationalen Umsetzung ausfindig, da die meisten Vorfälle nicht gemeldet werden.

Vorfälle in der Internetsicherheit wirken sich wesentlich auf die Gesellschaft aus. Im Folgenden werden fünf bekannte Beispiele aufgelistet:

- Im Jahr 2012 wurden Millionen Passwörter aus Geschäftsnetzwerken freigelegt
- 2011 zerstörte der Sturm Dagmar Millionen von skandinavischen Kommunikationslinks
- 2011 hat das Versagen eines Britischen Datenzentrums dazu geführt, dass Millionen von Geschäftskorrespondenzen unterbrochen wurden
- 2011 wurde ein Abkommen verletzt, wodurch die Kommunikation von Millionen von Nutzern freigelegt wurde
- 2010 hat ein chinesischer Telefonanbieter 15% des weltweiten Internetverkehrs für 20 Minuten für sich beansprucht

Jedes Mal hat sich auf Millionen von Bürgern und Unternehmen ernsthaft ausgewirkt. Die meisten Vorfälle werden jedoch nicht erfasst oder auch nur festgestellt. Dr. Marnix Dekker and Chris Karsberg, Co-Autoren des Berichts, behaupten: *„Vorfälle im Netz werden bei ihrer Entdeckung meist geheim gehalten, wodurch sowohl Kunden als auch Politiker im Dunkeln tappen bezüglich Häufigkeit, Auswirkung und Gründe.*"

Der neue Bericht "Cyber Incident Reporting in the EU" bietet einen Überblick über bestehende und geplante Gesetzgebungen (siehe beigefügte Grafik). Er enthält Klausel der obligatorischen Berichterstattung über Zwischenfälle aus Artikel 13a des Telecom-Paketes und Artikel 4 der E-Privacy-Richtlinien und schlägt eine e-ID Regelung nach Artikel 15 und Artikel 30, 31, 32 des Datenschutzgesetzes vor. Die Studie zeigt Gemeinsamkeiten und Unterschiede zwischen den Gegenständen und Sichtweisen der EU Internet-Sicherheitsstrategie. Der Bericht stellt auch die Bereiche für die Verbesserungen vor. Zum Beispiel war nur eines der oben genannten Ereignisse im Rahmen der nationalen Regulierungsbehörden, was darauf hinweist, dass es Lücken in der Regulierung gibt. Aus diesem Grund sollte der EU-weite Austausch von Berichten über besondere Vorkommnisse verbessert werden.

Kürzlich wurden große Fortschritte gemacht: Eine ENISA-Arbeitsgruppe für nationale Regulierungsbehörden hat sowohl einen gemeinsamen Satz von Maßnahmen zur Gefahrenabwehr, als auch ein Vorfallbericht-Format entwickelt. Dies ermöglicht eine einheitliche Umsetzung von Artikel 13a. ENISA erhielt kurz darauf Berichte von über 51 großen Zwischenfällen von den Regulierungsbehörden, in dem die Auswirkungen beschrieben, Ursachen erfasst, Maßnahmen ergriffen und Erkenntnisse aufgelistet sind. Dieser Beitrag wird

als Übungsmaterial für die European cyber security strategy und European cyber security exercise verwendet. Der Geschäftsführende Direktor der ENISA, Professor Udo Helmbrecht, kommentierte: *"Indirekte Berichterstattung ist wichtig, um ein Bild der echten Internet-Sicherheit zu erhalten. Die EU Cyber Security Strategy ist ein wichtiger Schritt und eines seiner weiteren Ziele ist es, den Umfang der Berichterstattung, wie in der Bestimmung von Artikel 13a, über den Telekommunikationssektor zu erweitern. "*

Hintergrund: European Cyber Security Strategy und Art 13a working group documents

Für Interviews: Ulf Bergstrom, Pressesprecher, ENISA, press@enisa.europa.eu, Mobil: + 30 6948 460 143, oder Dr. Marnix Dekker, ENISA, marnix.dekker@enisa.europa.eu

Übersetzung. Das Englische Original ist die einzige maßgebliche Fassung.
http://www.enisa.europa.eu/front-page/media/enisa-auf-deutsch
www.enisa.europa.eu