

13. Dez. 2011

www.enisa.europa.eu

„Klärung der Berichterstattung über Cybersicherheitsvorfälle: Richtlinien zur Umsetzung der neuen Fernmeldegesetzgebung zur Sicherheit und Integrität „Artikel 13a“

ENISA, die Agentur für „Cybersicherheit“ der EU hat heute zwei technische Richtlinien herausgegeben. Die erste beschreibt, wie das vorgeschriebene [Berichterstattungssystem für Cybersicherheitsvorfälle](#) durch Telekommunikationsbetreiber umgesetzt werden kann, ferner Parameter und Schwellenwerte sowie die Form des Berichts; die zweite legt dar, welche [spezifischen Sicherheitsmaßnahmen von Telekommunikationsbetreibern](#) vorgenommen werden sollten.

Die neue Fernmeldegesetzgebung (EU-Direktive 2009/140/EC) bietet [unter anderem](#) Kunden Schutz vor Sicherheitslücken. Artikel 13a der neuen Gesetzgebung fordert von den Telekommunikationsbetreibern, Sicherheitsvorfälle zu melden und Sicherheitsmaßnahmen vorzunehmen, um die sichere und ununterbrochene Zustellung von Kommunikationsdiensten über europäische Telekommunikationsnetzwerke zu gewährleisten.

Im Jahr 2010 haben ENISA, die Europäische Kommission (EK) sowie die Ministerien und Regulierungsbehörden für Telekommunikation (NRAs – National Telecom Regulatory Authorities) der Mitgliedsstaaten, mit der Arbeitsaufnahme in der „Art13 Arbeitsgruppe“ begonnen, um Klarheit in die aktuelle Berichterstattung zu bringen und eine konsistente Implementierung des Artikels 13a zu erreichen. Diese Gruppe erzielte bei zwei Richtlinien einen Konsens: **Technische Richtlinie über die Berichterstattung bei Cybersicherheitsvorfällen** und **Technische Richtlinie für [minimale Sicherheitsmaßnahmen](#)**.

„Eine Klarstellung darüber, wie Cybervorfälle gemeldet werden sollten und wie Artikel 13a auf konsistente Weise implementiert werden kann, gibt eine klare Grundlage für den europäischen Telekommunikationsbereich. Dies wird die Barrieren für grenzübergreifend tätige europäische Telekommunikationsanbieter entfernen“, erklärten Dimitra Liveri und Marnix Dekker, die Herausgeber der beiden Dokumente.

„Vorfallberichterstattung und minimale Sicherheitsmaßnahmen sind wichtige Werkzeuge, um Kunden, Unternehmen und Regierungen Vertrauen in die Sicherheit von Telekommunikationsdiensten zu geben. Nach dem jüngsten [Diginotar](#)-Fall gibt es zudem eine wachsende Unterstützung für den Ausbau dieser Art von Gesetzgebung auch über den Telekommunikationssektor hinweg“, erklärte Professor Udo Helmbrecht, Executive Director von ENISA.

Die [Richtlinie für Vorfallberichterstattung](#) unterrichtet NRAs über zwei Arten von Vorfallberichterstattungen, die in Artikel 13a dargelegt werden: dem jährlichen Zusammenfassungsbericht über bedeutende Vorfälle an ENISA und EK sowie Ad-hoc-Berichte über Vorfälle für andere NRAs im Falle grenzübergreifender Vorfälle. Die Richtlinie definiert



13. Dez. 2011

www.enisa.europa.eu

den Rahmen für die Vorfallberichterstattung, die Vorfallparameter und die Grenzwerte. Darüber hinaus enthält es eine Berichtsvorlage für die Übermittlung von Vorfallberichten an ENISA und EK, und es wird erklärt, wie die Berichte von der ENISA verarbeitet werden. Die Richtlinie für Minimale Sicherheitsmaßnahmen berät NRAs über die mindestens vorzunehmenden Sicherheitsmaßnahmen, die Telekommunikationsbetreiber treffen sollten, um die Sicherheit ihrer Netzwerke zu gewährleisten.

Für den vollständigen Bericht:

[Technical Guideline on Incident Reporting](#)

[Technical Guideline on Minimum Security Measures](#)

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

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

