16. Dez. 2011

www.enisa.europa.eu

Schutz des Cyberspace: Erreichen eines effizienten grenzüberschreitenden Informationsaustauschs zwischen „digitalen Feuerwehren“

Die ENISA, die Europaische Agentur für „Cybersicherheit“ hat eine Studie über die rechtlichen und regulatorischen Aspekte des Informationsaustausch und grenzüberschreitender Zusammenarbeit nationaler/staatlicher CERTs (Computer Emergency Response Teams) in Europa veröffentlicht. Der Bericht analysiert, welche Auswirkungen diese Aspekte auf den grenzüberschreitenden Informationsaustausch zwischen den CERTs haben. Das Ergebnis zeigt, dass ein empfindliches Gleichgewicht zwischen Forschung, Verwaltung und Minderung von Computerstörfällen einerseits und der Anerkennung von Rechten und Pflichten, die von bestimmten rechtlichen und regulatorischen Rahmenwerken vorgegeben werden (darunter Bestimmungen zum Schutz von Daten und der Privatsphäre), andererseits besteht.

CERTs sind bei der grenzüberschreitenden Koordination von IT-Vorfällen unerlässlich und um ihre wichtige Rolle ausfüllen zu können, müssen sie Informationen austauschen. Bei grenzübergreifendem Informationsaustausch müssen komplexe gesetzliche Faktoren berücksichtigt werden. CERTs der verschiedenen Länder haben unterschiedliche rechtliche Grundlagen für die Anfrage nach und die Weiterleitung von Informationen an andere Teams. Bei den ausgetauschten Informationen kann es sich außerdem um persönliche Daten handeln, die spezifischen Bestimmungen zum Schutz der Privatsphäre unterliegen. Darüber hinaus haben CERTs, auch nationale/staatliche CERTs, voneinander abweichende Aufträge. Die Studie identifiziert diese rechtlichen und regulatorischen Faktoren und beurteilt, welche Auswirkungen diese auf den grenzüberschreitenden Informationsaustausch zwischen den CERTs haben. Eine Erkenntnis der Untersuchung ist unter anderem, dass der Datenschutz, die Datenspeicherung und die Verpflichtung zur Zusammenarbeit mit Vollstreckungsbehörden, die größten Herausforderungen für eine grenzüberschreitende CERT-Kooperation sind.

Der geschäftsführende Direktor der ENISA, Professor Udo Helmbrecht, dazu:
„CERTs sehen sich konfrontiert mit einem schwierigen Balanceakt zwischen der Erforschung, Verwaltung und Minderung von Störfällen einerseits und dem Schutz von Privatsphäre, Daten und Integrität andererseits. Sicherlich darf grenzüberschreitender Informationsaustausch nicht als Gefahr für die Grundrechte angesehen werden, denn der Austausch ist eine Voraussetzung für effiziente Reaktionen auf Internet-IKT-Vorfälle wie auch für den Schutz gerade dieser Rechte. Mangelhafte Cybersicherheit kann zu einer Unterminierung der Ausübung Ihrer Menschenrechte führen.“

Beispiele für Empfehlungen für mittel- und langfristige Eingriffsmaßnahmen sind unter anderem:

- Verdeutlichung der Unterschiede zwischen den nationalen rechtlichen Rahmenwerken;
- Einführung einer EU-Gesetzgebung, welche die Zuständigkeits- und Tätigkeitsbereiche der nationalen/staatlichen CERTs berücksichtigt;
- Vorgabe eines Grenzbereichs für Störfälle, die eine Reaktion von nationalen/staatlichen CERTs und Informationsaustausch erfordern;
- Erklärungen, warum CERTs persönliche Daten an zuständige Behörden weitergeben müssen, um Klarheit darüber zu schaffen, unter welchen Umständen diese Daten grenzübergreifend ausgetauscht werden müssen;
- Einbeziehung der gesetzlichen Grundlagen bei Informationsanfragen.

VOLLSTÄNDIGER BERICHT

Hintergrund: Mitteilung der Europäischen Kommission über den Schutz kritischer Informationsinfrastrukturen

Ansprechpartner für Interviews: Ulf Bergstrom, Sprecher von ENISA, press@enisa.europa.eu, Handy: + 30-6948-460-143, oder Silva Portesi, Expert CERT-relations Q enisa.europa.eu

http://www.enisa.europa.eu/front-page/media/enisa-auf-deutsch

Übersetzung**. Das Englische Original** ist die einzige maßgebliche Fassung.