

7. Dez. 2011

www.enisa.europa.eu

„Kampf gegen Cyberbedrohungen: Lücken werden geschlossen. EU-Agentur veröffentlicht Bericht über proaktive Erkennung von Störungen der Cybersicherheit, der die "digitale Feuerwehr" effizienter machen soll

Die Agentur gibt heute einen [Bericht](#) heraus, der 16 Mängel bei der Erkennung von Vorfällen in Bezug auf die Netzsicherheit aufdeckt. Wie der Bericht offenbart, werden nicht alle verfügbaren Werkzeuge von der "digitalen Feuerwehr", den Computer Emergency Response Teams (CERTs), in ausreichendem Maß genutzt, um Cyberbedrohungen effizient zu bekämpfen. Die Agentur stellt daher auf europäischem/nationalem Niveau 35 Empfehlungen an Anbieter und Nutzer von Daten zusammen, um die Defizite abzumildern.

Die [Studie](#) ergab, dass die CERTs derzeit nicht alle verfügbaren externen Quellen voll nutzen. Gleichermäßen sammeln viele CERTs weder Daten über entsprechende Vorfälle, noch teilen sie diese mit anderen CERTs. Das ist besorgniserregend, denn der Informationsaustausch ist der Schlüssel für eine effektive Bekämpfung von Schadsoftware und schädlichen Aktivitäten - besonders wichtig beim länderübergreifenden Kampf gegen Cyberbedrohungen.

Mängel. Die 16 Mängel bei der Aufdeckung von Vorfällen werden im Bericht gründlich analysiert. Zu den größten technischen Lücken gehören ungenügende Datensicherheit (Falschmeldungen bei den gelieferten Daten, mangelnde Lieferpünktlichkeit) sowie fehlende Standardformate, -werkzeuge, -ressourcen und -fähigkeiten. Das bedeutendste rechtliche Problem beinhaltet Datenschutzgesetze, die den Informationsaustausch erschweren.

"CERT-Manager der jeweiligen Regierungen sollten den Bericht dazu nutzen, die aufgedeckten Mängel zu beseitigen, indem sie mehr externe Quellen zur Information über Vorfälle und zusätzliche Werkzeuge zur Informationssammlung nutzen, um die Lücken zu schließen," so [Professor Udo Helmbrecht](#), Geschäftsführender Direktor von ENISA.

35 Empfehlungen, welche die Defizite entschärfen sollen. Für Datenanbieter konzentrieren sich die wichtigsten Empfehlungen darauf, wie man die CERTs besser erreichen kann, sowie auf bessere Datenformate, auf besseren Datenversand und auf eine Verbesserung der Datenqualität. Für Datenverbraucher werden zusätzliche Aktivitäten von CERTs empfohlen, um die Qualität der Dateneingabe zu verifizieren, sowie die spezifische Anwendung neuer Technologien. Auf europäischer oder nationaler Ebene sind schließlich eine Balance zwischen Datenschutz und



7. Dez. 2011

www.enisa.europa.eu

Datensicherheit sowie die Bereitstellung von gemeinsamen Formaten, Möglichkeiten zur Integration statistischer Vorfallmeldungen und eine Erforschung von Datenverlusten erforderlich.

Hintergrund: Proaktive Erkennung von Vorfällen ist die Aufdeckung von schädlicher oder böswilliger Aktivität noch ehe Beschwerden oder Schadensberichte eingehen. Als solches ist sie der Eckpfeiler für das Portfolio effizienter CERT-Dienste. Sie kann die Effizienz der Aktivitäten von CERTs enorm verbessern und so [ihre Fähigkeiten im Umgang mit Vorfällen stärken - einen der Basisdienste von nationalen und staatlichen CERTs](#).

[Vollständiger Bericht](#)

Hintergrund: [Digital Agenda for Europe, Aktion 38](#)

Ansprechpartner für Interviews: Ulf Bergstrom, Sprecher von ENISA, press@enisa.europa.eu, Handy: +30-6948-460-143 oder Agris Belasovs oder Andrea Dufkova, CERT-Relations@enisa.europa.eu

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

Übersetzung. Das Englische Original ist die einzige maßgebliche Fassung.

