Die Europäische Agentur ENISA gibt Abschlussbericht und Videoclip über „Cyber Europe 2010“, die erste europaweite Übung zur Internetsicherheit für öffentliche Stellen, heraus

Die europäische Agentur für Netz- und Informationssicherheit, ENISA, hat ihren Abschlussbericht über die erste europaweite Übung zur Internetsicherheit für öffentliche Stellen, „Cyber Europe 2010“, herausgebracht. Der Bericht unterstreicht die Notwendigkeit für mehr Übungen zur Internetsicherheit in der Zukunft, verstärkte Zusammenarbeit zwischen den Mitgliedsstaaten sowie die Bedeutung des Privatsektors in der Gewährleistung der IT-Sicherheit. ENISA hat zur Unterstützung des Berichts außerdem einen Online-Videoclip veröffentlicht.

Die Unterstützung von europaweiten Übungen zur Internetsicherheitsbereitschaft ist für die EU innerhalb ihrer „Digitalen Agenda für Europa“ eine Priorität und soll gewährleisten, dass Unternehmen und Bürger geschützt sind, wenn sie online sind.

Die Übung „Cyber Europe 2010“ wurde am 4. November 2010 durchgeführt. Ihr Ziel war die Förderung von Kommunikation und Zusammenarbeit zwischen den Ländern im Fall von groß angelegten Cyberattacken. Mehr als 70 Fachleute aus teilnehmenden öffentlichen Einrichtungen arbeiteten zusammen, um mehr als 300 simulierte Hackerattacken abzuwehren, die darauf ausgelegt waren, das Internet und kritische Onlinedienste in ganz Europa lahm zu legen. Während der Übung fand ein simulierter Verlust der Internetanbindung zwischen den Ländern statt, der zur Vermeidung eines (simulierten) totalen Netzwerkzusammenbruches eine grenzübergreifende Zusammenarbeit erforderlich machte.

Die Auswertung der Übung fand auf drei Ebenen statt:
1. National
2. Europaweit und
3. Gesamt.

Die wichtigsten Erkenntnisse des Berichts umfassen Folgendes:
- Die IT-Einrichtungen der Mitgliedsstaaten kommunizieren auf vielfältigste Weise. Die Harmonisierung von Standard-Betriebsverfahren würde zu einer sichereren und effizienteren Kommunikation zwischen ihnen führen.
- Die Fähigkeit der Teilnehmer, die relevanten Kontaktstellen innerhalb von Organisationen zu finden, variierte. Im Falle einer wirklichen Krise haben rund 55% der Länder kein Vertrauen darin, den richtigen Kontakt schnell genug auszumachen, selbst dann, wenn ein Verzeichnis erhältlich ist.
- Die Teilnehmer waren in gleich großem Ausmaß geteilter Meinung darüber, ob ein „Single Point of Contact“ (Einzige Kontaktstelle) oder „Multiple Points of Contact“ (Mehrere Kontaktstellen) besser wären. Eine einzige Kontaktstelle wäre einfacher; jedoch gibt es heute realistischerweise mehrere Kontaktstellen.
Mit mehreren Kontaktstellen vermeidet man auch eine einzige Fehlerquelle.

Die Hauptempfehlungen des Berichts umfassen Folgendes:
- Europa sollte weiterhin Übungen zum Infrastrukturschutz kritischer Informationen (CIIP) abhalten: 86% der Teilnehmer fanden den Probelauf entweder „sehr“ oder „extrem“ nützlich.
- Der Privatsektor kann zur Wertsteigerung zukünftiger Übungen beitragen, indem er die Authentizität erhöht.
- Die Lehren, die aus der Übung gezogen werden können, sollten mit denjenigen ausgetauscht werden, die andere Übungen (auf nationaler oder internationaler Ebene) veranstalten.
- Mitgliedsstaaten sollten sich intern gut organisieren, indem sie zum Beispiel nationale Kontingenzpläne und -übungen entwickeln und testen. Europäische Länder sind auf nationaler Ebene auf vielfältige Weisen organisiert. In Anbetracht der Unterschiede hinsichtlich Strukturen und Verfahren ist es wesentlich, dass man weiß, wen man kontaktieren sollte.

Der Dialog über die Notwendigkeit einer einzigen Kontaktstelle oder mehrerer Kontaktstellen auf EU-Ebene sollte weitergeführt werden, und ENISA kann der Vermittler dieses Dialogs sein.

- Es sollte ein Strategieplan für europaweite Übungen erstellt werden. Dieser würde eine Definition von Standardverfahren und -strukturen für groß angelegte Ereignisse beinhalten

„Der Cyber-Europe-Bericht identifiziert Art und Weisen, wie unsere wirtschaftlichen und gesellschaftlichen Aktivitäten sicherer gestaltet werden können. ENISA verpflichtet sich zur Unterstützung von europäischen Übungen, Verfahren und Plänen zum Schutz der Infastruktur der Informationskommunikationstechnologie, von der wir alle zunehmend abhängiger werden“, sagte Prof. Udo Helmbrecht, Geschäftsfuhrender Direktor der ENISA.

Ein **Videoclip** zum Thema „Cyber Europe 2010“ ist hier erhältlich).

Hintergrundinformation:

Aktionsplan zum Infrastrukturschutz kritischer Informationen (Critical Information Infrastructure Protection, CIIP)
Digitale Agenda
sowie die kürzliche Mitteilung bezüglich CIIP vom 30.03.2011

Für den **gesamten Bericht**.

Für Interviews oder weitere Informationen: Ulf Bergstrom, Pressesprecher, ENISA, press@enisa.europa.eu, Handy: +30-6948-460-143, oder Panagiotis Trimintzios, Experte, ENISA, panagiotis.trimintzios Q enisa.europa.eu.

Übersetzung. Das Englische Original bleibt die maßgebliche Fassung.