IP/10/1459

Brüssel, den 4. November 2010

Digitale Agenda: Experten für Netzsicherheit erproben Abwehrfähigkeit bei erster gesamteuropäischer Simulation

Die europäischen Experten für Netzsicherheit testen heute ihre Abwehrmechanismen in der ersten gesamteuropäischen Simulation von Cyberangriffen. Bei „Cyber Europe 2010" werden die Experten versuchen, simulierte Angriffe von Hackern auf kritische Online-Dienste in mehreren EU-Mitgliedstaaten abzuwehren. Das Szenario der Simulation sieht vor, dass die Internetverbindungen zwischen den beteiligten europäischen Ländern schrittweise ausfallen oder erheblich eingeschränkt werden, so dass Bürger, Unternehmen und öffentliche Einrichtungen am Zugang zu wesentlichen Online-Diensten gehindert werden. Bei der Übung müssen die Mitgliedstaaten zusammenarbeiten, um einen simulierten Totalzusammenbruch des Netzes zu verhindern. Die Übung wird von EU-Mitgliedstaaten mit Unterstützung der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) und der Gemeinsamen Forschungsstelle (JRC) veranstaltet. Nach der heutigen Übung sollen weitere und noch komplexere Szenarien folgen, die allmählich von der europäischen auf die globale Ebene übergehen. Die Unterstützung EU-weiter Einsatzübungen zur Cybersicherheit ist eine der Maßnahmen, die in der Digitalen Agenda für Europa zur Stärkung von Vertrauen und Sicherheit im Netz vorgesehen sind (siehe IP/10/581, MEMO/10/199 und MEMO/10/200.

Neelie Kroes, Vizepräsidentin der Europäischen Kommission und zuständig für die Digitale Agenda, wird das britische Cyber-Abwehrzentrum während der Simulation besuchen. Sie sagte in diesem Zusammenhang: „Diese Übung zur Prüfung der Abwehrbereitschaft Europas gegen Cyber-Bedrohungen ist ein wichtiger Schritt zum Aufbau einer Zusammenarbeit bei der Bekämpfung von Bedrohungen für wichtige Infrastrukturen im Netz, damit sich Bürger und Unternehmen im Netz sicher fühlen."

Im Rahmen der heutigen Simulation „Cyber Europe 2010" werden Experten in ganz Europa ihre Reaktionsfähigkeiten bei einem simulierten Hackerangriff auf kritische Online-Dienste testen. Im Szenario der Übung ist vorgesehen, dass Internetverbindungen zwischen europäischen Ländern schrittweise ausfallen oder erheblich eingeschränkt werden und dass im schlimmsten Fall tatsächlich alle wesentlichen länderübergreifenden Verbindungen in Europa stillliegen.

In der Simulation wären Bürger, Unternehmen und öffentliche Einrichtungen am Zugang zu kritischen Online-Diensten (z. B. *e*-Government) gehindert, wenn es nicht gelingt, den Verkehr aus den beeinträchtigten Verbindungen umzuleiten. Die Übung basiert auf einem Szenario, bei dem im Laufe eines Tages ein Land nach dem anderen mit immer größeren Zugangsproblemen zu kämpfen hat. Alle teilnehmenden Mitgliedstaaten müssen zusammenarbeiten, um eine gemeinsame Lösung für die fiktive Krise zu finden.

Diese Übung zur Netzsicherheit soll die Fähigkeit der Mitgliedstaaten im Umgang mit solchen Störungen des Netzes verbessern und die Kommunikationsverbindungen und -verfahren für den Fall einer echten massiven Bedrohung des Netzes auf die Probe stellen. Bei der Übung soll getestet werden, inwiefern die Kontaktstellen in den teilnehmenden Ländern, die Kommunikationskanäle und die Art der übertragenen Daten den Anforderungen entsprechen und wie gut die Mitgliedstaaten über Rolle und Funktionen ihrer Partner in den anderen Mitgliedstaaten unterrichtet sind.

Die Übung zur Netzsicherheit wurde von den EU-Mitgliedstaaten in Abstimmung mit der Europäischen Agentur für Netz- und Informationssicherheit (ENISA) und mit Unterstützung der Gemeinsamen Forschungsstelle der Europäischen Kommission geplant. Alle EU-Mitgliedstaaten sowie Island, Norwegen und die Schweiz werden aktiv oder als Beobachter teilnehmen. Abhängig von ihren jeweiligen Strukturen sind auch verschiedene Behörden der Mitgliedstaaten beteiligt, z. B. Kommunikationsministerien, Behörden für den Schutz kritischer Informationsinfrastrukturen, Krisenmanagementorgane, nationale Computersicherheits-Einsatzdienste (CSIRT), nationale Behörden für Informationssicherheit sowie Sicherheits- und Nachrichtendienste.

Hintergrund

Die ENISA wurde 2004 eingerichtet. Am 30. September 2010 schlug die Kommission eine Stärkung und Modernisierung der ENISA vor, um die EU, die Mitgliedstaaten und private Interessenträger beim Ausbau ihrer Fähigkeiten und ihrer Bereitschaft zur Verhinderung, Erkennung und Abwehr von Angriffen auf die Netzsicherheit zu unterstützen (siehe IP/10/1239, MEMO/10/459).

Am 30. September 2010 legte die Kommission außerdem einen Vorschlag für eine Richtlinie vor, die es ermöglichen soll, die Urheber von Angriffen auf die Netzsicherheit und die Hersteller entsprechender Schadsoftware zu verfolgen und härtere strafrechtliche Sanktionen gegen sie zu verhängen. Darüber hinaus wären die Mitgliedstaaten verpflichtet, im Falle von Cyberangriffen schnell auf dringende Hilfeersuchen zu reagieren, wodurch die justizielle und polizeiliche Zusammenarbeit in Europa in diesem Bereich an Wirksamkeit gewinnen würde (siehe MEMO/10/463).