# Bisher größte Übung zur Cyber-Sicherheit in Europa

@Enisa_EU #CyberSecurity #CyberEurope2014

Aus 29 europäischen Staaten kommen heute mehr als 200 Organisationen und 400 Experten zum Thema Cyber-Sicherheit zusammen, um Maßnahmen zur digitalen Gefahrenabwehr zu simulieren. Cyber Europe 2014 ist eine eintägige Übung, die von der Europäischen Agentur für Netzwerk- und Informationssicherheit (ENISA) organisiert wurde. Unter den Teilnehmern sind neben verschiedenen Internetsicherheitsfirmen und nationalen CERT-Teams (Computer Emergency Response Teams) auch Ministerien, Energieversorger, Finanzinstitute sowie Internet Service-Provider. Bei der eintägigen Simulation testen sie ihre bisher ergriffenen Maßnahmen und Verfahren zur Abwendung von großangelegten Cyber-Angriffen.

#CyberEurope2014 ist die größte und umfassendste Übung dieser Art in Europa. Mehr als 2000 unterschiedliche IT-Sicherheits-Szenarien werden hierbei simuliert, darunter der Datenklau von sensiblen Informationen, Attacken auf die Verfügbarkeit von Internetdiensten, Angriffe auf das Design von Webseiten und Cyber-Angriffe auf wichtige Infrastruktureinrichtungen wie Energie- und Telekommunikationsnetzwerke. Die Simulation findet in verschieden Übungszentren in ganz Europa statt und wird von einem zentralen Kontrollzentrum koordiniert.

Die Vize-Präsidentin der Europäischen Kommission @NeelieKroesEU sagte: „Die Zahl und Komplexität von Cyber-Attacken steigt täglich. Dieses Problem kann nicht von einem einzelnen Nationalstaat oder wenigen zusammenarbeitenden Staaten gelöst werden. Ich bin froh, dass die EU, die Institutionen der EU und die EFTA-Mitgliedsstaaten mit der Europäischen Agentur für Netz- und Informationssicherheit zusammenarbeiten. Nur diese Zusammenarbeit wird langfristig unsere heutige Gesellschaft und Wirtschaft schützen."

Der Geschäftsführende Direktor von ENISA, Prof. Udo Helmbrecht, über die bisherigen Fortschritte: „Vor fünf Jahren gab es noch keine Strategie für die Koordination der Zusammenarbeit der EU-Mitgliedsstaaten im Falle eines Cyber-Angriffes. Heute sind wir über die geschaffenen Rahmenbedingungen in der Lage einen möglichen Angriff auf europäischer Ebene einzudämmen. Die heutige Übung wird uns zeigen wo wir stehen und welche nächsten Schritte ergriffen werden müssen, um eine Verbesserung zu erreichen".

Ferner soll mit den #CyberEurope2014 Simulationen folgendes erreicht werden: Die Überprüfung der Strategie zum Austausch operationaler Informationen über Internetsicherheitskrisen in Europa, die Verbesserung nationaler Fähigkeiten zur Bewältigung von Cyber-Krisen, die Erforschung des parallelen Informationsaustausches zwischen privaten und öffentlichen, privaten und privaten sowie nationalen und internationalen Ebenen. Außerdem sollen Richtlinien zum Management von multinationalen Cyper-Krisen - die sogenannten EU-Standard Operational Procedures (EU-SOPs)- getestet werden.

## Hintergrund

Dem ENISA Threat Landscape report (2013) zufolge, haben die Hacker die Effektivität ihrer Attacken verbessert. Von diesen Entwicklungen sind alle Länder betroffen. Zahlreiche Hacker haben Wissen und Fähigkeiten entwickelt, die nun dazu benutzt werden können alle Arten von Zielen, egal ob staatliche oder private, zu unterwandern.

Im Jahr 2013 stieg die Zahl der Internet-basierten Angriffe weltweit um fast ein Viertel und die Gesamtzahl der Datenschutzverletzungen lag 61 Prozent höher als noch im Jahr zuvor. Diese Datenschutzverletzungen führten zum Verlust von zig Millionen Datensätzen und mehr als 552 Millionen ungeschützten Identitäten. Wirtschaftsschätzungen zufolge kosteten Spionage und Cyber-Attacken im Jahr 2013 weltweit zwischen 300 Milliarden und einer Billion Dollar.

## Cyber Europe 2014

Die Tests sollen zeigen, wie große Krisen auf die wichtigen Informationsinfrastrukturen wirken. Später werden die Ergebnisse dieser Übung von den ENISA-Experten in einem Report veröffentlicht.

#CyberEurope2014 wird alle zwei Jahre von ENISA organisiert. Dieses Jahr nehmen neben 26 EU-Mitgliedsstaaten auch drei EFTA Staaten und die Institutionen der Europäischen Union teil. Die Tests finden in drei Phasen über das ganze Jahr verteilt statt: Die Technische Phase beinhaltet das Erfassen von Störungen, die Untersuchung, die Schadensbegrenzung und den Informationsaustausch (im April beendet). Die operationale und taktische Phase, welche heute beginnt und bis ins Frühjahr 2015 andauert, umfasst die Analyse des Krisenmanagements, der Kooperation und Koordination, sowie der Beratung und des Informationsaustauschs. In der letzten Phase, der strategischen Phase, werden die getroffenen Entscheidungen, der politische Einfluss und öffentliche Angelegenheiten näher untersucht. Diese Übung wirkt sich nicht auf wichtige Infrastruktureinrichtungen, Systeme oder deren Dienste aus.

In punkto Cyber-Sicherheitstrategie für die EU und der geplanten Richtlinie für eine gleichmäßig hohe Netz- und Informationssicherheit (NIS) fordert die Europäische Kommission die Entwicklung von nationalen Krisenplänen und regelmäßige Übungen, welche die Sicherheit von großen Netzwerken, die Reaktion auf den Störfall und die Notfallwiederherstellung testen sollen. ENISAs neues Mandat zeigt wie wichtig solche Übungen für das Vertrauen in Online-Dienste in Europa sind. Die EU-SOPs wurden in den letzten drei Jahren getestet, auch während der CE2012.

## Useful links

Cyber security in the Digital Agenda

ENISA's Cyber Crisis Exercises

ENISA's briefing pack on CE2014

Press Release CE2014 Technical Level Exercise: TLEx

Neelie Kroes - Follow Neelie on Twitter

Contacts

Email: comm-kroes@ec.europa.eu, c3e@enisa.europa.eu
Tel: +32.229.57361 Twitter: @RyanHeathEU, @enisa_eu