Gemeinsam stärker: ENISA veröffentlicht „Cyber Europe 2014 After Action Report“

Heute veröffentlicht ENISA die öffentliche Version des „After Action Report” zu der paneuropäischen Cybersicherheitsübung „Cyber Europe 2014“ (CE2014). Dieser Bericht, der von den Mitgliedstaaten genehmigt wurde, gibt einen generellen Überblick über die komplexe Cybersicherheitsübung, die 2014 durchgeführt wurde.

Das Hauptziel von „Cyber Europe 2014” war es, den Mitgliedstaaten eine Kooperationsübung für den Fall einer Cyber-Krise zu ermöglichen. Die in drei Phasen aufgeteilte Übung bot Möglichkeiten zur Bewertung der Effektivität der Kooperations- und Eskalationsprozesse bei grenzübergreifenden Cyber-Störfällen, die die Sicherheit von wesentlichen Dienstleistungen und Infrastruktur beeinträchtigen, während gleichzeitig die einzelstaatlichen Kapazitäten und Krisenpläne für Organisationen sowohl aus dem öffentlichen als auch dem Privatsektor getestet wurden.

Die Übung, die von ENISA alle zwei Jahre organisiert wird, wurde gemeinsam mit Vertretern aus den teilnehmenden Ländern geplant und erforderte sechs (6) Planungskonferenzen in ganz Europa. Diese Übung, die über **1500 Teilnehmer** aus **29 EU und EFTA-Mitgliedstaaten** zusammenbrachte, deckte **zum ersten Mal alle drei (3) Phasen** der Cyber-Vorfallsreaktion ab – die **technische**, die **operative** sowie die **strategische** – von denen sich jede in die nächste Phase ausweitet und folgendes beinhaltet:

- Phase 1 – Technisches Level (28.-30. April 2014, **49 Stunden**): Störungserfassung, Analyse und Schadensminderung, Informationsaustausch.
- Phase 2 – Operatives Level (30. Oktober 2014, **10 Stunden**): Warnung, Kooperation, kurzfristige Krisenbewältigung, Entwicklung eines gemeinsamen Lagebildes.
- Phase 3 – Strategisches Level – **zum ersten Mal getestet** – (25. Februar 2015): Entscheidungsfindung basierend auf dem gemeinsamen Lagebild, hochrangige Politikdebatten zur langfristigen strategischen Krisenbewältigung.

Der Bericht zeigt, dass die gemeinsame Fähigkeit zur Bewältigung großräumiger Cybersicherheitsvorfälle in Europa seit 2010, als die erste „Cyber Europe”-Übung durchgeführt wurde, erhebliche Fortschritte gemacht hat. Der Austausch von Echtzeitinformationen zwischen den Ländern erwies sich als wertvoll für rasche Entscheidungsverfahren. Die **EU-Standardarbeitsverfahren** (EU-SOPs), die zur Unterstützung dieser Kooperationsaktivitäten genutzt werden, stellen den Mitgliedstaaten Leitlinien zur Verfügung, von denen diese im Falle von großräumigen Cybersicherheitsvorfällen Gebrauch machen können. Diese werden unter Berücksichtigung des sich entwickelnden Kontextes der Cyber-Sicherheitspolitik in Europa stetig weiter verbessert.

Die Kooperation wurde als Schlüsselelement hervorgehoben, welches einen Beitrag zu einem erhöhten Verständnis, Vertrauensbildung und einer schnelleren Reaktion leistet. Die **Cyber-Übungsplattform (CEP)**, die von ENISA für die Planung, Durchführung und Auswertung von Übungen entwickelt wurde, erwies sich als starkes Instrument. Das CEP wird zurzeit von ENISA weiterentwickelt, um in Zukunft Cyber-Übungen auszurichten und technische Lösungen zu präsentieren. Achtundneunzig Prozent (**98%**) der Teilnehmer der technischen Phase signalisierten Interesse an einer Teilnahme bei der nächsten Übung.

ENISAs Geschäftsführer Udo Helmbrecht *sagte: „Die Lektionen, die aus Cyber Europe 2014 gezogen wurden, sind zahlreich und liefern uns die Grundlage für bahnbrechende Arbeit im Bereich der Zusammenarbeit bei Cyber-Krisen, einem sich entwickelnden Feld, in dem die EU und ENISA führend sind. Wir verpflichten uns, den Aktionsplan mit Unterstützung der Mitgliedstaaten zu implementieren, um die Cyber-Krisenvorsorge auf nationaler sowie auf EU-Ebene weiter zu verbessern.“*

Das Szenario

Das Szenario für „Cyber Europe 2014" bezog sich auf einen ordnungspolitischen Vorschlag der EU, bei dem es um Energieressourcen ging. Während der technischen Phase der Übung mussten sich die Mitgliedstaaten und die EU-Institutionen mit **Cyber-Störfällen** wie dem **Herausschleusen von Informationen**, Open Source Intelligence, **Malware**-Analyse von Mobiltelefonen, **Denial-Of-Service-Angriffen**, und **Advanced Persistent Threats** auseinandersetzen. Die operative Phase von „Cyber Europe 2014" schloss sich mit einer Eskalation der Lage an, die zu einer Serie von **großräumigen Cyber-Angriffen** auf mehrere kritische Infrastrukturen und zahlreiche Online-Dienstleistungen führte. Schließlich verschärfte die strategische Phase von „Cyber Europe 2014" die Krise weiterhin, durch die massive Beeinträchtigung verschiedener Energieinfrastrukturen mitten im kalten Winter, den Bruch kritischer Schlüsseltechnologien, sowie eine zunehmend besorgte öffentliche Meinung.

Den Bericht in voller Länge finden Sie hier

Für einen schnellen Blick auf „Cyber Europe" schauen Sie sich folgendes Video von ENISA an:

https://www.enisa.europa.eu/media/news-items/preparing-for-the-unknown-a-peek-into-cyber-europe

Für Interviews und Presseanfragen:

Bitte kontaktieren Sie **Cyber Crisis Cooperation**: c3@enisa.europa.eu