ST. PÖLTEN UNIVERSITY
OF APPLIED SCIENCES

/computer science
& security

/fh///
st.pölten

IRIS24 Cybersicherheit

Cyber-Übungen auf europäischer Ebene

Tímea Páhi

23.05.24

Cyber Exercises

Definitions

- **Cyber Exercises** sind organisierte Aktivitäten, bei denen simulierte Cybervorfälle genutzt werden, um die Reaktionsfähigkeiten, Prozesse und Zusammenarbeit von Organisationen zu testen und zu verbessern.
- **Cyber Ranges** sind interaktive und simulierte Plattformen, die Netzwerke, Systeme, Werkzeuge und Anwendungen nachbilden. NATO CR ist eine Plattform und ein Datenzentrum, das es der NATO ermöglicht, ihre größten Cyberverteidigungsübungen und -ausbildungen durchzuführen, wie die Cyber Coalition und die Coalition Warrior Interoperability Exercise (CWIX).

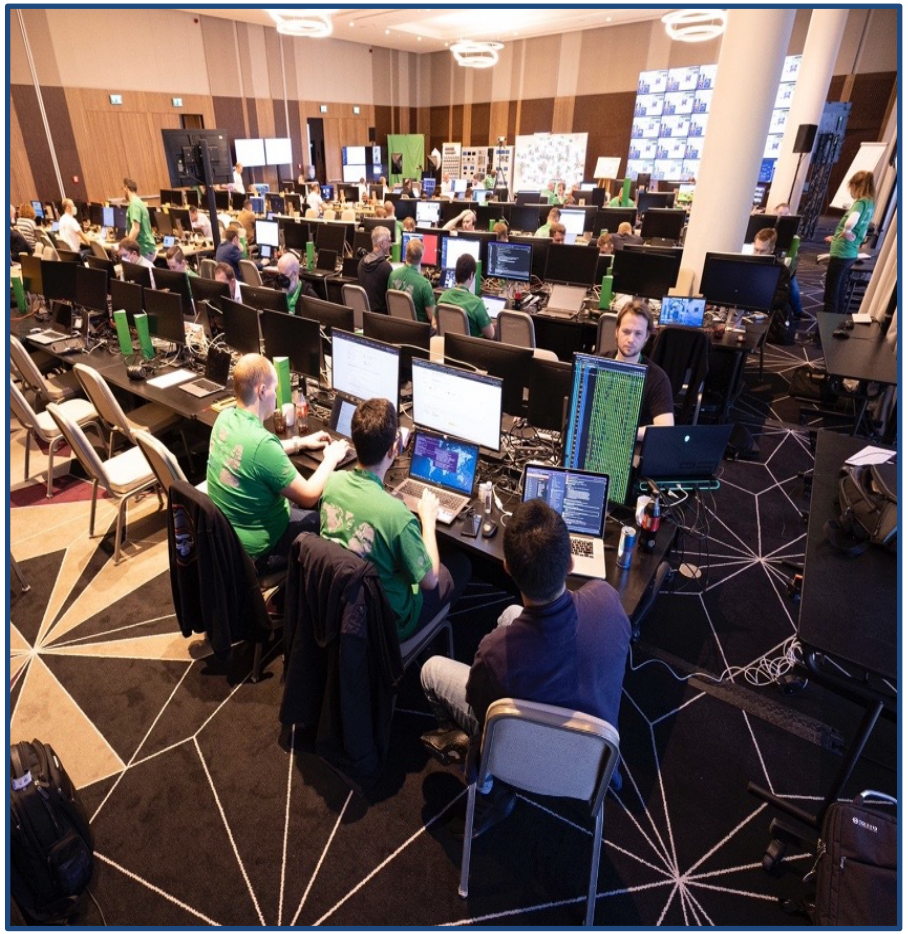
Ziele und Vorteile:

- **Bewertung der Bereitschaft:** Überprüfung der Fähigkeit zur schnellen und effektiven Reaktion auf Cybervorfälle.
- **Identifikation von Schwachstellen:** Aufdeckung von Sicherheitslücken in Netzwerken, Systemen und Prozessen.
- **Verbesserung der Zusammenarbeit:** Förderung der Koordination und Kommunikation zwischen verschiedenen Abteilungen und externen Partnern.
- **Schulung und Sensibilisierung:** Praxisnahe Schulung von Mitarbeitern im Umgang mit Cyberbedrohungen.

Cyber Exercises

Typen von Cyber Exercises:

- **Tabletop-Übungen:** Szenariobasierte Diskussionen, bei denen theoretische Reaktionen auf Cybervorfälle analysiert werden. Kein Einsatz realer Systeme.
- **Live-Fire-Übungen (Read-Blue-Purple Team Übungen):** Realistische Simulationen mit echten Angriffen auf isolierte Systeme, um praktische Reaktionsfähigkeiten zu testen.
- **Hybrid-Übungen:** Kombination aus theoretischen Diskussionen und praktischen Simulationen, um umfassende Tests und Schulungen zu ermöglichen.
- And many more!



ENISA Cyber Europe

Organisator: Europäische Agentur für Netz- und Informationssicherheit (ENISA)

Ziel: Verbesserung der Koordination und Zusammenarbeit zwischen EU-Mitgliedstaaten bei der Reaktion auf groß angelegte Cyberangriffe.

Umfang: Beteiligung zahlreicher öffentlicher und privater Organisationen aus verschiedenen Sektoren, um realistische Bedrohungsszenarien zu simulieren.

Häufigkeit: Alle zwei Jahre. Cyberangriffe auf Energie- und Rohstoffinfrastrukturen nehmen seit 2017 zu, wobei die Zahl der Angriffe im Jahr 2022 einen Rekordwert erreicht hat. Cyber Europe 2024 wird die 7. Ausgabe dieser europaweiten Übungsreihe sein und im Juni 2024 stattfinden.

ENISA Cyber Europe

CYBER EUROPE 2024

POWERED BY ENISA

NATO Cyber Coalition

Organisator: NATO

Ziel: Verbesserung der Cybersicherheitsfähigkeiten und der operativen Zusammenarbeit zwischen NATO-Mitgliedstaaten und Partnern.

Umfang: Simulation komplexer Cyberangriffe und koordiniertes Vorgehen zur Verteidigung von Netzwerken.

Häufigkeit: Jährlich.

Die Cyber Coalition ist das Flaggschiff der jährlichen kollektiven Cyberverteidigungsübung der NATO und eine der größten der Welt. Sie wird vom Alliierten Kommando für Fragen der Umgestaltung unter der Leitung des Militärausschusses geplant und durchgeführt. Die Übung der Cyber-Koalition wird vom Estnischen Zentrum für Cybersicherheitsübungen und -ausbildung (CR14) durchgeführt, dem neuesten Cyber-Bereich in Tallinn zur Unterstützung der NATO-Verbündeten und Partner.

NATO Locked Shield

Organisator: NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE)

Ziel: Test und Verbesserung der Fähigkeiten von Cyberverteidigungsteams in einer realistischen und intensiven Umgebung.

Umfang: Teilnahme von Teams aus der ganzen Welt, die in Echtzeit auf simulierte Angriffe reagieren müssen.

Häufigkeit: Jährlich.

Locked Shields 2024, die weltweit größte Live-Feuer-Übung zur Cyberverteidigung, steht kurz bevor und unterstreicht das Engagement der globalen Gemeinschaft im Kampf gegen Cyberbedrohungen. Diese einzigartige jährliche Übung, die vom NATO Cooperative Cyber Defence Centre of Excellence (CCDCOE) organisiert wird, geht über herkömmliche Cyber-Übungen hinaus, indem sie Experten aus verschiedenen Disziplinen einbezieht, um die Vielschichtigkeit von Cyber-Bedrohungen zu bewältigen. In diesem Jahr werden etwa 4000 Experten aus mehr als 40 Ländern während Locked Shields in einer simulierten Umgebung zusammenarbeiten, um die Infrastruktur einer fiktiven Nation und eines fiktiven Landes zu schützen.

CCDCOE
Cooperative Cyber Defence Centre of Excellence
Tallinn, Estonia

LOCKED SHIELDS 2024

CISA Cyber Storm

Organisator: US-Behörde für Cybersicherheit und Infrastruktursicherheit (CISA)

Ziel: Bewertung und Verbesserung der nationalen Reaktionsfähigkeit auf groß angelegte Cybervorfälle.

Umfang: Beteiligung von Regierungsbehörden, Privatsektor und internationalen Partnern.

Häufigkeit: Alle zwei Jahre.

Cyber Storm IX: April 2024: Die CISA veranstaltete im April 2024 die neunte Auflage der nationalen Cyber-Übung Cyber Storm IX. Über 2.200 Teilnehmer aus aller Welt überprüften ihre Cyber-Resilienz und Koordinationsmechanismen als Reaktion auf einen verteilten Angriff auf die Cloud-Ressourcen von Organisationen. Zu den Reaktions- und Wiederherstellungsmaßnahmen gehörten die interne Zusammenarbeit, die Koordinierung mit der Reaktion auf einen Vorfall und mit Cloud-Anbietern, öffentliche Nachrichtenübermittlung und die Berichterstattung auf Bundesebene.

Andere Cyber Übungen

LÜKEX

Cyber Übungen und das Recht

NIS2-Richtlinie:

- **Überblick:** Aktualisierung der ursprünglichen NIS-Richtlinie (Network and Information Security Directive) durch die EU im Jahr 2022.
- **Ziel:** Stärkung der Cybersicherheit und der Resilienz kritischer Infrastrukturen in der EU.

Anforderungen der NIS2:

- **Sicherheitsmaßnahmen:** Unternehmen und Organisationen in bestimmten Sektoren müssen robuste Sicherheitsmaßnahmen implementieren.
- **Meldepflicht:** Verpflichtung zur Meldung von erheblichen Cybervorfällen an nationale Behörden.
- **Cyber Exercises:** Regelmäßige Durchführung von Cyber Exercises zur Bewertung und Verbesserung der Sicherheitsmaßnahmen.
- **Verantwortlichkeit der Geschäftsführung:** Geschäftsführungen sind verpflichtet, sicherzustellen, dass ihre Organisationen die NIS2-Anforderungen erfüllen, einschließlich der regelmäßigen Teilnahme an Cyber Exercises.

Call to Actions

- **Regelmäßige Teilnahme:** Organisationen sollten regelmäßig an Cyber Exercises teilnehmen, um ihre Fähigkeiten zu testen und zu verbessern.
- **Zusammenarbeit:** Enge Zusammenarbeit mit nationalen und internationalen Cybersicherheitsbehörden zur Optimierung der Sicherheitsstrategien.
- **Schulung und Weiterbildung:** Kontinuierliche Schulung und Sensibilisierung der Mitarbeiter für aktuelle Bedrohungen und Reaktionsstrategien.
- **Juristische Beratung:** Sicherstellen, dass alle rechtlichen Verpflichtungen im Zusammenhang mit der NIS2-Richtlinie erfüllt werden, um rechtliche Konsequenzen zu vermeiden.
- **Dokumentation und Reporting:** Sorgfältige Dokumentation aller durchgeführten Cyber Exercises und der daraus gezogenen Erkenntnisse zur Nachweisführung gegenüber Aufsichtsbehörden.