CCS
Cyber Conflict Simulator

Supervision Case Study

Croatian Financial Services Supervisory Agency (HANFA)
DORA - Testing Digital Operational Resilience of Supervised

The Problem

In preparation for the implementation of **The Digital Operational Resilience Act (DORA) –** Regulation (EU) 2022/2554, Croatian Financial Services Supervisory Agency (HANFA) responsible for supervision and regulation of the Croatian non-banking financial market aimed to:

- **Raise awareness** about the importance of establishing robust incident response management processes in **compliance with DORA**.
- **Evaluate the maturity** of these processes and assess the readiness of supervised entities to respond effectively to cyber incidents.

DORA and its accompanying regulatory technical standards (RTS) mandate the development of policies and ICT incident management processes, including the creation and testing of response and recovery plans for cyberattacks and other relevant scenarios.

To achieve these objectives, HANFA conducted a **digital operational resilience test** using a pre-defined scenario method. Eleven supervised entities from the non-banking financial market participated. The goal of the exercise was to simulate a cyber incident, resolve it up to the recovery stage, and submit a **major incident intermediate report**.

Key Challenges:

- Designing a scenario adaptable to organizations with vastly different business models.
- Coordinating simultaneous communication with eleven entities during exercise.
- Collecting and analyzing real-time data through reliable communication channels.

The Solution

To address these challenges, HANFA utilized the capabilities of the **Cyber Conflict Simulator (CCS)** to model the cyber incident scenario affecting the usual ICT infrastructure, business services, and operational environments of the eleven supervised entities.

Key Features of the Solution:

- **Simultaneous Management**: The CCS allowed centralized control of events, messages, and injects across all participant organizations.
- **Custom Interfaces**: Each entity accessed a dedicated graphic interface tailored to their specific scenario, providing real-time information to their incident response teams and HANFA.
- **Real-Time Monitoring**: HANFA team monitored each organization's progress, issuing guidance or requests for additional information through the CCS communication module.

Scenario Overview:

A **supply chain attack** was simulated, involving the compromise of a solution provider for a business-critical application. This led to:

1. Compromise of ICT systems.
2. Exfiltration of confidential data, including clients' personal information.
3. Disabling of the business-critical application.

The scenario was based on tactics, techniques, and procedures (TTPs) of real criminal groups, informed by current threat intelligence and risk assessments.

Remote Execution:
The exercise was conducted remotely, with CCS instances hosted on the HANFA's infrastructure. Supervised entities accessed their simulation environments via web browsers, ensuring seamless participation without additional hardware requirements.

The Results

1. **Simultaneous Digital Operational Resilience Testing**

   Incident response teams from all eleven organizations participated simultaneously, conducting testing in their individual simulation environments. A wide range of stakeholders, including crisis management teams, business process owners, communications and legal departments, data protection officers, and management, were actively involved.

2. **Management and Key Business Function Engagement**

   The CCS's **business loss visualization tools**, such as gauges, graphs, and indicators, were pivotal in driving decisions by business process owners and senior management during the incident.

   Injects from attackers, media, and supervisory bodies prompted immediate action from legal and communication departments, ensuring a comprehensive incident response.

   Accelerated simulation time allowed entities to experience the full lifecycle of the incident within a condensed timeframe.

3. **Enhanced Analysis Capabilities**
   The CCS **recorded all activities** performed by each entity during the exercise. These logs enabled HANFA to:

   - Compare written incident response procedures with real actions taken during the simulation.
   - Provide detailed feedback and recommendations for improvement.

4. Lessons Learned for Supervised Entities
The exercise assessed each organization's maturity in:

- Incident response management framework as prescribed by internal policies.
- Operational capabilities to respond effectively to a cyber incident.

Key takeaways:

- Awareness of the **business impact** of cyber incidents significantly increased across all organizational levels, including senior management.
- The results created a foundation for improving both management frameworks and operational procedures for future incidents.

Conclusion

By leveraging the Cyber Conflict Simulator, HANFA successfully conducted a comprehensive digital resilience test across eleven diverse organizations. This initiative not only raised awareness about the importance of operational resilience under DORA but also highlighted areas for improvement in supervised entities' incident response processes.

The exercise established a blueprint for ongoing improvements in cyber incident management and strengthened the digital operational resilience of supervised entities, ensuring their readiness to meet future regulatory and cybersecurity challenges.