PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 28 - numero 6089 di Mercoledì 27 maggio 2026

Sicurezza informatica: un kit per esercitazioni efficaci

Le indicazioni di ENISA per pianificazione, esecuzione e valutazione delle esercitazioni di cybersecurity e il kit di strumenti di supporto con una serie di modelli e materiale guida per consentire ai pianificatori di organizzare esercitazioni efficaci.

Come già anticipato in un articolo di qualche settimana fa, nel **febbraio 2026**, l'European Union Agency for Cybersecurity ha pubblicato **"The ENISA Cybersecurity Exercise Methodology ? End-to-end guide on how to plan, run and evaluate an exercise"**, un documento tecnico completo che offre indicazioni strutturate su come progettare e condurre esercitazioni di cybersicurezza efficaci.

Questa metodologia nasce dall'esperienza pluriennale di ENISA nell'organizzazione di esercitazioni come **Cyber Europe** e si propone di fornire un quadro teorico e operativo per aiutare organizzazioni, enti pubblici e governi a costruire esercizi realistici che mettano alla prova capacità tecniche, processi decisionali e cooperazione tra team.

Obiettivo della metodologia

La pubblicazione si configura come un **framework end-to-end** che guida l'intero ciclo di vita di un'esercitazione di cybersicurezza, dalla fase di preparazione fino alla valutazione finale. Secondo ENISA, l'obiettivo è *supportare le organizzazioni nello sviluppo e nella pianificazione di esercizi significativi ed efficaci, capaci di migliorare le competenze, i processi e le politiche interne*.

> La metodologia offre un quadro teorico completo per pianificare, eseguire e valutare esercitazioni di cybersicurezza, garantendo che i profili e i soggetti coinvolti siano presenti nei momenti appropriati.

Struttura della guida e benefici per le organizzazioni

Il documento ENISA è pensato come una guida modulare, che può essere adottata per esercitazioni di diversa natura e complessità. Tra i punti chiave troviamo:

- **Definizione degli obiettivi**: identificare il *perché* dell'esercitazione prima del *cosa* e del *come* è fondamentale per impostare correttamente scenari e metriche di valutazione.
- **Coinvolgimento degli stakeholder**: la metodologia sottolinea l'importanza di coinvolgere ruoli e competenze eterogenee, dai team tecnici agli stakeholder di governance, per assicurare una risposta completa e coordinata.
- **Ciclo completo di esercizio**: la guida copre tutte le fasi, dalla pianificazione logistica e scenaristica, all'esecuzione operativa, fino alla raccolta di dati e alla valutazione delle prestazioni.

L'adozione della metodologia ENISA porta diversi vantaggi tecnici e organizzativi:

- **Capacità di risposta migliorata**: simulare scenari di attacco consente di identificare lacune nei processi di incident response e di rafforzare le procedure operative.
- **Allineamento con normative europee**: esercitazioni ben strutturate aiutano le organizzazioni a dimostrare conformità a normative come la **Direttiva NIS2** e l'**EU Cybersecurity Act**.

- **Resilienza complessiva**: l'approccio end-to-end facilita la costruzione di una cultura di sicurezza più robusta e consapevole, integrando teoria e pratica.

In sintesi, la metodologia non è solo teorica, ma incorpora *lezioni apprese da esercitazioni reali*, best practice e strumenti che possono essere adattati ai diversi contesti organizzativi.

Le esercitazioni basate su questa metodologia possono spaziare da simulazioni tabletop (basate su discussioni e scenari) fino a esercitazioni tecniche e *cyber range* che coinvolgono sistemi reali. L'obiettivo è mettere alla prova non solo la tecnologia, ma anche le capacità decisionali, la comunicazione e la cooperazione interfunzionale.

Vediamo alcuni capitoli presenti nella guida.

Design (Progettazione)

La fase di **Design** costituisce il fondamento metodologico dell'intero esercizio. Qui vengono definiti gli obiettivi, il contesto e l'impostazione generale dell'esercitazione.

> La progettazione dell'esercitazione deve partire dalla definizione chiara degli obiettivi, dei risultati attesi e del contesto operativo, identificando gli stakeholder coinvolti e il livello di maturità dell'organizzazione.

In questa fase si determinano:

- gli obiettivi strategici e operativi
- il tipo di esercitazione (tabletop, tecnica, full-scale)
- il perimetro (organizzazione singola o multi-ente)
- i partecipanti e i ruoli
- il livello di complessità dello scenario
- i criteri di successo e le metriche di valutazione

Un elemento centrale è la definizione dello scenario, che deve essere:

- realistico
- rilevante rispetto al contesto di rischio
- coerente con le minacce attuali (es. ransomware, supply chain attack, data breach)

Questa fase garantisce che l'esercitazione sia allineata agli obiettivi organizzativi e produca risultati misurabili.

Preparation (Preparazione)

La fase di **Preparation** traduce il design in componenti operativi concreti, rendendo l'esercitazione pronta per essere eseguita.

> Durante la preparazione, tutti gli elementi dell'esercitazione vengono sviluppati in dettaglio, inclusi scenari, injects, materiali di supporto e pianificazione logistica, garantendo che i partecipanti siano adeguatamente coinvolti e informati.

Le principali attività includono:

- sviluppo dettagliato dello scenario narrativo
- creazione degli **injects** (eventi simulati che guidano l'evoluzione dell'esercizio)

- definizione della timeline degli eventi
- preparazione di documentazione e materiali operativi
- assegnazione dei ruoli (player, facilitatori, osservatori, valutatori)
- configurazione dell'ambiente tecnico (per esercitazioni pratiche)
- validazione interna dello scenario

Gli injects rappresentano un elemento chiave: consentono di simulare eventi progressivi che mettono alla prova la capacità di risposta dei partecipanti, mantenendo alta la pressione decisionale e la coerenza narrativa.

Execution (Esecuzione)

La fase di **Execution** è il momento operativo in cui l'esercitazione viene svolta e i partecipanti interagiscono con lo scenario simulato.

> Durante l'esecuzione, i partecipanti affrontano gli scenari e reagiscono agli eventi in tempo reale, mentre facilitatori e controllori introducono injects per guidare l'evoluzione dell'esercizio.

Durante questa fase:

- lo scenario viene attivato
- gli injects vengono introdotti secondo la timeline
- i partecipanti prendono decisioni e reagiscono agli eventi
- vengono simulate situazioni di crisi realistiche
- facilitatori e controller gestiscono il flusso dell'esercizio

L'obiettivo non è "risolvere" lo scenario, ma osservare:

- la qualità delle decisioni
- la capacità di coordinamento tra team
- l'efficacia della comunicazione interna ed esterna
- la prontezza nella gestione degli incidenti

Questa fase rappresenta il momento di maggiore valore pratico, in quanto consente di testare in condizioni controllate la preparedness dell'organizzazione.

Moving Forward (Valutazione e miglioramento)

La fase finale, **Moving Forward**, è dedicata all'analisi dei risultati e al miglioramento continuo delle capacità organizzative.

> La fase post-esercitazione si concentra sulla raccolta dei feedback, sull'analisi delle prestazioni e sull'identificazione delle lezioni apprese, con l'obiettivo di migliorare processi, competenze e capacità organizzative.

Le attività principali comprendono:

- raccolta feedback da partecipanti e osservatori
- sessioni di debriefing strutturato
- analisi delle performance rispetto agli obiettivi
- identificazione di gap tecnici, organizzativi e procedurali
- redazione del report finale
- definizione di azioni correttive e migliorative

Il risultato finale è un insieme di **lesson learned** che alimentano:

- aggiornamenti delle procedure di incident response
- miglioramenti nei processi decisionali
- programmi di formazione e awareness
- future esercitazioni più mature e mirate

Conclusioni

La metodologia ENISA rappresenta un approccio completo e strutturato alla progettazione e gestione delle esercitazioni di cybersicurezza. Le quattro fasi ? **Design, Preparation, Execution e Moving Forward** ? costituiscono un ciclo continuo che consente alle organizzazioni di trasformare ogni esercitazione in un'opportunità concreta di crescita.

Grazie a questo framework, le organizzazioni possono:

- migliorare la propria resilienza cyber
- testare processi e tecnologie in scenari realistici
- rafforzare la collaborazione tra stakeholder
- allinearsi alle migliori pratiche europee e ai requisiti normativi come la Direttiva NIS2

In un contesto di minacce in continua evoluzione, l'adozione di metodologie strutturate come quella proposta da ENISA non è solo una buona pratica, ma un elemento strategico fondamentale per la sicurezza informatica moderna.

RXY

ENISA - The ENISA Cybersecurity Exercise Methodology - End-to-end guide on how to plan, run and evaluate an exercise

Scarica i modelli del kit di strumenti di supporto per la metodologia delle esercitazioni di sicurezza informatica dell'ENISA.

www.puntosicuro.it