Corso

Normativa NIS2

IN-FORMAZIONE SRL - Via Riccardo Grazioli Lante, 9 - 00195 Roma
P.IVA 07252070722 - Tel. : 0687153208 - info@musaformazione.it

CORSO NORMATIVA NIS2

MODULO 1: INTRODUZIONE ALLA NIS2 E NORMATIVA DI SICUREZZA

- Introduzione alla NIS2
    - Obiettivi e finalità della direttiva.
- Confronto con la NIS1: principali novità.
- Soggetti interessati (Operatori di servizi essenziali e Fornitori di servizi digitali).
- Normativa Europea e Italiana di riferimento
    - Regolamenti correlati (GDPR, Direttiva eIDAS).
- Ruolo delle autorità competenti e del CSIRT (Computer Security Incident Response Team).

MODULO 2: COMPRENDERE LE MINACCE E RISCHI CYBER

- Tipologie di minacce informatiche
    - Attacchi malware (ransomware, spyware, virus, trojan).
    - Phishing e social engineering.
    - Vulnerabilità delle infrastrutture critiche (ICS, SCADA).
- Analisi dei rischi
    - Valutazione delle minacce specifiche per settori regolamentati dalla NIS2.
    - Esempi di attacchi recenti e il loro impatto su servizi essenziali.
    - Introduzione alla gestione del rischio
    - Framework di gestione del rischio e strategie di mitigazione.

MODULO 3: MISURE DI SICUREZZA E BUONE PRATICHE

- Implementazione di politiche di sicurezza basate sulla NIS2
    - Sicurezza delle reti e dei sistemi di informazione.
    - Misure preventive e reattive obbligatorie.
- Gestione delle identità e accesso

- Ruoli e privilegi: principio del minimo privilegio.
- Autenticazione multifattore (MFA) e crittografia.

- Sicurezza del cloud e servizi esterni
  - Requisiti di sicurezza per fornitori terzi.
- Governance della sicurezza nelle catene di approvvigionamento.
- Cultura della sicurezza aziendale
  - Coinvolgimento del personale e formazione continua.
  - Esempi di policy interne per una maggiore consapevolezza.

MODULO 4: INCIDENT RESPONSE E GESTIONE DELLE CRISI

- Piani di risposta agli incidenti
- Fasi della gestione di un incidente: identificazione, contenimento, eradicazione, ripristino.
  - Case study su attacchi cyber a servizi essenziali.
- Ruolo del CSIRT Coordinamento nazionale e cooperazione europea.
- Come segnalare e rispondere a un incidente secondo le direttive NIS2.
  - Comunicazione durante la gestione delle crisi
  - Comunicazioni interne ed esterne in caso di incidente.
  - Esempi di gestione della comunicazione con le autorità competenti.

MODULO 5: OBBLIGHI NORMATIVI E CONFORMITÀ ALLA NIS2

- Obblighi di notifica
  - Tempi e modalità di segnalazione degli incidenti.
  - Conseguenze per la mancata conformità (sanzioni e responsabilità).
- Audit e monitoraggio della sicurezza
  - Processi di audit obbligatori per i soggetti regolati.
  - Strumenti per il monitoraggio continuo della sicurezza.
  - Raccomandazioni per la conformità
- Strategie per implementare efficacemente le richieste NIS2 in azienda.

MODULO 6: ESERCITAZIONI PRATICHE E SIMULAZIONI

- Simulazione di un attacco informatico
- Attività pratiche su come individuare e rispondere a un attacco (phishing, ransomware).
- Analisi di incidenti passati
- Revisione di incidenti reali in ottica NIS2: errori, lacune, best practice.
- Sessione di domande e risposte

CONCLUSIONI E VALUTAZIONE

- Riepilogo dei concetti principali.
- Punti chiave da ricordare.
- Valutazione finale.