Cybersecurity - Governance e normative recenti

Comprendere i rischi e misurare i problemi

A distanza

3 giorni (21 Ore)

Open : 1.990,00 € +IVA
Packaged in azienda : 5.380,00 € +IVA +10% di Project Management (Quota riferita ad un gruppo di 10 pax max)
Customized : Su richiesta

WebCode: IT.12

La crescente interconnessione delle reti, lo smart working, l'adozione del Cloud, l'utilizzo dei servizi in modalità SaaS, la proliferazione di applicazioni e servizi web sono tutte evoluzioni tecniche che **indeboliscono** la sicurezza complessiva dei sistemi informativi e vedono un notevole aumento dei **rischi** che gravano sui dati aziendali.

La sintesi tecnica proposta in questo corso consentirà ai partecipanti di identificare le **nuove minacce** e comprendere quali cambiamenti tecnici e organizzativi possono consentire di **proteggerli**.

Il corso proporrà inoltre le **recenti normative** (ad es. **NIS e NIS2**) che impongono ad aziende identificate come "importanti ed essenziali" l'adozione di procedure e sistemi di sicurezza ad hoc.

A chi è rivolto

Per chi

- Qualsiasi responsabile del reparto IT coinvolto nella sicurezza di aziende private e pubbliche
- Responsabili della sicurezza di aziende importanti ed essenziali tenute ad implementare le normative NIS e NIS2
- Responsabili della sicurezza di aziende operanti nel settore finanziario
- Responsabili della sicurezza di soggetti critici

Prerequisiti

Nessuno

Programma

1 - Stato dell'arte ed evoluzione della cybersecurity

- Cybersecurity: nuovi attori e nuovi ambiti
- Sicurezza e legale
- Agenzia per la Cybersicurezza Nazionale (ACN)
- ENISA ruoli attuali ed evoluzione futura
- Standard di sicurezza e certificazioni

2 - Evoluzione della analisi di rischio

- Comprendere l’analisi del rischio
- Identificazione delle minacce
- Rischio IT vs rischio sui dati
- Rapporto analisi del rischio e trattamento del rischio
- Misure di sicurezza e ROSI

3 - Governo della sicurezza

- Indicatori di sicurezza efficaci
- Matrice delle competenze informatiche
- Evoluzione delle funzioni del RSSI
- Ruoli e missioni del DPO

4 - Sviluppi tecnologici

- Stato delle minacce e metodologie di attacco
- Dissezione di un APT
- Nuove architetture sicure
- Automazione e sicurezza
- IA e sicurezza
- Sicurezza dei sistemi embedded e iot
- Sicurezza nello sviluppo
- Sicurezza nell'ambiente cloud
- Mobilità e sicurezza

5 - Monitoraggio e gestione degli incidenti

- Service and application mapping
- Sicurezza offensiva: vulnerability assessment nad penetration test
- Monitoraggio della sicurezza Gestione degli incidenti, SIEM, SOC, CSIRT
- Resilienza informatica

6 - Recenti normative europee ed italiane

- Direttiva UE 2016/1148 e 2022/2555: ambito di applicazione (soggetti essenziali ed importanti)
- Direttiva UE 2022/2556: ambito di applicazione (settore finanziario)
- Direttiva UE 2022/2557: ambito di applicazione (soggetti critici)
- Normativa italiana e recepimento delle direttive UE
- Implementazione, certificazione e sanzioni

Obiettivi del corso

- Conoscere l'entità dei rischi che gravano sulle informazioni dell'azienda
- Comprendere l'evoluzione delle analisi dei rischi per far fronte alle nuove minacce
- Identificare i rischi associati all'emergere di nuove tecnologie
- Sapere come implementare una governance efficace
- Comprendi il valore di avere un monitoraggio e una gestione degli incidenti di nuova generazione
- Conoscere le nuove normative europee ed italiane, chi ed entro quando le deve implementare e come farlo

Esercitazioni

- Particolare enfasi è posta sulle **best practices** di governance della sicurezza.
- Una formazione **completa** durante la quale si alternano fasi di contributi teorici, scambi, condivisione di esperienze e simulazioni.

Date 2026

Ultimi posti Edizione garantita

dal 23 feb al 25 feb	dal 16 set al 18 set
dal 27 mag al 29 mag	dal 11 nov al 13 nov