Sicurezza informatica: lessico, concetti e tecnologie per non specialisti

Comprendere la cybersecurity

A distanza

2 giorni (14 Ore)

Open : 1.490,00 € +IVA
Packaged in azienda : 3.300,00 € +IVA +10% di Project Management (Quota riferita ad un gruppo di 10 pax max)
Customized : Su richiesta

WebCode: IT.13

La sicurezza informatica è diventata una **preoccupazione** per tutti gli utenti di Internet e dei Sistemi Informativi così come lo è stata -ormai da molto tempo- per i professionisti IT.

Se per alcuni di noi la nozione di sicurezza informatica è ancora confusa, addirittura astratta, è pur vero che tutti noi, nella nostra vita quotidiana, cominciamo a misurarne l'importanza.

Questo seminario di "divulgazione" spiega il suo concetto, i suoi acronimi, il suo gergo e presenta i diversi mezzi disponibili per realizzarlo. Permette quindi chiaramente ai partecipanti di **familiarizzare** con la sicurezza informatica e di avere le conoscenze necessarie per comunicare e **collaborare** con i team tecnici interni, fornitori di servizi o fornitori specializzati nel settore.

A chi è rivolto

Per chi

- Venditori, specialisti di marketing, futuri consulenti, project manager o responsabili della formazione che si evolveranno nel mondo della sicurezza informatica
- Chiunque desideri comprendere la sicurezza informatica per ottimizzare la propria collaborazione con gli specialisti del settore

Prerequisiti

Nessuno

Programma

1 - Principi generali di sicurezza informatica

- Aree interessate: confidenzialità, integrità, disponibilità (CIA)
- Approccio generale da adottare / analisi dei rischi
- Nozioni da sapere: autenticazione semplice e forte, Defense in Depth, piani di Disaster Recovery e Business Continuity

2 - Comprendere i diversi tipi di vulnerabilità e attacchi

- Malware: cavalli di Troia, virus, rootkit, spyware, ransomware, cryptolocker...
- Attacchi: terminali, reti, applicazioni (Sniffing,DoS, DDoS...)

- Attacchi di password, SQL injection, furto di identità e data exfiltration
- Attacchi non malware: attacchi di phishing
- Valutazione del rischio

3 - Conoscere il funzionamento dei sistemi di protezione dedicati a:

- Soluzione per la gestione delle password (PAM)
- Crittografia simmetrica: AES
- Isolamento delle infrastrutture critiche mediante la configurazione di reti virtuali (VLAN)
- Crittografia dei collegamenti remoti (Zero Trust Network Access/ZTNA, VPN SSL e VPN IPSec)
- Autenticazione di accesso: autenticazione forte, Network Access Control (NAC) e Role Based Access Control (RBAC)
- Filtraggio: firewall di protocollo e applicativi
- Protezione delle applicazioni Web: WAF (Web Access Firewall)
- Log server e SIEM (Security Information and Event Management)
- IAM (Gestione di identità e accessi)
- DLP (Data Lost Prevention) - Data Masking - Crittografia
- Software fingerprint e MAC (Mandatory Access Control)
- Altre aree specifiche

4 - Utilizzare piattaforme di sicurezza specializzate

- Piattaforma cloud di sicurezza (SecaaS: sicurezza come servizio)
- Piattaforma di sicurezza e gestione mobile EMM (Enterprise Mobility Management)
- Piattaforma di sicurezza NGFW (Next Generation of Firewall).

5 - Usa la combinazione di attrezzature per proteggere

- Internet (comunicazione e transazione): crittografia PKI (Public Key Infrastructure)
- Reti wireless Wi-Fi: 802.11i (802.1X/EAP...) / WPA / WPA2 / WPA3
- Terminali e applicazioni mobili e telelavoro (ODE, containerizzazione, App Store, software footprint, App Wrapping...) / Standardizzazione del terminale e pubblicazione dell'applicazione (TS-WEB, VDI...)
- BYOD (uso di attrezzature personali nel contesto professionale)
- Protezione da cloud e Big Data (crittografia, furto di dati, flussi di dati, ecc.)

6 - Misurare l'impatto dell'implementazione della sicurezza su:

- Le prestazioni complessive del sistema del computer
- Architettura del sistema informativo

7 - Affidati ai repository per gestire la sicurezza IT

- ACN: Agenzia Cybersicurezza Nazionale
- ENISA (organizzazione europea - gestione del rischio)
- NIST e ISO (norme seguite dai principali attori del settore della sicurezza)
- CSA (Cloud Alliance Security) / CSA Big Data / CSA Mobile
- GDPR (Obbligo legale di privacy)
- NVD/CVE

8 - Principali tendenze

- Limiti delle attuali soluzioni di sicurezza
- Security Service Edge (SSE): Secure Web Gateway, Cloud Access Security Broker, Zero Trust Network Access, Firewall as a Service
- Cybersecurity: uso dell'intelligenza artificiale e del machine learning
- Software Defined Perimeter (SDP)
- blockchain

Obiettivi del corso

- Comprendere i concetti, le tecnologie e le soluzioni di sicurezza della rete di computer per lavorare con specialisti e gestire i fornitori di servizi
- Acquisire la visione globale della sicurezza
- Conoscere i ruoli delle parti interessate nel settore e il loro lavoro
- Identifica nuovi problemi associati alla sicurezza IT

Esercitazioni

- Una descrizione delle tecnologie e dei concetti illustrati con **esempi** di soluzioni concrete e usi attuali.
- La divulgazione di tecnologie complesse rendendole **accessibili** a specialisti non IT e di sicurezza.

Date 2026

Ultimi posti Edizione garantita

dal 9 mar al 10 mar	dal 8 ott al 9 ott
dal 4 giu al 5 giu	dal 3 dic al 4 dic