**CORSO CYBER SECURITY**

**PRESENTAZIONE**

L'obiettivo del corso è quello di fornire le conoscenze principali riguardanti la cyber-security sia per quanto riguarda i principi che le metodologie alla base della sicurezza dei sistemi informatici e delle reti di telecomunicazioni, dal punto di vista tecnico ma anche organizzativo. Le varie problematiche, sempre declinate con un approccio molto concreto e aderente alla realtà, verranno introdotte per mezzo di **casi aziendali di studio** ed esempi tratti dall’attualità. L’intenzione è sia quella di fornire le conoscenze di base per potersi districare nel mondo della cyber-security sia di essere in grado di valutare con occhio critico i propri sistemi aziendali anche alla luce dell’evoluzione che sarà necessaria nei prossimi anni, ad esempio per quanto concerne gli aspetti più legati al contesto normativo e all’utilizzo dell’AI.

**OBIETTIVI**

## Introdurre i principali problemi della cyber-security

## Apprendere i concetti di base e la metodologia tipica di questo settore

## Essere in grado di individuare le principali problematiche di sicurezza dei propri sistemi

## Essere in grado di valutare criticamente le soluzioni presenti sul mercato

## Permettere di individuare i maggiori trend di evoluzione della cyber-security

## Individuare gli aspetti più rilevanti dal punto di vista normativo e relativamente all’AI

**MODALITÀ DI FRUIZIONE E DURATA**

Il corso, della durata di 32 ore, prevede 7 sessioni a distanza da mezza giornata e un’ultima giornata full time con esempi presso l’aula e la Linea Pilota Bi-Rex.

**Argomento 1 - Introduzione alla sicurezza informatica**

**Contenuti**

* Concetti e principi di base della sicurezza informatica.
* Casi di studio: analisi iniziale di alcuni esempi tratti dall’attualità (Internet of Things e Industria 4.0, dispositivi mobile).
* Terminologia essenziale del mondo della sicurezza: il concetto di minaccia, le tipologie principali degli attacchi e le risorse di un sistema.
* Il concetto di vulnerabilità informatica: definizione per mezzo dell’analisi di alcuni esempi notevoli.
* Principi e meccanismi fondamentali per la progettazione (e l’implementazione) di un sistema “ragionevolmente sicuro”.
* La sicurezza come processo: l’importanza della formazione continua del personale diversificata a seconda dei ruoli e delle competenze. La necessità di “consapevolezza” del problema da parte di tutti gli utilizzatori dei sistemi. L’analisi del valore delle risorse. Il problema dell’interazione tra figure non tecniche e tecniche in ambito aziendale.Superficie d’attacco e alberi d’attacco, valutazione (e riduzione) del rischio per mezzo di strumenti tecnologici, organizzativi ed anche assicurativi.
* Non solo tecnica: gli attacchi più comuni sono di tipo “social engineering” (ingegneria sociale). Inganni via e-mail ma non solo, l’importanza di definire procedure aziendali che tengano conto anche degli aspetti di sicurezza.
* La mitigazione delle minacce e la corretta gestione delle vulnerabilità che non possono essere eliminate. Il concetto di “finestra di vulnerabilità”.

**Argomento 2 - Strumenti e meccanismi di base per la protezione dei sistemi**

**Contenuti**

* Meccanismi di autenticazione tra innovazione e limiti (password, token, biometria, meccanismi multi fattore, accesso per mezzo di app di autenticazione, problemi dell’autenticazione via SMS, passkey);
* Meccanismi di autorizzazione (schemi per il controllo degli accessi alle risorse di sistema): chi può accedere a cosa?
* Breve introduzione ai meccanismi crittografici (es. crittografia simmetrica, a chiave pubblica) e breve discussione di alcuni utilizzi pratici (crittografia dei backup, certificati SSL, e-mail crittografate, PEC).
* Esercitazione: “giochiamo” con l’infrastruttura di rete Bi-Rex e con la linea pilota. Sono sicure o vulnerabili? Analisi della superficie d'attacco. Definizione del “threat model” e delle principali contromisure applicabili.
* Esercitazione: esempio pratico di attacco ai protocolli HTTP/HTTPS (pharming), il problema dell’integrità dei sistemi e il concetto di “trust” (fiducia) nelle comunicazioni e dei sistemi.
* Qual è il livello di sicurezza dei sistemi attualmente in commercio? Ad esempio, i sistemi mobile (Apple e Android) quanto sono sicuri? La migrazione di sempre più servizi da fisso a mobile (es. online banking) quali rischi comporta?

**Argomento 3 - Attacchi, contromisure e prospettive future**

**Contenuti**

* Ransomware: presente e futuro dei meccanismi di estorsione.
* Internet of Things, in quale modo l’Internet delle cose modifica le politiche di sicurezza aziendali e in generale la sicurezza di Internet?
* Case histories: pompe per insulina, il mercato delle vulnerabilità.
* Cloud computing: una componente essenziale di (quasi) tutti i sistemi attuali, con enormi vantaggi e qualche rischio da non sottovalutare.
* Industria 4.0: breve analisi di sicurezza dei sistemi produttivi connessi ad Internet.
* I rischi delle politiche BYOD (bring your own device) e la loro gestione corretta. Il problema dell’espansione del perimetro aziendale (e personale).
* Firewall e antivirus: cosa sono esattamente? Si tratta di strumenti ancora attuali in una politica di gestione della sicurezza aziendale oppure sono superati?
* Alcuni cenni di sicurezza delle reti (sia cablate ma soprattutto wireless).

**Argomento 4 - Aspetti normativi della CyberSecurity, Intelligenza Artificiale**

**Contenuti**

* Breve introduzione al “Regolamento Europeo in materia di protezione dei dati personali (GDPR UE 2016/679)”. Discussione degli aspetti rilevanti per la sicurezza dei sistemi e le procedure da seguire in ambito aziendale.
* Come può un’impresa che ha a disposizione un budget (piuttosto) limitato, migliorare il proprio livello di sicurezza? Alcuni punti di partenza, per mezzo di documenti e metodologie liberamente disponibili:
  + Laboratorio Nazionale di Cyber Security (CINI)
    - libro Bianco sulla Cyber Security;
    - framework Nazionale per la Cybersecurity (15 Controlli Essenziali per la Cybersecurity).
* Aspetti normativi:
  + “Misure per un livello comune elevato di cibersicurezza nell'Unione” (NIS-2)
  + “Cyber Resilience Act” (CRA)
  + “Artificial Intelligence Act” (AI Act)
* Certificazioni: ISO 27001
* AI e CyberSecurity:
  + Attacchi al Machine Learning
  + Data poisoning
  + Uso del ML per identificare outlier e soggetti anomali
  + Difesa e Attacchi AI-driven
  + Etica e privacy nell’AI