Executive Program

Corso Cyber Security
PROTEZIONE DEI SISTEMI INDUSTRIALI E DEI SERVIZI

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 sia organizzativo, sia tecnico. 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.

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 le sessioni esercitative presso l'aula e la Linea Pilota BI-REX.

DESTINATARI DEL CORSO

Il corso è rivolto a tutte le funzioni aziendali coinvolte a diverso titolo nel processo per garantire la sicurezza informatica, sia per quanto riguarda la parte decisionale (apicale) e organizzativa, sia per le funzioni più tecniche e operative. A titolo esemplificativo: imprenditori, IT manager, programmatori, integratori di sistemi, responsabili sicurezza, qualità e organizzazione, responsabili del personale.

CONTENUTI

Il contenuto dei moduli verrà distribuito nelle varie giornate di lezione in base alla coerenza degli argomenti svolti ma concentrando prevalentemente nell'ultima giornata di lezione (in presenza) le testimonianze aziendali e gli esempi pratici sulla linea pilota BI-REX.

Executive Program

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

DOCENTI

Gabriele D'Angelo
È ricercatore confermato presso l'Università di Bologna. La sua attività principale di ricerca è incentrata sui temi della simulazione dei sistemi complessi e sulla sicurezza delle reti. Insegna Cyber Security in vari corsi dell'Università di Bologna e alla Bologna Business School.

GIORNATE DI LEZIONE:

Mercoledì 4 Maggio (dalle 9 alle 12.30 – online);
Venerdì 6 Maggio (dalle 9 alle 12.30 – online);
Mercoledì 11 Maggio (dalle 9 alle 12.30 – online);
Venerdì 13 maggio (dalle 9 alle 12.30 – online);
Mercoledì 18 Maggio (dalle 9 alle 12.30 – online);
Venerdì 20 Maggio (dalle 9 alle 12.30 – online);
Mercoledì 25 Maggio (dalle 9 alle 12.30 – online);
Venerdì 27 Maggio (dalle 9 alle 13.00 e dalle 14.00 alle 17.30 – in presenza).

MODULO 1

INTRODUZIONE ALLA SICUREZZA INFORMATICA

CONTENUTI

- Concetti e principi di base della sicurezza informatica (i.e. cyber-security).
- Case histories: analisi iniziale di alcuni esempi tratti dall'attualità (sicurezza delle automobili, Internet of Things e Industria 4.0, smartphone).
- 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 (case histories: i ransomware, il caso FBI vs. Apple).
- 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 (phishing e ransomware) 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".

MODULO 2

STRUMENTI E MECCANISMI DI BASE PER LA PROTEZIONE DEI SISTEMI

CONTENUTI

- Un caso famoso di attacco ransomware: intervento della società Bonfiglioli.
- 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);
- Meccanismi di autorizzazione (schemi per il controllo degli accessi alle risorse di sistema): chi può accedere a cosa? Come si garantisce il rispetto della confidenzialità delle informazioni in presenza di una gerarchia aziendale? Case histories: Edward Snowden (NSA leak) e il recente Twitter Hack.
- 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?

MODULO 3

ATTACCHI, CONTROMISURE E PROSPETTIVE FUTURE

CONTENUTI

- Un caso famoso di Ransomware: intervento della società Var Group.
- 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 e pacemaker.
- 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.
- Case histories: Stuxnet e Flame.
- 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).
- Esercitazione: la tua azienda è vulnerabile? A quali attacchi? Scopriamolo assieme.
- Le criptovalute (es. Bitcoin, Ethereum, Monero) stanno avendo un enorme aumento della capitalizzazione e una grande successo sulla stampa. Di cosa si tratta? Quali sono i collegamenti con il tema della sicurezza informatica e sul loro eventuale utilizzo in ambito aziendale (ad esempio come sistemi di pagamento)? Una delle innovazioni legate alle criptovalute è la struttura dati utilizzata nella loro implementazione, chiamata blockchain. A che cosa serve?

MODULO 4

NORMATIVA, QUADRO NAZIONALE ED EUROPEO (DA UN PUNTO DI VISTA TECNICO)

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.
- Lo stato della cybersecurity in Italia: "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionali (DPCM 17/02/2017)". Architettura istituzionale ed impatto sugli operatori privati che forniscono servizi al pubblico.
- Una nuova certificazione europea: "European cybersecurity certification scheme (EUCC)".
- 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).
- Breve introduzione al EU Cybersecurity Act
- Casi aziendali da progetti di ricerca applicata realizzati con Università e aziende del consorzio Bi-Rex

CLICCA QUI per iscriverti o compila in tutte le sue parti la seguente scheda e inviala scansionata a **massimo.pulvirenti@bi-rex.it**

Ogni iscritto al corso avrà come bonus SU RICHIESTA l'accesso gratuito per un anno a tutti i contenuti della piattaforma di e-learning **bi-rex.skills4business.it**

DATI DI ISCRIZIONE DEL PARTECIPANTE

Cognome e nome

Cell. e-mail

Titolo di studio

Funzione aziendale/Profilo

DATI PER LA FATTURAZIONE

PRIVATO

Intestazione e indirizzo

Partita I.V.A./ C.F. Codice SDI PEC

PARTECIPAZIONE A TITOLO AZIENDALE

Ragione sociale

Settore ☐ PMI ☐ Grande Azienda ☐ Altro

Indirizzo Cap Comune Prov

Referente amministrativo E-mail Tel.

Intestazione e indirizzo

Partita I.V.A./ C.F. Codice SDI PEC

Prezzo intero

☐ **Corso Cyber Security:** 1400€ + IVA
Sconto ***10%*** a partire dal 2°iscritto

Prezzo Consorziati e Partner BI-REX o PMI:

☐ **Corso Cyber Security:** 1200€ + IVA
Sconto ***10%*** a partire dal 2°iscritto

Voucher Fondi Interprofessionali
BI-REX ha attivato un servizio a supporto dell'ottenimento di voucher formativi a copertura del costo di iscrizione attraverso i principali fondi

MODALITÀ DI ISCRIZIONE

L'iscrizione dovrà avvenire entro il **5° giorno lavorativo** antecedente l'inizio del corso. L'iniziativa verrà realizzata al raggiungimento del numero minimo di 8 iscritti. In caso di mancato raggiungimento di tale numero, BI-REX si riserva la facoltà di disdire il corso, comunicandolo all'indirizzo del partecipante entro 2 giorni dalla data di inizio prevista. In tal caso, al partecipante /Azienda che ha già provveduto al pagamento della quota di iscrizione verrà offerta la possibilità di partecipare ad un altro corso o verrà restituita la quota di iscrizione.

CONDIZIONI DI PAGAMENTO

La quota di iscrizione deve essere versata al momento della conferma del corso. Il pagamento deve essere effettuato mediante bonifico Bancario intestato a **BI-REX codice IBAN: IT41 V030 6902 4781 0000 0017 142 presso Intesa Sanpaolo – Filiale 68109 - BOLOGNA SEDE**. BI-REX provvederà all'invio della fattura, via email, al ricevimento della quota di iscrizione.

DISDETTA DELLA PARTECIPAZIONE

Qualsiasi rinuncia deve pervenire, in forma scritta, entro **4 giorni lavorativi** dall'inizio del corso. In caso di rinuncia pervenuta dopo tale termine o di mancata presenza del partecipante ad inizio corso o di ritiro durante lo stesso BI-REX è autorizzato a trattenere l'intera quota se già versata. La presente scheda dovrà essere inviata a BI-REX via email all'attenzione del responsabile dei servizi di formazione e consulenza, Massimo Pulvirenti (massimo.pulvirenti@bi-rex.it). Per chiarimenti è possibile contattare BI-REX allo 051 0923251.

Acconsento al trattamento dei miei dati personali per rimanere informato su iniziative analoghe, ricevere comunicazioni informative e promozionali, nonchè newsletter, da parte di Bi-Rex [Leggi l'informativa sulla privacy qui: **clicca qui per leggere l'informativa**

☐ SI ☐ NO

I dati raccolti saranno trattati ai sensi del regolamento europeo sulla protezione dei dati (Reg. UE 2016/679).
Si fornisce il consenso al trattamento dei propri dati personali in riferimento all'informativa ricevuta

☐ SI ☐ NO

DATA TIMBRO E FIRMA