FORMAZIONE ON LINE

SBS
SCUOLA BENI STRUMENTALI

CYBERSECURITY

strumenti e metodi per migliorare la protezione della propria azienda

Percorso specifico per aziende produttrici di meccanica strumentale

SBS PROPONE UN PERCORSO APPROFONDITO PER LA SICUREZZA RETI ED ANALISI FORENSE DEL CYBER ATTACK.

Siamo tutti sempre più interconnessi, ed il rischio di lasciare una "porta aperta" virtuale significa lasciare entrare in azienda "ospiti indesiderati". Il percorso proposto, in collaborazione con Swascan, inizia con un **primo modulo rivolto a tutti i dipendenti aziendali**. Infatti il Corso di Social Engineering ha lo scopo di sensibilizzare il personale aziendale e diffondere la cultura sulla cybersecurity
Il **secondo modulo affronta la tematica degli attacchi** dal punto di vista del funzionamento dei macchinari industriali. Il **terzo modulo riguarda la capacità di costruire una rete** informatica capace di sostenere attacchi informatici. Il **quarto ed ultimo modulo riguarda la risposta all'incidente**, cosa imparare dal medesimo e cosa fare per evitare altri incidenti informatici in futuro.

I moduli avranno un approccio pratico e gli esempi riportati riguardano aziende produttrici di macchinari.

PARTNER TECNICO
SWASCAN

Swascan è una Cyber Security Company innovativa nata da un'idea di Pierguido Iezzi e Raoul Chiesa.
Da ottobre 2020, Swascan srl è parte integrante del Gruppo Tinexta S.P.A.

La prima azienda di Cyber Security Italiana proprietaria di una piattaforma di Cyber Security testing e di un centro di eccellenza di Cyber Security Research:

- Premiata da Cisco come piattaforma di Cyber Security;
- Vanta il riconoscimento in collaboration with Cisco;
- Eccellenza Cyber Europea riconosciuta dall' ECSO (European Cyber Security Organization);
- Selezionata tra le top 20 soluzioni al Mondo per l'analisi del Rischio Tecnologico da Markets & Markets.

Swascan TINEXTA GROUP

Swascan Academy

1 SOCIAL ENGINEERING: TECNICHE DI ATTACCO E DI DIFESA

CONTENUTI

Social Engineering è il termine usato per una vasta gamma di attività malevoli compiute attraverso le interazioni umane. Utilizza la manipolazione psicologica per indurre gli utenti a commettere errori di sicurezza o a fornire informazioni sensibili. Gli errori commessi dagli utenti sono molto meno prevedibili, il che li rende più difficili per le aziende da **identificare e contrastare** rispetto a un'offensiva basata su malware.

OBIETTIVI

L'obiettivo del corso è di preparare il personale aziendale a **riconoscere gli attacchi informatici** perpetrati tramite tecniche di Social Engineering e non cadere in trappola.
Saranno illustrati i concetti base di Social Engineering, gli aspetti psicologici e le tecniche di manipolazione sul quale gli hacker fanno leva per sferrare attacchi informatici e rubare dati sensibili. Verranno presentati esempi pratici di casi reali al fine di **comprendere i vettori di attacco del Social Engineering e costruire una difesa efficace**.

DESTINATARI

Il corso di Social Engineering è **rivolto a tutto il personale aziendale** in quanto non richieste conoscenze tecniche pregresse.

PROGRAMMA FORMATIVO

- Definizione di Social Engineering
- L'evoluzione nel tempo del Social Engineering
- Obiettivi di un attacco di Social Engineering
- Il sistema operativo "uomo"
- Le vulnerabilità della psicologia umana
- Gli attacchi di Social Engineering ai giorni nostri
- Il fattore di rischio umano
- Incrementare il livello della human security
- Elaborare una policy di sicurezza aziendale
- Come difendersi dagli attacchi di Social Engineering
- Misure di sicurezza
- Riconoscere un attacco
- Cosa fare in caso di attacco
- Esercitazioni in aula, demo live e casi reali di Phishing e Smishing

1 SOCIAL ENGINEERING: TECNICHE DI ATTACCO E DI DIFESA

FORMATORI

VINCENZO LENA
Cyber Security Expert
e Digital Forenser

Dopo una laurea in Informatica, ha conseguito diverse certificazioni, quali: specializzazione in "Scienze criminologiche, investigative e politiche della sicurezza", C.P.E.H. - Certified Professional Ethical Hacker, C.D.M.A. - Certified Dynamic Malware Analyst, Maestro della protezione dati & data protection Designer presso Istituto Italiano per la Privacy e la Valorizzazione dei Dati e Qualifica A/L.A. UNI EN ISO/IEC 27001/2770. Ha ricoperto diversi ruoli in svariate aziende come esperto in sicurezza informatica, sino ad attività di digital forensics.

PIERGUIDO IEZZI
CEO e co-founder
di Swascan

Ex Ufficiale di carriera presso l'Accademia Militare di Modena, laureato in Scienze dell'Informazione, con oltre 30 anni di esperienza nel mondo della Cyber Security. Ha alle spalle un'ampia gamma di attività operative relative a Tecnologia, Innovazione, Cyber Security e gestione aziendale. Autore di diverse pubblicazioni, collabora regolarmente a diversi giornali e pubblicazioni. Keynote speaker e testimonial presso università, eventi nazionali e internazionali.

2 FONDAMENTI DI SICUREZZA NEL MONDO OT

CONTENUTI

Negli ultimi mesi abbiamo visto ripetuti "incidenti informatici" che hanno avuto impatti, a volte anche gravi, sul normale funzionamento di impianti industriali.
Le **vittime sono state sistemi di automazione, controllo e telecontrollo** che gestiscono impianti e macchinari industriali di Aziende automobilistiche, di aziende alimentari ed industrie chimiche, meccaniche e siderurgiche, ma anche sistemi che gestiscono blocchi operatori in ospedali, grandi edifici ed infrastrutture come aeroporti, acquedotti, ecc.
Malware, come Wannacry, Industroyer e Petya, **hanno colpito impianti sfruttando vulnerabilità diffuse in reti e sistemi OT**.
Per "ICS/OT Security" si intende la protezione da rischi informatici di tutti questi sistemi e le reti alle quali partecipano e/o sono collegate.

OBIETTIVI

L'obiettivo è di **acquisire la conoscenza dei principi e della terminologia di base** della sicurezza nel mondo dell' in modo da poterli applicare nei contesti aziendali.
ICS (Industrial Control System) e **OT** (Operation Technology) sono l'insieme dei sistemi utilizzati sull'impianto per automazione (di fabbrica), controllo di processo, supervisione, monitoraggio, telecontrollo, raccolta dati e gestione di impianti.

DESTINATARI

Questo corso è rivolto ad **IT Manager, Business Manager, IT Auditor, Professionisti IT, CIO, CTO, IT Project Manager, IT Service Manager, Responsabili della Qualità** ed a tutto il personale aziendale interessato a comprendere le dinamiche di gestione di un sistema informatico di sicurezza.

PROGRAMMA FORMATIVO

- Introduzione alla ICS/OT cyber security industriale
- Differenze Safety e Security, ICS/SCADA Security
- La security in ambienti ICT ed ambienti industriali/utility
- Terminologia, scenari e tecnologie, perché e come proteggere gli impianti
- Gli aspetti della sicurezza
- Minacce e vulnerabilità dei sistemi di controllo
- Analisi e Valutazione dei rischi
- La protezione dei sistemi su impianti delle Infrastrutture Critiche
- Standard Industriali, IEC ed ISO internazionali
- Introduzione al ciclo PDCA (Plan-Do-Check-Act)
- Metodologie di protezione HW/SW: Antimalware, IDS/IPS, Firewall, ecc.
- Definizione del perimetro elettronico
- Security Network cablata e Wireless security. Aspetti organizzativi
- Analisi di casi aziendali: aziende produttrici di macchinari

2 FONDAMENTI DI SICUREZZA NEL MONDO OT

FORMATORI

OMAR MORANDO
OT Cyber Security Expert

Cyber security advisor ed ethical hacker, si occupa di penetration testing e analisi vulnerabilità con specializzazione in ambito OT e Automotive. Ha maturato oltre 20 anni di esperienza nel settore dell'automazione industriale (di cui 15 in Schneider Electric) con sistemi SCADA, PLC, bus di campo, I/O remoti. Si occupa di formazione e diffusione dei temi della protezione della privacy, sicurezza informatica e protezione dei dati. Progetta e sviluppa software per sistemi embedded e per mobile robotics.

3 INTRODUZIONE ALLE RETI E ALLE INFRASTRUTTURE

CONTENUTI

La capacità di **gestione di una rete**, di sistemi informativi ed infrastrutture è **requisito primario per tutte le aziende** che hanno bisogno di scambiare informazioni interne all'azienda e rivolte al pubblico.
Il corso introduce gli studenti agli argomenti relativi al **networking**, partendo dai fondamenti fino alle applicazioni di **routing** e **switching**.

OBIETTIVI

L'obiettivo del Corso è di a**cquisire la conoscenza dei principi e della terminologia di base** per il lavoro nel campo delle reti e della sicurezza nonché di **acquisire consapevolezza nella gestione di hardware e software**.

DESTINATARI

Questo corso è rivolto **ad IT Manager, Business Manager, IT Auditor, Professionisti IT, CIO, CTO, IT Project Manager, IT Service Manager, Responsabili della Qualità** ed a tutto il personale aziendale interessato a comprendere le dinamiche di gestione di un sistema informatico di sicurezza.

PROGRAMMA FORMATIVO

- Introduzione alla ICS/OT cyber security industriale
- Network Fundamentals
- LAN Switching Fundamentals
- Routing Fundamentals
- Infrastructure Services
- Infrastructure Maintenance
- Analisi di casi aziendali

FORMATORI

FEDERICO CIULLA
Principal Information Security Architect

Federico Ciulla, CISSP, CISM, CCSK, CCNA, CCNP, CCDP, CSSA, FCNSA, è un professionista con più di 14 anni di esperienza e un ampio background tecnico nella creazione di infrastrutture di rete e della relativa messa in sicurezza delle stesse. Nel passato è stato Lead Network Security Engineer per importanti progetti relativi all'implementazione di reti ed infrastrutture di security di nuova generazione ed attualmente si occupa di Information Security, Privacy e Compliance.

4 INTRODUZIONE ALL'INCIDENT RESPONSE

CONTENUTI

Nella vita di tutte le aziende, prima o poi, si verificano eventi di crisi che possono mettere a prova l'operatività aziendale. I **manager devono essere in grado di gestire e affrontare situazioni nuove** e impreviste che possono mettere in difficoltà la professionalità di un individuo. Gli eventi esterni o interni all'azienda che influenzano le normali attività di un'azienda, se non sono gestiti tempestivamente e con la giusta strategia, possono rivelarsi molto dannosi e, nei casi più estremi, possono portare al fallimento.

OBIETTIVI

Lungo il corso di formazione sull'Incident Response gli studenti si concentreranno su come **progettare, sviluppare e implementare correttamente i piani di risposta agli incidenti di sicurezza**.
I partecipanti impareranno a conoscere tre aspetti importanti dell'incident response: l'**analisi dell'impatto aziendale, il piano di continuità aziendale e il piano di disaster recovery**. Dopo aver completato il corso, sapranno come prepararsi agli incidenti e come attuare il processo di mitigazione per aiutare la propria azienda anche nell'immediato.

DESTINATARI

Questo corso è rivolto ad **IT Manager, Business Manager, IT Auditor, Professionisti IT, CIO, CTO, IT Project Manager, IT Service Manager, Responsabili della Qualità** ed a tutto il personale aziendale interessato a comprendere le dinamiche di gestione di un sistema informatico di sicurezza.

PROGRAMMA FORMATIVO

- Network Fundamentals
- Information Security Incident Management
- Incident Management
- Policy e procedure di Incident Response
- Response Capability
- Incident Response Plan
- Business Continuity Management
- Disaster Recovery Management
- Response e Recovery Plan
- Post-Incident Management
- Investigation
- Analisi di casi aziendali: aziende produttrici di macchinari

FORMATORI

MANUEL CACITTI
Senior Information Security Consultant

Esperto di sicurezza dei dati e auditor, opera da oltre 15 anni su progetti nazionali e internazionali finalizzati all'implementazione e mantenimento di sistemi di gestione per la sicurezza delle informazioni, continuità operativa, analisi e gestione del rischio, protezione delle infrastrutture critiche, IT security governance e auditing. Collabora come docente con alcune università nazionali e academy private. Certificato CISA, CDPSE, ITIL, LeA ISO 27001, 22301, 20000, 90001, è membro di molte associazioni di settore, tra cui ISACA, AICA, AIIC, AIP, Federprivacy, Privacy Network, Centro Studi Sicurezza ITASFORUM.

	Corso	Durata	Calendario	Quota di partecipazione	
				QUOTA ASSOCIATO	QUOTA NON ASSOCIATO *
1	Social Engineering: Tecniche di attacco e di difesa	8 ORE	10 e 17 marzo dalle 14 alle 18	500,00 €	600,00 €
2	Fondamenti di sicurezza nel mondo OT	8 ORE	6 e 13 aprile dalle 14 alle 18	700,00 €	850,00 €
3	Introduzione alle reti e alle infrastrutture	8 ORE	4 e 11 maggio dalle 14 alle 18	550,00 €	750,00 €
4	Introduzione all'Incident Response + L'analisi forense dell'Incident Response	16 ORE	25 maggio e 1,8,15 giugno dalle 14 alle 18	1.000,00 €	1.400 €

INFORMAZIONI AGGIUNTIVE

Acquisto di tutti i pacchetti (con possibilità di far frequentare diversi partecipanti)

quota Associati	quota NON Associati *
2.300,00 €	3.300,00 €

Early Bird

Le aziende che si iscriveranno entro il 31/12/2021 riceveranno uno sconto del 15% sulla quota di partecipazione del percorso (non cumulabile con altre scontistiche).

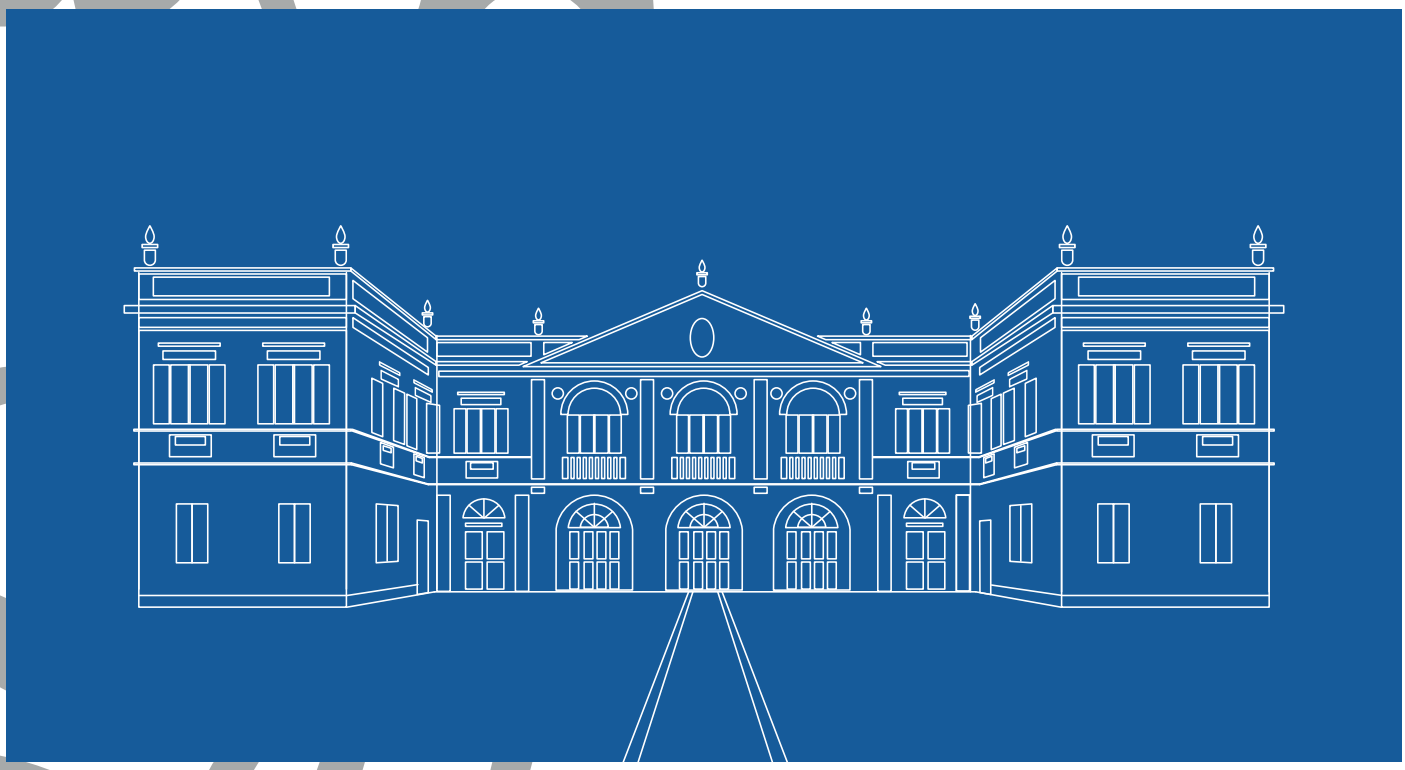
Acquisto di partecipazioni multiple sconto del 10%

*Associati e non Associati ad:
- Acimac
- Amaplast
- Ucima

La quota di iscrizione è considerata al netto da iva.

SBS
SCUOLA BENI STRUMENTALI

Lo staff di SBS è a disposizione per rispondere in modo mirato alle vostre esigenze attraverso progetti formativi elaborati su misura e soluzioni customizzate



IN COLLABORAZIONE CON

ACIMAC
Associazione Costruttori Italiani Macchine Attrezzature per Ceramica

UCIMA
Unione Costruttori Italiani Macchine Automatiche per il Confezionamento e l'Imballaggio

AMAPLAST
ASSOCIAZIONE NAZIONALE COSTRUTTORI DI MACCHINE E STAMPI PER MATERIE PLASTICHE E GOMMA

NFIMA

SBS - Scuola Beni Strumentali
Via Fossa Buracchione, 84 - 41126 Baggiovara (MO)
T. 39 059 472 6320 - formazione@scuolabenistrumentali.it
www.scuolabenistrumentali.it