"Difesa delle Infrastrutture Critiche: hacking e contromisure"

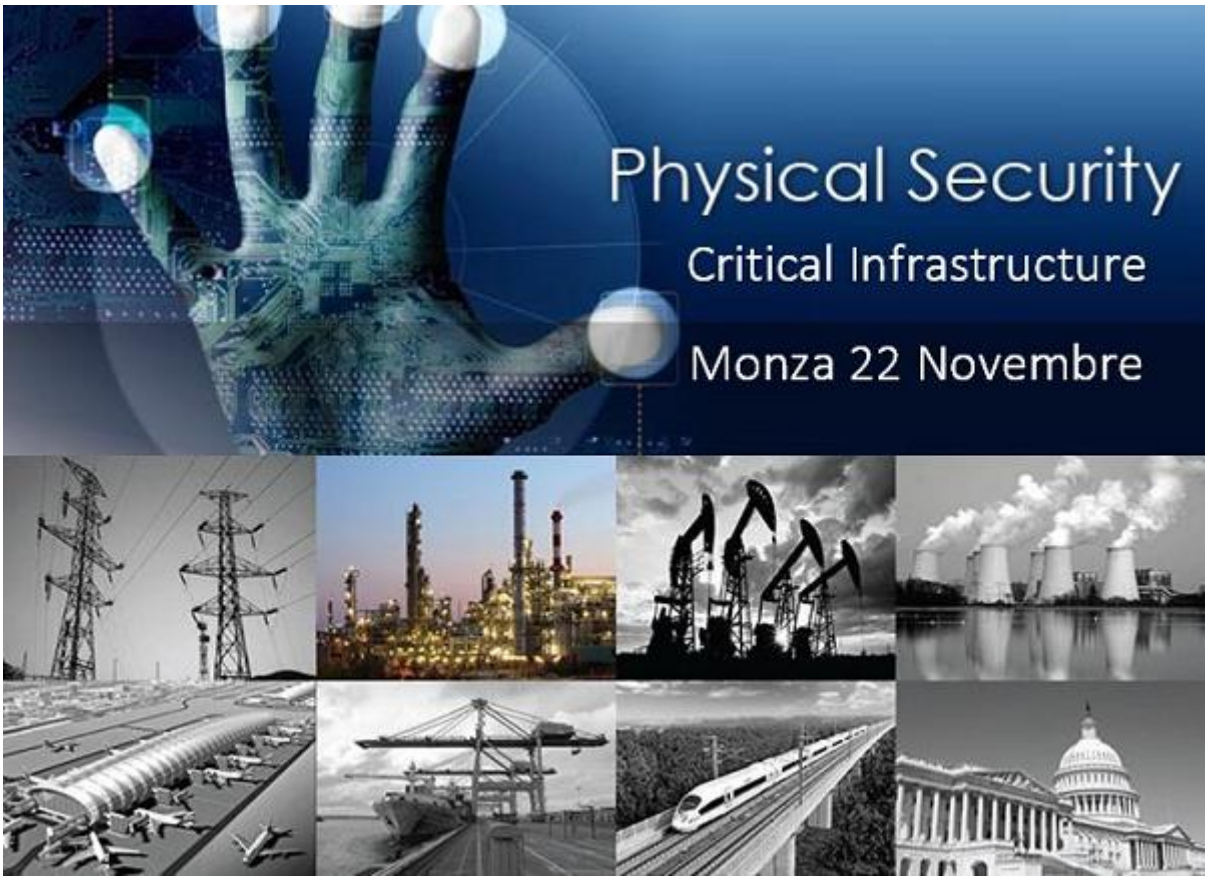
con dimostrazione live di un ATTACCO INFORMATICO

Monza, 22 novembre 2018

presso il **CENTRO CONGRESSI di ASSOLOMBARDA,**

via Petrarca 10, Monza (zona Villa Reale)

La partecipazione è **gratuita** e strutturata in un'**unica giornata** con due sessioni a tematiche diverse, **dalle 9.00 alle 13.30 e dalle 14.30 alle 17.30.**



SEMINARIO GRATUITO DI FORMAZIONE TECNICA

organizzato da **CIAS Elettronica**, **Betafence Italia** e **Spark Security** in collaborazione con **NCP Italy Srl (Networking Competence Provider)**

CON IL PATROCINIO ALL'EVENTO DELLE ASSOCIAZIONI DI SETTORE

AIIC (Associazione Italiana esperti in Infrastrutture Critiche)

A.I.PRO.S. (Associazione Italiana Professionisti Sicurezza)

A.I.P.S. (Associazione Installatori Professionali Sicurezza)

AIPSA (Associazione Italiana Professionisti Security Aziendale)

ASSISTAL (Associazione Nazionale Costruttori di Impianti e dei Servizi di Efficienza Energetica - ESCo e Facility Management - CONFINDUSTRIA)

ASSOSICUREZZA (Associazione Nazionale Costruttori e Distributori di Sistemi di Sicurezza)

RIFS (Rete Installatori Forum Sicurezza)

EVENTO RICONOSCIUTO

CERSA – Organismo di certificazione riconosce **4 Crediti Formativi** per seminari, convegni e conferenze promossi da CIAS Elettronica in base a quanto previsto dagli schemi di certificazione di riferimento, ai fini del mantenimento e rinnovo della certificazione "**Professionista della Security**" – **UNI 10459** delle figure professionali certificate

evento riconosciuto

TÜV Italia riconosce l'attribuzione di **4 Crediti Formativi**, validi ai fini dell'aggiornamento formativo richiesto dallo schema **CEI "Esperti di impianti di allarme, intrusione e rapina".**

A TUTTI I PARTECIPANTI VERRÁ RILASCIATO ATTESTATO DI FREQUENZA

valido per la richiesta dei crediti formativi

RICHIESTO RICONOSCIMENTO

Il riconoscimento di **6 CFP** al presente evento è stato richiesto all'**Ordine degli Ingegneri di Monza e Brianza**, che ne valuterà i contenuti formativi professionali e le modalità di attuazione

Il riconoscimento di **6 CFP** al presente evento è stato richiesto **all'Ordine dei Periti Industriali e dei Periti Industriali Laureati della Provincia di Monza e Brianza**, che ne valuterà i contenuti formativi professionali e le modalità di attuazione

CONTENUTI

Il seminario sarà rivolto a **Security Manager, IT manager, amministratori di rete, responsabili di CED e tecnici IT** nonché di interesse per **network design, system integrators** e chiunque altro abbia il bisogno di acquisire valide competenze nel settore della sicurezza.

Oggi, infatti, la rete è un asset ormai fondamentale per ogni azienda e il tema della sicurezza della rete è sentito in modo prioritario. Il seminario mira ad evidenziare **le problematiche di sicurezza delle reti** suggerendo le **migliori soluzioni** da attuare al fine di proteggersi da accessi e utilizzi indesiderati e/o malevoli.

Durante l'incontro formativo verranno trattati nello specifico gli argomenti relativi alla **sicurezza** delle **reti LAN** e delle **reti WiFi** e dell'**accesso Internet**, integrando alla teoria una dimostrazione dal vivo di un **reale attacco informatico** ad un sistema di videosorveglianza IP con l'obiettivo di mostrare gli strumenti e le tecniche degli **hacker professionisti**. Verranno altresì illustrate le soluzioni IP specifiche per le **Infrastrutture Critiche secondo la direttiva 114/2008CE e la normativa EN50151 e CEI 73-3.**

PROGRAMMA DEL CORSO

9.00 – 9.30: Registrazione Partecipanti

9.30 – 9.45: Introduzione ai lavori e saluti delle Associazioni di Settore

09.45 – 13.00: Prima sessione (formatore **Dott. Giuseppe Tetti** – NCP Italy)

Introduzione

- I principi della sicurezza informatica
- Autenticazione, Riservatezza, Integrità, Disponibilità
- Modelli e approcci concreti

La sicurezza nelle reti LAN

- Meccanismi di Layer 2 switching
- Realizzare una rete dotata di adeguati requisiti di sicurezza
- Disponibilità del servizio: ridondanza e Spanning Tree Protocol
- Tecniche di "port aggregation" per la ridondanza di link paralleli
- Rouge switch e loro isolamento: BPDU Guard
- Controllo dei fenomeni di broadcast storming
- Prevenzione degli attacchi di MAC Flooding: tecniche di port-security
- Accesso autorizzato agli switch di rete: lo standard 802.1x
- Tecniche di isolamento degli utenti: protected port
- Tecniche di isolamento dei gruppi: VLAN
- VLAN Hopping, MAC Spoofing, DHCP Snooping
- Attacchi Manin the Middle con ARP Poisining e Tecniche di mitigazione con Dynamic ARP Inspection

La sicurezza nelle reti WiFi (prima parte)

- Caratteristiche delle reti wireless
- Controllo della copertura: gestione delle frequenze e attenzione alle interferenze
- Utilizzo dei WLAN Controller
- Roaming e QoS
- Punti deboli nello standard 802.11
- Scanning attivo e passivo
- SSID Broadcasting e policy di buon senso

13.00 – 13.30:

- Soluzioni full IP per le infrastrutture critiche secondo la direttiva 114/2008CE, la normativa EN50151 e 73-3 (**CIAS Elettronica**)
- Dalla protezione elettronica alla protezione fisica per una sicurezza a 360° delle Infrastrutture Critiche (**Betafence Italia**)
- L'Intelligenza Artificiale a servizio del controllo perimetrale: quali vantaggi (**Spark Security**)

13.30 – 14.30: Fast lunch

14.30 – 15.45: Seconda sessione formativa

La sicurezza nelle reti WiFi (seconda parte)

- Accesso non autorizzato e tecniche di autenticazione
- MAC Filtering
- Lo standard 802.11x

- Intercettazione delle comunicazioni
- Algoritmi di cifratura
- Gli algoritmi WEP/WPA/WPA2
- AP overloading e tecniche di flooding
- Rogue e Fake AP

Accesso a Internet

- Scelta della tipologia di accesso
- Collegamenti e ISP ridondati
- Protezione mediante Firewall
- Tecniche di packet inspection
- Utilizzo dei proxy
- NAT traversal e applicazioni Cloud
- Accedere alla rete in modo sicuro: le VPN e il protocollo IPsec
- Sonde IPS/IDS e sistemi di logging
- Attacchi DDos, e il servizio di cleaning del traffico
- Monitoring proattivo: l'utilizzo del protocollo SNMP

15.45 – 16.30: "Cyber Security: novità e strategie di Cisco Systems." (**Dott. Mauro Fattori** – Cyber Security Consulting Systems Engineer – Cisco Systems)

Ore 16.30 – 17.15: "Hacker in azione. Live!!" (**Dott. Francesco Tornieri** – Cultore della materia presso l'Università Cattolica del sacro Cuore e membro del ISSA e ISECOM)

Dimostrazione dal vivo di un attacco informatico portato ad un sistema di videosorveglianza consumer. Saranno mostrate ed eseguite in tempo reale le principali tecniche e gli strumenti tipici di un hacker professionista per la violazione di sistemi di sicurezza ICT.

Ore 17.15 – 17.30: chiusura lavori e discussione

I PARTNERS

Errore. Riferimento a collegamento ipertestuale non valido. **Errore. Riferimento a collegamento ipertestuale non valido.** **Errore. Riferimento a collegamento ipertestuale non valido.** **Errore. Riferimento a collegamento ipertestuale non valido.**

IL MEDIA PARTNER

Errore. Riferimento a collegamento ipertestuale non valido.

ISCRIZIONE

on line sul sito cias: http://www.cias.it/news-ed-eventi/

Per informazioni scrivere a: eventi@cias.it