Programma*

Mercoledi 15 Novembre 2023

12:00 – 12:30 – Tips

Essential Toolkit for Cyber Security Risk Management

Verranno forniti gli strumenti chiave di analisi del rischio informatico in un'ottica di nuovi modelli e framework per valutare l'esposizione al rischio di una impresa.

- Approcci e strumenti per il Cyber Risk Assessment: Come valutare l'esposizione ai rischi Cyber di un'impresa?

15.00 – 16.00 – Talk

SICUREZZA IT / OT: Integrazione, Convergenza e Resilienza nella sicurezza industriale e l'integrazione tra sicurezza fisica e logica

La convergenza e l'integrazione tra tecnologia dell'informazione (IT) e tecnologia operativa (OT) è sempre piu un aspetto di particolare rilevanza che coinvolge i processi industriali e il settore produttivo. L'evoluzione dei sistemi da questo punto di vista comporta notevoli vantaggi e allo stesso tempo rischi di sicurezza che devono essere gestiti se le aziende vogliono proteggere le proprie risorse dagli attacchi informatici.

Ne parleremo con i maggiori esperti di questo settore e con le imprese industriali e manifatturiere che hanno affrontato questo aspetto con scelte di successo.

- I vantaggi dell'integrazione della sicurezza fisica e la Cyber Security

*programma provvisorio ad uso interno

business international
The Executive Network

SICUREZZA
INTERNATIONAL SECURITY & FIRE EXHIBITION

Giovedi 16 novembre 2023

10.00 – 11.30 – Talk

Il quadro in continua evoluzione della situazione geopolitica internazionale e il panorama degli attacchi espone il nostro Paese ad una escalation di minacce, in particolare dal fronte informatico. Oggi, gli attacchi cyber sono diventati la quotidianità e le preoccupazioni rispetto a questo tema restano fra le priorità della security (fisica e digitale), tanto che il PNRR prevede importanti investimenti in presidi e competenze di cybersecurity e fondi per la ricerca.
Ne parleremo in questo evento con i referenti istituzionali del Ministero della Difesa e dell'ACN-Autorità nazionale per la cybersicurezza, principali esperti di geopolitica e di Cyber security e con i C-level delle principali aziende rappresentanti delle infrastrutture critiche italiane.

10:00 Saluto di Benvenuto
Relatore da definire, Fiera Milano

10:10 CYBER CRIME: Le nuove frontiere della cybersecurity nazionale e internazionale. Il ruolo delle aziende e delle istituzioni

- La nuova situazione geopolitica e il panorama degli attacchi: l'escalation della minaccia informatica
- Scenari internazionali e interventi urgenti per alzare il livello di difesa del Paese e creare un sistema di sicurezza unico e integrato
- La sicurezza delle infrastrutture critiche nazionali
- Lo sviluppo e il rafforzamento della cybersecurity in Italia e i primi investimenti del PNRR
- I Trend dell'innovazione digitale e l'impatto sui modelli di sicurezza

11:30 Chiusura dei lavori

12.00 – 12.40 – Tips

Durante gli interventi saranno illustrate le principali tendenze degli attacchi Cyber sulla base delle più recenti analisi di settore a livello nazionale e internazionale (come il White Hat 2023) e a seguire verranno presentati una serie di casi, anche di pubblico dominio, dove apprendere a pieno il concetto di Lesson Learned nella Cyber Security ed imparare dagli errori degli altri a tutelarsi.

- **HACKER TRENDS: le minacce più attuali e come proteggersi**
- **LESSON LEARNED nella Cybersecurity**

15:00 – 16:00 – Talk

ARTIFICIAL INTELLIGENCE: La nuova frontiera del cyber

Diventano sempre piu ampie le applicazioni pratiche e le opportunità di sfruttare l'Intelligenza Artificiale. Tra le maglie di queste innovative frontiere digitali però si intravede il rischio Cyber che queste opportunità potrebbero comportare. In questo incontro i maggiori esperti specialistici si confronteranno sul futuro e sull'impatto nel business delle «emerging technologies» che stanno rivoluzionando il nostro modo di vivere e lavorare offrendo spunti per una analisi degli strumenti offerti dalla Cyber Threat Intelligence.

- AI: Quali sono le opportunità, i rischi e come prevenirli
- Strumenti e strategie di Cyber Threat Intelligence
- Blockchain e Cybersecurity

*programma provvisorio ad uso interno

Venerdi 17 Novembre 2023

10:00 – 11:00 – Talk

CYBER SECURITY COMPLIANCE: i nuovi adempimenti introdotti dalle recenti evoluzioni normative italiane ed europee ed i riflessi organizzativi, procedurali e tecnologici

La continua evoluzione del quadro normativo e i relativi adempimenti che questi introducono rendono sempre più prioritario affrontare il tema della Cyber Security Compliance. L'evento raccoglie i contributi dei principali esperti di settore di taglio legale che mostreranno e daranno indicazioni ai partecipanti su come allineare le procedure e le eventuali tecnologie a supporto per rendere la propria organizzazione veramente compliant.

Quali sono le novità introdotte dalle normative internazionali come il Cyber Resilience Act nel campo del software e la normativa DORA nel settore finanziario?

Numerose sono le normative che impattano sulle aziende (GDPR, 231, ecc) quali sono gli adempimenti richiesti e le criticità da affrontare per l'adeguamento?

Cosa cambia per le aziende italiane? Come è possibile organizzare la propria azienda per essere compliant

12:00 – 12.40 – Tips

Quali sono i rischi e i danni che può provocare una inefficace gestione della cybersecurity nell'ecosistema SMART CITY e SMART BUILDING

Con lo sviluppo delle applicazioni e le opportunità offerte dalla digitalizzazione dei sistemi domotici e di controllo le Smart City e gli edifici forniti di questo tipo di sistemi innovativi sono sempre piu esposti ai rischi cyber trattandosi di tecnologie e applicazioni in rete che possono presentare diverse vulnerabilità dal punto di vista della Cybersecurity.

Gli edifici intelligenti si basano su innumerevoli sensori IoT e server collegati in Internet per automatizzare funzionalità come il controllo dell'illuminazione, del clima e degli ascensori, il rilevamento degli incendi, la videosorveglianza e l'accesso tramite badge.

Innovazione e sicurezza devono necessariamente procedere allineati. Ne parleremo con i maggiori esperti di settore da punto di vista della progettazione e delle tecnologie di protezione disponibili.

- Sicurezza Urbana, Smart City e Smart Building: I nuovi paradigmi per lo sviluppo di sistemi integrati e intelligenti
- La vulnerabilità dei Sistemi domotici: punti critici degli smart building in un'ottica di Cyber Security
- Come mettere in sicurezza telecamere di videosorveglianza e i sistemi di domotica integrata

15.00 – 16.00 – Talk

Lo sviluppo della CYBER AWARENESS

L'anello debole di qualsiasi catena di sicurezza è rappresentato dagli esseri umani. Il social engineering cerca di sfruttare questa debolezza facendo leva sugli aspetti psicologici del comportamento umano, come la vanità, l'avidità, la curiosità, l'altruismo, il timore nei confronti dell'autorità per spingere le persone a rivelare informazioni o consentire l'accesso a un sistema informatico. I truffatori utilizzano il social engineering in quanto è più facile spingere una persona a rivelare le proprie password rispetto all'ottenere tali informazioni mediante tecniche di hacker. Per questo motivo la creazione di consapevolezza e la sensibilizzazione su tutti questi aspetti diventa

fondamentale. Come anche la creazione di un Sistema di sviluppo delle competenze professionali in grado di supportare e prevenire eventuali criticità. Ne parleremo con i principali esponenti delle categorie di settore ed enti specializzati.

- Cos'è il Social Engineering e come prevenirlo
- Il ruolo della formazione e l'addestramento in ambito Cybersecurity