Cyber Security Arena

Nuovi trend per la Sicurezza: Come difendersi dai cyberattachi?

15-17 Novembre 2023 @ SICUREZZA – Fiera Milano Rho

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.

Secondo il *WEF Global CyberSecurity Outlook 2023* l'intelligenza artificiale (AI) e l'apprendimento automatico (20%), la maggiore adozione della tecnologia cloud (19%) e i progressi nella gestione dell'identità e dell'accesso degli utenti (15%) sono i fattori che avranno più peso sulle scelte e le strategie di gestione di rischio informatico nei prossimi due anni.
Il 43% dei leader aziendali ritiene probabile che, nei prossimi due anni, un attacco informatico colpisca materialmente la propria azienda e questo rende fondamentale il presidio e monitoraggio real time dei possibili attacchi.

Tutti i principali studi ed osservatori confermano la crescita degli attacchi cyber, ulteriormente accelerato dal rapidissimo trend di sviluppo tecnologico della digitalizzazione che ha esposto il nostro paese, le aziende e tutti i cittadini a rischi cyber molto sfidanti. Tuttavia responsabili della sicurezza, CISO e vertici d'azienda anche se oggi comunicano in modo più diretto e più frequente, continuano a parlare lingue diverse.
La sicurezza è un ecosistema e la cultura della sicurezza si crea anche attraverso la realizzazione di iniziative formative volte da un lato alla sensibilizzazione dell'utente finale e dall'altro alla creazione di skill specialistiche altamente professionali per potenziare il valore dei nostri giovani talenti e per aumentare, estendere o evolvere le competenze di reskilling di alcuni tipi di figure professionali senior.

L'edizione 2023 di Fiera Sicurezza vedrà protagonista nuovamente la **Cyber Security Arena**, ideata e sviluppata da Business International – Fiera Milano con l'obiettivo di fornire una visione ampia sugli scenari futuri della Cyber Security in azienda. L'Arena ospiterà ogni giorno i **Cyber Security Talks** incontri di approfondimento con esperti di settore che daranno la propria visione sui principali trend del settore ed i **Cyber Security Tips**, momenti formativi di breve durata con consigli e suggerimenti da mettere subito in pratica.

I principali argomenti al centro del dibattito di Cyber Security Arena 2023:

- La nuova situazione **geopolitica** e il panorama degli attacchi
- Lo **sviluppo** della cybersecurity in Italia e i primi investimenti del PNRR
- I **Trend** dell'innovazione digitale e l'impatto sui modelli di sicurezza
- Approcci e strumenti per il **Cyber Risk** Management: Come valutare e misurare l'esposizione ai rischi di un'impresa?
- Cyber Security **Compliance** i nuovi adempimenti introdotti dalle recenti evoluzioni normative italiane ed europee ed i riflessi organizzativi, procedurali e tecnologici
- Lo sviluppo di **Cyber Awareness**: il ruolo della formazione e addestramento in ambito Cybersecurity
- Cybersecurity & **Data Protection**: Comprendere l'importanza della protezione dei dati e come attuare strategie mirate
- I temi di frontiera del cyber: **AI e Blockchain**
- Creare consapevolezza sui danni che può provocare una inefficace gestione della cybersecurity nell'ecosistema delle Smart City e dello Smart Building

*programma provvisorio ad uso interno

Programma*

Mercoledì 15 Novembre 2023

INNOVAZIONE

14:30 – 15:00 – Tips

Essential Framework 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?

Speaker:
Greta Nasi, Director of the Master of Science in Cyber Risk Strategy and Governance, Università Bocconi e Politecnico di Milano

INNOVAZIONE

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 più 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, 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

Modera: **Greta Nasi**, Director of the Master of Science in Cyber Risk Strategy and Governance, Università Bocconi e Politecnico di Milano

Speaker:
Alessandro Manfredini, Presidente, AIPSA
Gabriele Faggioli, Presidente, Clusit
Michele Fabbri, Cyber Security Group Director, CISO, De Nora

*programma provvisorio ad uso interno

Giovedì 16 novembre 2023

INNOVAZIONE

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 e del Copasir, principali esperti di geopolitica e di Cyber security e con i C-level delle principali aziende rappresentanti delle infrastrutture critiche italiane.

10:00 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

Modera: **Alessia Valentini**, Giornalista, Tech Writer and Cybersecurity Advisor

Speaker:
Matteo Perego di Cremnago, Sottosegretario alla Difesa con delega alla Cybersecurity, Ministero della Difesa
Bruno Frattasi, Direttore Generale, ACN
Lorenzo Guerini, Presidente, Copasir
Giuseppina Di Foggia, Amministratore Delegato, Terna

11:30 Chiusura dei lavori

*programma provvisorio ad uso interno

INNOVAZIONE

12.00 – 12.20 – 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.

LESSON LEARNED nella Cybersecurity
Stefano Fratepietro, Ceo, Tesla Consulting e Cso, Be Shaping the Future

INNOVAZIONE

14:30 – 15:30 – Tips

ARTIFICIAL INTELLIGENCE: La nuova frontiera del cyber

Diventano sempre più 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

Speaker:

L'intelligenza artificiale è sicura?
Fabio Roli, Professor of Computer Engineering Professor of Computer Engineering, Università degli Studi di Genova

BLOKCHAIN: Il paradigma innovativo nell'elaborazione delle informazioni
Francesco Bruschi, Head at Blockchain & Distributed Ledger Observatory, Politecnico di Milano

*programma provvisorio ad uso interno

business international
The Executive Network

SICUREZZA
INTERNATIONAL SECURITY & FIRE EXHIBITION

Venerdì 17 Novembre 2023

NORMATIVE

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

Speaker:
Marco Soffientini, Avvocato esperto di Privacy e Diritto delle Nuove Tecnologie
Paolo Di Serio, Head of Product Cyber Resilience, Leonardo
Andrea Lisi, Avv. e titolare, Studio Legale Lisi, Presidente, ANORC professioni, e Componente del Comitato di Esperti presso il Sottosegretariato alla Presidenza del Consiglio con delega all'innovazione tecnologica

INNOVAZIONE

11.00 – 12.00 – 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.

- Hacker Trends le minacce più attuali e come proteggersi
- Cos'è il Social Engineering e come prevenirlo
- Il ruolo della formazione e l'addestramento in ambito Cybersecurity

*programma provvisorio ad uso interno

Speaker:

Alvise Biffi, Vice Presidente, Assolombarda con delega a Organizzazione, Sviluppo e Marketing Presidente Futurenext e CEO Secure Network e Banksealer
Giulio Iucci, Presidente, Anie Sicurezza
Leonardo Querzoni, Professore Associato Dipartimento di Ingegneria Informatica Automatica e Gestionale Antonio Ruberti, Università degli Studi di Roma "La Sapienza" e Presidente, CYBER 4.0 - Cybersecurity Competence Center

INNOVAZIONE

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

Stefano Panzieri, Professore Ordinario Dipartimento di Ingegneria civile, informatica e delle tecnologie aeronautiche, Università degli Studi "Roma Tre"

*programma provvisorio ad uso interno