22° Forum ICT Security

23 e 24 ottobre 2024, Roma

23 Ottobre 2024

08:00 - 09:00
Welcome Coffee and Networking

09:00 - 09:10
Saluto di Benvenuto di **Bruno Frattasi**, Direttore Generale dell'Agenzia per la cybersicurezza nazionale

09:10 - 09:30
Luca Tagliaretti, Executive Director, European Cybersecurity Competence Center (ECCC)

09:30 - 10:20
Cloud Security e Zero Trust: Una strategia integrata per gestire la cyber-resilienza delle organizzazioni

Con l'accelerazione della digitalizzazione (digital transformation), sempre più abilitata dall'adozione di tecnologie cloud, le organizzazioni si trovano di fronte alla necessità di proteggere ecosistemi di dati, asset, applicazioni e servizi sempre più complessi, interconnessi e distribuiti.
I relatori condivideranno esperienze pratiche e best practice su come implementare architetture Zero Trust in ambienti cloud privati, ibridi e multi-cloud. Verrà in particolare analizzata l'importanza di una progettazione basata sull'analisi continua del rischio e gestione identità (umane e non) e come le soluzioni ML/GenAI possano essere utilizzate per migliorare le azioni di monitoraggio, analisi minacce e difesa da attacchi sempre più rapidi e sofisticati.

- **Giovanni Ciminari**, Head of Cybersecurity in Sogei;
- **Matteo Macina,** CISO TIM - ok foto e bio aggiornate
- **Alessandro Menna**, Chief Security Officer di Italgas
- **Andrea Licciardi***, Cybersecurity Manager di Tecnimont

Moderatore: **Alberto Manfredi**, Cofondatore e Presidente, CSA Italy

10:20 - 10:40
Come Creare Malware e Difendersi con il Modello Zero Trust

In un mondo in cui chiunque, grazie anche all'intelligenza artificiale, può creare malware efficaci, esiste comunque un modo per proteggersi. Partendo da una postura nella quale tutte le entità sono considerate non attendibili per impostazione predefinita, scopri come l'adozione dei principi di Zero Trust può mantenere al sicuro sia i tuoi dati che l'operatività, indipendentemente dai tentativi di hacking da parte umana o automatizzata.

Cristiano Guerrieri, Solution's Engineer, Threatlocker

10:40 - 11:00
Oggi tutti parlano di identificazione delle minacce, ma della remediation chi se ne occupa?
Oggi le aziende devono affrontare la sfida complessa della cyber security, che richiede una filiera 24/7 di identificazione delle minacce e mitigazione delle stesse. Il mercato sta indirizzando l'attenzione soprattutto verso una capacità di detection in grado di identificare anche le minacce più complesse. Tuttavia, è fondamentale che la risposta venga resa operativa attraverso attività di remediation efficaci. Spesso, infatti, anche le migliori identificazioni vengono ostacolate da catene del soccorso frammentate e al di sotto degli standard richiesti per mitigare le minacce in modo adeguato.
Veronica Leonardi, CMO & Investor Relator di Cyberoo

11:00 - 11:40 → **Coffee Break and Networking**

11:40 - 12:00
Strategia dei Dati e Intelligenza Artificiale. Il nuovo Ordine (economico e giuridico) del Mercato
Valeria Falce, Jean Monnet Professor in Digital Transformation and AI Policy - Professore ordinario di Diritto dell'economia nell'Università Europea di Roma

12:00 - 12:20
Generative AI's Emerging Disruption of Cybersecurity
Artificial Intelligence stands to be the most significant technology in history. In this presentation, Jim Reavis, founder of Cloud Security Alliance and its AI Safety Initiative, discusses Generative AI and how it will fundamentally transform cybersecurity in a few short years. Jim will provide the perspective of attackers, defenders and policy makers and outline the key steps industry must take to combat the risks and leverage the opportunities of Large Language Models and other forms of Generative AI.
Jim Reavis, CEO of the Cloud Security Alliance

12:20 - 12:40
Machine Learning e Homomorphic Encryption: Il Futuro dell'Intelligenza Artificiale Privacy-Preserving
In uno scenario tecnologico e scientifico in cui la privacy dei dati assume un'importanza crescente, la capacità di processare dati criptati tramite l'Intelligenza Artificiale rappresenta la nuova frontiera tecnologica e l'anello mancante che elimina il bisogno di decriptare i dati per elaborarli, permettendo di costruire pipeline di memorizzazione, trasmissione ed elaborazione realmente capaci di garantire le privacy. Questo intervento esplorerà il futuro dell'Intelligenza Artificiale applicata a dati e modelli criptati, evidenziando le potenzialità offerte dalla combinazione di soluzioni avanzate di machine e deep learning con sistemi di Homomorphic Encryption. L'obiettivo è illustrare come queste tecnologie possano garantire un ambiente privacy-preserving senza compromettere l'efficacia e la potenza dell'AI.
Manuel Roveri, Professore Ordinario del Politecnico di Milano e Co-founder di Dhiria s.r.l.

12:40 - 13:00
Allarme Data Breach: 7 attacchi su 10 in EMEA hanno rubato i tuoi dati. Attenzione anche alle minacce interne!

L’aumento dei data breach globali, è allarmante. Nel 2023, in EMEA, ci sono stati oltre 8.300 attacchi informatici noti, di cui il 72% con data breach riusciti. In Italia, l’incremento è del 65%, contro l’11% globale.
Fattore umano critico: Il 68% delle violazioni deriva da errori umani indotti da attacchi di ingegneria sociale o negligenza. Ma cresce anche la minaccia interna: l’insiding, compiuto da dipendenti o ex dipendenti con accessi aziendali, è responsabile del 12% degli attacchi.
Gli impatti sono enormi: il costo medio globale di una violazione dei dati è di 4,45 milioni di dollari, con l’Italia all’ottavo posto (3,6 milioni di $).
L’obiettivo a cui mirano i Cyber criminali è portar via dati e informazioni sensibili per chiedere un riscatto o bloccare la continuità del business, mettendo in ginocchio le aziende colpite, che sempre più spesso, sono PMI senza strumenti idonei a difendersi.
Prevenire l’errore umano è il primo passo per difendersi. Remotegrant, con l’approccio Zero Trust e il modello sandbox, protegge efficacemente i pc e i dati aziendali da minacce interne ed esterne, impedendo la data exfiltration. Nel corso dell’intervento approfondiremo casi concreti per industry, perché oggi nessun settore è immune al rischio cyber.
Valerio Pastore, Founder di Cyber Grant Inc

13:00 - 13:20
Come sfruttare l'intelligenza artificiale nel ciclo OSINT
Dario Beniamini, Senior Solutions Consultant at NUIX, CEO and Co-Founder of Intellexia Srls, and an instructor of SEC497 Practical Open-Source Intelligence at SANS Institute

13:20 - 14:20 → **Lunch and Networking**

14:20 - 14:40
Sovranità digitale & Intelligence
Come soddisfare la compliance delle nuove normative europee come NIS 2 e DORA e garantire la sovranità digitale delle proprie informazioni ed infrastrutture.
Le soluzioni di Cyber Threat Intelligence Cerbeyra e l'ecosistema VIANOVA per la sicurezza ed il controllo delle informazioni e delle infrastrutture ICT delle organizzazioni.
Francesco Arruzzoli, Responsabile Centro Studi, Cerbeyra

14:40 - 15:00
Verso un Computing Continuum (IoT, Edge, Cloud e Dataspaces) sicuro
Il Computing Continuum è intrinsecamente caratterizzato da un elevato grado di eterogeneità e di decentralizzazione, il che – oltre a generare complessi problemi di interoperabilità e di scalabilità – porta ad un allargamento significativo della superficie di attacco globale. Affinché il Computing Continuum sia effettivamente utilizzabile in contesti reali, occorre costruire dei meccanismi affidabili, che consentano di raggiungere livelli di fiducia soddisfacenti in tutte le zone che lo compongono: l’IoT, l’Edge, il Cloud e i Dataspaces. Il talk presenta quello che si potrebbe definire un approccio di tipo “best effort” alla sicurezza del Computing Continuum. Da un punto di vista concettuale, l’approccio si basa sull’estensione/adattamento del paradigma del Trusted Computing al nuovo contesto operativo. Viene presentata anche un’architettura concettuale, in cui l’approccio proposto è implementato mediante un framework di servizi, strumenti e tecniche che possono essere composti dinamicamente ed in maniera flessibile.
Luigi Romano, Prof. Ordinario Sistemi per l'Elaborazione dell'Informazione, Università degli Studi di Napoli Parthenope – Presidente Centro Regionale Information

Communication Technology (CeRICT)

15:00 - 15:50
Sanità digitale e PNRR, il ruolo delle sicurezza informatica e delle nuove tecnologie
La digitalizzazione della sanità italiana, spinta dal PNRR, apre un mondo di possibilità ma anche di sfide. Il panel si addentrerà in questo terreno complesso, esplorando come le nuove tecnologie si intrecciano con le normative vigenti. Verrà discusso come rendere i sistemi sanitari più interconnessi, garantendo al contempo la sicurezza dei dati sensibili dei pazienti e si esaminerà il ruolo dell'intelligenza artificiale nei diversi ambiti di applicazione, considerando le implicazioni etiche e legali. Si affronteranno le questioni legate al cloud computing e alla protezione dei dati personali in un contesto sanitario sempre più globalizzato e non mancherà un'analisi della telemedicina e di come l'identità digitale stia cambiando l'accesso ai servizi sanitari. Infine, gli interventi esploreranno le sfide poste dall'Internet of Medical Things, dove dispositivi medici connessi richiedono nuovi approcci alla sicurezza e alla privacy.
L'obiettivo del panel è tracciare un percorso che bilanci l'innovazione tecnologica con la tutela dei diritti fondamentali nel quadro della trasformazione digitale prevista dal PNRR. Un viaggio attraverso le frontiere della sanità digitale, dove tecnologia e diritto si incontrano.

- **Marco Armoni**, Associate Professor New York University - Presidente Comitato Scientifico Ente Nazionale per la Trasformazione Digitale presso la Presidenza del Consiglio dei Ministri;
- **Mario A. Bochicchio**, Università di Bari, CINI Digital Health National Lab;
- **Matteo Lucchetti**, Direttore Cyber 4.0;
- **Matteo Montesi,** Direttore UOC Sistemi ICT dell'ASL Roma 3;
- **Mauro Moruzzi**, Dipartimento per la Trasformazione Digitale presso la Presidenza del Consiglio dei Ministri - Program Manager per l'organizzazione dei servizi di Sanità Digitale;
- **Luca Nicoletti**, Capo del Servizio Programmi Industriali, tecnologici, di ricerca e formazione di ACN;

Moderatrice: **Stefania Stefanelli**, Avvocata e Professoressa associata di diritto privato nell'Università degli studi di Perugia

16:00 → **Chiusura dei Lavori della prima giornata**

24 Ottobre 2024

08:00 - 09:00
Welcome Coffee and Networking

09:00 - 09:10
Saluto di benvenuto

09:10 - 10:00 Tavola Rotonda

Direttive NIS 2 e CER e Regolamento DORA, Sicurezza informatica e resilienza per le infrastrutture critiche

Questa tavola rotonda approfondisce le implicazioni tecniche e strategiche dell'implementazione delle direttive NIS2 e CER e del regolamento DORA nel contesto della cybersecurity e della resilienza operativa delle infrastrutture critiche. Esperti di rilievo nel settore analizzeranno la sinergia tra queste normative, focalizzandosi sulla loro integrazione nei paradigmi di sicurezza IT/OT esistenti.
I relatori esamineranno l'evoluzione dell'architettura di sicurezza nei contesti OT caratterizzati da requisiti stringenti di safety e continuità operativa esplorando l'utilizzo di digital twin per la simulazione e validazione di contromisure in ambienti industriali complessi.
La discussione affronterà le sfide della supply chain security, analizzando strategie di gestione del rischio delle terze parti e l'impatto delle nuove normative sulle PMI integrate nelle filiere critiche. Verranno esplorate metodologie avanzate di threat intelligence sharing, con focus sulle peculiarità del settore OT e sulla necessità di framework di condivisione verticali.
Si esaminerà il ruolo delle certificazioni nel nuovo contesto normativo, valutando criticamente il loro impatto sulla responsabilizzazione degli attori coinvolti e la loro applicabilità in ambienti industriali eterogenei. Infine, si discuterà l'evoluzione della governance della cybersecurity attraverso un confronto sulle responsabilità del board e sull'importanza di programmi di formazione mirati per il top management.
Questo panel offre una prospettiva tecnica e strategica sulle sfide emergenti nella protezione delle infrastrutture critiche, delineando un approccio olistico alla resilienza cibernetica nell'era della convergenza normativa e tecnologica.

- **Luisa Franchina**, presidente dell'Associazione Italiana esperti in Infrastrutture Critiche
- **Rocco Mammoliti**, Chief Information Security Officer del Gruppo Poste Italiane
- **Ivan Monti**, Chief Information Security Officer (CISO) di Ansaldo Energia
- **Yuri Rassega**, CISO di Enel;

Moderatrice: **Paola Girdinio**,Presidente del Centro di Competenza START 4.0, Presidente dell’Osservatorio Nazionale per la Cyber Security, Resilienza e Business Continuity dei Sistemi Elettrici - Professore Ordinario di Elettrotecnica presso la Facoltà di Ingegneria dell'Università degli Studi di Genova.

10:00 - 10:20

Security Twin e Dati Sintetici per la resilienza di un’infrastruttura ICT/OT

Le infrastrutture critiche sono bersagli attraenti perché la riduzione dei loro servizi comporta impatti sociali, economici e potenziali turbolenze sociali. La scoperta proattiva delle intrusioni è fondamentale per anticipare e gestire il rischio complessivo. Il principale problema posto dalla proattività è l’obsolescenza dei dati sulle intrusioni provocata dalla rapida e continua evoluzione delle infrastrutture, dalle nuove strategie di attacco, e dalla continua scoperta di vulnerabilità. Questa dinamicità impedisce di formulare previsioni mediante dati storici. Un security twin è un modello digitale della infrastruttura specializzato per analisi di sicurezza. L'integrazione del security twin e del twin della minaccia permette di simulare in modo accurato le intrusioni generando proattivamente dati sintetici accurati ed aggiornati sulle intrusioni. Questi dati sono la base per una gestione proattiva del rischio.
Fabrizio Baiardi, Professore ordinario di informatica presso il Dipartimento di Informatica dell'Università di Pisa dove coordina il gruppo di ICT risk assessment &

management

10:20 - 10:40
Test di sicurezza avanzati: La sicurezza va oltre la compliance
Con il crescente impatto di normative come NIS2 e il Cybersecurity Act, sul mercato del software aumenta il rischio che le richieste di conformità sovrastino gli sforzi per la sicurezza. La conformità fornisce una base essenziale, ma la vera sicurezza richiede un approccio proattivo e tecniche di test avanzate. In questo intervento, discuteremo di questo rischio in relazione a SAST (Static Application Security Testing), un controllo di sicurezza fondamentale ampiamente utilizzato nell'industria.
Luca Compagna, Security Researcher

10:40 - 11:00
Gestione Continua dell'Esposizione alle Minacce, un approccio strategico alla Cybersecurity
Nel panorama in continua evoluzione della cybersecurity, l'alleanza strategica tra Skybox e Itway segna l'inizio di una nuova era del Continuous Threat Exposure Management (CTEM). Questa collaborazione sfrutta le avanzate capacità di gestione della visibilità e dell'esposizione al rischio di Skybox, potenziate dalla sua robusta intelligence sulle minacce, per fornire una protezione senza precedenti alle organizzazioni. Integrando i servizi professionali di Itway, Skybox offre una visibilità completa degli ambienti di rete complessi, permettendo alle organizzazioni di identificare, prioritizzare e risolvere efficacemente le vulnerabilità. Attraverso l'uso dell'intelligence avanzata sulle minacce di Skybox, le aziende possono prevedere le potenziali minacce e mitigare i rischi in tempo reale. Questo intervento esaminerà come la collaborazione tra Skybox e Itway fornisca alle organizzazioni gli strumenti necessari per rafforzare le loro difese, garantendo un'infrastruttura digitale resiliente e sicura.
Angelo Salice, Manager Cyber Security & Resiliency, Itway
Alessio Fasano, Country Manager, Skybox

11:00 - 11:40 → **Coffee Break and Networking**

11:40 - 12:00
Protezione avanzata, Bitdefender Gravityzone piattaforma integrata per la gestione del rischio.
Negli ultimi anni, la sicurezza degli endpoint ha subito notevoli progressi per combattere minacce emergenti altamente sofisticate,nonché per affrontare crescenti ostacoli operativi come personale limitato e tempo eccessivo speso dagli analisti.
Tuttavia, affidarsi esclusivamente alla protezione di endpoint protection non è più sufficiente, è necessaria una vera e propria piattaforma integrata di gestione del rischio. Gli attaccanti informatici mirano e sfruttano i punti deboli derivanti da configurazioni errate degli endpoint e applicazioni vulnerabili, causando violazioni alla sicurezza.
I team addetti alla sicurezza devono comprendere e valutare l'impatto sui rischi, assegnare priorità e risolvere rapidamente i problemi di configurazione, comprese le nuove vulnerabilità software, per ridurre al minimo i vettori di attacco, anche in considerazione delle nuove normative e nuovi framework di sicurezza come NIS2.
La soluzione integrata di gestione del rischio di Bitdefender offre una maggiore visibilità e strumenti di rimedio automatico necessari per affrontare questi rischi. Come servizio integrato di gestione del rischio, oltre alle sue capacità di prevenzione ed XDR, Bitdefender GravityZone riduce la superficie di attacco anche nei Cloud Pubblici,

semplifica la complessità di implementazione e gestione, e fornisce visibilità e mitigazione dei rischi approfonditi, il tutto attraverso una piattaforma comune e un'unica console.
Giovanni D'Amato, Manager, Sales Engineering - South & East Europe, Bitdefender

12:00 - 12:20
Self-Sovereign Identity and Distributed Ledger Technology: Innovations in Digital Identity Management for Users and Machines
L'approccio tradizionale di gestione dell'identità, ad oggi diffuso nella grande maggioranza degli scenari in cui è richiesta la mappatura informativa di asset umani o organizzativi o tecnologici, presenta documentati e documentabili rischi per la privacy, vulnerabilità CIA a più livelli e inefficienze spesso dovute anche a mancanza di adeguata formazione del personale. La ricerca di soluzioni contingenti, o basate su elementi tecnologici ormai datati, si rivela inefficace, non sostenibile, e priva di caratteristiche di compliance orizzontale legal-tech. La Self-Sovereign Identity (SSI) e le architetture BlockChain Distributed Ledger Technology (DLT) based offrono un forte elemento di innovazione tecnologico/sociale per Organizzazioni e Pubbliche Amministrazioni che intendano introdurre un modello di identità digitale inedito e sfidante, all'interno di un contesto di gestione informativa oggi più che mai estremamente insidioso e di grande attualità. L'obiettivo di divulgazione selettiva degli attributi di identità, permettendo ai proprietari dei dati di scegliere quali siano disposti a condividere in circostanze specifiche, può trovare opportuna realizzazione tecnica in strumenti a disposizione by design delle architetture informative costruibili sul paradigma BlockChain. L'intervento fornirà spunti di approfondimento su temi chiave per la SSI via BlockChain, come user control & consent, security & privacy, cryptographic innovation, portability del dato, nonché una panoramica tecnologica delle architetture DLT.
Igor Serraino, Independent ICT Advisor - Java Senior - 4.0 Analyst - Cybersecurity - CBSP BlockChain - ISC2 CC

12:20 - 12:40
eIDAS_2 e la nuova conservazione digitale: l'evoluzione dei servizi trust nell'ambito dell'Unione Europea
Regolamento eIDAS ha introdotto un quadro normativo armonizzato per l'identità digitale e i servizi fiduciari nell'Unione Europea. Il 20 maggio 2024 è entrata in vigore la revisione eIDAS 2, con l'obiettivo di rafforzare ulteriormente questi aspetti. Tra le principali novità figurano il Portafoglio Digitale Europeo e nuovi servizi qualificati come l'archiviazione elettronica. CSQA, primo ente italiano accreditato per la certificazione eIDAS, possiede il know-how per il processo di certificazione dei Conservatori a Norma.
Anna Conte, Responsabile Sviluppo Servizi Digitali & Cybersecurity di CSQA
Andrea Castello, Responsabile di Schema Servizi Digitali di CSQA

12:40 - 13:00
Opentext

13:00 - 13:20
Cyber Threats 2030*
Rossella Mattioli, Network and Information Security Expert at European Union Agency for Network and Information Security (ENISA)

13:20 - 14:20 → **Lunch and Networking**

14:20 - 14:40

Quando i computer quantistici romperanno la nostra crittografia?

I computer quantistici rappresentano una minaccia imminente per la crittografia asimmetrica attuale, tra cui RSA2048 e ECC256. Negli ultimi anni, abbiamo visto emergere quantum computer accessibili tramite il cloud, segnando un progresso significativo in questo campo. Tuttavia, i computer quantistici odierni non sono ancora sufficientemente avanzati per eseguire il software necessario per rompere la nostra crittografia. Come possiamo prevedere quando arriverà il "quantum fallout day"? Comprendere questo momento è essenziale per adottare misure preventive efficaci. Durante questo talk, esploreremo lo stato dell'arte degli attacchi quantistici alla nostra crittografia, e discuteremo le strategie per monitorare i progressi di questa tecnologia. Inoltre, esamineremo le tecniche che possono aiutarci a proteggere i nostri dati in un futuro dominato dai computer quantistici.

Alessandro Luongo, Researcher in quantum algorithms at CQT (Centre for Quantum Technologies)

14:40 - 15:00

La governance delle *quantum technologies:* sfide etiche e di policy

Le *quantum technologies* stanno rivoluzionando il mondo, aprendo nuove prospettive in settori come la farmaceutica, lo studio del clima e la finanza. Tuttavia, il potenziale computazionale senza precedenti di queste tecnologie comporta anche rischi significativi, in particolare per la cybersicurezza. I quantum computer permetteranno infatti di infrangere la crittografia attualmente utilizzata per proteggere i dati sensibili. Sebbene la *quantum resistant cryptography* possa mitigare questi rischi, è fondamentale riflettere su come le queste tecnologie possano contribuire a una società più equa e a un futuro sostenibile. Al momento, la nostra comprensione degli impatti sociali di queste tecnologie è limitata, il che rende necessario affrontare questioni come l'accesso equo alle quantum technologies specialmente nei Paesi in via di sviluppo, le implicazioni etiche e il rispetto dei diritti umani. È essenziale sviluppare un approccio responsabile a queste tecnologie che consideri attentamente i potenziali rischi e coinvolga tutte le parti interessate nel processo di sviluppo, basandosi su principi come la prevenzione dei rischi e l'inclusione.

Lorenzo Pupillo, Associate Senior Research Fellow e Head of the Cybersecurity@CEPS Initiative, Centre for European Policy Studies (CEPS)

15:00 - 15:50

Industry 5.0: Sfide e Strategie per la Cybersecurity nell'Era della Convergenza Uomo-Macchina

L'avvento dell'Industry 5.0, caratterizzato dall'integrazione delle tecnologie AI-driven e dalla collaborazione uomo-macchina, presenta opportunità straordinarie e sfide significative per la cybersecurity. Nel corso della sessione si parlerà di come garantire la gestione delle identità e degli accessi, la sicurezza di AIIoT e IIoT, oltre alla sicurezza software e hardware, senza dimenticare il ruolo dei gemelli digitali e della simulazione in tempo reale che si convertiranno in leve strategiche per la prevenzione delle minacce. In un mondo sempre più basato sui data, sarà altresì fondamentale saper: affrontare le sfide della gestione dei dati impiegati per addestrare l'AI, garantire la sicurezza della supply chain, essere conformi alla galassia normativa che è destinata ad impattare sulle organizzazioni , i.e. NIS2, Cyber Resilience Act, IEC 62443, AI Act, nuovo Regolamento Macchine, ecc.. L'obiettivo è fornire ai partecipanti gli strumenti per sviluppare strategie di cybersecurity robuste e flessibili, essenziali per navigare con successo la transizione verso l'Industry 5.0.

- **Angelo Candian**, Business Segment Manager Digital Connectivity and Power,

Siemens
- **Luca Greco**, Chief Information Security Officer, Italtel
- **Stefano Longari,** Professore presso il Politecnico di Milano e per l'Università Bocconi
- **Fabrizio Patriarca,** Senior Security Technical Specialist, IBM

Moderatrice: **Federica Maria Rita Livelli,** Business Continuity, Risk Management and Cyber Resilience Expert

16:00 → **Chiusura dei Lavori, conclusione della manifestazione**