FORUM 2024
CYBER 4.0

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

4C PER IL FUTURO PROSSIMO DELLA CYBERSICUREZZA NELLE IMPRESE ITALIANE:

Competenze, Capacità, Cooperazione, Concretezza.

KEY TAKEAWAYS DEL FORUM CYBER 4.0 2024

con il patrocinio di

Commissione europea

Ministero delle Imprese e del Made in Italy

hosted by

LUISS

CIRCA 400 TRA RAPPRESENTANTI ISTITUZIONALI, PROFESSIONISTI DEL MONDO PRIVATO, ESPONENTI DI ORGANIZZAZIONI DI SETTORE, PMI, START-UP E STUDENTI HANNO PARTECIPATO IL 3 E 4 GIUGNO 2024 ALLA SECONDA EDIZIONE DEL FORUM CYBER 4.0.

L'evento, che quest'anno ha ricevuto il patrocinio della Commissione Europea e del Ministero delle Imprese e del Made in Italy, si è svolto presso il The Dome dell'Università Luiss e ha visto il coinvolgimento di oltre 60 relatori in oltre 20 sessioni di approfondimento sui temi di maggiore rilevanza per l'azione del Centro.

QUESTI I PRINCIPALI TAKEAWAYS DELL'EVENTO:

Il quadro normativo e di politiche nazionali in materia di cybersecurity è in forte evoluzione, sia in virtù dell'adozione delle numerose disposizioni normative dell'Unione Europea, tra cui spiccano: l'adozione della Direttiva NIS 2, in vigore dal 17 ottobre prossimo, la finalizzazione del Cyber Resilience Act, e l'adozione di Cyber Solidarity Act e del Regolamento DORA, ma anche la finalizzazione e la prossima adozione dell'AI Act, sia in virtù di una strutturazione sempre più articolata del quadro di cybersicurezza nazionale, che – sotto la guida dell'Agenzia di Cybersicurezza Nazionale – sta coinvolgendo un numero sempre maggiore di istituzioni e entità di settore per l'implementazione della Strategia Nazionale 2022-2026.

Rilevano in particolare, per il diretto coinvolgimento del Centro di Competenza Cyber 4.0, le azioni in carico al Ministero delle Imprese e del Made in Italy

- il rafforzamento delle competenze di cybersicurezza nazionali, a favore delle Pubblica Amministrazione – attraverso la formazione dei livelli apicali, e di incremento generale della consapevolezza pubblica – attraverso un piano di seminari su temi di attualità;

- il Piano Industria Cyber Nazionale, volto a favorire una collaborazione diretta tra ricerca e industria, lo sviluppo di start-up e PMI innovative nel territorio nazionale e il rafforzamento di competenze e professionalità di settore, anche attraverso l'azione dei centri di trasferimento tecnologico istituiti dal Ministero – tra cui Cyber 4.0.

(Per maggiori informazioni qui l'intervento della dott.ssa Eva Spina, Capo Dipartimento per il Digitale, la Connettività e le Nuove Tecnologie del MIMIT: https://www.cyber40.it/wp-content/uploads/2024/06/Eva-Spina.pdf)

Le istituzioni nazionali di riferimento lavorano a stretto contatto con gli organismi comunitari che la Commissione Europea ha istituito per gestire gli investimenti dei prossimi anni in materia di cybersecurity. A tal proposito, fondamentale è il ruolo dello European Cybersecurity Competence Center, con base a Bucarest, nell'attuazione dei programmi Digital Europe e Horizon, volte a rafforzare la capacità e la competitività dell'industria cyber in Europa. Particolare attenzione alle call in corso di assegnazione e a quelle in fase di lancio, che prevedono allocazioni per oltre 100 Mln EUR.

(https://cybersecurity-centre.europa.eu/news/new-call-proposals-under-digital-europe-programme-eur-102m-support-deployment-actions-area-2024-06-17_en).

In tema di fondi, il PNRR – e più specificamente le attività previste sotto la Missione 4, Componente 2, Investimento 2.3, "Potenziamento ed estensione tematica e territoriale dei centri di trasferimento tecnologico per segmenti di industria" – offre un'opportunità unica per imprese di ogni dimensione di co-finanziamenti a fondo perduto per supportare la transizione digitale sicura e la promozione di innovazione tramite ricerca industriale e sviluppo sperimentale. Il MIMIT, titolare della misura, ha creato un ecosistema di oltre 50 Centri di Trasferimento Tecnologico, che includono: un potenziamento significativo dell'azione degli 8 Centri di Competenza, gli European Digital Innovation Hub e i Seal of Excellence (EDIH), le European Testing Facilities, Gli European Digital Infrastructure Consortium e le Case delle Tecnologie Emergenti. La rete dei Competence Center, in particolare, racchiude 318 aziende private, 59 università ed enti di ricerca e 32 enti pubblici e ad essa è allocata circa un terzo della misura complessiva e ad essi è affidato il ruolo di guida e formazione alle imprese sulla transizione 5.0 e quello di supportare l'innovazione per la realizzazione di nuovi prodotti, processi e servizi attraverso tecnologie avanzate. Resta aperta la sfida del post PNRR, in cui si dovrà affermare una nuova governance interistituzionale nelle politiche di investimento e sostegno alle imprese.

(Per maggiori dettagli questo l'intervento della dott.ssa Donatella Proto, Dirigente UdM PNRR del MIMIT: https://www.cyber40.it/wp-content/uploads/2024/06/Sfida_innovazione_digitale_PNRR_Silvestri_Proto.pdf).

Il quadro delle minacce è in continua evoluzione e in progressivo aumento sia in termini di impatto che di numerosità degli eventi che hanno interessato organizzazioni pubbliche e private operanti nel territorio nazionale. Il Clusit rileva un aumento del 65% nel numero degli attacchi nel 2023, a fronte di un incremento globale che invece non ha superato il +12%. Le vittime sono distribuite in modo pressoché completo su tutti i settori merceologici, con una prevalenza negli ambiti Healthcare, Government, Finance e ICT e circa il 40% degli attacchi ha avuto impatti critici.
Cinque sono i megatrend che si evidenziano nel breve periodo:

- **Impatto della geopolitica:** La minaccia dei conflitti in corso e potenziali porterà ad attacchi informatici sia sponsorizzati dallo Stato sia collaterali che richiedono misure di sicurezza informatica rafforzate.

- **Tecnologie emergenti:** È diffuso il timore che l'utilizzo di tecnologie emergenti come l'intelligenza artificiale generativa, l'informatica quantistica, e l'edge computing farà avanzare rapidamente le capacità di attacchi cyber.

- **Evoluzione normativa:** Normative in evoluzione come DORA, CRA, NIS 2, AI Act e crittografia postquantistica porteranno a sfide sempre più complesse di conformità per le organizzazioni.

- **Skill Gap:** La carenza di professionisti qualificati comporta maggiore vulnerabilità agli attacchi informatici e tempi di risposta più lenti agli incidenti di sicurezza.

- **Politiche dei Costi:** Quanto evidenziato ai punti precedenti porta a un continuo aumento degli investimenti necessari, che dovranno essere bilanciati rispetto alle esigenze di consolidamento e di efficienza, portando quindi alla necessità di ridefinire le politiche dei costi aziendali.

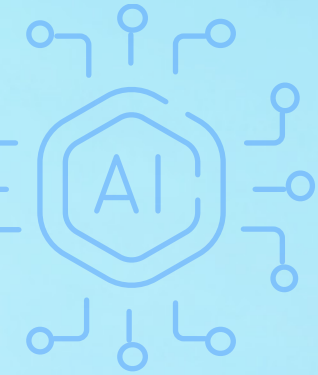
(Per maggiori dettagli questi gli interventi di Alessio Pennasilico (Clusit): https://www.cyber40.it/wp-content/uploads/2024/06/Alessio-Pennasilico.pdf e di Nicola Vaniin (Cassa Depositi e Prestiti): https://www.cyber40.it/wp-content/uploads/2024/06/Nicola-Vanin.pdf)

Nel medio-lungo periodo le previsioni al 2030 di ENISA vedono le seguenti sfide prevalenti in materia di cybersecurity, in ordine di criticità:

- **ATTACCHI ALLA CATENA DI FORNITURA DELLE DIPENDENZE SOFTWARE**
- **CARENZA DI COMPETENZE**, che continuerà ad essere un problema grave, nonostante le iniziative avviate e in corso;
- **ERRORE UMANO E SFRUTTAMENTO DI SISTEMI LEGACY ALL'INTERNO DI ECOSISTEMI CYBER-PHYSICAL**
- **SFRUTTAMENTO DI SISTEMI NON AGGIORNATI E OBSOLETI ALL'INTERNO DEL ECOSISTEMA TECNOLOGICO INTERSETTORIALE**
- **AUMENTO DELLA SORVEGLIANZA DIGITALE NEI REGIMI AUTORITARI / PERDITA DI PRIVACY**
- **CROSS BORDER ICT SERVICE PROVIDERS COME SINGLE POINT OF FAILURE**
- **CAMPAGNE AVANZATE DI DISINFORMAZIONE**, a scopi geopolitici, ma anche per mero ritorno economico
- **AUMENTO DELLE MINACCE IBRIDE AVANZATE**
- **ABUSO DELL'IA**, inteso soprattutto come manipolazione di algoritmi e applicazioni
- **IMPATTO FISICO DELLE INTERRUZIONI NATURALI/AMBIENTALI SULLE INFRASTRUTTURE DIGITALI CRITICHE**, anche e soprattutto a causa del cambiamento climatico

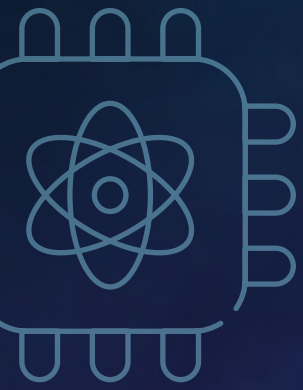
(Per maggiori dettagli questo l'intervento di Rossella Mattioli (ENISA): https://www.cyber40.it/wp-content/uploads/2024/06/Rossella-Mattioli.pdf).

Le PMI risultano le entità a maggior rischio di attacco cyber, sia a causa di misure tecniche e organizzative di difesa generalmente più basse, sia a causa di un livello medio di consapevolezza delle minacce che è minore rispetto a realtà più strutturate. Le occasioni offerte dal PNRR stanno supportando un numero crescente di realtà medio piccole negli interventi di adeguamento e potenziamento delle difese, ma deve essere data continuità all'azione in corso, e farla diventare iniziativa permanente e di sistema. Le normative in corso di attuazione, peraltro, rischiano di trovare largamente impreparate numerose PMI che intervengono nella catena di fornitura di soggetti essenziali e importanti e creare una fase di stallo del sistema produttivo nazionale, con conseguente rischio di perdita di quote di mercato anche a livello internazionale.



Nel periodo 2010-22 la Cina ha registrato il 61% dei brevetti AI, gli Stati Uniti il 21%, il resto del mondo il 16% e solo il 2% l'Unione europea e il Regno Unito insieme (2024 AI Index report). Uno scenario che pone questioni rilevanti in merito allo sforzo che l'Unione Europea dovrà mettere in atto nel breve periodo per supportare con azioni strategiche e opportuni aiuti la ricerca sul tema. Nel gennaio 2024 la Commissione Europea ha varato il pacchetto sull'innovazione in materia di AI per sostenere start-up e PMI in tale settore (https://digital-strategy.ec.europa.eu/en/library/communication-boosting-startups-and-innovation-trustworthy-artificial-intelligence). Dal punto di vista normativo, si è fatto molto, anche a livello nazionale e l'Europa è la prima regione al mondo ad essersi dotata di uno strumento ampio e omnicomprensivo (EU AI Act) che indirizzi lo sviluppo dell'Intelligenza Artificiale lungo un percorso di tutela dei diritti fondamentali e di governance chiara e puntuale. Un grande sforzo attende tutti affinché gli strumenti delineati possano produrre risultati nel più breve tempo possibile. Non v'è alcun dubbio che ciò rappresenti una grande opportunità per le imprese italiane.

La tecnologia blockchain, dopo il picco di interesse dell'ultimo biennio, sembra aver raggiunto il livello di maturità atteso e la sua applicazione a casi concreti consente di sfruttare le sue caratteristiche distintive, tanto nel comparto produttivo e nella Pubblica Amministrazione. In termini di cybersecurity, rilevano in particolare: la decentralizzazione dei dati, che rende più difficile per i criminali informatici accedere a interi database da un unico punto di accesso, l'immutabilità dei dati, che riduce il rischio di frodi e manipolazioni, le caratteristiche di tracciabilità e trasparenza, che la rendono ideale per aumentare il livello di fiducia nei processi produttivi (e.g. nella filiera agro-alimentare), e per la possibilità di integrazione in scenari complessi per migliorarne la sicurezza (e.g. nel comparto automotive).



Il quantum computing presenta opportunità nel medio-lungo periodo, ma pone anche nuove sfide per la cybersicurezza che devono essere affrontate su una tempistica più breve. Il livello di maturità tecnologico è in crescita, ma le applicazioni pratiche sono ancora limitate e principalmente sperimentali. Gran parte della ricerca si focalizza sullo sviluppo di algoritmi che possano accelerare la soluzione di problemi altamente complessi. Applicazioni pratiche sono previste anche per l'ottimizzazione dei processi industriali, in contesti quali la simulazione di materiali e la modellazione finanziaria. Ambito più maturo è quello della Distribuzione di Chiavi Quantistiche (QKD), per il quale esistono già dimostratori stabili, alcuni sviluppati anche nel contesto dei progetti cofinanziati da Cyber 4.0.

La crittografia post-quantistica rappresenta poi un'area di interesse molto attuale, anche inn considerazione della necessità sempre più impellente di poter disporre di algoritmi di crittografia che possano resistere agli attacchi dei futuri computer quantistici. Si prevede infatti che questi abbiano il potenziale per decifrare molti degli attuali algoritmi di crittografia, come RSA e ECC, mettendo a rischio la sicurezza dei dati. Le aziende devono pertanto diventare "crypto-agili", ovvero essere in grado di adattarsi rapidamente a nuovi standard di crittografia man mano che vengono sviluppati.

Tema centrale e filo conduttore degli interventi dedicati alla formazione e all'awareness in ambito cybersecurity, ha riguardato innanzitutto gli approcci perseguiti a livello nazionale ed europeo per far fronte al problema dello "skill shortage". Carenza e divario di competenze in cybersecurity, e più in generale in tutta l'area ICT, caratterizzano infatti il panorama nazionale sia a livello accademico, sia a livello del tessuto imprenditoriale e di amministrazioni pubbliche. La mancanza di figure professionali e di esperti di settore, per quanto endemica, trova possibili soluzioni nell'adozione di programmi di insegnamento ad ampio respiro, che possano coinvolgere studenti e docenti a partire dalla scuola primaria, fino alle università e agli Istituti Tecnici Superiori.

Oltre agli interventi in ambito scolastico, i cui effetti potranno essere apprezzati sul lungo termine, le realtà che più direttamente risentono della carenza di competenze risultano essere le imprese e le pubbliche amministrazioni. In quest'ottica le iniziative di Cyber 4.0, anche grazie alla sua natura di partneriato pubblico-privato, hanno la capacità di intervenire direttamente su più fronti, con linee di azione in grado di coinvolgere e fornire aiuti e incentivi a imprese, PA e scuole.

Per quanto riguarda le imprese, tali attività però non possono prescindere dall'adozione di un approccio didattico efficace, a lungo termine e adeguato al contesto. Proprio in questo senso risulta fondamentale agevolare l'adozione graduale di approcci innovativi alla formazione aziendale, che prevedano attività di gamification e learn-by-doing anche attraverso l'utilizzo di tecnologie emergenti.

Infine, per quanto riguarda l'upskilling in ambito PA, oltre alla programmazione di attività di formazione che prediligono approcci Top-Down, coinvolgendo in primo luogo l'alta direzione, un tema di forte interesse è costituito dalla diffusione di una cultura che metta al centro le responsabilità condivise in ambito di sicurezza cibernetica. Prendendo ad esempio le iniziative volte all'implementazione del cloud nazionale, in ambienti dove l'approvvigionamento tecnologico passa quasi sempre per provider e catene di fornitura esterni, un approccio vincente consiste nell'individuazione di matrici di responsabilità che garantiscano, da un lato, che il servizio fornito sia sicuro e, dall'altro, che il servizio sia gestito in sicurezza da responsabili interni adeguatamente formati.

La linea di azione più efficace e radicale per contrastare il problema dello "skill shortage" in ambito ICT e cyber, è rappresentata dalle iniziative e dai programmi rivolti agli studenti, a partire dalle scuole primarie. L'obiettivo consiste nel consentire un inserimento nel mondo del lavoro di nuove figure professionali, che, indipendentemente dal settore di interesse, accompagnino a una forte competenza in ambito tecnologico, una solida cultura della sicurezza delle informazioni.

Nella sessione specifica dedicata agli studenti, si sono susseguiti interventi di coloro che hanno avuto l'opportunità di fruire delle iniziative del Centro. La prima testimonianza è stata quella di Mhackeroni, un team italiano di CTF (Capture The Flag) fondato nel 2018 da un gruppo di studenti appassionati di cybersecurity provenienti da diverse istituzioni accademiche, uniti per combinare le loro forze e raggiungere l'obiettivo finale della qualificazione alle finali di DEFCON CTF. Successivamente è stato presentato CyberX Mind4Future, un progetto avanzato di formazione in cybersecurity organizzato da Cyber 4.0 in collaborazione con Leonardo. E' stato poi il turno del contest "Let's Cyber Game" lanciato per gli studenti degli Istituti Tecnici Superiori (ITS), offrendo un'opportunità di apprendimento pratico attraverso una competizione volta allo sviluppo di un videogioco formativo in ambito cybersecurity e cybercrime. Infine, è stato presentato il progetto "A Scuola Connessi", un programma educativo per le scuole medie e superiori volto a sensibilizzare gli studenti sulle minacce informatiche e sulle pratiche di sicurezza online.

CYBER 4.0
CYBERSECURITY
COMPETENCE
CENTER

Grazie

cyber40.it