ItaliaSec Cyber Summit 2024 Annual Report_

ItaliaSec
SECURING ITALY FROM CYBER THREATS

Issued March 2024

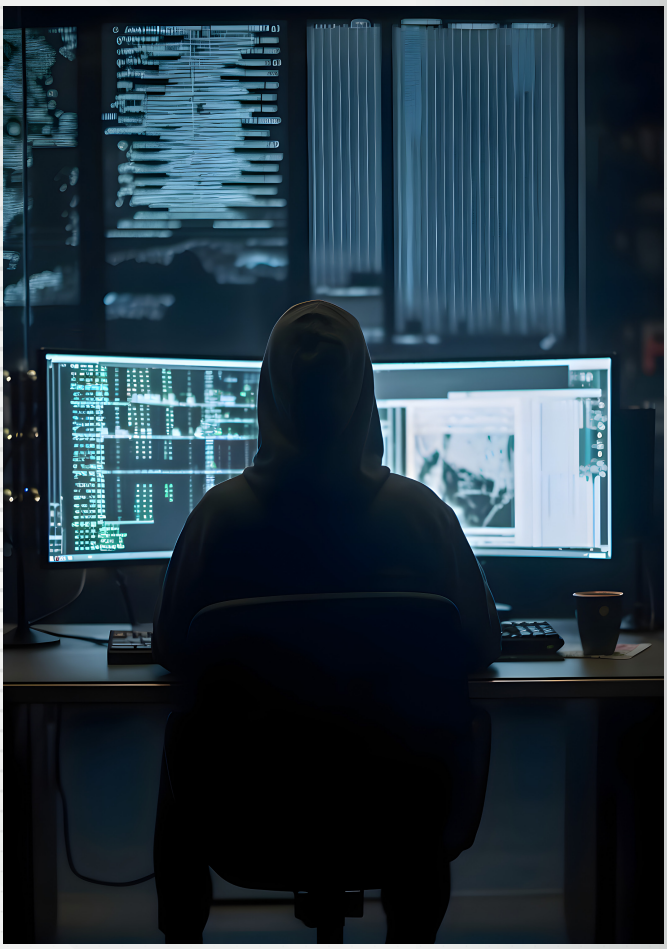
Foreword_

Da otto anni QG Media organizza ItaliaSec Summit, conferenza dedicata ai professionisti della cyber security dei settori pubblico e privato. ItaliaSec fa parte della nostra Cyber Series, un portfolio globale di conferenze nazionali o regionali mirate a riunire i responsabili della sicurezza informatica al fine di condividere esperienze dirette, scambiare opinioni e fare networking.

Per ogni evento nel portfolio Cyber Series, produciamo un rapporto come questo, in cui esploriamo temi scottanti e argomenti di rilievo, trattati poi in maniera più approfondita nel corso dei rispettivi summit a cadenza annuale. Includiamo, inoltre, interviste esclusive rilasciate dagli esperti che compongono il nostro Steering Committee e dai relatori che interverranno durante ItaliaSec Summit. Si noti che le opinioni espresse dagli intervistati appartengono al singolo individuo, non corrispondono necessariamente a quelle del datore di lavoro né intendono costituire una dichiarazione ufficiale da parte di quest'ultimo.

Il tema e filo conduttore di ItaliaSec Summit 2024 è il seguente: Oltre la Protezione: Trasformare la Cyber Security in un Vantaggio Competitivo che Crea Valore.
Ogni intervento terrà conto di questo obiettivo, centrale al successo di qualsiasi strategia di cyber sicurezza. In un contesto di crescenti tensioni geopolitiche (che si traducono in un aumento e una maggior 'severity' degli attacchi informatici) e dove gli alti costi associati agli investimenti nella sicurezza informatica costituiscono spesso una barriera, è fondamentale riuscire a comunicare il reale valore della cyber security.

Il rapporto inizia con una panoramica degli incidenti più significativi registrati negli ultimi sei mesi e ulteriori dati per gettare



luce sul contesto attuale. Seguono degli approfondimenti o focus su cloud security, intelligenza artificiale, supply chain e rischio di terze parti, sicurezza OT, cyber resilience, il ruolo del CISO e cyber skills gap, accompagnati da commenti di esperti di settore. Infine, verranno proposte una breve conclusione e alcuni spunti, basati sulle conversazioni avvenute tra i membri dello Steering Committee.

Ci auguriamo che troviate i contenuti del rapporto stimolanti. Contattaci all'indirizzo info@qgmedia.io se avete domande o desideriate ulteriori approfondimenti su qualsiasi informazione contenuta nel report.

Buona lettura,

Author:
Cecilia Limonta
ItaliaSec 2024 Program Director

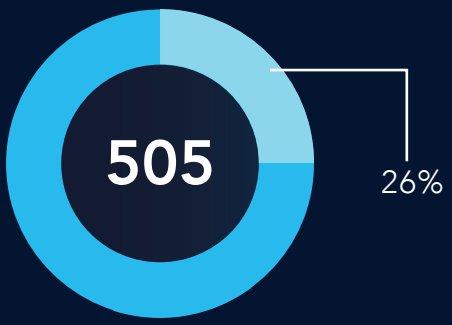
Table of **Contents_**

Contesto_

L'ultimo anno ha visto la sicurezza informatica finire frequentemente in prima pagina e raggiungere posizioni più alte che mai nell'agenda delle priorità di governi e aziende. La portata e la gravità degli attacchi, infatti, continuano ad aumentare di anno in anno, e ne sono vittime attori sempre più grandi e importanti. Come emerge dal Rapporto CLUSIT 2023, "dal 2022 siamo entrati in una nuova fase di guerra cibernetica diffusa, nel contesto di crescenti tensioni internazionali tra superpotenze e di un conflitto ad alta intensità combattuto ai confini dell'Europa". Consigliamo vivamente di consultare il Rapporto CLUSIT 2024 per una panoramica completa e dettagliata degli attacchi a livello globale e nazionale.

NUMERO DI ATTACCHI CYBER

Dal **2018** a giugno **2023**, nel Rapporto sono stati censiti **505 attacchi** noti di **particolare gravità** che hanno coinvolto **realtà italiane**, di cui ben **132** (il 26%!) si sono verificati **solo nei primi 6 mesi** del **2023**



Oltre il **56%** degli attacchi ha avuto **conseguenze** di **gravità** "**critica**" o "**elevata**"

La **media mensile** di attacchi è risultata di **232 attacchi**

Aumentano ancora gli **attacchi cyber**, **+65% nel 2023** in Italia

Contesto a Livello Mondiale

Anche a livello mondiale, come emerge dal rapporto Global Cyber Security Outlook 2024 compilato dal World Economic Forum:

1 Livello di Sicurezza Informatica

Il numero di organizzazioni che mantengono livelli di "minimum viable cyber security" è calato del 30%.

2 Prospettiva sulla Resilienza Informatica

Più del doppio delle PMI rispetto alle grandi aziende afferma di non possedere sufficiente cyber resilience per soddisfare i loro requisiti operativi critici.

3 Prospettive sull' Intelligenza Artificiale

Meno di un intervistato su 10 crede che nei prossimi due anni l'intelligenza artificiale generativa darà il maggior vantaggio ai difensori piuttosto che agli attaccanti.

4 Prospettiva sulle Competenze Informatica

Solo il 15% di tutte le organizzazioni ritiene che le competenze informatiche e l'istruzione incrementeranno e miglioreranno significativamente nei prossimi due anni.

Focus_

Attraverso i dati raccolti tramite gli evaluation form compilati dai partecipanti all'edizione 2023, e le conversazioni con i membri dello Steering Committee 2024, emerge che la sicurezza del cloud, l'AI, il rischio di terze parti, la cyber resilience, il cyber skills gap e le competenze del CISO sono tra le maggiori preoccupazioni per i professionisti della sicurezza. Cresce inoltre l'interesse verso la protezione degli ambienti OT, e l'integrazione di competenze specifiche in questo ambito in cui la conoscenza di principi tradizionali di sicurezza IT non è sufficiente.

In questa sezione, ci focalizziamo su ogni tematica singolarmente, elaborandola attraverso commenti e opinioni di membri della community di ItaliaSec.

1 Part 1: Cloud Security

La sicurezza del cloud continua a essere tra le priorità più alte per molti CISO. Si pensi che a livello globale, come emerge dal rapporto Global Digital Trust Insights 2024 di PwC, un sondaggio che coinvolge 3,876 business e tech leader, la sicurezza del cloud è la principale preoccupazione in termini di rischio informatico per quasi la metà (47%) degli intervistati.

Alcune organizzazioni hanno da poco iniziato il loro percorso di migrazione, mentre altre stanno adottando strategie ibride multi-cloud avanzate. Ma indipendentemente dalla fase di implementazione, una delle sfide più grandi nel cloud computing è proteggere la sicurezza dei dati, derivante dai rischi unici che questa tecnologia comporta.

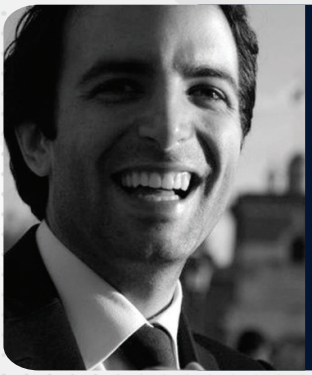
INTERVIEWS

Per molte aziende, una delle grandi sfide attuali è proteggere i dati nel cloud. Attraverso e grazie alla tua esperienza, quali sono i consigli principali che puoi condividere con i colleghi?

Guido Barbero
ICT CTO & CISO
IVECO • GROUP

Il trend dello spostamento dei workload applicativi verso il cloud computing è molto significativo, per cogliere tutti i vantaggi di flessibilità, costi e rapidità di esecuzione offerto da queste piattaforme. Diventa quindi fondamentale capire in che modo l'organizzazione protegge le proprie risorse basate sul cloud, in questi ambienti esistono delle solide basi per costruire sistemi sicuri e affidabili, ma è anche necessario implementare strumenti e pratiche ottimali: la corretta gestione della configurazione dei server, il controllo degli accessi alla rete e agli utenti, la crittografia dei dati, il monitoraggio delle potenziali minacce, ecc.

Sul cloud sono già presenti diverse funzionalità di sicurezza native, che possono essere utilizzate con la giusta configurazione ma è anche possibile implementare delle tecnologie comparabili con quelle utilizzate sulla rete on-premise (ad esempio i firewall di nuova generazione), infine ora è disponibile anche una nuova famiglia di soluzioni che migliorano la visibilità e il controllo della postura di sicurezza dell'ambiente cloud (Cloud Native Application Protection, Cloud Secure Posture Management...)



Giampiero Bonfiglio
CISO Italy & Greece
L'ORÉAL

La mia esperienza mi ha insegnato l'importanza di adottare un approccio olistico alla sicurezza dei dati, che includa tanto la prevenzione quanto la capacità di risposta agli incidenti.
Primo, è fondamentale implementare una robusta politica di accesso basata sui minimi privilegi, assicurando che ciascun utente acceda solo ai dati necessari per le sue funzioni.

Inoltre, l'adozione di soluzioni di crittografia end-to-end per i dati in transito e in riposo è essenziale per proteggere le informazioni sensibili da accessi non autorizzati.
Un'altra pratica raccomandata è l'impiego di una gestione efficace delle identità e degli accessi, compreso l'uso dell'autenticazione multifattore, per rafforzare ulteriormente la sicurezza.

Infine, mantenere una strategia proattiva di formazione dei dipendenti sulla sicurezza è cruciale, poiché gli errori umani spesso costituiscono il punto debole nelle difese aziendali. Condividendo queste pratiche, spero di contribuire a elevare gli standard di sicurezza nell'ecosistema del cloud.

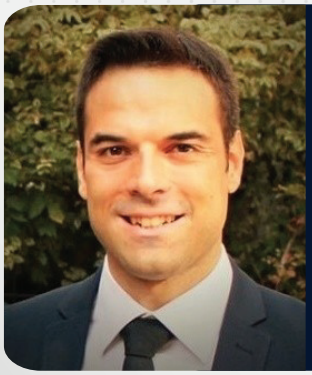
2 Part 2: Intelligenza Artificiale

La tecnologia dell'intelligenza artificiale generativa è diventata accessibile a livello mainstream verso la fine del 2022. Sicuramente, da un lato l'intelligenza artificiale presenta una serie di rischi che non possiamo ignorare, oltre ad aver attirato l'attenzione dei cyber criminali, che cercano modi per sfruttarla ai propri fini. Dall'altro, se utilizzata correttamente può presentare vantaggi notevoli e aprire nuove opportunità per i cyber difensori.

Nel contesto aziendale, possiamo avvalerci dell'intelligenza artificiale per accelerare il rilevamento delle minacce, velocizzare una serie di processi e risposte, proteggere identità e dati... Così mantenendo i team di sicurezza informatica aggiornati e in controllo. Ma come farlo correttamente?

INTERVIEW

Al momento, uno dei temi scottanti è quello dell'Intelligenza Artificiale. Quali sono a tuo parere le considerazioni fondamentali che un CISO deve tenere a mente, quando contempla la possibilità di implementare AI in ambito security?



Daniele Luzi
Head of EMEA South Practice
Google Cloud

L'Intelligenza Artificiale rappresenta un punto di svolta per la sicurezza digitale, e da un nostro recente studio più del 40% degli intervistati vede proprio questo ambito come una delle migliori applicazioni dell'AI. Come Google abbiamo individuato tre aree che aiutano a colmare il cosiddetto "Defender's Dilemma", ovvero l'inevitabile gap tra attaccanti e difensori, ora amplificato dall'AI:

- **Sicurezza:** Come le altre tecnologie, anche l'AI ha bisogno di security by-design e by-default
- **Potenziamento:** Investimenti mirati, partnership tra pubblico e privato ed un approccio regolatorio efficace che permetta alle aziende di ottenere il massimo dall'AI, ma limitandone l'uso agli attaccanti.
- **Avanzamento:** Ci impegniamo a portare avanti la ricerca che aiuta a generare scoperte rivoluzionarie nella sicurezza basata sull'AI.

Così come accogliamo positivamente le scoperte in ambito farmaceutico e scientifico, siamo anche entusiasti del potenziale dell'AI nel risolvere le sfide in materia di sicurezza, avvicinandoci ad un mondo digitale più sicuro ed affidabile.

INTERVIEW

Come ritieni che le nuove tecnologie, e nello specifico l'AI generativa, possano essere sfruttate al meglio per tutelare la sicurezza della tua organizzazione?

Luca A. Giusti
CISO and Head of Infrastructure

L'avvento dell' AI, specie quella generativa, è sicuramente un argomento ormai a conoscenza di tutti. Nell'ambito della sicurezza delle informazioni l'AI costituisce tanto un rischio quanto un'opportunità. Strumenti basati sull'AI generativa possono mettere in grado degli attaccanti anche privi di specifica esperienza di realizzare soluzioni tecniche, che vanno dal coding alla realizzazione di soluzioni di phishing, in pochi minuti e con il minimo sforzo.

Lato infosec, possiamo e dobbiamo utilizzare gli stessi strumenti per permetterci di controllare e validare le informazioni che potrebbero essere state contraffatte o modificate per veicolare un attacco, ma, al contrario di quanto a disposizione degli attaccanti, siamo tenuti a seguire delle regole, etiche, morali e legali, che dall'altra parte sono mancanti, con evidente svantaggio.

È fondamentale implementare l'AI tra gli automatismi di sicurezza in modo da utilizzarne il potenziale per fare ricognizione e identificazione delle minacce, riducendo i falsi positivi e identificando le nuove tecniche di attacco e compromissione e ridurre il più possibile l'impatto delle minacce zero day.

---

3 Part 3: Supply Chain e Rischio di Terze Parti

Per qualsiasi realtà, i partner nel proprio ecosistema sono sia la risorsa più grande che il maggior ostacolo per un futuro digitale sicuro e resiliente. Secondo dati pubblicati dal World Economic Forum a gennaio 2024, il 41% delle organizzazioni che hanno subito un incidente significativo negli ultimi 12 mesi riportano che sia stato causato da terze parti.

L'attuale approccio di molte organizzazioni alla sicurezza della supply chain non è in linea con la realtà odierna, caratterizzata da un ecosistema di partner complesso e interdipendente. Oggi occorre stabilire partnership più strategiche con i fornitori, e focalizzarsi su monitoraggio e gestione continui dei profili di rischio di tali fornitori, al fine di rafforzare la resilienza operativa.

INTERVIEWS

Grazie alle esperienze che hai maturato in realtà operanti in settori diversificati e di differente complessità, puoi riassumere i tre step essenziali per mitigare il rischio di terze parti?

Vincenzo Calabrò
Information Security Officer
MINISTERO DELL'INTERNO

Tutte le organizzazioni che operano nel digitale hanno la necessità di acquisire prodotti o servizi dell'ICT da terze parti. Le odierne catene di approvvigionamento sono caratterizzate da dinamismo, stratificazione e complessità, proprietà che rendono difficile, a volte irrealizzabile, la visibilità e la tracciabilità dei componenti e di tutti i livelli di produzione, in pratica appaiono come una sorte di buco nero. Ciò aumenta i rischi della sicurezza anche quando le proprie difese sono abbastanza buone.

Un approccio ottimale, in grado di ridurre i rischi ad un livello accettabile, prevede l'impiego di un metodo in grado di identificare, valutare e mitigare i rischi associati alla natura globale e distribuita delle catene di fornitura. Per prima cosa è necessario che l'organizzazione si procuri le evidenze che gli consentano di verificare: le competenze del fornitore, le caratteristiche del prodotto, il metodo di distribuzione e il controllo operativo del prodotto. Successivamente, occorre valutare queste informazioni, attraverso un sistema di monitoraggio e controllo, per verificare la corrispondenza nel tempo.

Infine, è opportuno effettuare periodicamente degli assessment con i fornitori per rivalutare il fattore di rischio. In sintesi, il metodo consente di creare una relazione di trust tra fornitore e cliente che prevede un'assunzione di responsabilità reciproca e una condivisione del rischio cyber.

Andrea Licciardi
Senior Cyber Security Manager
TECNIMONT

Proverò a sintetizzare un concetto che richiede sicuramente degli specifici approfondimenti ma in sintesi la gestione del rischio di terze parti è cruciale e può essere affrontata in tre passaggi fondamentali:

- **Valutazione:** Iniziare con una rigorosa valutazione dei rischi, identificando e classificando le terze parti in base al livello di rischio che rappresentano. Questo include la revisione delle loro politiche di sicurezza, i processi di gestione dei dati e le prestazioni storiche.
- **Due Diligence:** Implementare un processo di due diligence continuo. Non si tratta solo di un'analisi iniziale, ma di un monitoraggio costante delle

prestazioni e del comportamento delle terze parti, assicurandosi che aderiscano agli standard richiesti, soprattutto in termini di cybersecurity e conformità normativa.

- **Contratti e Compliance:** Assicurarsi che tutti i contratti con terze parti includano clausole chiare su responsabilità, obblighi di conformità, e requisiti per la segnalazione di incidenti. Inoltre, è fondamentale svolgere regolari audit e verifiche incrociate per garantire l'aderenza alle policy stabilite.

4 Part 4: Sicurezza OT

Secondo l'ultimo State of Operational Technology and Cybersecurity Report di Fortinet, nel 2023, il numero di intervistati che considera "altamente maturo" il livello di sicurezza OT della propria organizzazione è sceso al 13% rispetto al 21% dell'anno precedente. Questo calo indica una crescente consapevolezza tra i professionisti OT e l'uso di strumenti più efficaci per valutare le capacità di sicurezza informatica delle proprie organizzazioni. I dati raccolti indicano inoltre che, quando si è verificato un attacco informatico, quasi un terzo (32%) degli intervistati sostiene che siano stati colpiti sia i sistemi IT che quelli OT, rispetto al 21% dell'anno precedente.

Inoltre, la stragrande maggioranza (95%) delle organizzazioni intervistate ha dichiarato che la quella della sicurezza OT ricada tra responsabilità del CISO.

Non sorprende, dunque, che i CISO all'interno della nostra ItaliaSec community manifestino crescente interesse verso l'argomento. Proteggere gli ambienti OT richiede competenze, processi e tecnologie diversi rispetto al proteggere gli ambienti IT, ed è sempre più necessario integrarle per proteggere l'azienda nel suo complesso.

INTERVIEW

Per molte aziende nel settore manifatturiero e nella infrastrutture critiche, una delle grandi sfide attuali è la sicurezza degli ambienti OT. Quali consigli puoi fornire a coloro che stanno compiendo i primi passi in questo ambito?

Francesco Corrado
Head of Cyber Security
FERRERO

I paradigmi introdotti dalla quarta rivoluzione industriale e la conseguente spinta alla digitalizzazione, necessaria e centrale per l'ottimizzazione dei processi produttivi (waste and energy optimisation, quality enhancement, remote and predictive maintenance, production optimisation, etc.), hanno imposto una trasformazione tecnologica che richiede necessariamente una convergenza tra due

mondi progettati per operare indipendentemente, quello IT e quello OT. Questi, per loro natura, risultano essere diametralmente opposti essendo disegnati per supportare processi e bisogni totalmente differenti. Il risultato di tale eterogeneità espone inevitabilmente le aziende a nuovi fattori di rischio, tra cui quello cyber, da identificare e gestire propriamente.

Nella dinamicità di tale contesto è necessario disegnare una strategia di sicurezza che sia motore abilitante alla trasformazione e al raggiungimento degli obiettivi di business, ma che al contempo gestisca pragmaticamente il rischio cyber. È necessario supportare attivamente lo step-change culturale investendo nelle persone e nella formazione, creare processi di cybersecurity che possano essere integrati nei processi di Business e definire Ruoli e Responsabilità chiari per il governo delle diverse tecnologie (spronando la collaborazione tra dipartimenti IT ed OT).

Ovviamente, ruolo rilevante lo assume anche il contesto tecnologico industriale in cui ci si trova ad operare; Questo, infatti, è caratterizzato da sistemi progettati per garantire requisiti molto stringenti in termini di Safety, Availability e Reliability, parametri evidentemente diversi da quelli alla base della sicurezza del mondo IT.

Ad aumentare vertiginosamente il rischio inerente alla convergenza tra i due mondi, acquisisce un ruolo rilevante l'obsolescenza tecnologica degli ambienti OT e le nuove necessità di connettività. Avere una chiara visibilità del perimetro da proteggere, implementare soluzioni di monitoraggio del traffico dati tra reti IT ed OT (che ovviamente devono essere propriamente segregate), regolare le connettività remote e l'utilizzo di dispositivi di archiviazione mobile (e.g. USB), ma soprattutto lavorare con i Vendor (che sono la chiave principale per la progettazione di sistemi/software industriali sicuri by design e supportati durante tutto il loro lifecycle) aiuta a garantire che tale rischio venga gestito propriamente.

Ritengo, inoltre, che la definizione di requisiti esterni, quali ad esempio la NIS 2, possano aiutare gli "addetti ai lavori" a sensibilizzare l'intero comparto manifatturiero ed industriale rispetto a queste tematiche.

5

Part 5: Cyber Resilience

La cyber resilience è fondamentale per mantenere operativo il business, ridurre l'impatto degli attacchi futuri e salvaguardare la fiducia dei clienti. Il concetto di resilienza deve a integrarsi a quello di sicurezza informatica: è necessario che le due discipline di resilience e security lavorino in tandem per aiutare le organizzazioni a gestire meglio il rischio informatico.

Tra le azioni da intraprendere: individuare i processi aziendali critici, implementare soluzioni di ripristino, stabilire protocolli con i principali fornitori per coordinare le risposte agli incidenti, creare un team interdipartimentale, condividere informazioni con colleghi nel settore in cui opera l'azienda attraverso processi formali per prevenire rischi sistemici, stabilire rapporti con le forze dell'ordine in termini sia di analisi che di risposta....

INTERVIEW

Quali sono le lezioni che hai appreso recentemente, o meglio consolidato, a proposito di cyber resilience? Come puoi tradurle in consigli per i colleghi?

Massimo Cottafavi
Director Cyber Security & Resilience

Cyber resilience è un termine molto abusato ma dietro al quale si cela prima di ogni altra cosa un'attitudine culturale che si sta gradualmente affermando all'interno delle aziende e che concerne la capacità di mantenere la propria coerenza strategica, adattando eventualmente l'approccio tattico, in un contesto economico, sociale e tecnologico nel quale il cambiamento e l'imprevedibilità sono diventate due costanti. Dal mio punto di vista alcuni elementi risultano più importanti di altri. Innanzitutto occorre adottare modelli e definire processi di lavoro snelli e reattivi.

In secondo luogo, occorre programmare e realizzare esercitazioni e simulazioni pratiche che permettano di familiarizzare ad ogni livello organizzativo con le azioni da porre in essere nel corso di una possibile "perturbazione" delle condizioni ordinarie. In ultimo occorre adottare criteri moderni di indirizzamento delle attività di security awareness in modo che gli utenti non vengano visti come possibili fonti di minaccia da neutralizzare ma come preziosi alleati in grado di intercettare e comunicare i segnali deboli.

---

6 Part 6: Le Competenze del CISO

Fino a una decina di anni fa, la regola per i professionisti della sicurezza era 80% competenze tecniche e 20% competenze trasversali, le cosiddette 'soft skills'. Nel 2024, se per alcuni affermare che le percentuali si siano invertite può sembrare esagerato, molti CISO sicuramente sembrano essere d'accordo sul fatto che le competenze tecniche e quelle trasversali abbiano almeno la stessa importanza. Si pensi a competenze quali comunicazione, problem-solving, conflict-management... Ma anche l'abilità di creare un work-life balance che permetta la sostenibilità del ruolo, e di evitare di essere vittima di burnout o esaurimento.

INTERVIEW

Quello del CISO è un ruolo sfaccettato, che richiede numerose competenze di diversa natura. Quali consigli validi avresti voluto ricevere prima di imbarcarti in questo percorso, e di conseguenza puoi condividere con la community?

Andrea Succi
CISO

FERRARI

Assumi una mentalità imprenditoriale: presenta la sicurezza informatica come un investimento, non come un costo. Promuovi il valore della sicurezza per il business e dimostra il suo impatto positivo. A tal fine investi nelle tue capacità di comunicazione e strategiche.
Costruisci una rete solida: il networking con altri CISO e professionisti della cyber è un modo eccellente per scambiare idee e best practices, ottenere supporto e consigli, rimanere aggiornati sugli ultimi trend e sulle ultime minacce.

Prenditi cura di te stesso: un ruolo di leader nella cyber security può essere estremamente stressante. Cerca di essere resiliente, assicurandoti di mantenere un sano equilibrio tra lavoro e vita privata per evitare burnout e mantenere la tua lucidità. Uno dei segreti è la flessibilità nell'integrazione tra vita e lavoro che deve avvenire in entrambi i versi. Se sei fresco mentalmente sarai efficace quando più ti servirà esserlo, per esempio durante la gestione di un incidente cyber improvviso.

Paolo Cannistraro
CISO

ENGIE

Per me il ruolo del CISO è uno dei più sfidanti e gratificanti. Per svolgerlo al meglio, occorre possedere una serie di competenze tecniche, manageriali e relazionali. Prima di intraprendere questo percorso, avrei apprezzato diversi consigli su come:

- Bilanciare competenza tecnica con comunicazione efficace: comunicare efficacemente tematiche legate alla sicurezza IT ai non tecnici, usando esempi e analogie. Un CISO deve essere in grado di comprendere minacce, rischi e soluzioni tecnologiche, ma allo stesso tempo essere capace di spiegare in modo semplice e persuasivo l'importanza della sicurezza ai dirigenti, ai dipendenti e ai clienti.

- Gestire con resilienza e flessibilità le pressioni e le sfide quotidiane, prioritizzando, delegando, monitorando e intervenendo. Un CISO deve affrontare ogni giorno situazioni complesse, impreviste e potenzialmente critiche.

- Costruire e mantenere relazioni solide con colleghi e partner esterni, condividendo, collaborando e riconoscendo il valore di ognuno. Un CISO non può lavorare da solo, ma deve fare affidamento su una rete di supporto interna ed esterna.

7 Part 7: Cyber Skills Gap

A ottobre 2023, uno studio di ISC2 ha riportato che il cosiddetto cyber skills gap avesse raggiunto la cifra record di quattro milioni di persone, e una ricerca di ISACA ha rilevato che il 62% dei team di sicurezza informatica fosse a corto di personale.

A gennaio 2024, un rapporto del World Economic Forum ha rivelato che il 71% delle organizzazioni coinvolte abbia posizioni aperte nel dipartimento sicurezza informatica.

I numeri parlano chiaro: bisogna agire rapidamente per colmare il divario, e aprire i propri orizzonti a soluzioni creative per attrarre talenti verso questa professione.

INTERVIEW

Parlando di cyber security skills gap, la carenza di risorse qualificate è una delle sfide principali per le aziende del territorio. Esistono strategie creative per rispondere al problema? Quali considerazioni puoi condividere a riguardo, e come ritieni che i settori pubblico e privato possano collaborare a tal fine?

Antonio Pisano
SVP Cyber & Info Security
LEONARDO

Il mercato del lavoro della "CyberSicurezza" è un po' alterato a causa degli ultimi accadimenti a livello globale, e la corsa all'accaparramento della migliore skill continua ad essere la protagonista nel relativo mercato delle professionalità. Le aziende ed il mondo accademico devono continuare a puntare su un modello di piena sinergia che consenta di "adottare" uno studente già durante gli ultimi anni di studio, formandolo in azienda al fine di renderlo immediatamente pronto a creare il giusto valore nell'impresa. Il CISO deve essere abile nel comprendere le tendenze del mercato della sicurezza e l'evoluzione delle nuove tecnologie (es. AI) al fine di ridirezionare rapidamente, all'occorrenza, gli investimenti di medio periodo.

La pubblica amministrazione deve ancor di più fungere da catalizzatore per agevolare lo sviluppo delle imprese continuando a realizzare infrastrutture resilienti e prestazionali, che consentano di offrire servizi tecnologici di "ultimo grido" a prezzi competitivi; in estrema sintesi possiamo banalmente dire che i servizi digitali devono costare meno ed essere più sicuri.

L'argomento cyber security skills gap è da ormai diversi anni presentato come uno dei principali problemi che le aziende moderne devono affrontare, ma nonostante ciò si fatica a trovare una soluzione. Nel cercare una possibile strategia ho provato a domandarmi il perché manchino e quali fossero queste competenze. Mentre siamo alla ricerca di personale formato e pronto ad affrontare le sfide cyber, gli scenari di rischio cambiano ad una velocità sempre crescente, questo comporta il considerare le risorse non sufficientemente qualificate e aggiornate. Forse stiamo guardando al problema da un punto di vista non corretto, potremo mai avere persone completamente qualificate? E se la risposta fosse no? In tal caso forse dovremmo avere il coraggio di assumere personale inizialmente non completamente qualificato, ma che abbia la volontà e il desiderio di acquisire competenze con il tempo e soprattutto stimolando in loro la ricerca di un costante e continuo aggiornamento di competenze nuove, costruendo un percorso di sviluppo di soft e hard skills allineato alle esigenze aziendali e misurandone i risultati come una metrica del raggiungimento degli obiettivi personali al pari di un obiettivo di business.

Conclusione_

Conclusione e Ulteriori Spunti_

Nel complesso, malgrado le tensioni geopolitiche che innescano attacchi state-sponsored, le innovazioni tecnologiche che consentono attacchi informatici più sofisticati e la carenza di figure professionali, non riteniamo che lo stato attuale della sicurezza informatica in Italia sia del tutto disastroso. È importante sottolineare come la comunità infosec abbia profuso grandi sforzi nella lotta contro il crimine informatico, e che sia importante mantenere un approccio positivo per quanto possibile, nell'ottica del non arrendersi. Lo spirito combattivo deve persistere.

Concentriamoci su quello che possiamo fare, e non su quello che non possiamo cambiare, tra cui:

- La creazione di un ente neutrale per la condivisione di indicatori di compromissione e vulnerabilità in tempo reale;
- Collaborazione sinergica tra aziende private e pubblica amministrazione, in maniera strutturata e sostenibile;
- Da un lato la formazione di giovani talenti nelle università, e dall'altro la formazione di figure professionali con precedenti qualifiche non necessariamente inerenti alla sicurezza informatica, ma con competenze trasferibili;
- La sensibilizzazione del top management in materia sicurezza per trainare gli investimenti all'interno di una visione strategica di crescita del business;
- L'implementazione strategica di nuove tecnologie, tra cui l'intelligenza artificiale, per l'automazione dei processi e la riduzione del carico di lavoro laddove possibile.

Per fare ciò, è sicuramente necessario unire le forze. Unisciti a noi a **Milano** dal 7 all'8 **maggio 2024** durante l'ottava edizione annuale di **ItaliaSec Summit**, per ascoltare interventi dei principali esperti di sicurezza informatica del paese, confrontarti con la community e discutere strategie concrete per rafforzare la tua security posture.

Tra gli argomenti che affronteremo nel corso delle due giornate:

- Il Panorama del Crimine Informatico nel 2023-24: Come Proteggersi e Cosa Aspettarsi in Futuro?
- Garantire la Resilienza Operativa Attraverso la Gestione della Sicurezza della Supply Chain
- Identificare e Priorizzare le Vulnerabilità per Rafforzare la Security Posture
- Applicazioni e Implicazioni dell'Intelligenza Artificiale, Attraverso la Lente della Sicurezza
- Come Affrontare con Successo le Sfide di Security Leadership, Team Building e Awareness
- Come Orientarsi nel Panorama delle Normative
- Come Possiamo Elevare la Sicurezza OT?

Scopri di più su cosa aspettarti durante il summit visualizzando il programma dettagliato dell'evento qui: **https://italy.cyberseries.io/agenda/**

Assicurati il tuo **pass gratuito*** con il codice sconto: **ITALIASEC-VIP** al checkout per avere accesso a entrambe le giornate, alle attività di networking e punti CPE per la tua partecipazione.

Registrati qui: **https://italy.cyberseries.io/register/**

*Offerta valida solo per i responsabili della sicurezza informatica. Vendor e consulenti possono ottenere uno sconto del 10% su un pass Vendor-Delegate con il codice: **ITALIASEC10**

Bibliografia ed Elenco Lettura_

- https://clusit.it/wp-content/uploads/download/Rapporto_Clusit_aggiornamento_10-2023_web.pdf
- https://www3.weforum.org/docs/WEF_Global_Cybersecurity_Outlook_2024.pdf
- https://www.pwc.com/us/en/services/consulting/cybersecurity-risk-regulatory/library/global-digital-trust-insights/pwc-2024-global-digital-trust-insights-main-report.pdf
- https://media.isc2.org/-/media/Project/ISC2/Main/Media/documents/research/ISC2_Cybersecurity_Workforce_Study_2023.pdf?rev=28b46de71ce24e6ab7705f6e3da8637e
- https://www.isaca.org/state-of-cybersecurity-2023
- https://www.fortinet.com/content/dam/maindam/PUBLIC/02_MARKETING/08_Report/report_2023-state-of-ot-cybersecurity.pdf
- https://go.crowdstrike.com/global-threat-report-2024.html
- https://www.bitsight.com/resources/gartner-top-trends-cybersecurity-2024
- https://pages.checkpoint.com/2024-cyber-security-report
- https://www.sonicwall.com/threat-report/
- https://cloud.google.com/resources/security/cybersecurity-forecast
- https://www.isc2.org/-/media/Project/ISC2/Main/Media/Marketing-Assets/CCSP/2023-Cloud-Security-Report-ISC2_final.pdf
- https://www.hornetsecurity.com/en/cyber-security-report/
- https://www.fairinstitute.org/2024-annual-cybersecurity-risk-report
- https://www.ibm.com/account/reg/us-en/signup?formid=urx-52629
- https://www.kroll.com/en/insights/publications/cyber/data-breach-outlook-2024
- https://www.cybsafe.com/whitepapers/2024-security-awareness-predictions-report/
- https://iclg.com/practice-areas/cybersecurity-laws-and-regulations/italy
- https://assets.kpmg.com/content/dam/kpmg/xx/pdf/2024/01/cyber-considerations-report.pdf
- https://www.forrester.com/bold/planning-guide-2024-security-risk/

Ringraziamo in Particolare_

- Guido Barbero, ICT CTO & CISO, Iveco
- Giampiero Bonfiglio, CISO Italy & Greece, L'Oreal
- Luca A. Giusti, CISO and Head of Infrastructure, IDM- Integra Document Management
- Daniele Luzi, Head of EMEA South Practice at Google Cloud, Google
- Vincenzo Calabrò, Information Security Officer, Ministero dell'Interno
- Andrea Licciardi, Senior Cyber Security Manager, Tecnimont
- Francesco Corrado, Head of Cyber Security, Ferrero
- Massimo Cottafavi, Director Cyber Security & Resilience, Snam
- Andrea Succi, CISO, Ferrari Group
- Paolo Cannistraro, CISO, ENGIE Italia
- Antonio Pisano, SVP Cyber & Information Security, Leonardo
- Simone Campera, Head of Cyber Security, CSM Ingredients

Per le loro interviste

Ed il Nostro Steering Committee 2024_

- Alessandro Marzi, Head of Group Cyber Defence - CISO, A2A
- Mariangela Fierro, Managing Director Cyber Security, Accenture
- Fabio Gianotti, CISO
- Yuri Rassega, CISO, Enel
- Daniele Luzi, Head of EMEA South Practice at Google Cloud, Google
- Guido Barbero, ICT CTO & CISO, Iveco Group
- Antonio Pisano, SVP Cyber & Information Security, Leonardo
- Alessio Setaro, Digital Solutions Leader, Leroy Merlin
- Lorenzo Mazzei, Head of Cyber Security BU, Lutech
- Enrico Maresca, CISO, Pubblica Amministrazione
- Bruno Sicchieri, CISO, MSC
- Daniela Mazzarone, VP, Head of Cyber Security Strategy & Governance, NTT Data
- Nicola Sotira, Head of CERT, Poste Italiane
- Sebastiano Moccia, COO & Vice General Manager, S3K
- Gian Fabio Palmerini, CISO, Webuild

Per il loro contributo alla creazione del programma