COMUNICATO STAMPA

THE INNOVATION GROUP presenta al
CYBERSECURITY SUMMIT 2024
di Milano, il prossimo 29 febbraio, la survey

"CYBER RISK MANAGEMENT 2024"

(realizzata in collaborazione con Cyber Security Angels - CSA)

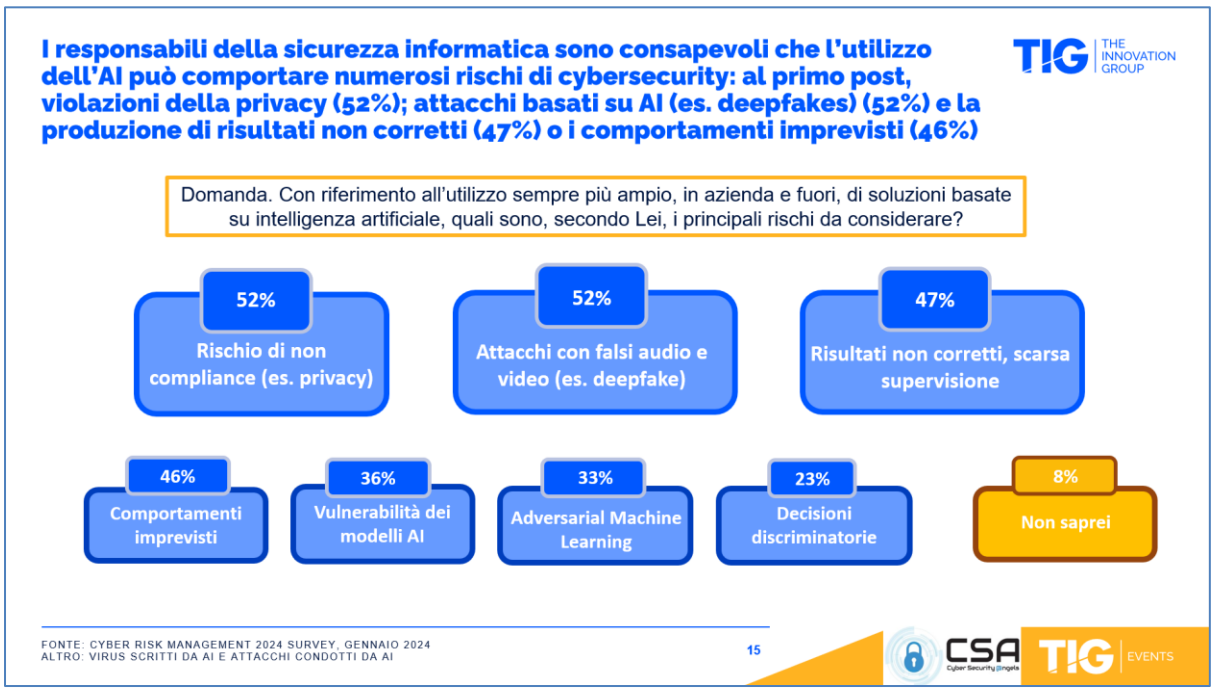
8 febbraio 2024 – A tre anni di distanza da quello che è stato l'inizio del più massiccio ricorso al digitale nella storia dell'uomo, con una digitalizzazione che continua ad accelerare, con un lavoro che diventa sempre più virtualizzato e una raccolta di big data che abilita i nuovi sviluppi dell'intelligenza artificiale, il rischio informatico è continuamente sul punto di sfuggire al nostro controllo.
Da tempo si invoca da più parti un **completo cambio di passo**, uno spostamento dell'attenzione sulla "cyber resilienza", che appare oggi (non solo perché richiesta dalle norme) un obiettivo più realistico da perseguire piuttosto che non la "cybersecurity". Quest'ultima sta diventando quasi un'illusione, vista la situazione in cui ci troviamo: attacchi molto sofisticati, incidenti caratterizzati da gravità crescente, difficoltà nell'erigere difese sufficienti, perimetro diffuso e situazione complicata da un'eterogeneità di ambienti da difendere, oltre che dalla progressiva perdita di controllo dell'IT almeno su una parte di questi.

Il paradigma è quindi cambiato: **cosa servirebbe però per la cyber resilienza**? Innanzi tutto, aver adottato un approccio al rischio informatico a livello aziendale; una comunicazione ad ampio raggio e una collaborazione e allineamento tra le parti interessate. Ad esempio, tutti i reparti che si occupano di rischio informatico dovrebbero essere coinvolti nella gestione degli incidenti informatici e le informazioni sulla cybersicurezza dovrebbero essere condivise in tutta l'azienda, per affrontare e risolvere i punti più deboli.

Le aziende sono oggi chiamate ad allineare tutte le attività di cybersecurity (le tecnologie, i processi, le persone, la governance, la compliance, i piani di gestione delle crisi e di risposta agli incidenti) in modo da costruire una reale cyber resilienza organizzativa. Oggi azienda o ente pubblico è infatti a rischio. L'indagine «**Cyber Risk Management 2024» di TIG e Cyber Security Angels – CSA** (condotta a gennaio 2024 su un campione di 166 aziende medio grandi, intervistando chi in azienda si occupa della gestione quotidiana della cybersecurity) mette in luce qual è lo stato di maturità delle aziende italiane nel percorso verso un'efficace gestione del rischio cyber. L'indagine sarà presentata nel corso del CYBERSECURITY SUMMIT 2024 di TIG, il prossimo 29 febbraio a Milano. Anticipiamo qui i principali risultati.

👉 GLI ATTACCHI CYBER SONO OSSERVATI IN GRAN NUMERO. Tutte le aziende (il 95% secondo la survey) ha osservato attacchi di phishing, il 52% spam / botnet; il 44% smishing/vishing; il 39% malware e il 36% CEO Fraud / Business email compromise.
Inoltre, una quota significativa di aziende (il 34%) afferma di aver subito un attacco ransomware: nel caso di aziende di grande dimensione, questa quota sale al 38%.

👉 METTERE IN SICUREZZA L'INTELLIGENZA ARTIFICIALE. Un tema che è emerso con prepotenza nell'ultimo anno è stato l'arrivo su larga scala delle applicazioni AI e dell'AI generativa. Dal punto di vista del Responsabile della cybersecurity, l'utilizzo dell'AI può comportare numerosi rischi di cybersecurity: al primo post, violazioni della privacy (52%); attacchi basati su AI (es. deepfakes) (52%); la produzione di risultati non corretti (47%) o i comportamenti imprevisti (46%).
Le aziende stanno però già reagendo: al fine di mitigare i rischi legati all'AI, si orientano infatti verso azioni mirate come la formazione del personale (54%) e la valutazione accurata del rischio di sicurezza associato all'AI (49%).



👉 COMPLIANCE EUROPEA ALLE PORTE. Manca poco tempo all'entrata in vigore di molte nuove norme europee. L'arrivo del regolamento europeo DORA (Digital Operational Resilience Act), la cui applicazione è prevista entro il 17 gennaio 2025, e della direttiva NIS2, entro il 17 ottobre 2024, introducono importanti responsabilità per il Board delle aziende: se un'impresa non rispetterà la NIS2, ad esempio, potrà subire una sospensione delle autorizzazioni, delle

concessioni, il CEO potrà essere sospeso dal suo ruolo. E con la NIS2, i settori impattati che rientrano nel perimetro cibernetico saranno molti di più, comprenderanno l'industria, l'agroalimentare, il chimico e il farmaceutico, che in Italia pesano molto. Le aziende si stanno preparando? Il percorso verso la conformità alle nuove norme europee è in divenire: solo un 7% delle aziende è già conforme, il 37% sta iniziando a muovere i primi passi. Quasi un quarto delle aziende non sa quali azioni intraprendere per essere conformi. Le aziende si mostrano mediamente mature su molti degli ambiti oggetto della nuova compliance europea, primo fra tutti l'autenticazione a più fattori. Ancora molto da fare invece per quanto riguarda la sicurezza della supply chain.

☛ PER LA CYBER RESILIENZA SERVIREBBE UNO SFORZO COMUNE E COORDINATO. Al momento però solo un 44% delle aziende si è posto il tema di collaborare attivamente con tutte le aree di business potenzialmente coinvolte, in modo da aumentare il controllo.
Per i responsabili della cybersecurity, la cyber resilienza si ottiene oggi con la formazione (81% degli intervistati), la tempestività della risposta (73%), test e simulazioni (63%) per verificare il livello di preparazione, visibilità estesa (55%) e threat intelligence (53%). Sono queste secondo i più le parole chiave di una efficace strategia per incrementare la cyber resilienza.

La ricerca sui temi della cybersecurity sarà presentata in anteprima durante il "CYBERSECURITY SUMMIT 2024" del prossimo **29 febbraio 2024 a Milano.**

La partecipazione al Summit è gratuita ed occorre registrarsi on line al seguente link: https://www.theinnovationgroup.it/events/cybersecurity-summit-milano-2024/?reg=1&lang=it

Per ulteriori informazioni:

Giorgia Fassoli
The Innovation Group S.r.l
giorgia.fassoli@tig.it

The Innovation Group, fondata nel 2009, The Innovation Group (TIG) è una società di servizi di consulenza e di ricerche di mercato indipendente, specializzata nello studio delle evoluzioni del settore digitale e nei processi d'innovazione abilitati dalle tecnologie e dalla conoscenza. Ci rivolgiamo ad aziende e organizzazioni dell'economia digitale che desiderano sviluppare strategie di crescita attraverso programmi e iniziative di go-to-market. Sviluppiamo analisi, ricerche, approfondimenti sul digitale, progettati per il mercato italiano. Mettiamo a disposizione piattaforme integrate di servizi e contenuti per facilitare gli scambi e le relazioni con i clienti, gli influencer, gli stakeholder e gli ecosistemi.
www.theinnovationgroup.it

CSA - Cyber Security Angels - è un gruppo di persone d'Azienda solitamente ICT & Security Manager, costituito per creare una rete di conoscenze dirette al fine di far fronte comune alle problematiche nascenti sul fronte della Cyber Security. Un incidente cyber o un problema di governance non deve essere causa di frustrazione, ma un'occasione per potersi confrontare tra colleghi competenti, non solo per trovare una soluzione, ma anche per allertare e aiutare altri colleghi a fare prevenzione. L'approccio migliore per affrontare questi problemi è lavorare in squadra sul campo affidandosi non solo ai report di un fornitore o a soluzioni proposte da un vendor.
Obiettivi della community fra le sole aziende è la Security by Sharing che vuol dire:

- *Aumentare la resilienza scambiando le informazioni su nuovi tipi di attacco. Avere dei suggerimenti su come proteggersi meglio svincolato da logiche di prodotto.*
- *Possibilità di scambiarsi informazioni sugli incidenti, sulla qualità dei prodotti, degli integratori e dei servizi.*
- *Neutralità al di fuori del network dei Vendor, Integratori e Consulenti con la garanzia della discrezione, anonimato e riservatezza.*
- *Chi crede che la cybersecurity italiana non sia un tabù ha la possibilità di conoscere in modo anonimo nuove startup nel bacino nazionale che propongono soluzioni e servizi innovativi.*
- *C'è la possibilità di verificare le referenze e i livelli di servizio per arrivare fino ad una piattaforma di ranking di chi si occupa di Cybersecurity.*
- *Canale di comunicazione condiviso su base etica per chiedere suggerimenti sui problemi e su come risolverli.*

https://cybersecurityangels.it