Security Intelligence in ambito aziendale, una sfida impegnativa

Security intelligence in ambito aziendale, una sfida impegnativa anche per un convegno. Chiediamo a Salvatore Castiglia, general manager di Kriptia un bilancio di quello organizzato il 20 giugno con un parterre di relatori di primissimo piano.

La Security Intelligence da sempre è un bene essenziale in cui le aziende hanno investito e che imprenditori illuminati hanno utilizzato come base per i loro progetti.
Purtroppo, negli ultimi anni si sta divulgando un trend piuttosto pericoloso che vuole il dirottamento della security aziendale nella cyber security, addirittura confondendo o sovrapponendo i ruoli. Le aziende non erano in passato – e spesso non sono oggi – preparate a rispondere alle minacce cyber, questo anche perché sempre meno aziende, soprattutto PMI, si affidano a società esterne per analizzare i loro rischi. Di conseguenza si nota come abbiano spostato gran parte dei budget di security fisica nella cyber security. Inoltre alcuni security manager senza nessuna competenza in cyber security ne sono diventati responsabili, unificando così i ruoli. Volendo fare un paragone, è come se l'HR manager diventi improvvisamente anche il responsabile commerciale. Sempre meno infatti si assiste a strutture organizzate, dove un team con diverse peculiarità lavora sul progetto e senza demandare al singolo manager la responsabilità (e quindi il budget) di tutto ciò che è security.
Il 20 giugno abbiamo voluto dare voce a quei professionisti che lavorano su settori diversi ma sempre in ruoli inerenti alla funzione di security aziendale. Abbiamo sentito dalla dott. ssa Gubbiotti e dalla dott.ssa Pieroni come i dati e la loro analisi sia un valore per le aziende e che non sempre queste siano disponibili ad investire soldi e tempo in questo tipo di attività. Abbiamo ascoltato il dott. Farris e il dott. Florio per quanto riguarda il tema della sicurezza fisica in relazione ai temi del Risk Management e della Travel Security. Abbiamo approfondito con il dott. Colella e l'ing. Tofalo il tema cyber nelle aziende e le relazioni tra cyber e fattore umano all'interno delle aziende. Per ultimo, ma non meno importante, con il prof. Pigoli abbiamo trattato l'uso dell'intelligence in ambito aziendale a fronte dell'ecosistema produttivo italiano, unendo così i temi di sicurezza fisica e cyber security.

Una delle conclusioni del convegno è la ritrovata centralità della persona, tutt'altro che scontata nell'era della A.I. Quali sono i presupposti che hanno portato a questa conclusione?
Il fattore umano è da sempre un tema centrale, in tutti i settori. Anche nell'automazione, senza dei bravi ingegneri non riusciremmo ad automatizzare nulla. Il sottile confine sta nel limitare l'utilizzo di AI e delle varie tecnologie di automatizzazione per velocizzare i processi e quindi essere più produttivi. Al contrario, sbagliando, si tende a pensare di poter sostituire semplicemente l'essere umano con la macchina.
Nell'ultimo periodo ho letto diverse notizie sull'automatizzazione di analisi e report. Mi preme però sottolineare che lo stesso concetto di analisi prevede una ricerca e comprensione di diversi elementi che spesso non possono essere sostituiti da un algoritmo.
Allo stesso tempo, il fattore umano spesso può rappresentare il punto debole della catena di security, basti pensare alle mail di phishing o ad un badge lasciato in auto. Entrambi questi esempi, per quanto sembrino due problemi inerenti a settori diversi (fisico e cyber), rappresentano invece allo stesso modo una criticità per la sicurezza dell'azienda, da trattare sia nella parte fisica che nella parte cyber.

Un'altra conclusione, più scontata, è la necessità di raggiungere le PMI, l'anello debole della cybersecurity, per aumentare il loro livello di sicurezza. Quali sono gli strumenti indicati?
In realtà le PMI spesso riflettono ciò che il mercato propone come best practise e di solito sono le grandi aziende a svolgere il ruolo di "influencer" in tutti i settori, dall'HR, alla contabilità, alla security. Quindi bisogna sottolineare che purtroppo anche i malcostumi e tendenze controproducenti alcune volte possono essere generate da multinazionali o associazioni di categoria, le quali spesso diffondono messaggi sbagliati o addirittura fuorvianti. Entrando nel merito, non sempre le PMI hanno le competenze per analizzare e comprendere questi messaggi e quindi si assiste ad amministratori di aziende di PMI che non disponendo di security manager affrontano anche problematiche complesse senza strategie adeguate, con il rischio di provocare danni maggiori.
Proprio per aiutare le PMI, Kriptia ha pensato di creare una piattaforma che possa gestire i rischi aziendali ed essere in linea con la normativa, rendendo così l'azienda sempre più compliant. Lo strumento che abbiamo creato si chiama Krion

e gestisce i rischi legati alla sicurezza con audit di security (cyber e fisico), analisi controparte e travel security.

Partenariato pubblico-privato: in che modo può venire realizzato in modo efficace?

Il partenariato pubblico-privato (PPP) nella security aziendale è una forma di collaborazione tra enti governativi e privati per garantire la sicurezza delle aziende e degli impianti. Questa forma di partenariato coinvolge solitamente organizzazioni governative responsabili della sicurezza pubblica, come forze dell'ordine, agenzie di intelligence e agenzie di sicurezza, insieme a società private che offrono servizi di sicurezza aziendale.

L'obiettivo principale del partenariato pubblico-privato nella security aziendale è proprio quello di migliorare la prevenzione e la gestione delle minacce alla sicurezza, proteggendo le aziende da rischi come il furto, il danneggiamento, l'accesso non autorizzato, la violazione dei dati e il terrorismo.

In un modello di PPP, le autorità governative possono fornire informazioni sulle minacce alla sicurezza, offrire consulenza sulla pianificazione e la gestione della sicurezza e partecipare a operazioni di intelligence condivise. Le aziende private, d'altra parte, contribuiscono con le proprie risorse e competenze nella sicurezza aziendale, mettendo in atto misure di sicurezza, ad esempio, implementando sistemi di sorveglianza avanzati, addestrando il personale aziendale alla gestione delle emergenze e fornendo servizi di consulenza sulla sicurezza.

A mio avviso, i vantaggi del partenariato pubblico-privato nella security aziendale includono una maggiore efficacia nella prevenzione e nella risposta alle minacce alla sicurezza, una condivisione più rapida e accurata delle informazioni pertinenti e una migliore allocazione delle risorse. Inoltre, esso può promuovere la collaborazione e la condivisione delle migliori pratiche tra le organizzazioni pubbliche e private, contribuendo a creare un ambiente di sicurezza più resiliente. Tuttavia, è importante garantire che il partenariato pubblico-privato nella security aziendale sia basato su una solida base legale, che vengano rispettati i diritti e le norme sulla privacy e che venga stabilita una chiara responsabilità delle attività svolte. La collaborazione deve essere trasparente e i ruoli e le responsabilità di ciascuna parte devono essere definiti in modo chiaro per evitare ambiguità o abusi di potere.

Quindi che ruolo ha la Security Intelligence nell'azienda e quali sono le sfide future?

La Security Intelligence svolge un ruolo fondamentale nell'azienda nel rilevare, analizzare e rispondere alle minacce alla sicurezza. Questa funzione si concentra sulla raccolta di informazioni provenienti da una varietà di fonti, inclusi i dati interni dell'azienda, le informazioni pubbliche, i rapporti di intelligence governativa e le informazioni provenienti da partner esterni. L'obiettivo principale della Security Intelligence è fornire una visione approfondita delle minacce e delle vulnerabilità per prendere decisioni informate e implementare misure di sicurezza adeguate.

Per quanto concerne le sfide future, sicuramente sarà sempre più rilevante la crescita del volume dei dati a disposizione, ciò richiede l'adozione di strumenti e tecnologie avanzate come, per esempio, il machine learning e l'intelligenza artificiale, per estrarre informazioni significative dai dati in modo rapido ed efficace. Questo a fronte di una "guida" umana che deve essere sempre garantita anche solo per verificare che siano rispettate le normative sulla privacy. Le sfide coincidono anche con minacce sempre più sofisticate e la Security Intelligence deve essere in grado di adottare misure preventive adeguate e tenere il passo con le ultime tendenze e tecniche utilizzate dagli aggressori.

Come si diceva per le PMI, la mancanza di personale qualificato in queste aree rappresenta sicuramente una sfida per molte aziende, che devono investire nella formazione interna o cercare soluzioni esterne per colmare questa lacuna.

In conclusione, per affrontare queste sfide è importante che le aziende investano nella Security Intelligence come parte integrante delle proprie strategie di sicurezza. Ciò include l'implementazione di infrastrutture tecnologiche adeguate, l'aggiornamento costante delle competenze del personale e la collaborazione con partner affidabili nel settore della security.

KRIPTIA
SECURITY AND SAFETY SOLUTIONS

Contatti:
Kriptia
Milano +39 02 40031293
Miami (USA) +1 888 2496107
info@kriptia.it