COMUNICATO STAMPA

«CYBERSECURITY IN AZIENDA», IL CONVEGNO DI CONFAPI BRESCIA E DEL COMANDO PROVINCIALE DELL'ARMA DEI CARABINIERI DI BRESCIA

Ufficio Studi Confapi Brescia: quattro imprese su dieci hanno subito attacchi informatici

Comando provinciale dell'Arma di Brescia: collaborazione con istituzioni e imprenditori per accrescere consapevolezza e sicurezza

Brescia, 15 marzo 2023 – La cybersicurezza rientra a pieno titolo tra le condizioni imprescindibili per la conduzione di qualsiasi attività, che sia produttiva o amministrativa, senza distinzioni. Un impegno composito, imperniato su cultura, consapevolezza, buone pratiche, tecnologie, investimenti e continui aggiornamenti. Per contribuire ad innalzare la conoscenza del tema, **Confapi Brescia** e **Comando Provinciale dell'Arma dei Carabinieri di Brescia** hanno realizzato il convegno dal titolo «**Cybersecurity in azienda: rischi, soluzioni, responsabilità e prevenzione**», ad un anno di distanza dal primo seminario condiviso dedicato al trattamento dei rifiuti e alla salvaguardia degli illeciti ambientali. Tali eventi si inseriscono nel perimetro delle attività previste dal **protocollo** sottoscritto a livello **nazionale** a giugno 2021 dalla Confederazione italiana della piccola e media industria privata **Confapi** e **Arma dei Carabinieri**. Un accordo che propizia l'organizzazione condivisa di iniziative informative su tre direttrici tematiche fondamentali per la tutela e il supporto alle imprese (tutela dell'ambiente e dei dati informatici e prevenzione infiltrazione criminale nelle imprese).
«Occasioni di incontro e confronto tra cittadini imprenditori e istituzioni, come quella organizzata oggi grazie alla collaborazione tra l'Arma dei Carabinieri e Confapi Brescia, permettono di favorire lo scambio di conoscenze e competenze e la diffusione di best practices in un settore, la cybersecurity, sempre più impattante sulle nostre vite quotidiane, in continua, rapida ed esponenziale evoluzione, consentendo così di accrescere il livello di consapevolezza e quindi anche di sicurezza - ha dichiarato il Colonnello **Vittorio Fragalà**, **Comandante Provinciale dei Carabinieri di Brescia**».

Cybersicurezza: l'indagine del Centro Studi Confapi Brescia

Il **40% delle aziende associate a Confapi Brescia ha già subito un attacco di natura informatica**. Questo è il primo dato che emerge dall'indagine condotta dal **Centro Studi di Confapi Brescia**, le cui conclusioni sono state presentate, in apertura di convegno, dal **presidente Pierluigi Cordua**. «Le nostre imprese hanno già vissuto direttamente i rischi provenienti dalla rete – ha affermato il presidente -. In particolare, hanno subito clonazioni di e-mail, furti di password (*31% degli intervistati*), ma la casistica di attacco è diversificata, a testimonianza di quanto una messa in sicurezza totale sia estremamente complessa». Le aziende associate, inoltre, si dimostrano in larghissima parte già attive nell'implementazione di strumenti e prassi volte al contenimento del rischio di attacchi informatici. «**L'89% delle imprese ha già investito in cybersicurezza** – continua Cordua -, dimostrando un impegno diretto alla tutela informatica». Due, però, le considerazioni emerse dallo studio. «Il **40% delle aziende dichiara di doversi affidare completamente a consulenti esterni**, a causa della difficoltà a comprendere prassi e soluzioni da attuare. Inoltre, per **41 associati su 100 le spese crescenti per la cybersecurity trovano complessa copertura nelle maglie dei bilanci aziendali e altre 23 registrano difficoltà**. Proponiamo, pertanto, questo convegno per permettere di diffondere una consapevolezza maggiore di rischi e strumenti che consentano di dare continuità agli interventi e agli investimenti a tutela del patrimonio informatico delle nostre associate».

Le dimensioni del fenomeno nel contesto attuale

«I dati del **Rapporto Clusit 2023** che abbiamo presentato ieri nel contesto del *Security Summit* ci devono mettere in allerta – afferma **Alessio Pennasilico**, membro del **Comitato scientifico di Clusit**, l'associazione italiana per la sicurezza informatica -. Gli **attacchi informatici** nel nostro Paese sono **cresciuti del 169%** nell'ultimo anno e quasi sempre vengono compiuti con tecniche note e standardizzate, messe a punto da quella che definiamo ormai l'industria del *cyber-crime*, con **impatto grave o gravissimo nell'83%** dei casi. Malware, vulnerabilità, phishing, social engineering ed account cracking sono ancora ampiamente utilizzati dai criminali informatici, che trovano ampio spazio laddove non sappiamo gestire correttamente i nostri account, non teniamo aggiornati i nostri

dispositivi, server o servizi, e clicchiamo incautamente link pericolosi nelle e-mail». Uno scenario pesantemente segnato dalle tensioni internazionali. «È innegabile come la congiuntura politico economica creatasi nel 2022, complice specialmente il conflitto russo-ucraino, abbia fatto da trampolino di lancio per intensificate attività di puro cyber – ha affermato **Pierguido Iezzi**, **CEO** di **Swascan**, tra i principali player italiani della sicurezza informatica -. Anche per il 2023, quindi, la fotografia dell'ecosistema digitale emergente è insidiosa. È chiaro, oramai, come ogni azienda sia un bersaglio raggiungibile e, grande o piccola che sia, ha operazioni, marchio, reputazione o canali potenzialmente a rischio. L'attenzione per migliorare le difese deve essere rivolta sia alla superficie e sia ai vettori di attacco per determinare cosa si può fare per mitigare le minacce e migliorare la resilienza e il ripristino. L'adozione di una **difesa informatica,** basata su **difesa predittiva**, **preventiva** e **proattiva**, diventa ancora di più **imprescindibile**». Atmosfere internazionali tese alle quali rispondono sistemi normativi in evoluzione. «I legislatori nazionale e UE stanno emanando norme idonee a rispondere alle sofisticate minacce informatiche – ha descritto l'avvocato **Matteo Piccinali**, partner dello **Studio legale Zaglio – Orizio** -. Si tratta di una legislazione rivolta ai grandi operatori, ma anche ai loro fornitori, in modo da garantire la sicurezza informatica lungo le filiere di settore. Anche le PMI, quindi, devono attrezzarsi con l'adozione preventiva di misure di sicurezza organizzative, documentali e contrattuali per la mitigazione del rischio, in modo da essere più affidabili per i propri partner commerciali e aumentare la possibilità di negoziare un'adeguata copertura assicurativa del rischio informatico».

Consapevolezza base della sicurezza

La cultura della sicurezza va instradata e, successivamente, seguita con rigore e attenzione. Ne hanno analizzato le caratteristiche fondamentali, gli strumenti, le principali aree di rischio, e trasferito le buone pratiche da seguire, il **tenente colonnello Francesco Tocci**, **Comandante del Reparto Operativo di Brescia**, il **tenente colonnello Cesare Nascè**, **comandante del Gruppo Carabinieri Forestale di Brescia** e il **maggiore Alberto Degli Effetti**, **Comandante del Nucleo Investigativo di Brescia**. «La security awareness consiste nel rendere le persone e le organizzazioni consapevoli delle attuali minacce informatiche, mettendo a disposizione gli strumenti più adatti per prevenire, riconoscere e reagire agli incidenti informatici (*data breach*) – ha affermato il tenente colonnello Tocci -. Nella cybersecurity occorre evidenziare la **centralità della persona**. Infatti, la resilienza o la fragilità di un sistema di cyber security sono fortemente condizionate dal fattore umano e dalle tipiche debolezze che contraddistinguono i nostri comportamenti (abitudinarietà, tendenza a fidarsi, superficialità, avversione verso le restrizioni, ect.): occorre quindi investire sulla persona, sulla sua formazione e aggiornamento. Infatti, sebbene non esista la sicurezza informatica assoluta, vi sono comportamenti, procedure, piani di azione, soluzioni da adottare nel quotidiano per ridurre il rischio di attacchi informatici». Il tenente colonnello Nascè ha approfondito il tema dei dati, della loro difesa, a partire dal **Regolamento Generale sulla Protezione dei dati (GPDR)** redatto con il fine ultimo di garantire ad ogni persona il diritto alla protezione dei dati di carattere personale. «L'approccio su cui si fonda il regolamento è basato sul rischio e su misure di accountability di titolari e responsabili del trattamento dei dati personali, i quali hanno l'obbligo di decidere autonomamente e proattivamente le modalità, le garanzie e i limiti del trattamento dei dati personali – ha descritto -. Il GDPO ha previsto altresì una serie di azioni obbligatorie nel caso in cui si verifichino incidenti informatici e violazioni di dati personali (Data Breach), una delle quali è la tempestiva notifica alle autorità di controllo competenti». Il maggiore Degli Effetti ha descritto le più frequenti tipologie di attacco informatico, offrendo un *vademecum* delle *best practices* che ne mitigano i rischi. «I più frequenti attacchi sono finalizzati ad estorcere del denaro dopo aver sottratto informazioni sensibili minacciandone la diffusione, oppure inducono in errore l'utente che, attraverso una serie di raggiri, viene convinto a comunicare dati personali quali il numero della carta di credito, le password, i conti correnti o, addirittura, a pagare somme di denaro direttamente on line». A fronte di uno scenario così vario, sono numerose le buone pratiche trasmesse, che «nella speranza di far riflettere chiunque a non sottovalutare il tema, **migliorano la propria sicurezza attraverso accorgimenti** di varia natura, quali ad esempio la scelta di una password adeguata, una policy della riservatezza del dato, la cancellazione delle nostre informazioni dai file temporanei che si alimentano automaticamente durante la navigazione e la necessità di dotarsi di sistemi di recovery plan e business continuity». In ambito aziendale, l'opera in tema di sicurezza informatica si sviluppa su due direttrici. «La **cybersecurity** si occupa principalmente di **proteggere le entità** dai rischi informatici – ha descritto **Fabrizio Fujani**, **Business Stream Manager TÜV Rheinland Italia S.r.l.,** primario ente di certificazione multinazionale tedesco -; la **sicurezza delle informazioni** si rivolge al **mantenimento della riservatezza**, dell'integrità e della disponibilità delle informazioni. La cybersecurity è pertanto rivolta al mezzo, l'information security al contenuto: due punti di vista convergenti su cui investire e crescere per essere oggi sostenibili da un punto di vista della Governance».

Strumento che accerta la bontà del percorso aziendale è «la certificazione secondo la ISO 27001:2022 che permette di dimostrare che la tua azienda sta seguendo le best practice sulla sicurezza delle informazioni e fornisce un controllo indipendente e qualificato sul fatto che la sicurezza delle informazioni sia gestita in linea con le best practice internazionali e gli obiettivi aziendali».

La cybersicurezza di una banca digitale. Il caso di illimity bank

illimity è un gruppo bancario ad alto tasso tecnologico e, attraverso la testimonianza del proprio **Chief Information Officer Filipe Teixeira**, ha trasferito una panoramica delle strategie di sicurezza informatica attuate per la tutela della propria operatività. La scelta, sin dalle origini, di optare per una struttura interamente digitale ha imposto una progettazione complessa, ma anche, in prima istanza, una riflessione rispetto alle caratteristiche sottese alla digitalizzazione stessa. «Era digitale significa un'esplosione di complessità – ha affermato il CIO di illimity -. Inoltre, necessita di un costante e strutturato adattamento per venire incontro alle aspettative dei clienti. Ed è proprio nell'identificazione di un giusto equilibrio tra le aspettative dei clienti e la cybersecurity la sfida fondamentale da vincere per un business come il nostro».

Ufficio Stampa – Confapi Brescia
Tel. 030 23076 - ufficiostampa@confapibrescia.it