VareseNews

CybergON presenta alle aziende come proteggersi dal fenomeno del cybercrime

Pubblicato: Mercoledì 18 Ottobre 2023

Le aziende italiane sono oggetto di una crescita vertiginosa di attacchi informatici. Nonostante le organizzazioni abbiano aumentato **il budget per soluzioni e servizi di cybersecurity,** nell'ultimo anno, secondo i dati del Clusit, si sono verificati **oltre 190 attacchi gravi in media al mese di cui l'80% con conseguenze importanti** quali interruzione del business, danni reputazionali e richiesta di riscatti.

Ma sotto questo trend si cela un secondo fenomeno che richiede l'attenzione e la responsabilità di ogni persona: la democratizzazione degli attacchi attraverso i meccanismi di social engineering.
Attraverso tecniche sofisticate che sfruttano i bias cognitivi, i cybercriminali ottengono informazioni personali tramite l'inganno. In questo scenario, **gli errori umani** acquistano così un ruolo e **impatto** sempre più **critico** sulle imprese e il risultato è che gli incidenti informatici che colpiscono aziende di ogni settore e dimensione sono all'ordine del giorno.

Queste sono le principali evidenze emerse nell'evento "**Cyber Things – Uomo e Tecnologia: le due dimensioni del SottoSopra"**, promosso da **CybergON,** la business unit di Elmec Informatica dedicata alla cybersecurity, che in questa **seconda edizione** ha esplorato la complessa **interazione tra mente umana e tecnologia**, tra dinamiche oscure legate all'individuo e dinamiche legate alle soluzioni di cyber attacco.

Hanno partecipato relatori d'eccezione come **Massimo Picozzi** (criminologo e medico specialista in

psichiatria e criminologia clinica), **Lisa di Berardino** (Vice Dirigente del Compartimento Polizia Postale e delle Comunicazioni della Lombardia), **Sonia Montegiove** (giornalista, informatica, formatrice e coordinatrice di Cyber Trials, programma gratuito di formazione e gaming per studentesse delle scuole superiori di II grado organizzato dal Laboratorio Nazionale di Cybersecurity del CINI), **Mattia Coffetti**(biohacker e informatico), **Marco Rossi** (CIO di una primaria azienda del settore alimentare italiana) e **Matteo Jemoli** (Responsabile scouting e Assistant General Manager della Pallacanestro Varese).

Il dibattito è stato aperto da **Alessandro Ballerio**, Amministratore Delegato di Elmec Informatica: "In questo momento storico le preoccupazioni di un'azienda sono i tassi di interesse, lo scenario internazionale, l'approvvigionamento energetico e tutto questo alimenta il rischio di abbassare la guardia. Tuttavia, le minacce informatiche non sono diminuite: nel secondo quarter del 2023 gli attacchi sono cresciuti del 36% secondo il Clusit e l'83% degli attacchi sono stati rivolti alle PMI. Un'azienda che subisce un attacco informatico può andare incontro almeno a due settimane di blocco dei sistemi informativi e per tornare a regime ci vogliono almeno 2 mesi. Sullo sfondo di questo scenario, che cosa possiamo fare? Parlarne in azienda per sensibilizzare e spingere queste realtà a investire in cyber security".

Nella sua **introduzione**, **Massimo Picozzi**, criminologo e medico specialista in psichiatria e criminologia clinica, ha analizzato come e cosa accade nella mente di un cyber criminale e come e cosa succede nella testa di chi continua a cadere in queste trappole: "Nel mondo digitale, i confini sono meno definiti e le dinamiche psicologiche possono essere ancora più intricate. Studiare i meccanismi che portano un individuo a commettere un crimine online, così come comprendere le motivazioni e le vulnerabilità delle vittime, richiede un approccio multidisciplinare che unisca psicologia, criminologia e tecnologia. I predatori digitali si caratterizzano per la cosiddetta triade oscura: narcisismo, psicopatia e machiavellismo. Il più grande studioso di personalità psicopatiche al mondo ha scoperto una cosa interessante: si era inventato un test per cogliere la patologia e dopo 20 anni lo ha modificato con il nome di business scan 360 che ha rivelato che dal 4 al 10% del top management a livello mondiale ha un profilo da serial killer. Un ultimo input con cui vi lascio è la tecnica di persuasione più efficace: la reciprocità. Significa che se qualcuno ci da qualcosa noi strutturalmente riteniamo di dover rispondere e ricambiare. Quindi ogni spinta gentile, anche detta Nudge, invita l'altro a un comportamento positivo, viceversa, cadiamo nella trappola".

> Massimo Picozzi racconta i predatori digitali: "Non siamo consapevoli delle minacce"

La successiva **tavola rotonda** ha permesso di confrontarsi sulle minacce e le **tecnologie nelle loro nuove versioni**, approfondendo un cambiamento che coinvolge confini prima **inesplorati:** la diffusione delle minacce informatiche che prendono di mira sia il professionista, sia il privato cittadino, passando dai canali di comunicazione personali sfruttando il metodo del social engineering per esfiltrare informazioni sensibili.

Sonia Montegiove, giornalista, informatica, formatrice e coordinatrice di Cyber Trials, programma gratuito di formazione e gaming per studentesse delle scuole superiori di II grado organizzato dal Laboratorio Nazionale di Cybersecurity del CINI ha affermato che**: "**Gli attacchi sono in crescita rapida: gli attacchi informatici sono cresciuti del 527% nel periodo 2018-22 e del 170% nell'ultimo anno secondo i dati del Clusit. Le realtà più attaccate sono la PA, attorno al 20% dei casi, e le aziende manifatturiere (19%). La minaccia principale continua a essere quella del ransomware e l'elemento umano è purtroppo ancora l'anello debole della catena su cui c'è ancora tanto da fare in termini di formazione. In una scala da uno a dieci, la sicurezza dello spazio digitale delle aziende presenta un livello variabile, ma generalmente si colloca al di sotto della soglia di un livello ottimale. Pertanto, è necessario educare e formare il personale a promuovere una cultura di sicurezza all'interno

dell'organizzazione".

Successivamente, **Marco Rossi**, CIO di una primaria azienda del settore alimentare italiane ha commentato: "Le aziende stanno ancora sviluppando la cultura del rischio e le PMI che pensavano di essere al riparo per la loro piccola dimensione sono sempre più esposte alle minacce informatiche. La tecnologia di attacco è diventata economicamente più accessibile e sono aumentati i cybercriminali che si accontentano di attaccare piccole realtà. Le PMI devono prepararsi ad affrontare i rischi legati alla non formazione dei dipendenti che ne indeboliscono le difese. Sembra un dettaglio, ma la prima attività da fare è eliminare i post-it con le password. Poi occorre puntare alla password protection sensibilizzando i dipendenti a tutelare il proprio account. Le imprese sono particolarmente focalizzate sui risultati immediati ma occorre che questa focalizzazione non vada a scapito della sicurezza informatica che deve essere progettata e non essere solo un rimedio".

A seguire, **Mattia Coffetti,** biohacker e informatico ha attinto alla sua esperienza personale aggiungendo che: "Una buona attività di formazione dovrebbe fornire anche una panoramica completa del fenomeno del social engineering per stimolare una riflessione critica. Ricordiamoci che tutti siamo targettizzati: l'ingegneria sociale viene utilizzata per il furto di identità attraverso i social media. I cybercriminali mirano a catturare la fiducia della persona e solo un'adeguata formazione consente di riconoscere le minacce. Per cominciare, le aziende devono promuovere un dialogo aperto tra dipendenti per valorizzare l'apprendimento continuo e conoscere le nuove tecnologie emergenti."

Lisa Di Berardino, Vice Dirigente del Compartimento Polizia Postale e delle Comunicazioni della Lombardia ha approfondito le minacce alle famiglie con cui si imbatte ogni giorno: "Quando ci imbattiamo in utenti e famiglie che sono finiti in trappola a causa di attacchi cyber, la prima cosa che facciamo è ascoltare attentamente le loro preoccupazioni, offrire un sostegno emotivo e informarli. Si sta verificando una democratizzazione del rischio. Siamo tutti coinvolti e tutti responsabili. Il phishing oggi è vishing, via telefono, o smishing, via SMS e occorre anzitutto mettere in atto piccole pratiche diligenti: ad esempio sapere che la banca non chiama direttamente al telefono; conoscere l'importanza di non lasciare i nostri dati su siti non affidabili; evitare di cliccare sulle proposte di investimento che richiedono cifre via via sempre più ingenti, e che spesso portano l'utente a farsi supportare da remoto da questi malintenzionati concedendo l'accesso al proprio computer. Come Polizia Postale forniamo informazioni chiare e accurate alle famiglie sulle azioni da intraprendere per risolvere la situazione con l'obiettivo di aiutarli a ricostruire la loro sicurezza online e prevenire futuri rischi".

Matteo Jemoli, Responsabile scouting e Assistant General Manager della Pallacanestro Varese ha invece illustrato un esempio positivo dell'utilizzo consapevole dei dati:"Utilizziamo i dati nella gestione dei giocatori per supportarli a migliorare le proprie performance. I nostri ricordi ci portano a valutare un giocatore per un canestro spettacolare, ma abbiamo necessità di capire quanti invece non sono andati a segno e perchè. Gli anaylitcs ci consentono di supportare il giocatore non con un'idea o una suggestione, ma con dei fatti concreti".

È stato poi presentato il **nuovo podcast "Cyber Things – Elmec & CybergON"** insieme a **Paolo Girella**, Direttore editoriale di Emons Record. Il podcast è interamente dedicato alla cybersecurity e vuole offrire un servizio a chiunque lo ascolti trattando temi e casi reali legati alle truffe online, al cyber bullismo, alle attuali cyber wars con moventi economici e molto altro. Le puntate sono già disponibili sulle principali piattaforme online.

La giornata è stata chiusa da **Filadelfio Emanuele**, CISO di Elmec Informatica Spa e Responsabile di CybergON, che ha voluto lanciare un messaggio: "La difesa richiede la responsabilità di tutti, dall'essere azienda, cittadino o genitore. Come CybergON ed Elmec Informatica forniamo la competenza e la capacità di mettere a terra un sistema di difesa efficace e sostenibile nel tempo con l'obiettivo di ridurre i rischi legati al cybercrime".

Tutti i partecipanti all'evento hanno avuto, infine, anche la possibilità di esplorare l'**"Hawkins Lab"** di

CybergON – dedicato alle diverse tecnologie di Cyber Security come SOC, OT Security, Zero-Trust, Cloud Security per comprendere come adottare le strategie di difesa e la resilienza in azienda – e visitare il Campus Tecnologico di Elmec che ha aperto le porte per l'occasione.

Redazione VareseNews
redazione@varesenews.it