CYBERSPIONAGGIO: IL CASO DEI FRATELLI OCCHIONERO. COME DIFENDERSI DAL CRIMINE INFORMATICO

L'economia altalenante, l'evoluzione tecnologica e l'internazionalizzazione del mercato, inducono sempre più a mettere al centro dell'attenzione pubblica i temi e i problemi connessi alla tecnologia informatica che avanza ormai con passo inarrestabile, favorita da un livello di controllo e monitoraggio così fragile da mettere a rischio infrastrutture e cittadini. Tra i principali rischi che invadono la rete si colloca ai primi posti il furto di informazioni a scopo di frode, siano esse personali, aziendali, sanitarie, economiche e politiche. Si tratta di un crimine esistente da sempre e che oggi più che mai, con l'avvento dell'evoluzione digitale, sta crescendo in maniera smisurata supportando i moderni criminali con sistemi nuovi e sempre più all'avanguardia e in grado di "rubare" dati preziosi raggiungendo le finalità illecite prefissate.

L'utilizzo abituale delle e-mail, il ricorso frequente a piattaforme digitali, social network e chat per condividere informazioni, esperienze, immagini, momenti di vita quotidiana, la pratica ormai diffusa degli acquisti on-line, l'effettuazione per via telematica di operazioni considerevoli, quali trasferimenti di fondi, operazioni finanziarie, quotazioni in borsa, facilitano notevolmente la libera circolazione di dati personali, rendendo tutti noi navigatori del web sempre più vulnerabili e indifesi, con conseguenti gravi danni economici e sociali.

Ed ecco che, ancora una volta, un recentissimo caso di cronaca ha riportato in auge negli ultimi giorni il problema del crimine informatico e dell'importanza sempre più sentita di adottare strumenti di protezione sicuri ed efficienti, nella vita lavorativa e ancor di più nella vita privata.

Eclatante, dunque, la vicenda giudiziaria sul presunto caso di cyberspionaggio che il 10 Gennaio ha condotto all'arresto dei fratelli Occhionero, Giulio e Francesca Maria, residenti a Londra ma domiciliati a Roma, lui titolare di una società di consulenza finanziaria, la Westlands Securities, finita a sua volta nell'inchiesta, accusati di aver sottratto informazioni dopo aver "iniettato il virus" nei computer di numerosi rappresentanti di spicco del mondo della politica, tra i quali l'ex Presidente del Consiglio Matteo Renzi, dell'economia, tra i quali il presidente della Banca Centrale Europea Mario Draghi, delle Forze dell'Ordine, della Massoneria, e ancora nomi noti di professionisti, sindacalisti e imprenditori.

Procacciamento di notizie concernenti la sicurezza dello Stato, accesso abusivo a sistema informatico aggravato e intercettazione illecita di comunicazioni informatiche o telematiche: sono queste le accuse mosse nei confronti dei fratelli Occhionero. L'indagine, condotta dalla Procura di Roma, ha avuto inizio nel marzo del 2016 quando un addetto alla sicurezza dell'Enav riceveva una mail da una casella di posta sospetta. Si procedeva dunque ad una verifica della mail in questione, verifica che identificava l'indirizzo IP del mittente, tra gli indirizzi "agganciati" con il phishing. La mail in questione conteneva un malware denominato EyePiramid, in grado di inoltrare tutti i dati del dispositivo infettato presso un server ubicato negli Stati Uniti. In sostanza, secondo gli investigatori gli Occhionero avrebbero estrapolato una copia di tali dati, sottraendoli prima che la vittima potesse accorgersene. È stato disposto il sequestro del server su cui sono stati archiviati tali dati, per poter poi procedere all'attività di analisi forense che, unita all'attività di indagine classica, fornirà maggiori sviluppi sul prosieguo della vicenda.

Alla luce delle ultime vicende che hanno interessato il fenomeno criminale informatico, è dunque lecito chiedersi se e come difendersi da tale tipologia di crimine.

"La sicurezza informatica, concetto sinora ben poco compreso dalle aziende italiane, sta rapidamente mutando, sotto la spinta di un'innovazione tecnologica costante e di un ruolo crescente e sempre più pervasivo dell'informatica - afferma Salvatore Piccinni, Senior Security e Intelligence Analyst di Inside Agency, agenzia specializzata in sicurezza, con sedi in USA, Russia, Emirati Arabi, Brasile, Svizzera, UK, Hong Kong e Sudafrica, e sbarcata anche in Italia, al fine di dare supporto alle aziende nella gestione e valutazione del rischio economico, finanziario e reputazionale di enti, persone fisiche, *stakeholder* e partner commerciali – *Purtroppo mancano ancora cultura e attenzione al fenomeno del crimine informatico e questo vuol dire che le aziende non attribuiscono la giusta importanza alla tutela dei dispostivi utilizzati quali strumenti per favorire crescita e innovazione. Oggi, circa il 40% delle informazioni aziendali viene archiviato su tablet e smartphone, i dati vengono dunque disgregati e riprodotti in innumerevoli copie. Nel periodo storico in cui viviamo, consentire ai propri dipendenti l'accesso alle informazioni aziendali, così come trasformare i dati in formato digitale sono procedure inevitabili. Tuttavia, far fronte ai rischi connessi a questa continuo progresso, richiede competenza e applicazione. La maggior parte dei dati privati, ma anche aziendali* – continua Salvatore Piccinni - *viene conservata non più su server di proprietà dell'impresa o della persona che possiede il dato ma sui server di cloud storage. Capire ad esempio cos'è il cloud, come funziona e come garantirne la sicurezza rappresenta oggi un aspetto critico non solo per il privato ma anche per imprenditori e manager. Ecco perché bisogna rispondere al fenomeno con tempestività e rapidità, investendo non solo in tecnologie ma anche nella cultura e nell'informazione. È fondamentale assumere dei comportamenti adeguati che scongiurino il rischio di essere "attaccati"* – prosegue – *Le aggressioni di social engineering vengono realizzate sempre più spesso sfruttando le debolezze della psiche umana sia tramite email che tramite Social Media e sistemi di comunicazione istantanei. Come difendersi? Credo sia fondamentale tenere a mente alcune semplici regole: in primo luogo, imparare a conoscere la minaccia per non andar incontro al rischio, investendo nell'ambito educativo e culturale; individuare sempre il contesto di riferimento e verificare l'identità del mittente del messaggio prima di cliccare su un link o aprire un allegato, ancor di più se sospetto; rimuovere account poco utilizzati o inutili, applicazioni scaricate e mai usate in modo da circoscrivere e rendere più controllabile la propria sfera di azione; utilizzare credenziali di accesso differenti per ciascun account a disposizione e modificarle con una certa frequenza; attribuire il giusto livello di sicurezza a tutto ciò che si fa in rete: sarebbe assolutamente rischioso, infatti, trattare dati strettamente riservati su un device con il quale siano stati scaricati film, musica o giochi illegalmente o dove siano stati installati software pirata, in quanto il dispositivo risulterà sicuramente esposto a virus di ogni genere e dunque non più sicuro. Si tratta di condotte che, seppur semplici e banali, qualora non venissero messe in pratica determinerebbero un incremento del livello di rischio per le informazioni in nostro possesso.*

Fondamentale, infine, soprattutto per le aziende medio-grandi, a prescindere dal settore produttivo – conclude Salvatore Piccinni - *affidarsi a professionisti altamente qualificati, in grado di analizzare e potenziare la sicurezza delle infrastrutture informatiche aziendali, attraverso verifiche di Vulnerability Assessment condotte da un ethical hacker per individuare eventuali debolezze di un sistema o di una rete, da sfruttare in un Penetration Test utile per valutare il grado di robustezza dell'infrastruttura attraverso la simulazione di un attacco vero e proprio. In sostanza, i nostri esperti si calano nei panni di un abile hacker con l'obiettivo di evidenziare i punti deboli della piattaforma, fornendo al cliente il maggior numero di informazioni sulle vulnerabilità tecnologiche riscontrate che ne hanno permesso l'accesso non autorizzato. Eseguire regolarmente un Penetration Test è necessario e utile alle aziende perché aiuta a comprendere se il livello di sicurezza esistente è sufficiente e dunque il know-how aziendale è al sicuro o se, al contrario, necessita di interventi migliorativi immediati."*