ATTACCO ALLE BANCHE

CARLO DEL BO, EXECUTIVE ADVISOR GRUPPO SICUREZZA, FORNISCE ALCUNI UTILI CONSIGLI PER DIFENDERSI DAI FREQUENTI ATTACCHI INFORMATICI AL SISTEMA BANCARIO.

Le banche sono costantemente sotto minaccia per quanto riguarda la Cyber Security. Quali sono le principali tipologie di attacco alle quali sono sottoposte?
«È un dato di fatto che le aziende di servizi finanziari sono e rimangono un obiettivo interessante per i cyber-criminali: non si tratta solo della frequenza, in continuo aumento, ma è la natura stessa degli attacchi informatici che sta cambiando, dal momento che si tratta di casi sempre più sofisticati e difficili da individuare.
I principali attacchi sono mirati ai loro utenti attraverso due metodologie:
Phishing: è sicuramente uno degli attacchi più diffusi, ma negli ultimi anni lo Spear Phishing estende l'analogia di pesca in quanto gli aggressori puntano specificamente su vittime ed organizzazioni di alto valore. Invece di cercare di ottenere le credenziali bancarie per mille consumatori, l'aggressore potrebbe trovare più lucrativo prendere di mira specifiche aziende.
Malware: pensati specificatamente per colpire gli utenti, intercettando e dirottando le loro transazioni su conti anonimi e non facilmente rintracciabili. Tra i malware più famosi ricordiamo Titan e Zeus, spesso questi virus della famiglia dei keyloggers vengono veicolati proprio tramite il phishing di mail».

Quali sono i Paesi più attivi al mondo nel lanciare attacchi informatici e quali misure possono essere adottate a livello internazionale per ridurre queste minacce?
«Dipende dalle tipologie di attacco, escludendo il cyberwarfare cioè la nuova guerra fredda che quotidianamente si combatte tra Paesi come America, Cina e Russia, la maggior parte degli altri attacchi proviene da stati specifici come ad esempio Ucraina, Bulgaria, Estonia, Francia, Inghilterra, Germania, ma sempre in generale da USA, Cina e Russia».

Come il sistema bancario si sta organizzando per migliorare la sicurezza dei propri sistemi informatici?
«I cyber attack sono in grado di produrre – potenzialmente – effetti confrontabili con quelli bellici e di incidere sull'esercizio stesso delle libertà essenziali per i sistemi economici e finanziari. I paesi più esposti sono proprio quelli occidentali, perché hanno infrastrutture critiche sofisticate IT based e di conseguenza più vulnerabili. La crescente complessità delle minacce e la virulenza degli attacchi, sempre più frequenti, rendono necessaria una gestione sincronizzata dei diversi elementi che costituiscono una soluzione complessa di cyber physical security ed una forte integrazione fra processi di gestione degli incidenti IT e processi aziendali, in modo da intercettare e gestire efficacemente i segnali di un potenziale attacco fino a sviluppare sistemi predittivi in grado di anticipare eventuali tipologie di attacco. L'attivazione del circolo virtuoso "più sicurezza uguale più qualità dell'offerta e maggiore fiducia della clientela" assume importanza strategica nell'attività finanziaria, che fonda la propria operatività sul trattamento altamente confidenziale dei dati».

Il singolo cittadino che cosa può fare per migliorare il proprio utilizzo in rete dei servizi offerti dalle banche on line?
«Aggiornare costantemente i propri dispositivi e seguire i canali informativi dei servizi bancari, è sicuramente il primo passo per un'adeguata politica di sicurezza ed utilizzo sicuro dei servizi online».

Quali sono le principali soluzioni che Gruppo Sicurezza offre, in generale, nel campo della Cyber Security?
«Gruppo Sicurezza offre servizi di consulenza e soluzioni specifiche per la Cyber Security, soluzioni che si basano sulle più innovative tecnologie di cyber intelligence e sistemi di analisi predittivi. Offre anche momenti formativi e di sensibilizzazione del management e dei dipendenti che sono indispensabili per aumentare la consapevolezza ai problemi cyber».

E per quanto riguarda specificatamente il settore bancario?
«Gruppo Sicurezza offre, oltre a servizi avanzati di Penetration Test e Vulnerability Assessment per valutare il livello di sicurezza dei sistemi ICT bancari, una soluzione di Cyber Security denominata "cyber safe", in grado di controllare on-line (24x7x365) dalle vulnerabilità dei sistemi al livello di rischio dei dati sensibili, dal controllo interno delle minacce al controllo esterno, sia logico che fisico, grazie anche alla più che trentennale esperienza nel campo della sorveglianza. Il Cyber Security Operation Center del Gruppo Sicurezza è in grado di controllare la presenza di varie forme di cyber minacce, non solo all'interno dei sistemi del cliente ma anche all'esterno, su internet. I motori di Intelligenza artificiale della piattaforma Ubiqum, controllano in tempo reale minacce di phishing, spam, web reputation, sentiment e data breach, presenti sulle fonti aperte (OSINT) e Dark Web. Il sistema di monitoraggio permette anche il controllo automatico compliance delle normative (GDPR) e delle «best practices» di sicurezza (SANS) per i dati personali e sensibili del cliente».

CYBER SECURITY E MITIGAZIONE DEI RISCHI FINANZIARI

Lo scenario in cui le aziende e i professionisti operano è sempre più costellato da innumerevoli e frequenti problematiche cyber. La protezione dei dati personali e sensibili di un'azienda o di uno studio professionale, deve rientrare nelle attività quotidiane per garantire una maggiore mitigazione a questa tipologia di rischi.
La messa in sicurezza della propria azienda è un processo interno che deve coprire gli aspetti tecnologici, formativi, metodologici ed economico-giuridici. Questo processo ha il compito di ridurre la superfice di attacco aziendale rispetto agli attacchi cyber che possono essere perpetrati sia dall'esterno che dall'interno di un'azienda e possono causare danni economici e d'immagine anche molto rilevanti.
Gruppo Sicurezza ed Helvetia Assicurazioni hanno recentemente concordato di offrire un servizio congiunto in grado di facilitare l'analisi dei rischi cyber e indirizzare la clientela ad attività propedeutiche alla revisione dei processi e delle tecnologie informatiche, nel rispetto di quanto richiesto anche dalla nuova normativa EU GDPR appena entrata in vigore.
L'esperienza tecnologica di Gruppo Sicurezza e quella assicurativa di Helvetia Assicurazioni rendono più facile la gestione dei rischi cyber, garantendo al cliente un monitoraggio costante della propria infrastruttura ICT, un aggiornamento continuo sui nuovi rischi e una copertura assicurativa post incidente.
"Siamo particolarmente fieri di aver siglato con Helvetia una collaborazione che possa aiutare l'imprenditore o il professionista ad incrementare la propria sicurezza cyber e facilitare le operazioni di controllo quotidiano, spiega Lorenza Bernasconi di Gruppo Sicurezza SA.