CYBERSECURITY, UN "MUST" PER LE BANCHE

FOCUS SUL LAVORO DA REMOTO E SULLE ACCRESCIUTE INTERAZIONI DIGITALI

OPINION PAPER

AURIGA
the banking e-volution

THE # NEXTGENBANK®

www.aurigaspa.com

Digitalizzazione e sicurezza informatica sono due concetti che vanno di pari passo. Con il trasferimento progressivo delle attività, bancarie e non, nel digitale, è necessario reimpostare la strategia di sicurezza, soprattutto per la gestione delle informazioni sensibili o dei dati degli utenti. Le istituzioni finanziarie sono chiamate a implementare strategie di sicurezza complete, intelligenti e proattive.

Per le istituzioni finanziarie le probabilità di subire un attacco informatico sono fino a 300 volte superiori rispetto a società di altri settori (in base al **Global Wealth Report** di BCG del 2019). Gli attacchi rivolti al settore finanziario, inoltre, si sono intensificati nell'ultimo anno anche per gli effetti del Covid-19, che ha pesantemente incentivato il lavoro a distanza e ha modificato le modalità di interazione banca / cliente. Sia la Banca Centrale Europea che il Fondo Monetario Internazionale hanno evidenziato l'aumento degli attacchi informatici mirati a obiettivi finanziari. E, nonostante non si siano registrati gravi violazioni alla sicurezza, le perdite delle istituzioni ammontano a diversi milioni di euro solo nell'ultimo anno.

Perché con la pandemia il tema della sicurezza è diventato più stringente? Perché c'è stata sicuramente un'evoluzione degli attacchi informatici rivolti sia alle banche che ai clienti di home banking, portando i team di security nel mondo finanziario a doversi confrontare su perimetri più ampi per garantire una maggiore sicurezza sui canali digitali. Nella situazione causata dalla pandemia, l'interazione con gli operatori bancari si è spostata necessariamente sui canali remoti perché il cliente ha progressivamente sempre più utilizzato l'interazione digitale per entrare in contatto con la propria banca. Per questo motivo, le banche devono riuscire, ancora più di prima, a mettere in sicurezza i dati personali durante l'assistenza remota (che avviene per esempio tramite webchat o videocall).

Questo spiega perché, in un contesto economico non certo semplice, la spesa delle organizzazioni per la cybersecurity sia comunque aumentata: secondo i dati dell'**Osservatorio Cybersecurity & Data Protection** del Politecnico di Milano, il mercato ha raggiunto un valore di 1,37 miliardi di euro, registrando un incremento di spesa del 4% rispetto al 2019. In particolare le organizzazioni hanno adottato soluzioni tecnologiche di sicurezza e protezione della rete e dei dispositivi usati dai consulenti, in primis soluzioni di endpoint security (per la protezione di ciascun dispositivo connesso alla rete) e di network & wireless security (che difendono l'infrastruttura da accessi impropri), che insieme hanno catturato ben il 55% degli investimenti censiti dall'Osservatorio.

SICUREZZA E LAVORO IN REMOTO

A seguito del lockdown causato dal Covid-19, i criminali informatici hanno trovato nuove strade nel mondo digitale per perpetrare i loro attacchi. Nel settore finanziario, le conseguenze di un leak di dati possono essere catastrofiche, poiché le informazioni di un utente possono essere utilizzate dai criminali, tra le altre cose, per accedere ai conti correnti e impossessarsi del denaro dei clienti.

La considerevole implementazione del lavoro in remoto ha portato fondamentalmente a un aumento di due tipi di attacchi: data leak finalizzata al furto di credenziali e manipolazione dei dati; l'introduzione di malware finalizzato alla crittografia delle informazioni e all'estorsione di entità pubblicando le informazioni personali di clienti e / o dipendenti.

In termini generali, le cause principali di questa esposizione agli attacchi informatici sono incentrate sulla mancanza di conoscenza della tipologia degli attacchi, alla scarsa manutenzione nell'aggiornamento dei sistemi utilizzati e alle cattive pratiche di sicurezza informatica, come la connessione a reti Wi-Fi non protette. Questo, insieme all'uso massiccio di nuove tecnologie, rende le organizzazioni vulnerabili, soprattutto se non sono stati stanziati gli investimenti necessari per mantenere protetti i sistemi.

D'altro canto, anche la rapida digitalizzazione dei canali bancari a seguito della pandemia è stata un fattore determinante nell'aumento degli attacchi informatici. Un processo che, in molte occasioni, è stato svolto in maniera rapida e disorganizzata, senza tener conto delle implicazioni che un sistema di sicurezza carente può avere per l'integrità della banca. L'implementazione delle operazioni remote deve essere accompagnata dall'integrazione di sistemi che proteggono l'accesso ai server.

In questo scenario generato dalla pandemia, infatti, il rapporto con la banca si è necessariamente spostato in molti casi su canali remoti per l'accesso ai servizi finanziari. La sfida ora, quindi, è migliorare l'esperienza complessiva del cliente qualunque sia il canale utilizzato. La banca deve garantire la sicurezza dei dati personali gestiti in un helpdesk remoto tramite webchat o videochiamata.

Fortunatamente, le moderne soluzioni di sicurezza per le istituzioni finanziarie proteggono anche le applicazioni critiche utilizzate sulle workstation remote, semplificando il processo di protezione e monitoraggio. La tecnologia più evoluta sfrutta il concetto di whitelisting per consentire l'accesso alle risorse di sistema in modo controllato. Ad esempio, le porte USB possono essere bloccate durante una videochiamata o un supporto remoto in cui il cliente fornisce dati personali, in modo che il file video non possa essere salvato su un dispositivo esterno.

BANCOMAT E DISPOSITIVI SELF-SERVICE: IL TARGET PIÙ COLPITO

Tuttavia, non dobbiamo dimenticare altri elementi che facilitano l'accesso ai criminali informatici. Gli sportelli automatici (ATM) sono l'anello più debole dell'ecosistema bancario per un semplice motivo: l'investimento per aggiornarli è praticamente inesistente. Ci troviamo di fronte a dispositivi collegati al sistema della banca ma che girano su sistemi operativi obsoleti, oltre ad avere barriere fisiche non adeguate. Jackpotting, MitM (man in the middle) o attacchi logici sono le tecniche più comuni per perpetrare furti.
Come gli sportelli automatici, i dispositivi self-service assistiti sono fisicamente accessibili e si basano su comunicazioni remote e interconnessione con l'infrastruttura IT, ereditando alcuni dei loro rischi e vulnerabilità.

L'Intelligenza Artificiale e il Machine Learning stanno giocando un ruolo sempre più importante nella sicurezza informatica, con strumenti che analizzano i dati di milioni di incidenti informatici e li utilizzano per identificare potenziali minacce, analizzando per esempio, l'account di un dipendente della banca che agisce in modo strano facendo clic sul phishing link o una nuova variante di malware.
Nel complesso scenario odierno è essenziale fornire le giuste misure di sicurezza per ogni workstation all'interno della banca. Le workstation sicure sono il fondamento delle reti protette, perché se un hacker può accedere a una workstation, l'intera rete può essere compromessa. Quando si parla di sicurezza informatica, nessun punto di accesso può essere trascurato se non si vuole esporre l'organizzazione a un rischio critico.

AURIGA
the banking e-volution

Auriga S.p.A.
Via Don Luigi Guanella, 17
70124 Bari - Italy
www.aurigaspa.com
headquarters@aurigaspa.com