COME CAMBIANO LE MINACCE ALL'HARDWARE

Gli attacchi all'hardware stanno tornando a crescere, sia attraverso nuove strategie contro POS e ATM, sia per la grande attenzione che la criminalità sta rivolgendo a nuovi device che hanno fatto il loro ingresso in azienda e nella routine dei clienti, come tablet e smartphone

L'hardware bancario continua a essere nel mirino della criminalità informatica. Oltre a smartphone e tablet, nuovi terminali dotati di capacità elaborativa ma non ancora "vissuti" dagli utenti con la giusta consapevolezza della necessità di adottare misure di sicurezza, la criminalità ha raffinato le strategie di attacco contro le macchine più tradizionali del mondo bancario, cioè POS e ATM. "Negli ultimi anni gli attacchi verso i POS erano diminuiti rispetto al picco del 2006, racconta Alessandro Fiorenzi, Esperto di Computer Forensics e membro del Clusit. Le soluzioni implementate dai produttori di hardware, come i sensori di apertura ed altri elementi che impediscono l'inserimento di device in grado di 'leggere' la strisciata e il PIN della carta hanno portato a un abbassamento consistente delle attività malevole verso i POS. Nell'ultimo anno c'è stato invece un nuovo aumento degli attacchi. Uno studio dell'università di Cambridge nel 2010 aveva evidenziato come posse possibile effettuare una transazione POS senza conoscere il PIN della carta, l'anno scorso all'evento Hack in The Box è stato reso pubblico uno studio dal nome significativo 'Chip & Pin is definitely broken' sulla debolezza dello standard EMV. E' poi tornata in auge anche la manomissione dei POS, che non vengono più aperti, ma sui quali vengono installati dei microskimmer, incollandoli all'interno della bocchetta di lettura del chip, soluzioni estremamente difficili da vedere e molto efficienti, accessibili spesso con connessioni wi-fi o bluetooth" o programmati per scaricare i dati all'inserimento di una particolare carta microchip.

Alessandro Fiorenzi
Esperto di Computer Forensics e membro di Clusit

Codice malevolo nel POS: solo un'ipotesi, per ora

Ma l'ultima frontiera degli attacchi contro i POS, per adesso solo a livello di "caso di studio" e non di realizzazione concreta, è l'ipotesi che qualcuno possa inserirsi nel processo di produzione del software ospitato sul POS. "Il POS è un terminale dotato di un processore e quindi di una capacità elaborativa, commenta Fiorenzi, che ospita un codice controfirmato digitalmente e installanto dalle banche sull'hardware che acquistano. Non mi risulta ci sia mai stato finora alcun caso concreto di questo tipo, ma è un'ipotesi realistica che un'organizzazione molto ben strutturata possa tentare di inserire una parte di codice malevolo nel software, installandolo su tutti i POS, che riuscirebbe a essere trusted verso gli apparati e a non essere facilmente individuabile: un'operazione che consentirebbe di radunare in poco tempo una mole di dati consistente".

Non c'è crisi per gli skimmer

Le minacce agli hardware tradizionali del settore bancario colpiscono anche gli ATM, e anche in questo caso nel mirino ci sono le carte di pagamento. "Quasi tutte le macchine gestiscono le carte utilizzando la modalità microcircuito, precisa Fiorenzi, ma viene mantenuta una compatibilità con il passato, quindi l'eventuale utilizzo della banda magnetica resta pericoloso: basta rubare il dato nelle tracce 1 e 3 della banda per accedere a una serie di informazioni sul conto. Ci sono poi le installazioni di skimmer e videocamere, che non conoscono crisi: bisogna prestare particolare attenzione agli ATM collocati in luoghi meno protetti rispetto a quelle che si trovano all'interno delle banche. Pensiamo ad esempio agli ATM collocati nei centri commerciali, sottoposti a una sorveglianza minore, e spesso anche installati in modo meno sicuro".

Smartphone e tablet a rischio

Nel settore bancario si stanno anche affermando nuovi device, sia per quanto riguarda l'offerta di servizi ai clienti finali sia nella routine lavorativa del personale, in primis smartphone e tablet. "Si tratta di terminali bellissimi, ma pensati per l'usabilità dell'utente finale, e non per la sicurezza, spiega Fiorenzi. Sono privi di tutte le accortezze necessarie a tutelare i dati e mantenerli riservati. Ci sono problemi di integrità, come nel caso di alcuni smartphone che non permettono una cifratura alta, ma anche una scarsa consapevolezza negli utenti finali, che espongono oggi smartphone e tablet al concreto rischio di un'infezione da malware, soprattutto sulle piattaforme più utilizzate, cioè iOS e Android. E se un utente finale in un certo senso 'accetta' il rischio, nel caso dei terminali aziendali parliamo di device che oggi nella maggior parte dei casi non sono gestiti in nessun modo, non sono neppure inseribili in sistemi aziendali di monitoraggio e sorveglianza, e rappresentano quindi una minaccia importante".

Fornire un primo livello di sicurezza

Per gli smartphone incominciano a esserci i primi sistemi di gestione, ma "stiamo ancora parlando di una minoranza di macchine, commenta Fiorenzi. Una soluzione parziale potrebbe essere l'implementazione di sistemi NAC basati su 802.1X: quando ci si collega alla rete aziendali si viene autenticati, e viene fatta scaricare sulla macchina una componente Java o ActiveX che analizza il device mobile alla ricerca di keylogger, sniffer e così via. Se il dispositivo supera i controlli viene concesso l'accesso alla rete aziendale altrimenti il device viene posto in un'area di remediation o addirittura viene negata la connessione alla rete aziendale. Così non viene garantita la totale sicurezza, ma si migliora un poco la situazione".

A.G.

E L'INTERNAL AUDITING INCONTRA L'IT

L'importanza della information forensics sta crescendo anche nell'ambito dell'internal auditing: le attività di vigilanza e di controllo si trovano infatti ad avere sempre più spesso a che fare con la verifica di dati e di operazioni avvenute sui sistemi aziendali. "Le tecniche di information forensics consentono di cristallizzare ciò che viene effettuato, spiega Fiorenzi, effettuando una sorta di 'carotaggio' delle attività IT, per andare poi a individuare e isolare una determinata informazione, ad esempio per dimostrare che un dipendente infedele ha inviato un dato a una azienda concorrente, oppure per tutelare l'azienda in qualche procedimento. Attualmente le strutture di internal auditing non sempre dispongono di personale con le giuste competenze, e per ovvi motivi di conflitti di interesse non possono avvalersi delle strutture interne: cresce quindi il ricorso a realtà esterne che hanno le giuste competenze per svolgere queste attività".