BancaFinanza

Mensile

Data 02-2017
Pagina 56/58
Foglio 1 / 3

SICUREZZA

Frodi bancarie: siamo tutti ad alto rischio

L'esplosione del digitale ha creato nuovi pericoli. Dall'evoluzione del phishing al ransomware, dai furti di identità alle transazioni fraudolente

LAURA FACCHIN
@laurafacchin73

Nonostante la tecnologia sempre più sofisticata il tema delle frodi, in ambito bancario - ma anche nelle assicurazioni e n vari altri settori di busness - resta uno dei nodi più spinosi da risolvere.

Le procedure per la prevenzione frodi di Experian in Italia esaminano oltre 10 milioni di richieste ogni anno. E puntano ad aiutare le imprese a rilevare e prevenire il fenomeno nelle fasi iniziali (sia richieste con carte di credito, sia telefoniche). Nel 2015, l'azienda ha lanciato una procedura legata allo Scipafi, il sistema pubblico di prevenzione: obiettivo del servizio è permettere il riscontro dei dati contenuti nei principali documenti d'identità, riconoscimento e reddito, con quelli registrati nelle banche dati degli enti di riferimento (attualmente quelle di Agenzia delle entrate, ministero dell'Interno, ministero delle Infrastrutture e dei Trasporti, Inps e Inail).

E i dati fanno riflettere: la percentuale più alta di allarmi (numero di *alert* rapportati al numero di transazioni) in termini di età vede le fasce più a rischio nei giovani e a seguire nelle persone più anziane. Le donne, sempre sulla percentuale di allarmi, sono più a rischio rispetto agli uomini, mentre dal punto di vista gegrafico, i primo posti sono occupati dai residenti all'estero e in Alto Adige; nelle prime dieci province ce ne sono, inoltre, otto meridionali e insulari (Napoli, Salerno, Bari, Foggia, Campobasso, Palermo, Catania, Siracusa).

BancaFinanza ne ha parlato con **Angelo Padovani**, amministratore delegato di Experian Italia e con **Andrea Prioreschi**, direttore information technology e processi di Santander consumer bank.

Quali sono gli ambiti e i settori nei quali siete più attivi con i vostri servizi per la sicurezza informatica? E quanto pesa il settore bancario?

Padovani. «In Italia Experian è attiva prevalentemente nel settore del credito, con una crescita negli ultimi anni anche in quelli assicurativo e telecomunicazioni».

Quali sono le frodi più pericolose che si sono sviluppate con la digital disruption?

Padovani. «Con la *digital disruption*, i confini un tempo tracciati non esistono più e la frode viene propagata grazie a due elementi: da una parte la pervasività della tecnologia in molti aspetti della vita quotidiana; dall'altra l'educazione e la cultura della sicurezza della singola persona. I rischi maggiori si manifestano con il furto d'identità. Si tratta di un'impersonificazione (totale o parziale) e riguarda l'utilizzo indebito di dati che possono essere riferiti a una persona in vita o anche deceduta. Op-

ANGELO PADOVANI
«Con la digital disruption, i confini di un tempo non esistono più e la frode viene propagata grazie a due elementi: da una parte la pervasività della tecnologia in molti aspetti della vita quotidiana; dall'altra l'educazione e la cultura della sicurezza della singola persona», sostiene l'amministratore delegato di Experian Italia.

CARD NOT PRESENT
Le frodi di tipo "Card Not Present" rappresentano il 60% di tutte le perdite connesse all'uso di carte nell'area Emea: le organizzazioni si trovano quindi ad affrontare la sfida di approvare i clienti legittimi e bloccare le transazioni fraudolente

pure, si manifesta con l'occultamento parziale della propria identità mediante l'impiego, in forma combinata, di dati relativi alla propria persona e l'utilizzo indebito di dati relativi a un altro. Uno dei temi di maggior interesse degli ultimi dieci anni e una delle minacce più serie a livello mondiale è poi il *cyber crime*. Ogni aspetto della vita quotidiana privata e lavorativa ormai è altamente informatizzato. Tutte le economie mondiali utilizzano la stessa infrastruttura di base, gli stessi software, hardware e standard, con miliardi di dispositivi connessi. I rischi legati al *cyber space* sono considerati, secondo una recente ricerca del World economic forum, come tra i maggiori rischi percepiti in termini di impatto e probabilità di verificarsi. Un aspetto collegato al fenomeno del *cyber crime* è la scarsa trasparenza: anche quando una frode informatica è individuata, spesso non viene comunicata. Oltre alla violazione della privacy, ci sono altre informazioni che a livello strategico non devono essere divulgate. Quindi, per ragioni competitive queste perdite di dati rimangono confidenziali. Proprio per questo, la maggior parte dei danni che derivano dal *cyber crime* sono difficili da quantificare: questo crea dei rischi nell'ecosistema del business a livello globale e in particolar modo alle Pmi. Inoltre, le frodi di tipo *Card Not Present* rappresentano il 60% di tutte le perdite connesse all'uso di carte nell'area Emea: le organizzazioni si trovano quindi ad affrontare la sfida di approvare i clienti legittimi e bloccare le transazioni fraudolente. Nonostante sia un canale pratico e molto utilizzato, internet è dunque uno strumento sostanzialmente anonimo, che rende sempre più difficile conoscere realmente i clienti. Quindi, gli approcci attualmente adottati in materia di prevenzione delle frodi comportano spesso un'esperienza negativa per i clienti».

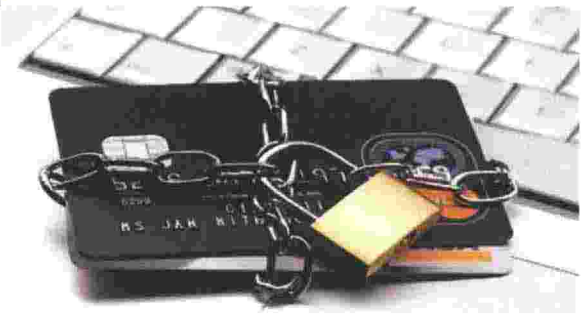
Prioreschi. «I maggiori rischi negli ultimi anni sono rappresentati dalla sottrazione delle credenziali degli utenti per l'accesso ai servizi di internet banking e dei dati relativi alle carte di credito attraverso il *phishing* e l'intercettazione delle comunicazioni (*man-in-the browser*). Un'altra formula subdola notata più recentemente è il blocco Pc e delle aree di rete ad accesso criptato e la conseguente richiesta di riscatto attraverso bitcoin».

Quali sono le fonti principali di pericolo per le frodi informatiche?

Prioreschi. «In primo luogo internet, con particolare riferimento alla diffusione delle diverse forme di virus (per esempio malware, ransomware, *social engineering*) sempre più sofisticati e in continua evoluzione; strettamente collegato all'ambiente internet c'è poi quello delle e-mail. Non solo *phishing*, ma anche messaggi di posta elettronica, destinati alle aziende. Messaggi che non sono, però, "normali": infatti, contengono virus che mirano a bloccare, oppure danneggiare i sistemi informativi che questi stessi malware infettano. In rapida crescita, in parallelo all'aumento dell'utilizzo delle applicazioni mobile, ci sono anche il download fake di app o finte *impression* pubblicitarie. A

ANDREA PRIORESCHI
«Una formula subdola notata recentemente è il blocco Pc e delle aree di rete ad accesso criptato e la conseguente richiesta di riscatto attraverso bitcoin», direttore information technology e processi di Santander consumer bank (sotto, la sede)

Tecnologia & Informatica



SISTEMA PUBBLICO DI PREVENZIONE
In Italia opera Scipafi, sistema pubblico di prevenzione che consente il riscontro dei dati contenuti nei principali documenti d'identità, riconoscimento e reddito, con quelli registrati nelle banche dati degli enti di riferimento

monte di tutto, ci sono le debolezze nei processi correlati alla gestione delle credenziali di accesso, con la duplice sfida, per le aziende, di individuare modelli di gestione che consentono di ridurre le complessità per il cliente senza assumere maggiori rischi».

Ci sono peculiarità o differenze fra l'Italia e il resto d'Europa?

Padovani. «In Italia opera Scipafi, il sistema pubblico di prevenzione che consente il riscontro dei dati contenuti nei principali documenti d'identità, riconoscimento e reddito, con quelli registrati nelle banche dati degli enti di riferimento: attualmente. quelle di Agenzia delle entrate, Ministero dell'interno, Ministero delle infrastrutture e dei trasporti, Inps e Inail. Questo riscontro si configura quindi come efficace strumento di prevenzione per i furti d'identità. Siano essi totali o parziali. Il sistema Scipafi è una best practice europea - e tra l'altro, è integrato in tutte le soluzioni Experian che permettono di effettuare il riscontro su questo sistema, sia al momento del controllo dell'anagrafica, sia alla richiesta di credito. In Italia ci sono vincoli sulla privacy tali per cui non si sono costituite ancora schemi di condivisione delle attività sospette antifrode. Quello che si può condividere a livello di attività fraudolente accertata in sede giudiziaria perde di significato. E questo accade a causa dei tempi lunghi che intercorrono dal momento in cui si verifica il tentativo di frode e la chiusura dei procedimenti giudiziari. Con il sistema Scipafi e la sua evoluzione verso la seconda fase di sviluppo si spera di superare questo limite ed avviare una nuova fase nella prevenzione frodi attraverso la condivisione delle richieste di credito sospette. In altri paesi come Gran Bretagna e Spagna, per esempio, sono invece attivi da tempo sistemi di condivisione delle frodi. Il sistema inglese si chiama Cifas ed è aperto sia a istituti bancari, sia a compagnie assicurative».

Come supportate le banche sul versante dei modelli antifrode, anche in termini di prevenzione?

Padovani. «Abbiamo investito in soluzioni che integrano le differenti fonti dati (pubbliche, proprie, condivise) per controlli a 360 gradi nella prevenzione delle frodi. In particolare, abbiamo potenziato recentemente la nostra soluzione antifrode *Detect Plus*, che si basa su un patrimonio informativo di decine di milioni di posizioni creditizie del credit bureau Experian Italia. Abbiamo quindi integrato nuovi fonti di dati, come gli archivi Scipafi e i nuovi database per la verifica dell'indirizzo fornito come residenza, che tendono a evidenziare eventuali anomalie come indirizzi virtuali, uffici pubblici, indirizzi non associato ad abitazioni o comunque più in generale indirizzi non esistenti. Un ulteriore controllo inserito è quello su numerazione della carta d'identità, data di rilascio e di scadenza, età del richiedente al momento del rilascio della carta d'identità e periodo di validità del documento in base alla normativa in vigore al momento dell'emissione della carta d'identità. L'azienda sta anche investendo molte risorse nello sviluppo di modelli analitici focalizzati sul rischio di frode in collaborazione con diversi istituti, con l'obiettivo di realizzare modelli di ottimizzazione dei controlli. Che riducano i "falsi positivi" e allo stesso tempo permettano di concentrare le verifiche sulle pratiche con più alto rischio. Contemporaneamente, stiamo portando anche sul mercato italiano le nostre soluzioni per prevenire le frodi digitali. Quella più recente è *Fraudnet*.

Qual è la sua caratteristica?

Padovani. «Che mette al centro delle verifiche antifrode il *device* con il quale il cliente accede al suo conto on line ed ai servizi erogati in rete. Poter accedere alle informazioni dal dispositivo di accesso è infatti un elemento fondamentale per poter identificare i frodatori. I dati forniti durante un login o una transazione potrebbero essere infatti falsi o rubati. Le informazioni che arrivano dal dispositivo invece sono difficilmente falsificabili e permettono quindi di avere più dati da analizzare per individuare eventuali incoerenze e far scattare i dovuti allarmi. Le informazioni del dispositivo vengono intercettate in tempo reale per generare un identificativo univoco (*device insight Id*). In questo modo, il dispositivo viene associato a ogni evento da esso generato, senza richiedere *call out*, *popup* o domande addizionali a cui il cliente deve rispondere. Per catturare un truffatore, bisogna ragionare come lui ed è per questo che Experian si avvale di esperti di frodi: la tecnologia utilizzata in *Fraudnet* è stata sviluppata dalle stesse persone che hanno passato decenni a contrastare le truffe, insieme a fornitori di servizi di pagamento, istituti finanziari ed esercenti in tutto il mondo.