IL MATTINO

27-LUG-2017
pagina 10
foglio 1

«I correntisti non rischiano nulla in caso di furto pagano gli istituti»

Intervista

Stasi, segretario di AbiLab «Bisogna però diffidare di chi chiede dati sul web»

Le regole anti-frode
Meglio accedere al conto scrivendo l'indirizzo nella barra di navigazione e non cliccare sul link

La difesa casalinga
Bisogna aggiornare i sistemi anti-virus e controllare spesso le operazioni compiute

«I clienti delle banche possono star tranquilli perché nel caso subiscano attacchi informatici non sono tenuti a pagarne le conseguenze, in questo senso le normative europee nel settore bancario sono molto chiare e regolamentano tutti i casi di operazioni non autorizzate o effettuate all'insaputa del cliente. È importante solo che, soprattutto nel mondo di oggi dove le operazioni avvengono sempre più spesso sul web, ci sia la necessaria attenzione nel tutelare determinati dati». Romano Stasi è il segretario generale di AbiLab, il consorzio dell'Associazione bancaria italiana che promuove e coordina le attività di ricerca sulle tecnologie informatiche e sui relativi attacchi.

Sono frequenti le incursioni di hacker sui conti online?
«I tentativi sono molti, ma solo una minima parte vanno a segno. Le statistiche indicano che oltre il 95% delle truffe non va in porto. Gli hacker possono entrare in possesso di informazioni statiche come ad esempio il numero di conto corrente o il nominativo del titolare, ma nel corso del tempo le banche hanno sviluppato delle contromisure per dare al cliente degli strumenti dinamici che sono quasi invalicabili a meno che non ci siano comportamenti avventati. Oggi grazie ai generatori di codici come i token o ai codici inviati tramite sms è quasi impossibile per i criminali prelevare dei soldi dai conti correnti perché sarebbe difficile reperire tutte queste informazioni contemporaneamente. Per prevenire ogni genere di truffa abbiamo dato un piccolo decalogo ai clienti per non cadere in subdoli tranelli».

Ad esempio quali comportamenti bisogna evitare?
«Bisogna diffidare di qualunque richiesta di dati relativi a carte di pagamento, chiavi di accesso all'home banking o altre informazioni personali ricevute su qualsiasi canale digitale. Per connettersi al sito della banca è preferibile scrivere direttamente l'indirizzo nella barra di navigazione e non cliccare su link presenti su e-mail e sms, che potrebbero invece condurre a siti contraffatti, molto simili all'originale. Controllare regolarmente le movimentazioni del conto corrente per assicurarsi che le transazioni riportate siano quelle realmente effettuate. Inoltre, come per tutti i casi di attacchi hacker, è sempre preferibile tenere aggiornato il sistema operativo e i software di protezione antivirus. Se si osservano questi comportamenti è pressoché impossibile venire attaccati».

È stato reso noto un attacco ad Unicredit, ma nei mesi scorsi nel resto del mondo questi raid sono stati frequenti e hanno fruttato anche grandi somme di danaro per i truffatori. Le banche italiane sono molto esposte?
«Le banche italiane sono esposte, ma anche in questi casi sono rari gli attacchi che riescono. Qualche mese fa è avvenuto un attacco alla banca del Bangladesh che si ritiene abbia fruttato oltre un miliardo di euro ai cybercriminali, ma in quel caso più che di un'incursione nella banca, si trattò di un furto d'identità che consentì agli hacker di entrare nei sistemi di pagamento. Un caso simile in Italia non è mai avvenuto, ma comunque la soglia di attenzione su questo genere di fenomeni è ai massimi livelli».

Qualche mese fa Il Mattino pubblicò un'inchiesta esclusiva sulla «black-box»: una piccola scatola ideata da hacker russi che, collegata ai bancomat, riusciva a sfruttare la vulnerabilità dei sistemi Atm e prelevare tutto il contante al suo interno. Sono avvenuti casi anche in Italia?
«In Italia sono avvenuti meno di dieci colpi di questo tipo e meno che nel resto d'Europa, ma ricordo che pochi giorni dopo la vostra inchiesta Europol riuscì ad arrestare criminali di varie nazionalità che agivano grazie alla black-box. Del resto gli sportelli sono spesso video-controllati e quindi siamo riusciti, in collaborazione con le forze dell'ordine, a fornire tutto il materiale utile alle indagini che in molti casi sono andate a buon fine. Inoltre abbiamo creato un tavolo tecnico tra le banche e i produttori di bancomat per risolvere questo genere di criticità, ma ovviamente anche su questo fronte bisogna essere attenti perché mentre si trova un rimedio ogni volta i cyber-criminali sono in grado di sviluppare nuove tecnologie per attaccare».

v.d.g.