Banche «Le cyber spie ci sono, state attente»

Era digitale e open banking offrono agli istituti di credito grandi opportunità, ma anche moltissimi rischi Gli esperti: «Ci sono aziende che sono state monitorate per mesi dagli hacker e non se ne sono accorte»

Entrare con tre o quattro click nel cellulare di qualcuno dall'altra parte del mondo, scaricarne foto e documenti, avere accesso alle password (che sono poi quelle che si usano un po' per tutto) e – più inquietante ancora – accedere al telefonino e utilizzarlo come microfono ambientale per ascoltare tutto quello che succede attorno all'ignara vittima. Comprare centinaia di migliaia di dati sensibili sul dark web (carte di credito, cartelle cliniche e chi più ne ha più ne metta), entrare nella casa ipertecnologica di qualcuno e divertirsi ad accendere e spegnere le luci a distanza (o a spegnere il termostato). Violare una webcam o – addirittura – disattivare un pacemaker e portare una persona alla morte. Non è la trama di un episodio di *Black Mirror,* ma il riassunto di quanto descritto ieri da alcuni esperti in un workshop (intitolato «Lo spionaggio nel settore bancario») organizzato alla sede del Gruppo Sicurezza di Savosa e a cui hanno partecipato molti dei responsabili della sicurezza degli istituti di credito presenti in Ticino. Già perché proprio le banche sono tra le principali vittime degli hacker e della criminalità informatica. E sono vittime in diversi modi. Possono veder attaccati i patrimoni dei clienti (per esempio se qualcuno riesce a violare gli account ebanking), ma possono anche essere vittime di spionaggio informatico. «E di casi eclatanti – ha sottolineato **Carlo Del Bo**, di Gruppo Sicurezza – ne abbiamo già visti diversi in Svizzera». Nel 2011 per esempio un ex dipendente di una banca elvetica ha venduto una lista di conti al Land tedesco del Nord Reno-Westfalia. Nel 2013 lo stesso è accaduto con un impiegato che ha venduto dati alle autorità fiscali tedesche, mentre nel 2014 liste di conti sono state vendute alle autorità americane, francesi e spagnole. Casi questi in cui c'era «una talpa» all'interno della banca. Ma una talpa (consapevole) non deve ormai neanche più esserci. Oggi – con le nuove tecnologie – il rischio è che gli impiegati senza saperlo portino all'interno dell'istituto dei malware (dei virus) contratti magari a casa. «È piuttosto semplice – ha spiegato **Francesco Arruzzoli,** anch'egli di Gruppo Sicurezza – accedere ai dispositivi elettronici di qualcuno. Lo si può fare in modo mirato, attraverso il phishing, e sfruttando un po' la psicologia umana». Arruzzoli non si è limitato alle parole, ma ha dimostrato con la pratica cosa si può fare. E molti dei presenti sono rimasti a bocca aperta (chi vi scrive ha sentito per un po' il desiderio di prendere il telefonino e buttarlo dalla finestra). «Possiamo conoscere una persona – ha sottolineato – guardando quel che scrive in Facebook o su Twitter. Conoscere i suoi hobby e le sue passioni. Poi possiamo inviargli un file, magari un PDF contenente materiale che potrebbe interessargli. PDF in cui inseriamo un virus e che, se viene aperto, ci darà libero accesso al suo computer o, peggio ancora, al suo telefonino». «Ci sono aziende – ha spiegato Del Bo – che hanno avuto per mesi delle spie nei loro sistemi informatici, e non se ne sono accorte. Spie che hanno avuto accesso a tutta la fase produttiva. Ed è un aspetto, quello dello spionaggio informatico, ancora trascurato». All'incontro ha partecipato anche **Richard Zoni** della Kobil, società specializzata nella protezione dei dati nel settore bancario. «Uno dei problemi principali per le banche – ha sottolineato – riguarda il fatto che i clienti chiedono loro di essere sempre più aperte e "openbanking". Ma per questo sono anche piu vulnerabili. I loro clienti rischiano furti d'identità». Per questo comunque esistono già ottime possibilità di protezione, per esempio il multi-device security (un sistema che, se si effettuano dei pagamenti tramite computer, chiede poi una conferma anche sul telefonino, o viceversa) o software che prima di autorizzare un'operazione controllano se uno dei dispositivi (telefono o PC) sono stati infettati. «Ci sono anche dispositivi – ha spiegato – che avvertono il titolare quando in corso c'è un prelevamento al bancomat. Questo per prevenire lo skimming delle carte». Per Arruzzoli in generale «il problema è che abbiamo connesso la nostra economia e la nostra società utilizzando piattaforme (il cloud, i social media e i telefonini, ndr) progettate per condividere informazioni ma non per proteggerle. E sono proprio le innovazioni a guidare la crescita del cyber rischio».

SICUREZZA Non tutte le aziende hanno preso pienamente coscienza dei rischi che corrono. Rischi monetari ma anche reputazionali. *(Foto Zocchetti)*

«Un settore ancora sottovalutato»

Durante la serata ha preso la parola anche **Luca Albertoni**, direttore della Camera di commercio. «Con la SUPSI – ha spiegato – abbiamo eseguito un sondaggio tra diverse grandi aziende ticinesi. Emerge che solo il 60% di esse ha effettuato una valutazione specifica del rischio legato alla cyber sicurezza. Spesso le aziende sono convinte che implementare delle contromisure sia troppo costoso, ma questo non è necessariamente vero. Soprattutto in considerazione dei rischi e dei costi che un attacco informatico potrebbe causare».
E si parla di grandi aziende, figuriamoci quelle più piccole. **J.R.**

DATI: SONO IL NUOVO ORO

Gli esperti hanno ricordato il caso Equifax, probabilmente il più massiccio furto di dati nella storia. Equifax è una società americana che si occupa del controllo dei crediti (esegue cioè una valutazione sulla solvibilità delle persone e indica in tempo reale se un creditore è affidabile oppure no). Nel luglio del 2017 il suo gigantesco database è stato hackerato e sono state rubate le identità digitali di 143 milioni di persone. Tra questi dati c'erano numeri di carte di credito, numeri di telefono, email e anche dati sanitari. E i vertici di Equifax hanno tenuto nascosta la vicenda per 60 giorni prima di avvisare le autorità. «E cosa ci si può fare – ha chiesto retoricamente Arruzzoli ai presenti – con i dati di 143 milioni di persone? Di certo gli hacker non li guardano tutti. E infatti sono stati presi e pubblicati nel dark web e venduti alla criminalità tradizionale. Criminalità che li ha usati, per esempio, per acquistare merce su Amazon e per rivendere poi simultaneamente lo stesso prodotto su eBay a metà del prezzo». Incassando milioni e rimbalzando da una nazione all'altra.

NOTIZIE**FLASH**

PREGASSONA

Dibattito «No Billag» stasera al Punto Città

La sezione del PPD e GG (Generazione Giovani) organizza per questa sera alle 18.30, nella sala riunioni del Punto Città di Pregassona, in via Sala 13, un dibattito pubblico sull'iniziativa «No Billag», in votazione il prossimo 4 marzo. La serata sarà moderata dal caporedattore del Giornale del Popolo, Gregorio Schira. Scenderanno in campo a discutere il consigliere agli Stati Filippo Lombardi, per il fronte dei contrari, e il giornalista Matteo Cheda, dalla parte dei sostenitori. Al termine della discussione verrà offerto un aperitivo ai partecipanti.

FERROVIE LUGANESI

Linea chiusa di notte tra Lugano e Agnuzzo

Le Ferrovie Luganesi (FLP) avvisano l'utenza che fino a domani, giovedì 8 febbraio, la linea ferroviaria sarà interrotta tra Lugano e Cappella Agnuzzo durante le ore notturne, ovvero dalle 21 alle 4.30, a causa di lavori in corso sulla rete. Il servizio alle fermate sarà comunque garantito da un autobus sostitutivo. La direzione delle Ferrovie si scusa per gli eventuali disagi che potrebbero essere arrecati agli utenti.

CARNEVALE

Il re e la regina Sbroja fanno ritorno in città

A partire da oggi anche Lugano si traveste. Re Sbroja inaugurerà i festeggiamenti con una visita alle case per anziani: alle 12.30 sarà alla Casa Serena, alle 14.15 alla Residenza La Meridiana e alle 15.30 al Castagneto. Domani pomeriggio alle 14 in piazza della Riforma, dopo la consegna delle chiavi al re, i ragazzi delle scuole sfileranno in maschera. Venerdì continueranno le visite agli istituti: alle 10 alla piazzetta Loreto, alle 11 all'OTAF di Sorengo, alle 12 alla Casa anziani Gemmo e alle 14 alla Residenza Maraini. Lunedì a partire dalle 11.30 sarà offerta la classica risottata in piazza della Riforma (in caso di cattivo tempo al Centro esposizioni).