DATAMANAGER.IT

Banche, bitcoin e un mondo che cambia in fretta

Banche, bitcoin e un mondo che cambia in fretta

di Giuseppe Badalucco , 21 luglio 2015

Il settore bancario Ã¨ in rapida trasformazione. Mobility, moneta virtuale, crowdfunding e social networking sono alcune delle nuove frontiere del mondo digitale che il settore finanziario si appresta a cavalcare. Un percorso verso il business digitale che presenta grandi opportunitÃ . Ma che allo stesso tempo necessita di grande attenzione alla sicurezza per conciliare le esigenze di protezione, riservatezza e privacy con quelle di apertura a clienti, partner e collaboratori

Sembra quasi di vederli. Dreadlock e piercing come contrappunto ai colletti inamidati dei superbanchieri di Wall Street. Sono i profeti, gli evangelisti dei bitcoin. Specialisti che sono riusciti a ritagliarsi uno spazio nei templi mondiali della finanza. O almeno in quelli dove Ã¨ rimasto quel briciolo di umiltÃ per capire che per rimanere competitivi occorre essere ancora piÃ¹ bravi nel fiutare il business e poi incorporarlo in fretta nella propria infrastruttura. Prima che altri provino a batterti sul tuo stesso terreno. Proprio quel che sembra abbiano fatto JPMorgan Chase e Goldman Sachs – non esattamente due startup e che di monete qualcosa capiscono – creando piccoli team di trader che si scambiano bitcoin. Per familiarizzare con questa valuta elettronica emergente. E studiarne gli effetti. Non unâ€™innovazione alla portata di tutti. La procedura per acquistare i bitcoin Ã¨ tuttâ€™altro che friendly. E neppure si puÃ² ancora parlare nÃ© di capillaritÃ nÃ© di diffusa accettazione della moneta elettronica. Le cose perÃ² potrebbero cambiare in fretta. Nel giro di una decina dâ€™anni, il numero di negozi disposto ad accettarlo potrebbe raggiungere la massa critica necessaria a decretarne il successo. Se davvero i bitcoin diventeranno un mezzo di pagamento diffuso e accettato, assisteremo a una ramificazione dellâ€™ecosistema che ha generato questa rivoluzione. E il ruolo delle banche â€“ sebbene i piÃ¹ radicali sostengano che i bitcoin sono nati anche per saltare la loro intermediazione â€“ molto probabilmente sarÃ ancora centrale nel processo.

Click To Tweet

L’anno della svolta

La scossa in effetti câ€™Ã¨ stata. PiÃ¹ di sei miliardi di euro. A tanto ammonta la cifra investita dal sistema bancario in tecnologie digitali. Per la precisione sei miliardi e 400 euro come certifica il rapporto Assinform 2015. Un budget in crescita rispetto allâ€™anno precedente. Â«Se analizziamo le dinamiche di investimento, emerge chiaramente che questâ€™anno il settore bancario ricomincia a investireÂ» â€“ ci dice

Giorgio Mosca, responsabile area sicurezza informatica di Assinform . Dopo anni di crisi, piÃ¹ contenuta rispetto ad altri settori (- 0,8% lo scorso anno, contro una media del 4 e 5%), la crescita nel 2014 si attesta a un + 0,8%. Solo un timido segnale di ripresa, nulla di eclatante, intendiamoci. PerÃ² si arrivava da cinque anni di crisi nera. E dunque il dato va valutato positivamente. Le prioritÃ di investimento secondo il Rapporto Abi Lab (Centro di ricerca e innovazione per la banca promosso dallâ€™ ABI) riguardano i processi di dematerializzazione dei documenti, la gestione della relazione con il cliente, lâ€™intercanalitÃ , la modernizzazione delle infrastrutture informatiche. Ma la vera novitÃ degli ultimi due anni Ã¨ rappresentata dalla crescita degli investimenti in servizi online, mobile banking e mobile payment in prima linea.

Â«Gli investimenti riguardano soprattutto i servizi Internet e mobileÂ» â€“ ci conferma Mosca. Questo dato certifica la maggiore attenzione del settore alla trasformazione digitale del business. Sempre di piÃ¹ una prioritÃ strategica per le banche. Tanto che oggi tutto il comparto, dal grande gruppo internazionale alle piccole realtÃ locali, Ã¨ impegnato nel lancio di nuovi canali dedicati allâ€™Internet e al mobile banking. Ma non solo. La corsa Ã¨ a riposizionare lâ€™offerta. E a cogliere nuove opportunitÃ , veicolando la vendita di prodotti che sino a pochi anni fa i clienti neppure cercavano in banca. Pensiamo al boom delle assicurazioni auto online, oggi una voce importante di ricavi per il settore. Una multicanalitÃ in cui il digitale fa la parte del leone. Un cambio di marcia che promette bene sia in chiave di servizi innovativi sia di incremento della domanda ICT piÃ¹ evoluta. Il segnale di una maggiore consapevolezza del settore circa lâ€™importanza di innovare. Anche perchÃ© nuovi attori e nuovi servizi minacciano di sottrarre quote di mercato e di rendere meno stretto quel rapporto tra banche e clienti costruito negli anni e mai come oggi a rischio di volatilizzazione.

Click To Tweet

Sullâ€™onda della spinta a innovare, anche lâ€™asse degli investimenti in sicurezza si sposta verso i servizi innovativi e non solo in direzione delle tradizionali misure di sicurezza volte a garantire il funzionamento efficace dei sistemi di gestione, la sicurezza delle transazioni, la continuitÃ del business, il disaster recovery, la protezione di dati e applicazioni da intrusioni e malcode. Ma unâ€™iniezione di denaro fresco destinato alla messa in sicurezza dei servizi utilizzati via web dagli utenti. Utenti che le banche avevano la necessitÃ di recuperare. A partire dal quadrante degli investimenti. Â«Servizi di questo tipo devono per forza accompagnarsi a unâ€™attenzione alla sicurezza. Per ragioni sia di natura regolatoria sia praticaÂ» â€“ premette Mosca. Â«Se si analizza lo spettro delle aree di investimenti delle banche nellâ€™ultimo periodo, appare chiaro che in questo momento di ripresa le banche cercano di riappropriarsi anzitutto della relazione con il cliente. Lavorando fondamentalmente sullâ€™Internet e mobile banking, sul crm e su tutto quello che serve per identificare i bisogni del cliente. E poi sulla sicurezza sia per motivi pratici che regolatoriÂ».

Un fattore questâ€™ultimo che contribuisce – almeno in parte – a far crescere la spesa globale. Lâ€™aumento delle minacce si traduce anche in maggiori investimenti? Senza dubbio le banche sono uno dei target principali degli attacchi. Quelli piÃ¹ recenti poi si

concentrano proprio su questi nuovi servizi web e mobile. Â«Di conseguenza, anche nella parte bancaria, i servizi di sicurezza giocheranno un ruolo crescente e la spesa di sicurezza Ã¨ probabilmente in crescitaÂ» â€“ conferma Mosca. Che gli investimenti crescano in valori assoluti nel settore bancario Ã¨ indirettamente confermato anche dal trend di crescita positivo degli investimenti in sicurezza tout court. Â«Consideriamo che in generale, la spesa in cybersecurity Ã¨ una di quelle che ha un trend di crescita piÃ¹ significativoÂ» â€“ afferma Mosca. E le proiezioni disponibili ci dicono che il dato sarÃ significativo anche nei prossimi anni. Â«A livello mondiale, si ipotizza una crescita del 9%, mentre per quel che riguarda lâ€™Italia, la crescita stimabile si aggira attorno allâ€™8,5%Â» â€“ dichiara Mosca. Valori di tutto rispetto. Che risaltano ancora di piÃ¹ se si confrontano con i dati che Assinform ci fornisce in relazione al valore del mercato (circa 772 milioni di euro in Italia) e al comparto digitale.

Questioni di budget?

La sicurezza Ã¨ una componente fondamentale del servizio nel settore bancario. Che va di pari passo con il livello del servizio associato. In altre parole: se non câ€™Ã¨ una sicurezza adeguata, il cliente lo percepisce subito. Con la diffusione sempre piÃ¹ massiccia dei servizi di web e mobile banking, questa esigenza Ã¨ se possibile ancora piÃ¹ sentita. E di cui le banche non possono non tenere conto. Per questo la sensibilitÃ ai temi della sicurezza si riscontra sin dalla fase di ideazione di un certo servizio. La security Ã¨ percepita come un elemento significativo e non accessorio di un servizio. Un tema affrontato sin nelle fasi iniziali di sviluppo di applicazioni e architetture. Un vincolo dal quale non si puÃ² derogare. Anche per via di una normativa piÃ¹ stringente. A livello nazionale ed europeo. Alcune raccomandazioni della BCE sulla sicurezza dei pagamenti Internet richiedono la presenza delle soluzioni piÃ¹ sicure esistenti sul mercato (one-time password, strong authentication). Diventa difficile persino progettare nuovi servizi digitali senza dover traguardare anche quelle misure che la BCE e BI hanno definito in termini di sicurezza. In questo quadro, qualcuno potrebbe essere indotto a credere che il budget rappresenti un problema nel settore. Come – in effetti – accade altrove. Ma non Ã¨ cosÃ¬. Â«Nel nostro Paese, il settore bancario Ã¨ tradizionalmente uno di quelli piÃ¹ sensibili, piÃ¹ soggetti a obblighi normativi e, anche per questo, con budget piÃ¹ elevati in materia di sicurezza delle informazioniÂ» â€“ rileva Fabio Guasconi, membro del direttivo CLUSIT .

Click To Tweet

Â«Dai dati del nostro rapporto, emerge chiaramente che la sicurezza Ã¨ una delle prioritÃ dâ€™investimento nel settore bancarioÂ» â€“ riprende Mosca di Assinform. Si tratta di perseguire continuitÃ , equilibrio e flessibilitÃ degli investimenti. Questo contesto inoltre ha portato a una maggiore analiticitÃ nel volume degli investimenti. Gli investimenti non sono piÃ¹ un esercizio arbitrario, ma correlati al rischio valutato analiticamente. Questo cambio di paradigma modifica completamente lâ€™approccio al problema. Non si tratta piÃ¹ di diffondere una maggiore cultura del business tra il personale di banca che segue lâ€™IT, quanto di aver definito delle valutazioni analitiche

che mettano in evidenza le soluzioni tecniche necessarie per proteggere i servizi digitali. E di conseguenza investire di piÃ¹. In altre parole, il range entro cui oscilla il budget destinato alla sicurezza Ã¨ il risultato di considerazioni sempre piÃ¹ analitiche. Se a un certo punto ci si trova a dover far fronte a un trend crescente di rischi e a perdite economiche ma si dispone di una valutazione dei rischi – passati e futuri – che restituisce la situazione di quel che si Ã¨ giÃ investito e si sta investendo, si possiede la forza organizzativa per giustificare e rafforzare gli investimenti in sicurezza informatica. E se necessario, lâ€™IT Ã¨ in condizioni di fare arrivare queste decisioni – e la normativa lo prevede â€“ sul tavolo dellâ€™AD e del board. CiÃ² dÃ ancora piÃ¹ forza a chi valuta la necessitÃ di investire di piÃ¹, potendo appoggiarsi a un processo strutturato di valutazione del rischio per trovare il giusto equilibrio tra le varie voci di investimento. In questo periodo, il tema interno alle banche Ã¨ di bilanciare gli investimenti tra la sicurezza del front-end e quella del back-end. Â«Le banche hanno sempre investito molto sulla sicurezza del back-end. Oggi, che gli investimenti si sono spostati sul front-end, le due aree si devono allineareÂ» â€“ spiega Mosca. Gli investimenti poi dovrebbero procedere in linea con la strategia che la banca delinea. Fare in modo cioÃ¨ che le risorse dedicate alla sicurezza siano coerenti con le scelte strategiche di fondo. Improntate se possibile alla continuitÃ . Ma allo stesso tempo abbastanza flessibili per adeguarsi al cambiamento. Come in effetti Ã¨ avvenuto con la giÃ citata svolta digitale e lâ€™accantonamento di budget dedicati alla sicurezza piÃ¹ consistenti.

Minacce e analisi dei rischi

Attenzione al problema della sicurezza e obblighi normativi incidono sui budget in materia di sicurezza delle informazioni nel comparto bancario.Â Budget adeguati, obblighi normativi e attenzione al problema pur costituendo un buon punto di partenza non sono di per sÃ© sufficienti a garantire un livello adeguato di sicurezza nÃ© a rispondere alle nuove minacce che ogni giorno si evolvono nel mondo, come spiega Guasconi diÂ CLUSIT.Â Assistiamo allo sviluppo di modalitÃ sempre piÃ¹ complesse. E cresce continuamente la cosiddetta superficie di attacco, cioÃ¨ il numero e lâ€™ampiezza di quelle che sono le aree che Ã¨ possibile sottoporre a un attacco. Â«Una realtÃ di cui bisogna tenere conto. La superficie dâ€™attacco cresce perchÃ© continuiamo ad aggiungere dispositivi e applicazioni. E tra le prime organizzazioni a farlo ci sono sicuramente le istituzioni finanziarieÂ» â€“ afferma Mosca. Una sfida impegnativa anche per le banche, che richiede una capacitÃ di risposta adeguata. Non solo. Â«Problematiche possono riscontrarsi da parte delle singole organizzazioni piuttosto che del sistema nel suo complesso, nel mettere in atto con un approccio dinamico le azioni di prevenzione, protezione e governance necessarie, lavorando sul piano tecnologico, organizzativo, di processoÂ» â€“ conferma Fabio Rizzotto, research director di IDC . Ed Ã¨ lecito chiedersi per esempio se lâ€™analisi dei rischiÂ eÂ dei danni che gli attacchiÂ informatici possono provocare sul piano del businessÂ eÂ dellâ€™immagine aziendale sia correttamente valutata dal settore bancario in Italia. Alcune recenti indagini di IDC Italia ci forniscono una prima bussola per orientarci tra la serie di rischi di business e IT percepiti dalle istituzioni bancarie.

Â«In termini di intensitÃ percepita, la perdita di dati personali/finanziari e potenziali danni alla reputazione sono ai primi posti. Non mancano anche i rischi legati a possibili sanzioni da parte di autoritÃ di controllo, oltre che i costi di intervento IT. Tuttavia, il settore bancario in Italia Ã¨ Â«consapevole dei rischi e dellâ€™esposizione â€“ dichiara Rizzotto di IDC. PerciÃ² non riteniamo che ci siano carenze sotto il profilo dellâ€™osservazione e della valutazione del fenomeno, seppur sfuggente e complessoÂ».

Click To Tweet

Problemi organizzativi

La trasformazione organizzativa e culturale potrebbe rappresentare un elemento di debolezza nel quadro degli ambiti di intervento delle banche. Â«Accanto agli aspetti di metodo e progettuali, nel percorso evolutivo Ã¨ importante prestare attenzione da un lato alle novitÃ tecnologiche (per esempio soluzioni di Security Intelligence o di Predictive Security) e dallâ€™altro alla crescita di attitudini e competenze. Chief security officer (CSO), security manager, risk manager dovranno sempre piÃ¹ bilanciare le competenze tecnologiche con le competenze di processo e applicative, la capacitÃ di relazione con il business, la capacitÃ di osservare fenomeni complessi, lavorando su dati e informazione, policy makingâ€¦Â» â€“ osserva Rizzotto. In questo senso disporre di una Â«struttura organizzativa dedicata alla sicurezza e una figura apicale che risponda ai vertici aziendali Ã¨ un passaggio fondamentale in questa prospettiva, giÃ intrapreso in altri settori in tutto il mondo ma che ancora langue in quello bancarioÂ» â€“ afferma Guasconi. Per esempio, il grande gruppo bancario con sedi e filiali in tutto il mondo dispone senza dubbio di strutture specializzate dedicate alla sicurezza. Che aggiornano e informano sullâ€™evoluzione degli attacchi e lo stato della sicurezza nel gruppo. Questi team gestiscono molti aspetti che riguardano la sicurezza, compreso la scelta dei prodotti e dei servizi che vengono acquistati centralmente e poi adattati alle singole realtÃ locali. Tuttavia, una struttura troppo centralizzata con un unico CSO per tutto il gruppo rischia di allontanarsi troppo dalle singole realtÃ e dai problemi locali. Inoltre, diventa difficile per questâ€™unico CSO riuscire a delineare una strategia unica adattabile alle peculiaritÃ (anche normative) dei singoli paesi. Un problema questo particolarmente evidente quando si tratta di compliance. La gestione centralizzata della sicurezza inoltre puÃ² generare situazioni di sovrapposizioni di policy. In ogni caso – anche quando si tratti di un gruppo presente solo sul territorio nazionale – lavorare sulla consapevolezza del management non Ã¨ mai un esercizio inutile. A partire dai chief information security officer (CISO). Ã¨ importante riuscire a sensibilizzare il top management. Portare cioÃ¨ allâ€™attenzione dei vertici i dati che riescono a dare una visione chiara dei problemi. In questo senso una comunicazione efficace tra le parti Ã¨ sempre auspicabile. Senza dubbio Ã¨ importante che gli uomini della security siano capaci di farsi ascoltare dal management. E per questo servono procedure che consentano un confronto periodico e la discussione dei risultati che si vogliono ottenere. Solo cosÃ¬ sarÃ possibile far accettare lâ€™idea che la sicurezza Ã¨ una componente essenziale della qualitÃ di prodotti e servizi e non un componente accessorio.

Click To Tweet

Formazione e continuitÃ

Il cybercrime ha ampiamente dimostrato di essere in grado di sfruttare efficacemente tutte le tecnologie disponibili, anche quelle piÃ¹ innovative, piegandole ai propri scopi. Allo stesso modo si serve delle persone. E delle loro debolezze. Per questo rimane sempre attuale puntare sulla formazione delle persone. Fare in modo che i propri collaboratori siano pronti, anche dal punto di vista mentale, ad affrontare e se possibile prevenire i nuovi attacchi Ã¨ un obiettivo che le aziende dovrebbero continuamente perseguire. Â«Ã¨ necessario sensibilizzare costantemente tutto il personale sullâ€™importanza del tema e sul comportamento da utilizzare, sfruttando le nuove tecnologie per garantire sempre un alto livello di sicurezza delle informazioniÂ» â€“ conferma Guasconi di CLUSIT. Un investimento il cui ritorno non Ã¨ sempre immediato, ma importante per lâ€™azienda. Purtroppo, il problema non si esaurisce formando il personale interno e riguarda soprattutto la clientela delle banche, prese da due necessitÃ . Da un lato rendere i servizi semplici da utilizzare da parte della clientela e dallâ€™altro mettere in campo delle misure che assicurino un elevato grado di sicurezza. Occorre cioÃ¨ muoversi nei riguardi del cliente sia per rafforzarne la consapevolezza sia per spingerlo allâ€™adozione di comportamenti di sicurezza adeguati alla gravitÃ della minaccia. Oggi, in modo sempre piÃ¹ capillare, un gran numero di istituzioni del settore bancario Ã¨ sceso in campo. Per esempio, Banca dâ€™Italia ha approntato un vademecum in cui si sintetizzano le misure di sicurezza fondamentali che banche e utenza debbono adottare. Tutte le banche poi emettono informative a livello contrattuale, cercando di rappresentare giÃ al momento dellâ€™adesione al servizio la natura degli eventuali rischi e il livello di attenzione che devono avere i clienti. Lâ€™azione di sensibilizzazione prosegue sia in filiale sia attraverso il contact center. Il rapporto ABI Lab conferma che queste azioni sono portate avanti da una percentuale elevatissima di banche. Abi LAB – inoltre – porta avanti nel mondo dellâ€™associazione bancaria unâ€™opera di sensibilizzazione attraverso la collaborazione con la polizia postale. Mentre per le aziende Ã¨ disponibile un documento specifico Linee guida sulla sicurezza informatica.

Click To Tweet

Uno sforzo che nasce da una constatazione precisa, lâ€™elevato grado di rischiositÃ rilevato. Secondo un sondaggio realizzato da Kaspersky Lab e B2B International, quasi la metÃ (42%) degli utenti Internet italiani crede che le attivitÃ bancarie tradizionali siano piÃ¹ sicure di quelle online. Tuttavia, nonostante questi timori, la maggior parte degli intervistati effettua alcuni pagamenti online senza prendere neppure le misure di sicurezza di base, mettendo i propri soldi e la reputazione delle banche a rischio. PerciÃ² va ancora una volta sottolineata la necessitÃ di fare formazione. La sicurezza poggia su un pilastro fondamentale: la consapevolezza del problema, che si ottiene soltanto attraverso la formazione e la sensibilizzazione. Le aziende associate che operano in questo settore tendono a dire che ci sono tre pilastri: la tecnologia, lâ€™organizzazione

e la consapevolezza. Non a caso, una buona parte delle vulnerabilitÃ sono strettamente collegate a temi quali il social engineering, lo spear phishing e tutte quelle forme di attacchi che fanno leva sulla mancanza di informazioni da parte delle persone che dovrebbero operare.Â Â«In Italia, il settore bancario Ã¨ tradizionalmente molto sensibile al rischio (operativo, di credito…), ma sfortunatamente il rischio relativo alla sicurezza informatica rientra sempre con una certa difficoltÃ nei modelli di calcolo del rischio a supporto delle decisioni strategiche e anche tatticheÂ» â€“ afferma Guasconi.Â La continuitÃ pertanto rappresenta un atout importante nella strategia di sicurezza di una banca. E per dare continuitÃ alla strategia di sicurezza, un buon punto di partenza Ã¨ di misurare lâ€™impatto degli investimenti e delle misure di sicurezza adottate. Â«La sicurezza Ã¨ sempre un compromesso tra diversi fattori: costi, rischi eÂ opportunitÃ . Massimizzare i ritorni di business da investimenti in sicurezza significa quindi anche misurare miglioramenti di processo e organizzativi, oltre che rispetto e â€œaderenzaâ€ alle normeÂ» â€“ dichiara Rizzotto di IDC Italia. Ritorna ancora una volta lâ€™importanza della formazione. Una preparazione adeguata consente allâ€™IT di rispondere alle sfide lanciate dalle minacce informatiche. Riuscire a misurare periodicamente e in modo sistematico lâ€™impatto degli attacchi, degli incidenti, dei falsi positivi conferisce un vantaggio importante allâ€™IT. Serve – una volta ancora – un aggiornamento continuo del personale IT sullâ€™evoluzione dello scenario cybercrime e sicurezza. Senza lesinare mezzi e risorse. Evitando in ultima analisi di interpretare la sicurezza come un modello passivo, proiettato soltanto verso la mera protezione di asset e dati, e non invece come un processo continuo che si deve integrare in modo armonico con la strategia digitale dellâ€™istituto finanziario.