DICEMBRE 2022

IL CAFFÈ DIGITALE

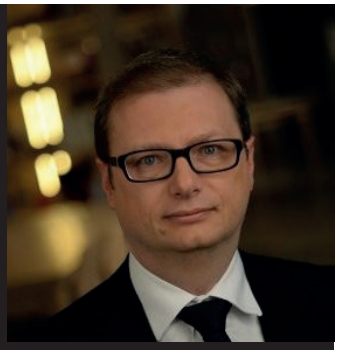
THE INNOVATION GROUP NEWSLETTER

TUTTE LE COLAZIONI DEL 2022

SOMMARIO

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

1



Alessio Pomasan, Banca Mediolanum

3

Andrea Provini, Fabio Cucciniello, Bracco Imaging Spa

6

Giorgio Striano, Luxottica

9

Valeria Rossi, Open Hub Med

12

Fabrizio Locchetta, Siram Veolia

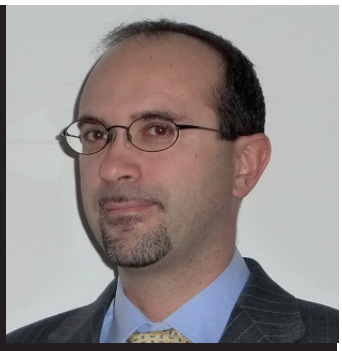
14

Francesco Fiaschi, Autostrade per l'Italia

16

Maria Teresa Basile, Telespazio

18



Raoul Brenna, Fastweb

22

Patrick Coggi, Banca del Ceresio

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Alessio Pomasan, Chief Information Officer, Banca Mediolanum

La sicurezza alla radice dei nuovi sviluppi

Roberto Bonino, Research and Content Manager
The Innovation Group

Lo scenario della cybersecurity si fa sempre più complesso, per il concorso di fattori che spaziano dalla regolare scoperta di nuove vulnerabilità in apparati e applicazioni all'affermarsi dell'era della employee mobility, con l'aumento degli accessi remoti e delle applicazioni cloud-based che fanno crescere il numero di dispositivi, dati e flussi da proteggere.

Abbiamo pertanto analizzato il tema, attraverso l'esperienza diretta di Banca Mediolanum, raccontata dal CIO Alessio Pomasan.

La stratificazione storica delle infrastrutture di cybersecurity porta con sé una certa dispersione dei potenziali punti di penetrazione può rappresentare un problema nella capacità di individuare le minacce effettivamente pericolose. Come avete affrontato questa problematica?

Per gestire al meglio questa situazione, occorre, come nel nostro caso, disporre a monte di un disegno robusto dell'architettura di sicurezza complessiva, in modo da evitare di trovarsi con sovrapposizioni o punti oscuri e i relativi impatti sui costi e sullo sforzo di gestione. Naturalmente, anche noi partiamo dall'evoluzione delle minacce, ma ci siamo ormai orientati verso un approccio di security by design. Ogni nuovo progetto che parte implica già nella fase di demand l'analisi di tutti i rischi di sicurezza collegati, per fare in modo che siano già integrate le misure di mitigazione necessarie.

Qual è il livello di automazione nella trattazione delle minacce, soprattutto quelle più comuni e apparentemente più semplici da contrastare?

Abbiamo fatto notevoli passi avanti, in diverse direzioni, arrivando in alcuni casi a integrare anche strumenti che impiegano l'intelligenza artificiale per contrastare la costante evoluzione dello scenario delle minacce. Anche alla luce del contesto pandemico che ha visto una crescita esponenziale di alcune tipologie di attacco, abbiamo accelerato l'implementazione della roadmap volta ad evolvere il livello di maturità dei presidi di difesa.

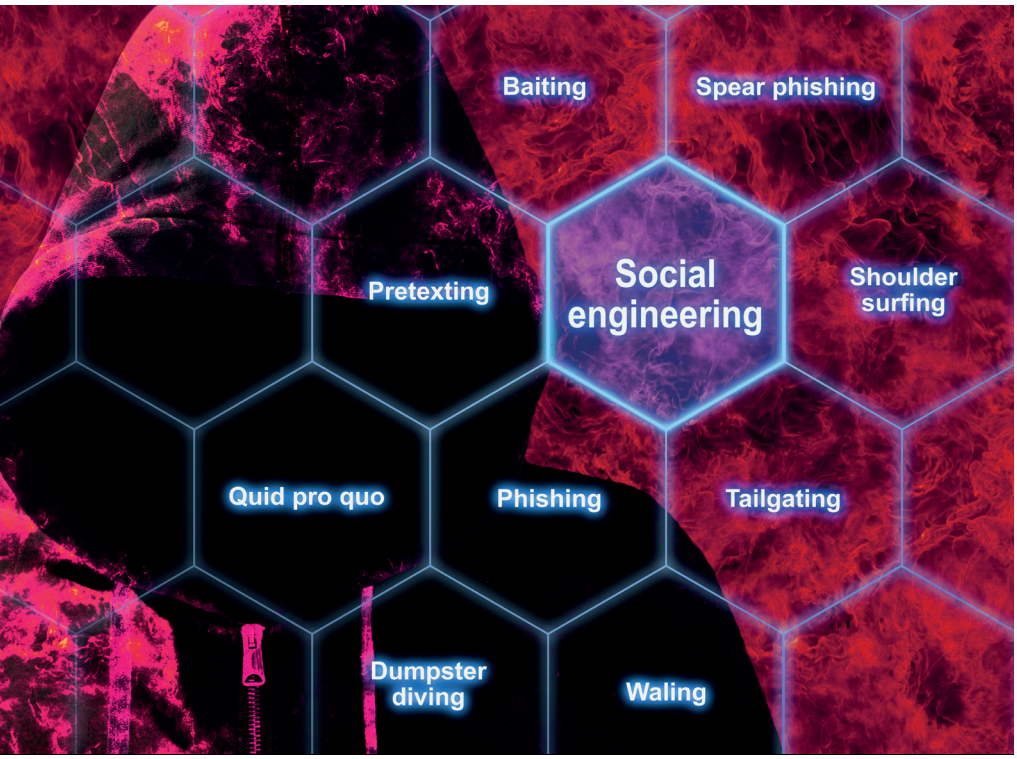
A mero titolo di esempio nel corso del el 2020 circa l'80% delle email ricevute dal nostro sistema di posta elettronica aziendale era spam : Ancora più importante è la velocità di risposta a fronte della rilevazione di ransomware/ malware sugli asset aziendali, con l'isolamento della risorsa attaccata: questo dà l'idea di quanto sia necessario disporre di automatismi sia per la trattazione di volumi importanti, sia per la velocità di risposta al fine di contenere possibili impatti all'Azienda.. L'automazione della gestione degli eventi di

sicurezza ci ha consentito di poter focalizzare gli impegni delle risorse a disposizione su temi più strategici e complessi, come ad esempio la threat intelligence e la prevenzione delle frodi verso i clienti. Infine, a tutto ciò si aggiunge il notevole sforzo dedicato al potenziamento delle competenze interne.

Quali sono le categorie di minacce che catalizzano maggiormente la vostra attenzione?

Probabilmente, la categoria di attacchi che richiede maggiore concentrazione è rappresentata dal social engineering, dove il livello di raffinatezza è diventato particolarmente elevato e la capacità di individuazione si è fatta più complessa.

Il nostro obiettivo è cercare il più possibile di arrivare a rilevazioni in tempo reale e addirittura di anticipare le mosse degli attaccanti; in questo senso, troviamo particolarmente utile poter far leva sulla threat intelligence, che porta a scandagliare anche il dark e deep Web.



Come avete affrontato il problema della cronica carenza di skill nel mondo della cybersecurity?

Da alcuni anni abbiamo ripensato tutta la strategia di sicurezza aziendale sia in termini di governance che di operations. Questo ha implicato anche un potenziamento della squadra in tutte e due le direzioni.
Il reperimento degli skill è certamente complesso di questi tempi, soprattutto per la difficoltà di individuare figure in grado di riconoscere i pattern sui quali occorre maggior attenzione e competenza. Per tenere il passo, abbiamo deciso di investire molto anche sulle competenze interne.

Come evolverà la vostra strategia nel prossimo futuro?

Esaminando il nostro percorso negli anni, possiamo dire di essere partiti con un approccio strettamente reattivo anche se fin da subito abbiamo realizzato che l'approccio di maggior valore per l'Azienda è quello preventivo: da qui la definizione e la realizzazione di una roadmap ben definita capace di far incrementare il nostro livello di maturità verso la cosiddetta Sicurezza Adattiva o "Full Stack" più adeguato a rispondere alle evoluzioni della nuova superfice di attacco, sempre più "liquida", e della complessità degli attacchi, andandone a considerare ed intercettare la strategia complessiva: a fronte di una minaccia, si connetteranno e correleranno le relazioni su tutto l'ambiente informatico dell'Azienda, analizzandone il significato globale per meglio rispondere alla minaccia.

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Andrea Provini, Global CIO e Fabio Cucciniello, Global CTO di Bracco Imaging Spa

Lavoro ibrido, cloud, edge: cosa cambia per le reti aziendali?

Roberto Bonino, Research and Content Manager
The Innovation Group

Molti sono i fattori di cambiamento che stanno rimodellando le infrastrutture di rete delle aziende. La progressiva migrazione al cloud o lo spostamento di potenza di calcolo verso le periferie, tipica dell'edge computing, si assommano alla riorganizzazione forzata dalla pandemia e alla conseguente adozione di modelli di lavoro ibrido. Tutto questo sta portando a un inevitabile allargamento del perimetro aziendale, con conseguenti ricadute sulle necessità di monitorare un'infrastruttura più articolata e adozione di forme avanzate di protezione.

Abbiamo provato a capire gli effetti di questo insieme di fattori di cambiamento con Andrea Provini, rispettivamente Global CIO di Bracco Imaging Spa e Presidente di AUSED e Fabio Cucciniello Global CTO di Bracco Imaging Spa.

In quale modo la fase emergenziale del 2020 e il successivo consolidamento del lavoro ibrido ha avuto ripercussioni sulle vostre necessità di connettività a 360° e, di conseguenza, come avete dovuto adattare l'infrastruttura di rete?

Provini: La pandemia non ha cambiato una strategia architetturale che si era già sedimentata nel recente passato, ma semmai ha permesso di verificare che le scelte effettuate fossero efficaci proprio in caso di situazioni particolari come quella verificatasi soprattutto nella prima parte del 2020. Avere un'infrastruttura ridondata può essere un elemento percepito come un costo superfluo in condizioni normali, ma il cambiamento di scenario di questi ultimi due anni ha dimostrato quanto sia importante muoversi per tempo e in chiave preventiva.

Cucciniello: Va detto che noi siamo una realtà con una popolazione nomade già piuttosto consistente anche prima della pandemia, quindi la nostra infrastruttura era già predisposta per gestire questa realtà. Lo stress un po' forzato dell'ultimo periodo ha solo richiesto qualche adattamento e l'accelerazione di decisioni già

pianificate, come l'adozione della multifactor authentication.

In quale misura viene già fatto uso di risorse acquisite in cloud e cosa comporta questo in termini di complessità di controllo e monitoraggio di tutte le risorse infrastrutturali dell'azienda?

Provini: Già dal 2015 abbiamo avviato un percorso cloud-first per ogni nostra evoluzione. La migrazione ha già riguardato la parte applicativa, mentre lo scorso anno siamo partiti con i data center, tutto in direzione del public cloud. Si può dire che siamo stati un po' dei precursori in ambito farmaceutico, dove il presidio sui dati era visto in passato come un dogma vincolante. Oggi misuriamo gli effetti positivi di questo passaggio anche in termini di sicurezza, oltre che di agilità e flessibilità. La prossima evoluzione in questa direzione riguarderà la business continuity e il disaster recovery.

L'evoluzione della relazione fra azienda e persone innescata dal consolidamento della modalità di lavoro ibrido sta portando alla revisione dei processi legati, per esempio, alla gestione dell'identità aziendale, per favorire l'accesso alle risorse aziendali

“location independent” in un contesto garantito e sicuro tanto per l’impresa quanto per dipendenti e collaboratori?

Provini: Abbiamo già sdoganato da tempo il concetto di identità digitale, proprio perché una grossa fetta della nostra popolazione aziendale è nomade per la natura stessa del proprio lavoro e, quindi, ha bisogno di un accesso dall’esterno flessibile e indipendente dal luogo in cui si trova o dal dispositivo utilizzato. Abbiamo semplicemente aumentato la portata di un’architettura già orientata in questa direzione. Semmai, si è enfatizzata l’attenzione verso la sicurezza, con strumenti utili a individuare comportamenti anomali legati all’identità e, quindi, al ruolo delle persone che accedono alla rete.

Avete già adottato un modello di sicurezza Zero Trust? Quali esigenze vi stanno eventualmente spingendo in questa direzione e quali sono i limiti o scogli ancora da superare?

Cucciniello: Si tratta di un percorso graduale e meditato. In realtà, preferiamo identificare i comportamenti anomali in modo puntuale ed efficace, mostrando un’adeguata reattività in caso di necessità. Progressivamente, arriveremo a definire regole che consentano di svolgere determinate attività solo a gruppi di utenti o dispositivi indentificati e controllati. In prospettiva, vogliamo aumentare le nostre capacità proattive, utili per prevenire incidenti, così come proteggere meglio le identità privilegiate e anche singoli documenti di particolare valore o delicatezza.

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Giorgio Striano, Chief Operating Officer di Luxottica

Il digitale permea la produzione in Luxottica

Roberto Bonino, Research and Content Manager
The Innovation Group

Non è certamente un periodo facile quello che sta attraversando il mondo della produzione industriale. Ancora condizionato da alcuni effetti di lungo termine collegabili alla pandemia, il settore si trova ad affrontare anche le difficoltà legate agli shortage e agli aumenti di costo delle materie prime, le complessità di pianificazione delle supply chain e anche gli effetti legati al conflitto russo-ucraino.

L'apporto delle tecnologie digitali ai processi di produzione tende a farsi sentire con maggior forza in periodi come questo, nel quale elementi congiunturali si assommano a evoluzioni collegate alle necessità di ricavare efficienza dai processi, raccogliere e interpretare i dati forniti dalle macchine e dai software, automatizzare attività in modo intelligente e fornire un apporto alle strategie aziendali in materia di sostenibilità aziendale.

Luxottica non è solo uno dei brand italiani più noti e diffusi nel mondo, ma è anche una realtà all'avanguardia nell'evoluzione dei processi produttivi. Per analizzarne lo stato dell'arte e gli sviluppi in corso, abbiamo fatto colazione con Giorgio Striano, Chief Operating Officer di una realtà globale di punta nel design, produzione e distribuzione di occhiali da sole e da vista.

In quale modo oggi la tecnologia digitale vi aiuta a ottimizzare i processi di produzione e quali strumenti utilizzate per razionalizzare e visualizzare i dati più funzionali ai vostri processi decisionali?

Siamo un'azienda verticalmente integrata e questo ci porta a gestire internamente tutti i processi industriali end-to-end, dal concept di un prodotto fino ai servizi post-vendita. La tecnologia funge da spina dorsale nella nostra organizzazione e il digitale è presente in tutti gli anelli della catena. In fase iniziale, ad esempio, la progettazione viene realizzata con l'ausilio di software grafico 3D e questo ci consente di velocizzare la successiva fase di fabbricazione. L'utilizzo delle stampanti 3D, inoltre, agevola il processo di prototipazione,

che porta poi alle attività di ingegnerizzazione, progettazione e industrializzazione, anch'esse fortemente digitalizzate. Il nostro settore, con un time to market molto veloce che segue le collezioni moda, trova nel digitale un importante alleato anche in fase di vendita, dove possiamo iniziare a vendere anche i prodotti che di fatto non sono ancora entrati in produzione, proprio grazie a strumenti innovativi presenti nei nostri showroom. Si tratta di tool che propongono ambienti immersivi nei quali viene presentato il modello digitalizzato degli occhiali, soprattutto di fascia alta, utilizzando rendering tridimensionali con colori e finiture identiche a quelle del prodotto fisico.

Quest'ultimo passaggio ha effetti diretti sull'ottimizzazione della produzione?

Si tratta di un elemento di grande importanza, perché occorre tener presente che ogni anno produciamo circa duemila nuovi modelli, differenziati poi per taglia e colori, per un totale di oltre 15mila SKU (Stock Keeping Unit). Tenendo conto che noi lavoriamo in una condizione di make to stock, dobbiamo disporre dei materiali in magazzino contando su previsioni di futura

vendita per regione, città e negozio per ogni singolo occhiale. Poter raccogliere ordini reali su prodotti presentati in modalità digitale, e quindi non ancora fisicamente disponibili, è molto importante; questo consente di iniziare ad alimentare i modelli previsionali di vendita con dati reali e non solo tramite algoritmi statistici. Questo è di grande aiuto per i modelli della fascia lusso che si solito hanno un ciclo di vita molto breve e quindi maggior rischio di obsolescenza.

Quali particolarità tecnologiche caratterizzano le fasi di produzione e consegna?

Innanzitutto, c'è un preventivo aspetto di industrializzazione, dove realizziamo internamente le varie componenti dei modelli. In produzione, poi, con il sistema Mes (Manufacturing Execution System) che abbiamo messo a punto, possiamo controllare in tempo reale il livello di funzionamento delle macchine, gli scarti di prodotto o le attività di avanzamento del semilavorato. Su alcuni tipi di modelli, inoltre, inseriamo certificazioni di originalità tramite chip RFID che consentono anche di tracciare il prodotto nei suoi spostamenti tra i vari magazzini fino alla spedizione al cliente, permettendo di avere una tracciabilità completa della singola unità, verificarne l'autenticità e combattere efficacemente il mercato parallelo.

Dove utilizzate soprattutto l'Industrial IoT e quali sono le frontiere di applicazione più avanzate?

Siamo un'azienda altamente automatizzata, ma abbiamo anche notevoli dimensioni e non è sempre facile reperire sul mercato tutto ciò di cui abbiamo bisogno. Abbiamo sviluppato al nostro interno un reparto dedicato alla progettazione, prototipazione e costruzione di sistemi di automazione funzionali al miglioramento dei processi e prodotti. L'automazione è utile per l'aumento di produttività ma anche per la riduzione del tempo di attraverso ed il miglioramento della qualità. Ad esempio con strumenti avanzati di visione è possibile individuare le possibili difettosità degli occhiali, cercando di replicare l'abilità "umana" a riconoscere possibilità difetti e con algoritmi di intelligenza artificiale è possibile risalire all'origine dei problemi e quindi ridurre gli scarti di prodotto.

Qual è il vostro rapporto con il dipartimento It?

Certamente non è più il tempo delle barriere e noi abbiamo stabilito un rapporto di collaborazione interfunzionale. Come abbiamo già detto, sviluppiamo molto al nostro interno e questo comprende anche, per esempio, strumenti di diagnostica che vengono utilizzati dagli ottici. La componente che si interfaccia con medici e pazienti è stata da noi progettata per creare una sorta di network fra tutti gli strumenti presenti in un negozio e poi dialogare, via cloud, con il database centrale. In casi come questi, chi si occupa degli applicativi lavora di concerto con chi produce gli strumenti. Allo stesso modo, c'è un team It per le fabbriche che dialoga stretto contatto con le persone deputate alla gestione operativa.

Valeria Rossi, Ceo di Open Hub Med

Le ambizioni di Open Hub Med, dal Mediterraneo verso il mondo

Roberto Bonino, Research and Content Manager
The Innovation Group

La gestione del traffico Web passa in Italia per i cosiddetti Internet eXchange Point (Ixp), situati in diverse aree grografiche (Mix a Milano e Namex a Roma sono i più importanti). A essi si è affiancata da alcuni anni Open Hub Med (Ohm), una società consortile con sede operativa a Carini, nel palermitano, che si è posto fin dalle origini l'obiettivo di creare un punto di aggregazione delle dorsali di rete, per agevolare lo scambio del traffico nel bacino mediterraneo, di diversificare le tratte che collegano i punti di approdo dei cavi sottomarini in Sicilia con l'Europa, oltre a offrire servizi di interconnessione e peering ai Paesi del Mediterraneo.

La compagine societaria comprende realtà come Atomo Networks, Eolo, Fastweb, In-Site, Exa Infra/Gtt, Italtel, Mix (Milan Internet Exchange), Retelit, Supernap, VuChain e Rete Xmed (rete di imprese costituita da operatori del territorio siciliano). Alla base del servizio, c'è un data center, progettato da In-Site nel 2016, che oggi si estende per oltre 1.000 metri quadrati.

A presiedere Open Hub Med è Valeria Rossi, con la quale abbiamo cercato di capire come il consorzio si ponga rispetto allo sviluppo auspicabile di mercato di trasporto dati in Italia più competitivo.

Open Hub Med è un consorzio a cui partecipano operatori e imprese interessate allo sviluppo dell'area quale polo delle telecomunicazioni nazionale ed internazionale, oltre al Mix. Quali sono le basi che ne stanno animando lo sviluppo e le relazioni con gli altri soggetti che operano in Italia su questo fronte, in particolare il Namex, che opera nella vostra stessa area territoriale?

Le basi che ne animano lo sviluppo sono legate al potenziale di traffico che può essere aggregato in Sicilia, area in cui insistono molti cavi sottomarini che provengono dal Nord Africa dal Middle East e oltre. La Sicilia, grazie alla vicinanza con i mercati emergenti dei Paesi d'oltremare, è la regione del Mediterraneo ottimale per il miglioramento

delle performance dello scambio traffico intra-operatori in termini di abbattimento delle latenze e di costi, con ricadute importanti anche a livello nazionale sia per l'apertura di un mercato di trasporto nazionale più competitivo che per l'opportunità di gestire in prossimità dati e processi computazionali, partecipando alle necessità di diversificazione dello storage dei dati e dell'erogazione di servizi cloud, elemento fondamentale per l' affidabilità, la continuità e la sicurezza dei servizi. In questo la presenza del Mix, tra i primi Ixp nel Sud Europa, è garanzia non solo tecnicamente dal punto di vista dell'erogazione dei servizi di interconnessione, ma anche di neutralità rispetto agli operatori che sono presenti.

Il Namex sta cercando di ricalcare a Bari un modello analogo, con un interesse all'approdo di cavi sottomarini che provengono principalmente dalla Grecia e dai Balcani, ma anche valorizzata negli ultimi anni dal cavo Aae-1, che dalla Cina raggiunge Marsiglia e che in Italia, per il tramite di Retelit, approda a Bari. Aae-1 è per altro già presente in OHM in quanto prolungato per via terrestre all'interno delle nostre facility di Carini. L'iniziativa di Bari non è nuova e, ad onor del vero, già in passato analogo tentativo del Namex non

Credits: Open Hub Med website

ebbe successo. Ma i tempi ora sono diversi anche se ritengo che una sinergia con l'iniziativa di Ohm sarebbe molto più proficua ed avrebbe un risultato più certo. Lavorare con successo per uno sviluppo del Sud richiede giocoforza fare sistema: piccole iniziative spot, a mio parere, sono disgreganti e rischiano di creare rumore di fondo più che portare ad un successo, in un mercato che per crescere richiede invece la creazione di una massa critica di interessi e di risorse. Proprio per questo abbiamo già iniziato a parlato con Namex e spero che si trovi lo spazio per una forte collaborazione.

Come vedete la possibile creazione di unico soggetto nazionale, situazione che si profila per esempio in Francia, per ottenere più massa critica a livello internazionale?

È quello che anticipavo sopra, riferendomi a Ohm e all'iniziativa di Namex a Bari. È importantissimo che non si disgreghino le forze per aumentare l'interesse sia a livello nazionale che internazionale. Il mercato in cui ci muoviamo vede soggetti enormi: cito Equinix come esempio che è coinvolta in Liguria nel progetto di futuro approdo del cavo 2Africa, che dall'India fa il periplo dell'Africa e tocca nel prolungamento a Est anche l'Italia a Genova. Si tratta di un esempio, ma ce ne sono altri. Competere con le risorse messe sul campo da questi soggetti è difficilissimo a maggior ragione se si portano avanti iniziative piccolissime e sparpagliate. Il Sud è una risorsa di tutto il Paese ed è in una posizione privilegiata, sarebbe un peccato non raggiungere l'obiettivo.

Quanti sono i vostri clienti oggi, verso quali operatori/ Isp state guardando maggiormente?

Oggi abbiamo circa 30 operatori presenti, tra operatori regionali e grandi operatori nazionali ed internazionali. Pur continuando ad operare per una maggiore presenza di operatori nazionali, le nostre strategie nel breve sono volte anche a portare in loco di operatori Tier-1 ed incrementare l'offerta del transito IP.

Quali aspettative riponete nelle prospettive aperte dal Pnrr?

Stiamo già lavorando ad un progetto promosso all'interno del Pnrr volto alla creazione di un polo tecnologico in ambito Life Science in cui Ohm è il riferimento per la parte infrastrutturale e in partenariato sia con aziende private che enti di ricerca del territorio. Vedremo se in futuro si apriranno ulteriori possibilità, certo è che in relazione ai servizi della/per la PA, mi aspetterei che Ohm venisse attenzionato e preso in considerazione anche quale uno degli elementi associati al Piano Strategico Nazionale, ad esempio quale punto per la collocazione di sistemi per il cloud nazionale, sia per evitare il lock-in di pochi grandi soggetti, sia per valorizzare e far crescere il Sud che anche tramite iniziative come la nostra può trarne vantaggio proprio in termini di crescita economica e di sviluppo.

Fabrizio Locchetta, CIO di Siram Veolia

Siram Veolia, verso il full-cloud con i giusti tempi

Roberto Bonino, Research and Content Manager
The Innovation Group

La trasformazione digitale è un dato di fatto nella stragrande maggioranza delle aziende italiane. A differire sono tempi e modalità di avvicinamento ed esecuzione di una strategia ormai chiaramente delineata. La presenza di componenti legacy non sempre facili da far evolvere, una certa resistenza culturale e le riflessioni sulla modalità di migrazione al cloud possono fungere da parziali freni a progetti improntati all'innovazione.

Siram Veolia è una realtà con caratteristiche da multinazionale, ma peculiarità specifiche della presenza sul territorio italiano che risale addirittura a oltre cento anni fa. Nel gruppo Veolia, che si occupa principalmente di acqua, rifiuti ed energia, Siram Veolia è fra le realtà di riferimento in Italia per la gestione dell'efficienza energetica, ed è anche un attore importante nei settori dell'acqua, dei rifiuti speciali e nei progetti di "smart city". In tale contesto, affianca clienti pubblici e privati nel percorso di trasformazione ecologica attraverso soluzioni sostenibili e tecnologicamente innovative.

Il Gruppo supporta i suoi oltre 1.800 clienti nella gestione e ottimizzazione dei servizi essenziali, contribuendo allo sviluppo sostenibile dei territori, assicurando riduzione dei consumi e dell'impatto ambientale. L'indotto Siram ha privilegiato fin qui la gestione di impianti energetici per numerose aziende del mondo sanitario, education, terziario e industria. Definito un percorso full cloud a livello di gruppo, la sua applicazione locale ha già prodotto risultati significativi, ma ancora riserva sfide legate al retaggio della tradizione, come spiega il CIO Fabrizio Locchetta.

Quali sono le aree dell'azienda che sono state oggi già coinvolte in progetti di trasformazione digitale e dove invece andrete a concentrarvi nel breve-medio termine?

Proprio per le caratteristiche del nostro business, dobbiamo tener presente che circa il 50% del nostro personale lavora sugli impianti dei clienti. I maggiori limiti verso una trasformazione digitale più compiuta derivano da questo. In generale, le applicazioni utilizzate per la gestione dell'efficienza energetica dei building (ad esempio i BMS, Building Management System) non si prestano a una facile gestione remotizzata. In compenso, abbiamo fatto notevoli passi avanti nell'implementazione dell'IoT, predisponendo sistemi basati su sensori e gestione dei dati per raccogliere le informazioni relative, ad esempio, alla qualità dell'aria o al rendimento degli impianti che gestiamo. Così come, a livello di impianto, molte componenti tecnologiche sono state migrate da soluzioni on-premise a infrastrutture cloud per favorire la gestione delle enormi quantità di dati raccolte dai siti e per aumentare sicurezza

e disponibilità dei sistemi e dei dati. Questo è il primo passo verso una digitalizzazione prevedibilmente più spinta per il futuro. All'opposto, abbiamo puntato molto negli ultimi anni sulla trasformazione digitale dei sistemi gestionali e amministrativi, per consentire il semplice accesso da browser alla maggior parte dei nostri sistemi da parte dei dipendenti. A medio termine, riteniamo che la digitalizzazione riguarderà il 95% della componente amministrativa dell'azienda e almeno il 50% di quella sul campo.

Avete fin qui riscontrato qualche ostacolo nei progetti eventualmente avviati? In quale misura si tratta di problemi strettamente tecnologici e quanto invece dipende da limiti culturali?

La tecnologia non rappresenta un limite oggi, mentre sul piano culturale abbiamo riscontrato qualche resistenza da parte dei colleghi, soprattutto nel passare da strumenti tradizionali ampiamente conosciuti e utilizzati ad applicazioni digitali che, per loro natura, presentano caratteristiche più standard e minori possibilità di essere adattate alle esigenze dei singoli utenti. Già nel 2018 siamo stati fra le prime aziende a migrare il nostro Erp su soluzione SaaS, causando non pochi disagi al personale, abituato da sempre ad automazioni e controlli implementati su misura per efficientare i processi e minimizzare gli errori.

Come avete affrontato la convivenza fra sistemi legacy e innovativi, in particolar modo la loro integrazione?

Negli ultimi mesi abbiamo avviato un progetto di data governance, che ci consentirà da un lato di armonizzare sulla piattaforma selezionata la maggior parte delle interfacce di integrazione create per alimentare i nostri data lake, e dall'altro di creare cataloghi di dati "certificati" all'interno dei nostri sistemi e nella produzione di report. Questo risponde parzialmente alla domanda. Noi lavoriamo in un contesto multicloud, con una componente on-premise ormai ridottissima, ma non è così semplice individuare una piattaforma di orchestrazione che soddisfi le nostre necessità. Stiamo anche valutando un modello che ci consenta di uscire dalla logica delle interfacce e creare un'architettura più aperta basata sulle moltissime Api che abbiamo implementato nel corso degli ultimi anni all'interno di un ecosistema ormai chiaramente indirizzato verso microservizi e container.

Francesco Fiaschi, CTO di Autostrade per l'Italia

Il cambiamento strutturale di Autostrade fa perno sul cloud

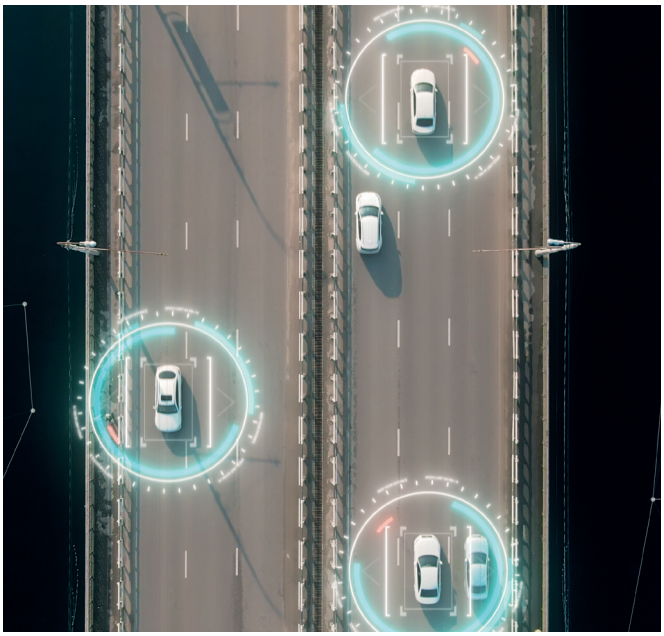
Roberto Bonino, Research and Content Manager
The Innovation Group

Si tende a identificare nel cloud uno dei principali fattori di trasformazione delle aziende in chiave digitale. Non è sempre così, in realtà, poiché la semplice migrazione in logica "lift & shift" di applicazioni o carichi di lavoro precedentemente ospitati nei data center interni cambia le modalità di fruizione, ma non agisce sui processi. Laddove alle spalle ci sia una strategia, con obiettivi ben definiti e modalità di esecuzione esplicitate, si può legittimamente parlare di digital transformation a tutti gli effetti.

Autostrade per l'Italia ha intrapreso recentemente un percorso di cambiamento profondo, con conseguente turnover di proprietà e management. In questo contesto, ha preso forma il piano Next to Digital, che si concentra su nove aree prioritarie, spaziando dalla gestione degli asset all'ottimizzazione del controllo di viabilità e traffico, dall'evoluzione delle modalità di esazione dei pedaggi all'innovazione dell'esperienza del viaggiatore. Solo nei prossimi tre anni, sono previsti investimenti di oltre 130 milioni di euro. La revisione dell'infrastruttura tecnologica è uno degli aspetti-cardine di questo processo di trasformazione. Ne abbiamo parlato con Francesco Fiaschi, CTO della società.

Su quali basi avete costruito il vostro cloud journey e come sta procedendo la modernizzazione infrastrutturale?

Siamo partiti dalla riorganizzazione e dalla digitalizzazione dei processi interni, sia di tipo core che non core. Questo progetto primario è stato accompagnato da diverse altre iniziative di trasformazione, tra le quali rientra anche il programma di ammodernamento, che va a incidere sulle architetture e le applicazioni It che non sono toccate direttamente dalla trasformazione digitale. Oggi ancora possediamo due data center interni, ma il piano prevede che nei prossimi tre anni la nostra componente architetturale e applicativa sarà migrata in cloud per il 60% del totale. La percentuale salirà di un altro 10% l'anno successivo. Si tratta di un



Il piano Next to Digital si concentra su nove aree prioritarie, spaziando dalla gestione degli asset all'ottimizzazione del controllo di viabilità e traffico, dall'evoluzione delle modalità di esazione dei pedaggi all'innovazione dell'esperienza del viaggiatore

obiettivo sfidante, ma riteniamo che il cloud metta a disposizione strumenti di costruzione dei processi digitali che possono agire come facilitatori. Inoltre, l'ammodernamento ci serve per fare efficienza soprattutto sul fronte dei processi operativi, distogliendo investimenti dalle componenti a basso valore aggiunto dell'IT.

Come avete costruito il percorso di migrazione e quali logiche lo hanno presieduto?

Nella nostra visione, oggi c'è il dato al centro dei processi e tutto ruota attorno a questo concetto. La trasformazione delle architetture e il loro conseguente passaggio nel cloud, con orientamento ai microservizi e alle architetture a eventi, serve a valorizzare i nostri asset, i dati aziendali e i processi rivisti in ottica moderna. Avendo posto il data lake al centro della nostra evoluzione e delle attività operative, concentriamo la nostra attenzione sulle informazioni che servono per prendere decisioni. A livello infrstrutturale, il nostro obiettivo di riferimento è la business continuity, estesa anche alle soluzioni di produzione, oltre che agli ambienti di test & sviluppo. Tutto questo testimonia come il cloud sia per noi un perno centrale della trasformazione e la scelta primaria per tutte le evoluzioni architetturali.

Privato, pubblico, ibrido: quale cloud model si adatta alla vostra realtà?

Nel processo di decisione iniziale, la componente che ha maggiormente catalizzato la nostra attenzione riguarda la sicurezza. Abbiamo fatto le opportune comparazioni fra i modelli proposti dal mercato e ne abbiamo concluso che non siano particolari elementi di differenziazione, poiché l'affidabilità deriva dall'utilizzo di pattern di costruzione delle architetture che siano intrinsecamente sicure e non lascino buchi o spazi pericolosi. Per questo abbiamo adottato la logica dell'infrastructure-as-a-code, che già integra modelli sicuri e in questo modo possono guadagnare in velocità dall'utilizzo del cloud pubblico.

Al di là degli aspetti tecnologici, dove ritenete di dover lavorare per migliorare il livello di protezione dei vostri workload e dati, pensando al mindset aziendale nel suo complesso, alla sensibilizzazione delle persone o a una visione che ancora deve consolidarsi a livello It?

Il mindset aziendale è strettamente collegato alla centralità del dato e all'importanza che si pone su questo aspetto. Le persone rappresentano sempre un potenziale veicolo di utilizzo non corretto degli strumenti aziendali, per cui poniamo attenzione a una forte cultura della sicurezza, all'accesso ai dati, all'utilizzo delle best practice. Cultura, conoscenza, attenzione all'implementazione delle architetture, test, alta affidabilità e ridondanza sono tutti elementi del mosaico di protezione di dati e workload.

Maria Teresa Basile, Head of It di Telespazio

Doveroso ma meditato il passaggio al cloud per Telespazio

Roberto Bonino, Research and Content Manager
The Innovation Group

La migrazione al cloud è da diverso tempo al centro dei processi di evoluzione tecnologica e strategica delle aziende. Infrastrutture, applicazioni e dati sono coinvolti a differente titolo e molte scelte, dalla prioritizzazione delle attività alla scelta dei provider di riferimento, possono dipendere da fattori e mindset ancora in grado di condizionarne l'attuabilità o la velocità di esecuzione.

I responsabili It devono tener conto di spinte ed esigenze non sempre allineate già all'interno dell'azienda, fra chi mette davanti a tutto la necessità della business continuity a tutti i costi e chi, proprio sul fronte tecnologico, deve far fronte anche alle problematiche di sicurezza. Il mondo sembra andare in una direzione ben definita, talvolta imponendo la propria legge a chiunque, ma non tutti i dubbi appaiono fugati e non tutti i dilemmi risolti.

Abbiamo provato ad analizzare la realtà di un soggetto molto particolare, come Telespazio, joint venture fra Leonardo e Thales, da sessant'anni impegnata nello sviluppo di soluzioni e servizi satellitari e per questo abbiamo incontrato la Head of It Maria Teresa Basile.

Quali tipologie di workload e relativi dati avete già portato in cloud e quali esigenze si celano dietro questa scelta?

Ci sono diversi elementi che concorrono a determinare le nostre scelte. Da un lato, stiamo certamente procedendo nella digitalizzazione dei processi aziendali e in vari casi le migliori soluzioni individuate sono cloud-native, quindi il passaggio diventa inevitabile. Tuttavia, tra le nostre line of business c'è la vendita di immagini satellitari che dopo il download, sottopone i dati a processi di post elaborazione anche impiegando forme di AI, come il machine learning, sulla base delle richieste dei clienti,: in questi casi vengono richieste risorse computazionali o di storage decisamente consistenti, che ha decisamente più senso gestire in una logica a consumo. Naturalmente, anche noi abbiamo l'esigenza di ottimizzare le risorse e i processi, per cui diventa conveniente centralizzare attività come backup, aggiornamenti, patching e gestione della security, in questo caso su cloud privato, ma non mancano situazioni in cui è il nostro cliente a chiederci l'erogazione di servizi in cloud, presso il suo provider di riferimento. Insomma, lo scenario è variegato, ma la direzione appare comunque ben delineata.

Come vi siete orientati per supportare da un lato l'attività di test & sviluppo e dall'altro il disaster recovery?

Già prima della pandemia abbiamo messo a fattor comune una serie di risorse aziendali, con particolare riferimento alla virtualizzazione, per cui abbiamo realizzato all'interno dell'azienda un cloud privato, destinato in modo particolare a chi si occupa di test e sviluppo di applicazioni, soprattutto

se orientate al business. Storicamente, poi, la nostra azienda si è sempre preoccupata sia della continuità del business che del disaster recovery, per cui la nostra infrastruttura è distribuita geograficamente, così come lo sono le nostre sedi sia in Italia che all'estero. La scelta del cloud privato ci ha consentito più agevolmente di aggiornare processi che esistono da oltre un decennio.

> **Abbiamo compreso quanto sia importante coinvolgere tutte le figure implicate in un processo, per cui vediamo dall'inizio di identificare un "cloud board" con le figure It, business, security e data protection, per analizzare ogni situazione, capire quali tipologie di dati siano coinvolte e fare una scelta orientata verso il provider più adatto**

Quella del private cloud è una scelta univoca o siete flessibili rispetto ai differenti modelli disponibili oggi?

Sul cloud non si può fare una scelta unidirezionale, perché dipende dal tipo di soluzione, dai dati sottesi, dai vincoli del vendor e da altri fattori. Per questo, lavoriamo anche con infrastrutture di cloud pubblico, così come l'attenzione sul tema della protezione dei dati ci porta in alcuni ambiti a mantenere rigidamente i dati in casa, demandando al cloud solo l'implementazione delle policy. Con il tempo, abbiamo compreso quanto sia importante coinvolgere tutte le figure implicate in un processo, per cui tutte le volte che ci troviamo a dover fare una scelta non scontata vediamo dall'inizio di identificare un "cloud board" con le figure It, business, security e data protection, per analizzare ogni situazione , capire quali tipologie di dati siano coinvolte e fare una scelta orientata verso il provider più adatto anche in base alle politiche di sicurezza proposte e alla concreta possibilità di poterne verificare l'attuazione.

Al di là degli aspetti tecnologici, dove ritenete di dover lavorare per migliorare il livello di protezione dei vostri workload e dati, pensando al mindset aziendale nel suo complesso, alla sensibilizzazione delle persone o a una visione che ancora deve consolidarsi a livello It?

Dal punto di vista it, abbiamo registrato una fase di cambiamento che ci ha portati a evolvere da coloro che eseguono operativamente determinati processi a coloro che si occupano più della configurazione iniziale e del monitoraggio di quello che accade. Le professionalità su questo fronte stanno cambiando: fra qualche anno forse faremo fatica a reperire persone in grado di fare il patching, ma ce ne saranno di bravissime a interagire con i cockpit che i cloud provider mettono a disposizione per comprendere il processo di patching che saranno loro ad aver eseguito. Il mindset aziendale, invece, è certamente cresciuto anche grazie all'effetto della pandemia e alla generalizzazione di alcune prassi di accesso e utilizzo di strumenti prima meno considerati, facendo scoprire anche agli utenti meno digitalizzati modalità di utilizzo delle soluzioni in precedenza sconosciute.

Raoul Brenna, Manager of Cybersecurity by Design, Vulnerability Management & Cybersecurity Awareness di Fastweb

Un percorso efficace per la Secutity Awareness

Elena Vaciago, Associate Research Manager
The Innovation Group

Quali sono i modi più efficaci per diffondere una cultura della sicurezza in azienda? Come impostare i contenuti, rivolgendoli a gruppi di persone con ruoli diversi in azienda? Sviluppare un programma di Security Awareness di successo è un'arte

Come far crescere e consolidare una cultura di Security Awareness in azienda?

Credo che l'elemento chiave sia sempre quello di trasferire alle persone un valore tangibile in quello che fanno. Ossia, il trasferimento della consapevolezza è più efficace se il destinatario è fortemente consapevole della profonda utilità di quello che sta apprendendo. L'approccio principale che ho utilizzato più volte nelle mie diverse esperienze di costruzione di programmi di formazione è quello "win win". A volte anche sotto lo slogan "proteggi te stesso per proteggere l'azienda". In pratica, chiarendo che le nozioni e gli atteggiamenti che si trasmettono sono utili per tutelarsi nella propria vita privata prima ancora che nel contesto lavorativo, (magari per difendersi da furti d'identità e frodi finanziarie che diventano sempre più credibili e personalizzate), le persone sembrano essere maggiormente stimolate a mettere in pratica una sana cultura di sicurezza informatica in tutti i contesti.

Un'altra via (e forse una fondamentale premessa) è quella di chiarire che i temi di sicurezza informatica non sono solo per tecnici. Anzi, che la materia è trasversale e ha delle ricadute in tutti i ruoli. Anche solo nel farsi le domande giuste. Ci saranno sempre aspetti "cyber" da considerare, sia che si stia avviando un progetto tecnologico ("ma è giusto che il sistema acceda a questi dati? E come lo fa?"), che si stia valutando un'iniziativa in generale ("si ha notizia di attacchi sofferti dai sistemi o servizi di questo tipo? O sviluppati dal medesimo fornitore?") o che si progetti una campagna di comunicazione ("ma se dico che gli utenti riceveranno un'email... Da dove devono aspettarsi di riceverla, per distinguerla dal phishing?").

Trovo che il modo migliore e con i risultati più efficaci e duraturi sia quando si riesce a trasferire alle persone il fatto che, lavorando con il giusto livello di consapevolezza su questi temi fin dall'inizio o "by design", si crea maggior valore per il business e si consolidano sistemi più resilienti.

Come realizzare contenuti formativi efficaci?

Il primo aspetto da considerare è certamente il capire molto bene cosa si vuole ottenere, e a quale target è diretta l'awareness, che è un concetto diverso rispetto alla formazione. Un conto è formare la persona attraverso contenuti di base un altro è trasferire nozioni che abilitano, se non l'adozione di best practice progettuali o

> **Una awareness generalista, magari rivolta a tutta la popolazione aziendale, ha un impatto diverso rispetto ad una focalizzata su gruppi specifici. Persone e ruoli diversi vanno ingaggiati in modi diversi**

tecniche, almeno la comprensione del fatto che ci siano elementi da considerare e incorporare nelle iniziative portate avanti in azienda.

Una volta chiarito il tipo di contenuto, anche il target è assolutamente rilevante. Una awareness generalista, magari rivolta a tutta la popolazione aziendale, ha un impatto diverso rispetto ad una focalizzata su gruppi specifici. Persone e ruoli diversi vanno ingaggiati in modi diversi. Ad esempio, le persone con una estrazione più tecnica potranno gradire la presenza di insight sul funzionamento di specifici attacchi (per comprendere meglio l'entità e la concretezza del rischio cyber attuale). Richieste o esigenze comuni sono, ad esempio, quelle di cercare di sintetizzare raccomandazioni in checklist, sebbene la natura stessa delle minacce informatiche poco si presti a schematizzazioni, o di proporre un mix di contenuti multimediali e/o interattivi. D'altro canto, non va sottovalutato il valore dei contenuti testuali, in cui si possono cristallizzare elementi su cui è bene che non ci sia ambiguità. Quando si tratta di impostare campagne rivolte a platee allargate, occorre quindi un compromesso tra tutti i fattori.

Sicuramente, nell'awareness, oggi, c'è un tema di velocità di fruizione: le persone sono letteralmente sommerse da contenuti informativi di ogni tipo; quindi, occorre prevedere ingaggi contenuti nel tempo (nell'ordine della decina di minuti) e ripetuti (ad esempio ogni qualche settimana) per tenere alta l'attenzione. Magari costruendo un percorso in cui ogni contenuto si leghi ai precedenti e in cui il fruitore è guidato attraverso un filo logico coerente.

Il tema del legame tra i contenuti si ripropone ancora più marcato quando si parla di formazione. Qui è molto apprezzata l'alternanza tra momenti di didattica frontale e momenti "hands-on", ma questi ultimi devono essere ben contestualizzati al contenuto trasferito e soprattutto organizzati con una logica di fruizione efficace.

Come testare il livello di preparazione raggiunto dalle persone?

Ecco, questo è un tema importante. Non credo che l'awareness debba necessariamente richiedere un momento di "verifica formale" della preparazione. Tuttavia, è evidente come sia necessario quantificarne l'efficacia, per affinare progressivamente i contenuti in un'ottica di continuo miglioramento. Tracciare i progressi compiuti in termini di efficacia dell'awareness può certamente essere d'aiuto, senza dimenticare l'importanza di un corretto tracciamento anche in funzione degli

obblighi di formazione derivanti dalla normativa di settore.

Sul come farlo, la risposta più immediata è quella dei "quiz". Introdurre piccoli momenti di ingaggio interattivi, sia durante l'erogazione che a posteriori, è un modo per tenere alta l'attenzione, e per individuare le aree su cui possono sussistere difficoltà. Tuttavia questo strumento non è in grado di restituire sempre e con estrema precisione il livello di preparazione raggiunto: per questo è importante prevedere anche modalità di ingaggio "situazionali".

L'utente deve essere posto di fronte ad uno scenario in cui si sollecita l'attivazione delle competenze idealmente acquisite, e il modo più immediato per farlo, è la simulazione pratica. Oggi si traduce ad esempio in campagne di phishing simulate, o altri esercizi simili. Questo apre una riflessione: cosa ci aspettiamo da questi momenti di "verifica"? Secondo la mia esperienza sono 3 gli indicatori principali per quanto riguarda l'efficacia dei programmi di awareness di questa tipologia:

- un primo indicatore è che la ripetizione delle simulazioni dovrebbe portare ad una diminuzione graduale nel tempo dei soggetti che falliscono nei test (e conseguentemente di quelli colpiti dagli attacchi);
- un secondo indicatore importante è la tempestività con cui chi identifica il phishing (o in generale l'evento anomalo) lo segnala. Questo è un tema fondamentale: se riesco a sollecitare una segnalazione da parte di un numero di persone statisticamente rilevante in un tempo molto breve, ho avuto successo. Dove "statisticamente rilevante" significa più alto del "rumore medio" delle altre segnalazioni. Nella pratica non pensiamo a numeri enormi: già una decina di segnalazioni concentrate in un periodo di tempo molto breve possono sollevare un alert!
- Infine, l'aumento del tasso di utilizzo dei canali di segnalazione corretti, che aiuta la sicurezza a diminuire la complessità di gestione migliorandone l'efficacia. Mi spiego: se l'azienda mette a disposizione l'oramai classico "bottone" per segnalare email sospette, è importante che le segnalazioni arrivino esattamente (e possibilmente solo) da questo. I contatti personali, le telefonate ecc. aiutano solo fino ad un certo punto.

È importante quindi, dopo ogni campagna, rileggere criticamente gli esiti e veicolare verso l'azienda i punti di forza e le aree di miglioramento riscontrate. Proprio per questo, rimango convinto del fatto che l'approccio basato su simulazioni pratiche (ad esempio il phishing,

ma non solo) debba rispettare tempistiche precise. Non credo sia utile spingere eccessivamente su una frequenza di simulazioni molto elevata: non si ha il tempo di far metabolizzare i risultati all'azienda e si rischia, potenzialmente, di sperimentare un incremento di segnalazioni riguardanti eventi non anomali.

In un'ottica di continuo miglioramento, Fastweb sta provando a ricreare situazioni di test realizzate attraverso interazioni con "chatbot", con l'obiettivo di consentire agli utenti di sviluppare un'interazione quanto più realistica possibile, in modo da poter cogliere con più efficacia i segnali e gli elementi che possono far scattare potenziali comportamenti non sicuri.

È possibile migliorare progressivamente il programma di Security Awareness nel tempo?

Non solo è possibile, ma aggiungerei anche che è doveroso. Come dicevo, non si può certamente avere la pretesa di trasformare tutti i dipendenti di un'azienda in esperti di sicurezza informatica. Ma il traguardo da porsi credo che sia sempre quello di trasferire quel giusto livello di consapevolezza che permette di far leva sulle persone per colmare i gap della tecnologia. Ovviamente, è fondamentale anche promuovere l'adozione di tecnologie innovative che a loro volta possono svolgere con più efficacia alcuni tipi di controlli.

Questo apre due temi a mio avviso. Il primo è certamente quello di rileggere sempre in modo critico i risultati dell'awareness erogata, ma anche di tenere sott'occhio le nuove minacce e i nuovi metodi con cui l'utente viene ingaggiato dagli attaccanti, così da affinare man mano i contenuti e assicurarsi di veicolare messaggi costantemente aggiornati. Naturalmente avendo sempre presente i destinatari: alcuni messaggi sono per tutti, altri per persone più tecniche, altre per chi fa un certo lavoro, ecc. Ma in ogni caso, con l'obiettivo di far sì che ciascuno possa contribuire a identificare e segnalare "anomalie" che, rispetto al proprio ambito di competenza, possano essere un segnale di un attacco in corso (per i più tecnici, un comportamento errato di un software, per chi più segue processi, un'email "stonata", ecc.)

Il secondo tema è invece quello della comunicazione: ho menzionato iniziative tecnologiche a supporto dell'utente, ma è importante anche che queste siano correttamente comunicate e spiegate agli utenti, perché ne possano trarre il massimo beneficio e non sollevino invece alert ingiustificati. Se si introduce ad esempio un nuovo controllo all'accesso quando ci si collega in VPN

(per citare un tema oggi molto diffuso) è bene che tutti gli utilizzatori sappiano quali nuovi comportamenti del software sono leciti, quali invece anomali. E a proposito di comunicazione, non mi stanco mai di ripeterlo, è altresì importante che a tutti sia ben chiaro a chi segnalare cosa e in che modo. Banalmente: se c'è un "bottone antiphishing", usiamo quello!

Cosa ti ha insegnato l'esperienza, una tua raccomandazione finale su questi temi?

Aumentare l'awareness delle persone è un percorso. Peraltro, è un percorso lungo, complesso, che presenta ostacoli e che in realtà non ha una fine, visto che il panorama degli attacchi è in continuo mutamento ed evoluzione anche in termini di sofisticatezza.

In questo contesto un utile suggerimento è quello di essere ricettivi, sia in termini di feedback che di lettura dei risultati delle attività, anche nei confronti delle nuove minacce in arrivo, così da comporre in ogni momento il miglior patchwork di iniziative. In particolare, inoltre, credo sia fondamentale far sentire tutti parte di uno sforzo complessivo, sia in termini di sicurezza dell'ambiente di lavoro che a favore della comunità e del singolo, mettendo le persone al centro. Un impegno che rientra all'interno di "Tu sei Futuro", la nuova visione strategica di Fastweb per aiutare tutti a costruire il proprio futuro con fiducia.

Patrick Coggi, Direttore Generale Banca del Ceresio

Il supporto al cliente nell'innovazione di Banca del Ceresio

Roberto Bonino, Research and Content Manager
The Innovation Group

La digitalizzazione ci aiuta a migliorare i processi interni, consentendo di abbandonare progressivamente la componente legacy e migliorando gli strumenti collaborativi per condividere meglio le informazioni e rafforzare il lavoro in team

Il territorio geograficamente ed economicamente più contiguo all'Italia è certamente quello della Svizzera Italiana. Vi operano molte realtà, impegnate in diversi ambiti, con un peso particolare per il finance, il manufacturing, i servizi e la sanità. In comune con il nostro territorio c'è senza dubbio una forte presenza di piccole e medie aziende, a fronte di un numero assai più contenuto di grandi organizzazioni. Molte di queste, poi, hanno rapporti diretti con l'Italia, per ragioni di business, condivisione di competenze e forza-lavoro o sedi.

Lo scenario appena descritto ha una ricaduta non dissimile sui processi di innovazione e trasformazione digitale, che le aziende della Svizzera Italiana hanno mediamente affrontato in modo diseguale, con alcuni casi di eccellenza, ma anche molte aziende che sono partite in modo estremamente cauto e legato a scelte decise da un management con atteggiamento tendenzialmente conservativo, come emerge da una recente ricerca qualitativa realizzata da The Innovation Group.

Fra le realtà con le idee più chiare e un percorso già piuttosto definito, troviamo Banca del Ceresio, da diverso tempo specializzata nell'offerta di servizi di gestione patrimoniale, consulenza finanziaria, intermediazione e custodia per clientela privata ed istituzionale. Abbiamo analizzato le strategie di trasformazione digitale con l'aiuto di Patrick Coggi, Direttore Generale dell'istituto.

Come si è strutturato fin qui il vostro cammino verso la trasformazione digitale?

Riteniamo che ogni evoluzione abbia senso se si pone al servizio del cliente. Dobbiamo tener presente che non siamo una transaction bank, ma ci concentriamo sul wealth management in un segmento di mercato molto alto e vogliamo proporre iniziative di interesse per il nostro mercato selezionato. Poniamo, innanzitutto, un accento particolare sugli aspetti analitici, allo scopo di fornire strumenti utili per comprendere l'andamento dei portafogli e crearsi, in prospettiva, report in autonomia. Sullo stesso solco, stiamo rafforzando la nostra presenza online anche per rendere più efficienti i processi di onboarding e di compliance. Aggiungiamo, poi, che facciamo parecchia ricerca nei nostri uffici di Londra, Milano e Lugano, ma questo lavoro viene ancora condiviso in modo talvolta inefficiente, per cui abbiamo digitalizzato anche questi flussi facendo leva su uno strumento di Crm adattato alle nostre necessità.

Come ha reagito l'organizzazione ai cambiamenti fin qui effettuati?

La digitalizzazione ci aiuta a migliorare i processi interni, consentendo di abbandonare progressivamente la componente legacy e migliorando gli strumenti collaborativi per condividere meglio le informazioni e rafforzare il lavoro in team. Il percorso evolutivo è tuttora in corso e quindi lo è anche il processo di accettazione, ma per le esperienze fin qui concretizzate sembra che tutto sia stato recepito in modo molto positivo. Certamente c'è un peso rilevante da attribuire al change management, perché non è possibile introdurre cambiamenti importanti senza un adeguato processo di accompagnamento.

Quale ruolo attribuite al cloud in supporto ai processi di trasformazione?

Non ci interessa una migrazione a tutti i costi. Stiamo andando verso un'infrastruttura ibrida ed è nostra intenzione portare sul cloud solo ciò che effettivamente porta con sé un vantaggio oppure non consente alternative.

Va sottolineato che oggi la normativa svizzera non consente di allocare in cloud dati e identificazioni dei clienti, né sul territorio né tantomeno all'estero, a meno di non aver ottenuto una precisa autorizzazione. Questo rappresenta un enorme freno allo sviluppo del cloud nell'industria finanziaria del nostro Paese e anche per noi le possibili aperture non potranno che andare in direzione della modalità di tipo privato.

Qual è il ruolo deil'It nelle strategie di innovazione?

In generale da noi c'è molta condivisione. A volte gli spunti arrivano dagli specialisti It, a volte addirittura dalla proprietà, poiché i nostri azionisti sono particolarmente appassionati di tecnologia. In qualche caso, anche i clienti ci segnalano di aver utilizzato qualche soluzione che vorrebbero ritrovare anche fra le nostre soluzioni. Si tratta di uno scambio continuo e generato in modo naturale.

Come avete affrontato fin qui il tema della carenza di competenze in ambito digitale?

Abbiamo una certa propensione a cercare al nostro interno i talenti che ci servono anche in campo tecnologico. Facciamo parecchia formazione interna e va detto che le nostre persone reagiscono bene. Siamo una realtà con un turnover molto basso e forte radicamento sul territorio, per cui la volontà di accettare i cambiamenti è certamente molto alta.

IL TEAM DEL CAFFÈ DIGITALE

Roberto MASIERO
Presidente
The Innovation Group

Ezio VIOLA
Co-founder
The Innovation Group

Emilio MANGO
General Manager
The Innovation Group

Elena VACIAGO
Associate Research Manager
The Innovation Group

Roberto BONINO
Giornalista, Research and Content Manager
The Innovation Group

Valentina BERNOCCO
Web and Content Editor
The Innovation Group

Loris FREZZATO
ICT Ecosystem

ISCRIVITI ALLA NEWSLETTER MENSILE!

Ricevi gli articoli degli analisti di The Innovation Group e resta aggiornato sui temi del mercato digitale in Italia!

COMPILA IL FORM DI REGISTRAZIONE SU

www.theinnovationgroup.it