OTTOBRE 2022

IL CAFFÈ DIGITALE

THE INNOVATION GROUP NEWSLETTER

NELLA DIGITALIZZAZIONE BISOGNA ESSERE AMBIZIOSI

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Raoul Brenna, Fastweb

CYBERSEC E DINTORNI

Le caratteristiche della cyber war emerse durante il conflitto in Ucraina

LA TRASFORMAZIONE DIGITALE

Diventare più sostenibili anche con la tecnologia

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

SOMMARIO

12

CYBERSEC E DINTORNI

Le caratteristiche della cyber war emerse durante il conflitto in Ucraina

Elena Vaciago

16

LA TRASFORMAZIONE DIGITALE

Diventare più sostenibili anche con la tecnologia

Valentina Bernocco

18

ICT ECOSYSTEM

Cloud e Sicurezza: l'integrazione intelligente di due mondi sempre più complessi

Loris Frezzato

L'EDITORIALE

Nella digitalizzazione bisogna essere ambiziosi

Roberto Masiero, Presidente

The Innovation Group

L'Italia ha compiuto progressi su infrastrutture di telecomunicazione, competenze e adozione del cloud sono apprezzabili. Ma con il Pnrr possiamo e dobbiamo accelerare.

Il Piano Nazionale di Ripresa e Resilienza è lo strumento che l'Italia si è data per accelerare la "doppia transizione", digitale ed ecologica, e per colmare il gap di sviluppo che la separa dai Paesi tecnologicamente più avanzati. Come The Innovation Group ci siamo proposti di monitorare (e di presentare nel nostro rapporto annuale, il "Digital Italy Report") lo stato di avanzamento degli investimenti in digitalizzazione previsti dal Piano, sia relativamente alla Missione 1 ("Digitalizzazione, Innovazione, Competitività, Cultura e Turismo") sia rispetto alle altre che presentano una componente di investimenti in digitale particolarmente significativi. Siamo al passo con la tabella di marcia per ottenere tutte le risorse a noi destinate dal Recovery Fund, ma oggi il necessario percorso verso la twin transition è attraversato da forti turbolenze legate ai rischi geopolitici, all'inflazione, alla crisi energetica e allo shortage delle materie prime e dei semilavorati: questi forti elementi di tensione impongono oggi alle nostre classi dirigenti delle scelte decise per garantire la continuità delle riforme e degli investimenti previsti dal PNRR e per evitare al Paese possibili scenari di crisi. La capacità di cavalcare la discontinuità tecnologica per far avanzare innovazione digitale e transizione ecologica nel pubblico e nel privato è, infatti, una parte fondamentale di queste scelte, e gli investimenti del PNRR sono oggi la chiave per una trasformazione concreta e profonda della nostra economia, della nostra Pubblica Amministrazione e della nostra società.

Nell'attuale contesto geopolitico e macroeconomico il digitale ricopre "un ruolo di assoluto primo piano, rappresentando una delle principali leve strategiche in grado di supportare e accelerare il processo di transizione in atto, e di limitare al minimo gli effetti negativi causati dalle situazioni emergenziali e dalle crisi geopolitiche, favorendo la resilienza e la ripresa competitiva delle principali economie mondiali", come scrive Agostino Santoni, vicepresidente di Confindustria con delega al Digitale, nel suo contributo all'interno del nostro report.

Ma che cosa vuol dire, esattamente, digitalizzare? Letteralmente, significa passare dalla forma analogica (quella della realtà materiale) ai bit, ma oggi quello di digitalizzazione è diventato un concetto assai più complesso. Per diventare digitali è necessario riorganizzare e talvolta stravolgere i processi, quelli aziendali così come quelli della Pubblica Amministrazione. Un'opera distruttiva e costruttiva insieme, che punta all'efficienza, alla produttività, alla semplificazione. E digitalizzare significa anche diventare "amici" del digitale, imparando a conoscerlo: qui si innesta il ben noto problema delle competenze, un problema che parte dalle sacche di analfabetismo informatico che ancora resistono in Italia e arriva alla difficoltà delle aziende di reperire professionisti specializzati nelle aree più innovative dell'informatica (la scienza dei dati, l'intelligenza artificiale, la cybersicurezza).

Non è un caso che molti degli autori che hanno contribuito al nostro "Digital Italy Report" abbiano citato il posizionamento dell'Italia nell'Indice Desi, ovvero l'indice con cui dal 2014, annualmente, la Commissione Europea misura i progressi delle nazioni Ue sul percorso della digitalizzazione. In un solo anno l'Italia ha migliorato la posizione in classifica: sul totale dei 27 Paesi Ue, era al ventesimo posto nel 2021 ed è salita al diciottesimo posto nell'indice Desi 2022. Il progresso è in parte dovuto alla realizzazione di nuove infrastrutture di rete a banda larga, così come all'allargamento dei servizi di Pubblica Amministrazione digitale. E oggi, forse anche grazie allo shock della pandemia e alla conseguente adozione del cloud computing, il 60% delle piccole e medie imprese italiane ha raggiunto almeno un livello base di intensità digitale. Inoltre abbiamo un po' ridotto il ritardo sulle competenze digitali di base, ma ancora nel 2022 oltre la metà dei cittadini italiani ancora non le possiede. Nel complesso l'Italia, la terza economia Ue per dimensioni, può e deve fare meglio.

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.

Fintech e ESG: una strada ancora in salita?

Ezio Viola, Co-Fondatore
The Innovation Group

Recentemente si è tenuta l'edizione 2022 del "Milan Fintech Summit" come testimonianza di come Milano possa diventare un polo di attrazione e di crescita di tutto l'ecosistema fintech non solo italiano. Quando nacque il primo Fintech District a Milano, lo si vedeva come il futuro. Oggi, è una realtà che cresce con più di 300 startup e con investimenti di circa 1.7 Mld di euro. Le fintech sono una presenza che sta diventando un fattore di innovazione di tutta l'industria dei servizi finanziari. Chi investe in Fintech, infatti, non sono solo i VC ma anche il Corporate VC di grandi istituti bancari con circa 500 Mil Euro. Ciò significa che l'ecosistema fintech sta realizzando tecnologie e servizi innovativi fondamentali per accelerare il processo di trasformazione digitale del sistema bancario.

Pietro Sella, CEO del Gruppo Sella, ha affermato che: "siamo di fronte al dischiudersi di una fase due dell'ecosistema fintech che dovrà sempre di più orientarsi ad essere un abilitatore di innovazione in partnership con banche, aziende e regolatori per gestire i nuovi rischi derivante dalle crisi in corso: geopolitico, climatico ed energetico ed avere un impatto sull'intera società".

Il valore economico deriverà sempre di più dall'impatto sui valori della società nei prossimi cinque anni. Le nuove tendenze riguarderanno ancor di più la creazione di un ecosistema di ESG FINTECH per costruire soluzioni e piattaforme per gestire l'impatto delle strategie ESG delle banche e i servizi ESG per le istituzioni finanziarie e per le aziende clienti dei diversi settori di mercato.

Questo ecosistema si appoggerà su una serie di enablers orizzontali riguardanti almeno tre elementi:

- la definzione di tassonomie per creare un linguaggio comune su che cosa significhi green e sostenibile o la transizione verso un modello sostenibile
- La disclosure che significa come capire le entità che impattano i fattori ESG e come rischi e opportunità impattano le entità costituenti i fattori ESG
- Dati e Metriche attraverso l'utilizzo di tecnologie avanzate di analisi dei dati e di AI e M/L

Il settore finanziario è impattato dai fattori ESG su diversi fronti:

- Mobilitazione dei capitali: come incorporare nelle decisioni di investimento e di credito/ finanziamento i fattori ESG misurandone l'impatto e con dei KPI
- Monitorare il commitment verso gli obiettivi ESG: strutturare il reporting sia volontario sia dettato dalle normative regolamentari e trovare le modalità di riallineare progressivamente i portafogli in base ai risultati raggiunti
- Misurare l'impatto e i rischi

Credit: milanfintechsummit.com

quantificando e qualificando l'impatto dei finanziamenti sostenibili e valutare l'impatto dei rischi climatici, ambientali e di transizione sui portafogli e sull'organizzazione nel suo complesso.

Se questa sono le sfide ma anche le opportunità che l'ecosistema fintech può cogliere per sé e per l'intero settore dei servizi finanziari, desta qualche perplessità se, guardando al settore delle startup fintech italiane, appare che la strada del Finetch verso i criteri Esg è lastricata di ottime intenzioni, ma resta irrimediabilmente in salita. Infatti da una recente ricerca realizzata da Excellence Consulting in collaborazione con il programma dell'acceleratore fintech Fin+Tech su un campione di 40 fintech nazionali, emerge che il 62% delle società riconosce l'importanza strategica dei fattori ambientali, sociali e di governance, e il 46% li considera un vantaggio competitivo 'essenziale' sia per raccogliere fondi/capitali che per vendere prodotti o stringere accordi commerciali, ma solo il 46% e il 31% realizzano rispettivamente politiche ambientali sostenibili/energetiche e di governance.

Più che al fattore della sostenibilità la ricerca evidenzia una maggiore attenzione rivolta al 'tradizionale' fattore social (85%) mentre solo il 46% già attua o ha programmato di investire nei prossimi anni in politiche ambientali e il 54% in governance. Sono ancora importanti, i ritardi nella comunicazione dei risultati agli stakeholders dove solo il 23% lo fa per quanto riguarda la sostenibilità aziendale e il 46% per il social.

Questa situazione fa emergere alcune criticità potenziali. C'è la necessità di allargare lo spettro dell'innovazione che il Fintech può portare alle tematiche ESG per sé e per l'intero settore finanziario e per essere credibile deve partire da sé stesso. Inoltre, rischia di rappresentare un limite anche per far crescere la collaborazione delle banche tradizionali con le fintech, poiché i temi ESG sono o possono diventare un punto di incontro e un fattore discriminante della scelta delle banche. È importante anche migliorare la capacità di comunicare di tali argomenti agli stakeholders che può essere non solo un freno alla capacità di raccogliere fondi ed emergere sul mercato, ma rischia di lasciare campo aperto a iniziative di green washing da parte di operatori spregiudicati. Diventa quindi fondamentale che l'ecosistema Fintech italiano sia capace di associare alla consapevolezza dell'importanza dei fattori ESG anche l'azione nell'essere oltre che innovativi, sempre più sostenibili.

Consumatori, investitori, dipendenti e gli altri stakeholder si aspettano che le fintech assumano un ruolo di guida nelle questioni ambientali e sociali, dal cambiamento climatico alla diversità, all'equità e all'inclusione. Per tenere il passo con le loro attese, una strategia ESG non strutturatanon è sufficiente e occorre formalizzarla e dimostrare concretamente l'impegno della fintech in ambito ESG.

Google Analytics e il problema del trasferimento dati extra UE, cosa significa per imprese e PA

Valentina Frediani, General Manager

Colin & Partners

Risale allo scorso 23 giugno il Provvedimento del Garante che ha, di fatto, reso illecito l'utilizzo di Google Analytics. La decisione, che segue l'ammonimento (pur senza una sanzione) della società Caffeina Media, ha ovviamente dato una notevole scossa ai rapporti tra il provider globale e la miriade di siti web che utilizzano i suoi strumenti (non solo Analytics).

Il nodo critico è rappresentato dalla questione del trasferimento dei dati all'estero. In assenza di una direzione normativa precisa, tale dibattito si fonda sull'analisi delle singole soluzioni al fine di verificarne le garanzie rispetto ai dettami del GDPR, almeno fino a quando non verrà stipulato e condiviso un nuovo accordo transatlantico.

Quali dati Analytics fa transitare in territori extra UE?

In primis l'indirizzo IP che, come noto, è a tutti gli effetti un dato personale in quanto permette di identificare l'utente e quindi l'interessato e soprattutto consente di ottenere ulteriori informazioni come il browser utilizzato oppure data e ora di navigazione.

Anche scegliendo di troncare le ultime cifre del codice IP, non si mette in atto una reale anonimizzazione ma solo una pseudonimizzazione. Anche se non visibili nei report del sito utente, Google resta in grado di risalire, tramite indirizzo IP completo in suo possesso, all'interessato. Questo significa violare il principio di accountability nell'utilizzo del servizio.

Ricordiamo che il GDPR chiede espressamente che il Titolare adotti misure tecniche ed organizzative adeguate, necessarie a garantire un idoneo livello di protezione dei dati personali dell'utente. In caso di trasferimenti extra UE l'onere in questione assume carattere maggiormente rilevante. Sta quindi ai singoli Titolari essere certi di rivolgersi, anche per questo tipologie di servizi, a fornitori in grado di dimostrare la loro affidabilità rispetto alle regole europee in tema di tutela dei dati personali.

Questo solleva, senza dubbio, una certa difficoltà da parte dei gestori dei siti nel far valere il proprio potere contrattuale rispetto a un big player come Google. L'asimmetria è evidente ed il Garante stesso ne ha tenuto conto nel suo Provvedimento (concedendo 90 giorni di tempo alla società per rimediare alla situazione), pur ordinando la sospensione dei flussi verso Google LLC con sede negli Stati Uniti.

Quali saranno quindi le possibilità per PA ed imprese?

Il primo passo per tutelare il proprio operato è quello di fare una analisi degli strumenti in uso. Analytics non è certamente l'unica possibile criticità sul fronte privacy e trasferimento dati extra UE. Una corretta mappatura della

Non basta la sola analisi preliminare a mettere al riparo le organizzazioni da interventi sanzionatori. Occorre mantenere una vigilanza attiva sui propri strumenti, sui fornitori e – in sintesi – su tutti i soggetti (responsabili e sub responsabili esterni) che risultino coinvolti in modo più o meno diretto, nel trattamento di dati personali.

compliance dell'intera filiera dei fornitori, che comprenda una verifica della conformità delle soluzioni in uso in ottica privacy by design,è il più importante strumento per la riduzione del rischio. Gli strumenti adottati devono rispettare quanto previsto dal GDPR per l'intero ciclo del dato. Qualora non sia possibile agire settandoli nel rispetto della logica dell'accountability e operando eventuali aggiustamenti anche a livello contrattuale, sarà necessario scegliere altre soluzioni.

Di certo questo tipo di interventi che si moltiplicano tra le Autorità garanti europee, saranno anche di stimolo per il mercato. Il meccanismo domanda – offerta potrebbe esserne positivamente ispirato.

L'importante, una volta individuate nuove opportunità conformi, è non abbassare mai eccessivamente la soglia di attenzione. Non basta la sola analisi preliminare a mettere al riparo le organizzazioni da interventi sanzionatori. Occorre mantenere una vigilanza attiva sui propri strumenti, sui fornitori e – in sintesi – su tutti i soggetti (responsabili e sub responsabili esterni) che risultino coinvolti in modo più o meno diretto, nel trattamento di dati personali.

Le caratteristiche della cyber war emerse durante il conflitto in Ucraina

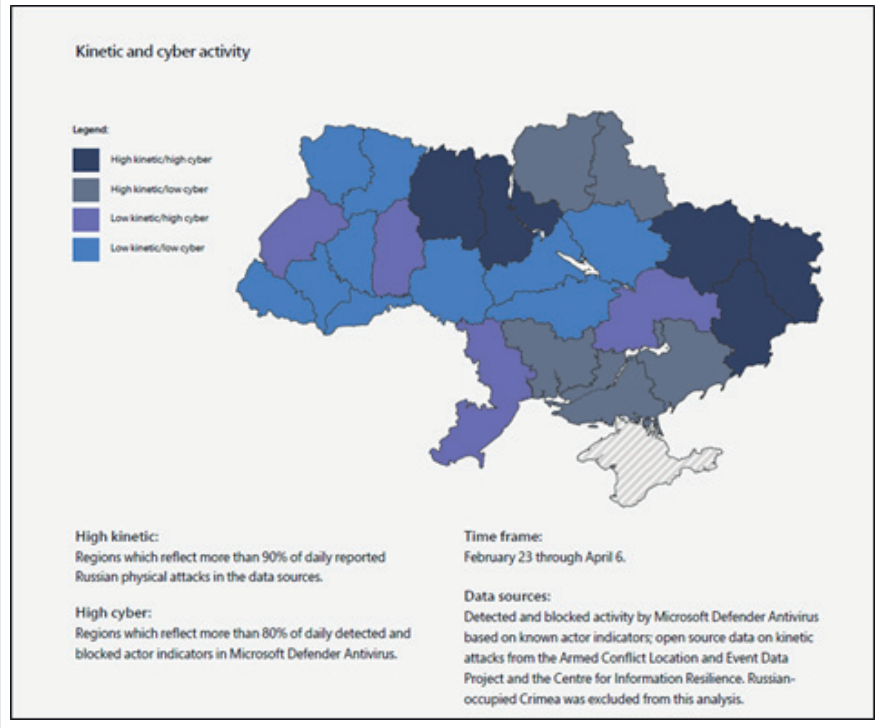
Elena Vaciago, Associate Research Manager

The Innovation Group

Secondo un rapporto specifico[1] della Digital Security Unit di Microsoft, ci sarebbero state, nelle prime sei settimane della guerra in Ucraina, almeno 237 azioni collegate ad attacchi cyber (contando solo quelli noti), condotte da 6 diversi gruppi di hacker legati al governo russo. Sarebbero state svolte operazioni distruttive (37 in tutto, di cui la maggior parte nella prima settimana della guerra) e di spionaggio cibernetico, a supporto delle azioni delle forze militari russe via terra, mare e aria.

Obiettivo dei russi era quello di mettere fuori servizio servizi pubblici e privati, installare malware distruttivo nelle reti ucraine. Il rapporto Microsoft ha identificato almeno 7 diverse famiglie di wiper (malware che distrugge i dati, rendendo inutilizzabili i sistemi) utilizzate in questi attacchi. I target principali sono stati da subito i siti governativi, i fornitori di energia e telecomunicazioni, gli istituti finanziari e gli operatori media. La maggior parte degli attacchi sono stati attribuiti, dall'Ucraina e da fonti dei Paesi occidentali, a entità governative russe, in particolare al servizio di intelligence russa GRU, che ha un ampio track report di azioni di questo tipo. In alcuni casi, sono stati anche sospettati gruppi di hacker considerati vicini al governo russo (come il gruppo di ransomware Conti, una delle organizzazioni di hacker più efficaci e strutturate).

Al momento non è accertato che gli obiettivi degli attacchi cyber fossero concordati preventivamente con le forze militari, ma è evidente che le azioni degli hacker hanno avuto lo scopo di fornire supporto alle azioni dell'esercito, o comunque di danneggiare reputazione e funzionalità dell'apparato governativo ucraino. La figura successiva mette in evidenza dove si sono concentrati gli attacchi cinetici e quelli informatici, mostrando che in molti casi ci sono stati obiettivi concordati tra gli hacker e l'esercito del Cremlino.



Dall'analisi delle cyber operation che hanno accompagnato l'intera operazione militare in Ucraina, emergono caratteristiche proprie della cyber war che la contraddistinguono fortemente da qualsiasi operazioni militare si svolga nel mondo fisico.

Innanzi tutto, va osservato che le nuove cyber armi hanno alcuni punti a loro vantaggio rispetto alla guerra tradizionale, che fanno sì che siano sempre più spesso utilizzate nei conflitti in tutto il mondo. Sono efficaci, non costano quanto un esercito, possono essere impiegate da remoto da qualsiasi posto e in qualsiasi momento. Non comportano la perdita di vite umane tra chi realizza l'attacco, mentre potrebbero farlo per chi è preso di mira (anche se ad oggi gli incidenti informatici procurati da attacchi che hanno causato vittime sono stati pochissimi). Infine, gli attacchi cyber sono difficilmente attribuibili a un singolo "esercito di hacker", e di conseguenza, si può sempre negare di avere sferrato un'azione di questo tipo.

Un attacco cyber, inoltre, non si svolge come un'operazione di guerra (che ha la sua data di inizio e, si spera, di fine), perché richiede in realtà una preparazione molto lunga e non è detto che abbia un termine. Nel caso delle cyber operation a cui stiamo assistendo in Ucraina, quelle svolte in questi mesi sono il proseguimento di un'attività iniziata almeno nel 2014 e continuata in questi ultimi 8 anni. La continua analisi di sistemi e reti in genere serve a conoscere bene le vittime (a volte, meglio di quanto esse non conoscano sé stesse), a identificarne vulnerabilità, quindi a predisporre gli strumenti più opportuni (spesso sviluppati ad hoc) da utilizzare successivamente, per sabotare dall'interno le reti rimanendo inosservati il più a lungo possibile.

Le 237 azioni individuate nel report Microsoft citato in precedenza sono state infatti classificate in:

- Azioni preparatorie o per predisporre gli strumenti,
- Azioni sulle reti,
- Azioni sui bersagli.

Si tratta nel complesso di molteplici e diverse attività che fanno parte di ampie catene di attacco, ossia, di sequenze di azioni che si completano su un numero inferiore di bersagli finali.

Le attività osservate durante il conflitto nel complesso hanno dimostrato che l'efficacia di un attacco digitale risiede molto di più in operazioni di spionaggio e furto di informazioni critiche per acquisire vantaggi strategici o condurre campagne di disinformazione, creare confusione nella popolazione e distrarre le difese da altri attacchi, che non nella capacità distruttiva come può essere quella di un missile. Se l'efficacia va misurata in base al risultato, il successo delle cyber operation durante il conflitto è stata modesta.

Un altro aspetto che caratterizza la cyber war è il fatto che lo sfruttamento di una particolare "cyber arma" è possibile solo poche volte: come minimo, chi avrà subito una determinata azione, avrà appreso come difendersi (o come sfruttarla – potenzialmente – a sua volta, in un contesto diverso). Ogni volta un gruppo hacker decide di realizzare un attacco, se questo andrà a buon fine, la vittima si renderà conto di essere esposta e di avere dei problemi da correggere: l'hacking etico è sempre servito a questo, a indentificare vulnerabilità che richiedevano immediata risoluzione. In seguito, chi ha subito l'attacco eleva le sue difese e lo stesso metodo non funziona più.

Un altro rischio da considerare (perché specifico della cyber war) è quello dello "Spillover". Poiché il cyber spazio non ha confini, è molto difficile limitare il campo degli effetti di un attacco. L'utilizzo di una certa tecnica di attacco non sarà limitato, potrà avrà conseguenze altrove. NotPetya è stato un grave attacco ransomware, avvenuto nel 2017, che aveva inizialmente come target aziende ucraine (banche, utilities, l'aeroporto di Kiev), ma si è poi diffuso in modo pandemico in tutto il mondo. Passando da una rete all'altra, ha procurato danni notevoli alla danese Maersk (trasporti), alla francese Saint-Gobain (materiali da costruzione), all'azienda farmaceutica irlandese MSD e al gigante spagnolo del cibo Mondelez.

Un malware può quindi dare origine a un'epidemia cibernetica globale: in un mondo interconnesso come l'attuale, le probabilità che un attacco cyber rivolto a un singolo Paese possano avere ripercussioni informatiche in altre parti del globo sono elevate. Tutti i Paesi hanno infrastrutture critiche a rischio: anche in Italia, nonostante i passi in avanti degli ultimi anni e l'arrivo di norme sempre più stringenti (dalla Direttiva NIS per le infrastrutture critiche, al Perimetro di Sicurezza Nazionale, alla costituzione dell'Agenzia Nazionale di Cybersicurezza, ACN), tuttora abbiamo lacune e manchiamo, a livello europeo, della capacità di orchestrare una difesa comune per sistemi e reti ICT.

Mancanza di unitarietà e investimenti limitati hanno frenato i passi in avanti. In Italia, dove ora 623 milioni di euro del PNRR sono allocati alla cybersecurity nel settore pubblico, il rischio è che potrebbero rimanere indietro le imprese più piccole e con meno fondi a disposizione. Aziende che facendo parte di filiere produttive sempre più ampie e diversificate, possono diventare esse stesse veicolo di diffusione di malware. Il sostegno anche tecnologico che è stato dato dal mondo occidentale all'Ucraina ha come risvolto positivo l'avvio di forma di "solidarietà digitale" che torna utile a tutti, perché permette di condividere informazioni critiche sulle tecniche utilizzate dagli attaccanti. Un'esperienza positiva da tener presente per il futuro.

La guerra di Putin e la nascita della Solidarietà digitale

Quella in Ucraina non è la prima cyber war degli ultimi anni. Come abbiamo descritto nell'articolo, non si è dimostrata finora molto efficace, sicuramente non ha contribuito alla resa dell'Ucraina o alla sostituzione del suo Governo, come era invece nelle intenzioni iniziali del Cremlino. Quello che ha dimostrato è stata da un lato la capacità degli ucraini e dei loro partner di allestire velocemente una reazione efficace nella difesa, mitigazione e contrasto delle minacce cyber. Dall'altro lato, sono emerse alcune debolezze nel coordinamento tra attacchi convenzionali e cyber delle forze russe, e l'impressione che le cyber armi russe non fossero poi così avanzate come si temeva. Un controllo più avanzato sulle tecnologie utilizzate nei terreni del conflitto avrebbe in effetti potuto creare maggiori danni.

L'aspetto forse più nuovo emerso durante il conflitto è stata la chiamata alle armi di eserciti di hacker volontari (Hacktivist, termine che nasce dalla fusione di Hacker e Activist). Negli anni precedenti, è probabile che molti degli stessi siano stati arruolati in operazioni di cyber war state-sponsored contro Paesi esteri, nella forma però di forze mercenarie (a fronte di guadagni economici). Il conflitto in Ucraina ha riportato invece in auge hacker che intervengono su base volontaria, per un proprio credo politico e in favore di una causa che li fa propendere in favore di un Paese o

del suo oppositore. Questa tendenza sta creando divisioni nei gruppi di hacker che non si erano mai osservate in precedenza: l'arruolamento finora era infatti motivato quasi esclusivamente da fattori economici. Si stima che l'IT Army che si è formata per l'Ucraina sia composta da almeno 300mila volontari che partecipano da ogni parte del mondo. Tra l'altro, senza un coordinamento centrale, con la possibilità quindi che gli effetti di queste azioni diventino da un momento all'altro imprevedibili.

L'altro tema importante è quello della "difesa coordinata", che sarà sempre più adottata per quanto riguarda il mondo digitale. I Paesi NATO si sono mossi rapidamente in questo senso: ad esempio, lo scorso 14 giugno, hanno fatto rientrare nel concetto di "attacco armato" (previsto dall'art. 5 del Trattato, che attiva la mutua difesa collettiva) anche gli attacchi cibernetici. L'alleanza atlantica continua a estendersi nel versante cyber, e sta abbracciando Paesi di tutto il mondo, come testimonia il recente ingresso della Corea del Sud nel Centro di cooperazione per la sicurezza informatica (NATO Cooperative Cyber Defence Centre of Excellence, CCDCOE); i colloqui tra Giappone e NATO per estendere la collaborazione in ambito cybersecurity e sicurezza marittima[2]; l'esercitazione cyber di aprile "Locked Shields 2022" a Tallin, in Estonia (a cui hanno partecipato anche Svezia e Finlandia[3]); la partecipazione ora anche dell'Ucraina al CCDCOE come "Contributing Partner" (e questo significherà che sarà condivisa tra tutti i Paesi partecipanti al centro NATO una conoscenza di prima mano sulle tecniche utilizzate dagli hacker russi negli ultimi mesi[4]).

In un mondo, quello digitale, in cui: le minacce evolvono rapidamente; le risorse per la difesa sono spesso inadeguate e insufficienti; gli attaccanti tendono a investire e a individuare tecniche sempre nuove e ad agire indisturbati; stiamo oggi assistendo a una risposta coordinata dei Paesi NATO che – anche in risposta al conflitto – coglie l'occasione per allargarsi e raggiungere portata globale. Nel recente Summit di giugno a Madrid sono stati presentati i piani della NATO per i prossimi anni ("Strategic Concept")[5]. Con riferimento alla difesa cyber si delineano:

- Nuove modalità di coinvolgimento diretto del settore privato della cybersecurity nella risposta agli attacchi dei gruppi di hacker russi. In particolare, sarà allestita una piattaforma per condividere informazioni e intelligence sugli attacchi;
- Investimenti per un miliardo di dollari in tecnologie emergenti per la difesa cyber (quantum computing, intelligenza artificiale, tecnologia spaziale), per il rafforzamento del DIANA (Defense Innovation Accelerator for the North Atlantic), per startup e tecnologie innovative per la difesa;
- Avvio di "virtual joint cybersecurity teams", gruppi volontari da avviare rapidamente e mettere in condizione di operare in simultanea per proteggere le reti e i sistemi dei Paesi membri dell'alleanza[6].

L'Unione Europea invece, afferma di puntare alla costruzione di una politica di sicurezza e difesa comune europea (basti vedere gli obiettivi della "Bussola strategica" resi pubblici a marzo di quest'anno[7]), ma sta dimostrando tempi di reazione e di allestimento delle opportune misure, oltre che di coordinamento tra le diverse parti, decisamente lunghi: la strategia punta a realizzare le azioni entro il 2030, quando invece l'emergenza è oggi.

(Articolo tratto dal Rapporto DIGITAL ITALY 2022 – IL VERDE, IL BLU E IL PNRR, presentato lo scorso 17 ottobre in occasione del Digital Italy Summit 2022).

[1] The hybrid war in Ukraine, Apr 27, 2022 | Tom Burt – Corporate Vice President, Customer Security & Trust, https://blogs.microsoft.com/on-the-issues/2022/04/27/hybrid-war-ukraine-russia-cyberattacks/

[2] Japan's Prime Minister to confirm revision of cooperation document with NATO, June 29 2022, https://www3.nhk.or.jp/nhkworld/en/news/20220629_28/

[3] Svezia e Finlandia sono già nella Nato (cyber), Formiche.net, Gaia Ravazzolo, 19/04/2022

https://formiche.net/2022/04/svezia-finlandia-nato-cyber/

[4] Ukraine to be accepted as a Contributing Participant to NATO CCDCOE https://ccdcoe.org/news/2022/ukraine-to-be-accepted-as-a-contributing-participant-to-nato-ccdcoe/

[5] NATO aims to take on Russia with its own cyber military-industrial complex, Politico, by Antoaneta Roussi and Laurens Cerulus, June 29, 2022 https://www.politico.eu/article/nato-plans-to-build-a-cyber-military-industrial-complex-russia-china-hacking/

[6] NATO Announces Virtual Rapid Response Cybersecurity Capability, Security Bloulevard, Teri Robinson on July 14, 2022

https://securityboulevard.com/2022/07/nato-announces-virtual-rapid-response-cybersecurity-capability/

[7] Una bussola strategica per rafforzare la sicurezza e la difesa dell'UE nel prossimo decennio, 21 marzo 2022 https://www.consilium.europa.eu/it/press/press-releases/2022/03/21/a-strategic-compass-for-a-stronger-eu-security-and-defence-in-the-next-decade/

Diventare più sostenibili anche con la tecnologia

Valentina Bernocco, Web and Content Editor
The Innovation Group

Gioco di squadra tra fornitori di digital tech, criteri Esg e una nuova cultura che avanza in azienda. La visione di Mugo, una startup che pensa in grande.

Agire secondo principi di sostenibilità comporta impegni su diversi fronti, dalla riduzione dell'impatto ambientale delle attività aziendali alla scelta di fornitori allineati agli stessi valori. La misurazione del carbon footprint e l'acquisto di crediti di carbonio certificati sono possibili ingredienti di una strategia aziendale orientata verso i criteri Esg. In quest'ambito opera Mugo, startup e società benefit italiana di climate tech nata nel 2020, che propone soluzioni per la misurazione e la compensazione dell'impatto ambientale, integrabili con gli esistenti software aziendali. Il nome allude al pino mugo, un sempreverde che punteggia le Alpi Orientali: un arbusto che ha grandi capacità di assorbire l'anidride carbonica, a dispetto delle sue piccole dimensioni. La convinzione di Benedetto Ruggeri, giovane imprenditore e fondatore di Mugo, è che ogni piccolo gesto possa fare la differenza.

Quanto le aziende italiane considerano i fattori Esg nelle proprie strategie?

Anche in Italia, dopo anni di proclami e spot, finalmente un numero sempre maggiore di aziende è interessato a integrare criteri Esg e di sostenibilità al proprio interno. Ad oggi, secondo una ricerca di PwC, un Ceo su tre ha iniziato un percorso di decarbonizzazione in azienda. Le società quotate sono senza dubbio quelle più attente e consapevoli delle performance Esg, soprattutto per incrementare le opportunità di investimento sul mercato. In generale le grandi aziende investono di più in sostenibilità rispetto alle Pmi. La reportistica, l'individuazione di obiettivi e la misurazione degli impatti sempre più stanno diventando parte di processi ordinari in azienda. Nel tessuto

imprenditoriale italiano però, nonostante piccole realtà che rappresentano casi di eccellenza in sostenibilità (molte BCorp e società benefit), esiste ancora un gap in termini di comprensione del tema e, di conseguenza, di opportunità che ne derivano. Il trend attuale spingerà nei prossimi anni sempre più Pmi (in particolare operanti nel settore consumer o all'interno di filiere sempre più controllate, quali moda e agroalimentare) verso l'adeguamento a questi nuovi standard come condizione necessaria per poter rimanere sul mercato.

L'attuale scenario di crisi energetica potrebbe accelerare o decelerare questo percorso?

Le aziende che fanno la differenza non possono che essere quelle che guardano nella stessa direzione dei propri consumatori. Infatti, è solo grazie alla consapevolezza dei consumatori che le aziende si impegnano per rispondere concretamente alla crisi climatica. Nel settembre 2019 più di sei milioni di persone sono scese in piazza per il clima e le aziende non hanno fatto altro che rispondere a questo trend, diventando in alcuni casi influencer di sostenibilità per il proprio mercato di riferimento. La crisi energetica in atto sta polarizzando il dibattito su posizioni rigide e difficilmente conciliabili. Situazioni estreme come quella che stiamo vivendo, però, richiedono soluzioni radicali e coraggiose di lungo periodo da parte di aziende e di governi. Non possiamo permetterci di rimettere in discussione la direzione intrapresa.

Quanto è complesso per un'azienda adottare tecnologie per la misurazione dell'impatto carbonico?

Le cosiddette attività di carbon accounting, intraprese per stimare l'impatto climatico di un'azienda, stanno diventando sempre più diffuse, a partire dalle categorizzazioni standard (come quella del GHG Protocol) per analizzare le emissioni dirette (Scope 1), quelle indirette ma sotto il controllo dell'azienda (Scope 2) e le altre emissioni indirette (Scope 3). Lo stesso si può dire per le attività legate alle emissioni di prodotti e servizi che vengono regolate da standard riconosciuti a livello internazionale.

Ma tale stima deve rappresentare una base di partenza. Che cosa fare con quel dato? Come interpretarlo? Sono queste le vere domande a cui ogni azienda è chiamata a rispondere per dare un vero valore alle informazioni raccolte ed è qui che tecnologia e innovazione possono aiutare a orientarsi. Nel nostro caso, utilizziamo la tecnologia per creare nuove esperienze per i consumatori dei nostri clienti, rendendo disponibili informazioni sull'impatto climatico di prodotti e servizi aggregando, categorizzando e confrontando migliaia di dati in tempo reale attraverso i nostri algoritmi.

Per una startup che si lancia su questo mercato quanto è difficile farsi largo tra i competitor?

Il mercato è in evoluzione e come tale anche i player che lo compongono. Per questo motivo, è fondamentale da un lato rendere il proprio business sempre più scalabile, dall'altro avere ben chiaro il posizionamento e i fattori chiave che rendono sempre unica la value proposition della startup. La presenza di grandi player in questo settore è una semplice attestazione della bontà di quanto stiamo facendo e delle potenzialità del mercato. Stiamo tutti lavorando per risolvere la crisi climatica attuale: andiamo quindi nella stessa direzione, come compagni di viaggio.

Cloud e Sicurezza: l'integrazione intelligente di due mondi sempre più complessi

Loris Frezzato, Channel Area Manager
The Innovation Group

La propensione a spostare infrastrutture, accesso alle applicazioni e l'attivazione del lavoro remoto è in evoluzione sul mercato per quantità e qualità.

La pandemia, ricordiamolo, ha fornito una giustificazione più che valida per questo passaggio epocale, che ha in qualche modo ridefinito le regole del lavoro, svincolandolo dal luogo fisico ma ha anche rivisto ruoli e funzionalità di molte tecnologie, sia già esistenti ma poco sfruttate fino ad allora, sia stimolando sviluppo o declinazioni di nuove tecnologie

L'ibrido è ormai quanto maggiormente viene desiderato e sponsorizzato sul mercato. La strategia di mantenere tutto il data center e le relative applicazioni on premise ha evidenziato le proprie debolezze proprio nel momento in cui "in house" proprio non si poteva andare per motivi di natura sanitaria.

Lo stesso chi gestiva il tutto con un proprio cloud privato, ha iniziato a considerare anche l'opzione di alleggerire il proprio data center spostando qualcosa su infrastrutture public.

Il public cloud è quindi salito rapidamente sul podio delle infrastrutture, facendo in un attimo svanire i dubbi sul trasferire asset anche fondamentali al di fuori delle mura infrastrutturali dell'azienda.

Chi timidamente spostando alcune funzionalità aziendali in una forma di hybrid cloud, chi coraggiosamente destinando al cloud pubblico gran parte degli accessi alle applicazioni per una completa gestione da remoto del lavoro, chi, ancora, sfruttando più di un cloud pubblico, in modo da distribuire su più provider in modalità multicloud o, addirittura, di edge cloud di prossimità.

I motivi? I costi, certamente, ancor più incisivi in un momento storico in cui conviene fare pagare la bolletta elettrica al proprio fornitore di infrastrutture piuttosto che accollarla sui bilanci aziendali

La flessibilità. La velocità e il time to market. E la volontà di svincolarsi da lock-in monovendor o monoprovider nel caso delle forme miste.

L'infrastruttura non è più lineare, non è più assimilabile al perimetro delle aziende ed è maggiormente vulnerabile.

Il cloud ne sfuma i confini, aprendo infinite porte d'accesso a chi vuole entrarci in maniera fraudolenta e non autorizzata.

Le forme ibride ne aumentano la complessità, rendendo difficile il controllo di eventuali punti deboli. E le soluzioni di sicurezza di un tempo non bastano più.

Più ibrida e complessa è l'infrastruttura e più ibrida e complessa è la strategia di protezione della stessa. Una sicurezza che si compone ormai di tanti tasselli a copertura dei tanti, infiniti, metodi di attacco che in continuazione scaturiscono dai sempre più sofisticati laboratori di ricerca e sviluppo del cybercrime.

Integrazione è la parola d'ordine, e anche qui si ragiona in termini di ecosistema

Si è arrivati a una complessità tale da rendere necessario un cambio di passo da parte dei fornitori di tecnologie.

Non più, appunto, fornitori, venditori, ma consulenti. Consulenti con elevate e specifiche competenze, in grado di capire quali ingredienti sono indispensabili per ogni singolo cliente, visto che una soluzione o un progetto composito di sicurezza, o anche di infrastruttura, non può andare bene per tutti.

The Innovation Group ha attivato un confronto su questi temi nell'ambito del proprio programma Ecosystem, all'interno di una Web Conference che ha raccolto esperienze e consigli da chi ha dovuto affrontare e risolvere queste problematiche.

"Cloud e Sicurezza: nome e cognome delle infrastrutture di oggi che guardano al domani" è il titolo dell'evento firmato TIG al quale, dopo un'overview e collocamento degli investimenti in cloud e sicurezza delle aziende italiane, ha partecipato Valentina Frediani, founder e CEO di Colin & Partners che ha affrontato il tema della responsabilità nella gestione dei dati anche legata alla territorialità, di unione europea o al di fuori di essa, temi che la situazione geopolitica ha sollevato e che apre interrogativi su dove è il caso di avere i propri dati e a chi darli in gestione, facendo diventare l'analisi preventiva e attenta di quanto deve essere indispensabilmente protetto: "Ci sono aspetti sostanziali di tutela del dato che devono essere valutati in una fase di preselezione, soprattutto in un momento in cui bisogna avere una visione generale di tutela della propria azienda", visto che il cloud pur non essendo una scatola chiusa, rischia di diventare inaccessibile in determinate condizioni.

Poi, ovviamente, i vantaggi del cloud sono tali da essere concretamente sfruttati per ottenere e fornire servizi da parte delle aziende e, da queste, verso i propri clienti consumer. Lo sa Haier, produttore di elettrodomestici, che proprio sulla connettività ha ridisegnato la manifattura dei propri prodotti, facendo intervenire anche l'AI nella

> **I vantaggi del cloud sono tali da essere concretamente sfruttati per ottenere e fornire servizi da parte delle aziende e, da queste, verso i propri clienti consumer**

loro fase di analisi. “Il tema del cloud per Haier è trasversale e tocca sia la vendita dei prodotti nel B2C, sia la produzione stessa dei prodotti e per la connessione del parco macchine alle app per una loro gestione intelligente, anche dal punto di vista della segnalazione dei dati per la manutenzione” è quanto ha commentato Simone Pezzoli, Group Chief Technology officer di Haier Europe.

Cloud la cui importanza sta diventando sempre più strategica anche per una azienda di distribuzione di energia quale è Engie, a quanto dichiara Angelo Cofone, Responsabile dell’area IT Governance di Engie Italia: “Abbiamo approcciato la cloud transformation sia per un rinnovo e trasformazione tecnologica dell’azienda ma soprattutto per abilitare l’innovazione nell’approccio strategico nella gestione nostra e del mercato.
Time to market, controllo costi e predisposizione all’integrazione per la costruzione di sistemi flessibili sono ormai i reali motivi e vantaggi che portano verso una strategia basata sul cloud. Siamo partiti lo scorso anno, ma contiamo di portare il 95% dei nostri sistemi in cloud nel giro di 3 anni”.

Marcello Fausti, CISO Italiaonline, ha invece affrontato il tema della sicurezza quando si parla di infrastrutture flessibili e in cloud, quali quelle utilizzate in un mercato regolato dallo smart working.

“Le motivazioni della migrazione al cloud sono diverse che in passato – ha dichiarato -. Prima la scelta era prevalentemente basata sul TCO, ora invece l’elemento determinante è la velocità nella realizzazione di progetti, possibile solamente grazie al cloud. Stiamo migrando nella cloud economy e il problema dei CISO, oggi, è di stare al passo, dal punto di vista della sicurezza, con l’innovazione e la trasformazione digitale, le quali stanno aprendo nuovi fronti e problemi dal punto di vista della protezione. Bisogna infatti attivare controlli tecnici anche sulla supply chain, proprio perché le aziende presto saranno meno “infrastrutturate” e più flessibili. Imponendo un cambio nei ruoli del SOC”.

La complessità, o meglio la sua gestione, sembra essere il pane quotidiano di Elmec, system integrator che ha impostato la propria proposizione cloud puntando a dare ai propri clienti il massimo dei benefici che questi dal cloud possono ottenere.

“Pur avendo un proprio data base, la logica di Elmec è quella di proporsi come advisor nei confronti del cliente, lasciando il massimo della libertà di scelta su quanto e cosa trasferire in cloud. O consigliando anche cosa non mettere in cloud” ha dichiarato Mirko Solimena, Presales Director, Elmec Informatica Spa, evidenziando il proprio “cloud best” nella proposizione ai clienti, che si basa sulla libertà di ottimizzare ogni tipo di applicazione o workload sia nel public, sia nel private cloud. Ossia dove i clienti preferiscono, senza imposizioni.

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