PA DIGITALE

A CHE PUNTO SIAMO

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Luigi Iaccarino
Vodafone

VOCI DAL MERCATO

Cyber Resilienza: strategie di risposta alle minacce cyber

TRASFORMAZIONE DIGITALE

L'AI generativa ci obbliga a riflettere su noi stessi

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

SOMMARIO

PA Digitale: a che punto siamo

Elena Vaciago, Research Manager
The Innovation Group

Il digitale per anni è stato considerato un'opportunità dalle amministrazioni pubbliche: per essere trasparenti, per semplificare le procedure, per modernizzarsi e diventare virtuose. Oggi lo scenario è diverso: il digitale è necessario e indispensabile in molteplici ambiti, farne a meno non è più possibile. La buona notizia, per quanto riguarda la PA italiana, è che questo processo è iniziato da molto tempo, negli anni la modernità digitale è progredita e ha visto protagoniste tutte le amministrazioni, centrali o locali.

Dal punto di vista soprattutto delle PA locali, in particolare i 7.900 comuni piccoli o grandi distribuiti su tutto il territorio nazionale, questo ha permesso di migliorare i servizi, ridurre i costi risparmiando su molte risorse, e soprattutto, avvicinarsi ai cittadini con uno scambio costante di informazioni di valore, incontrandone i bisogni reali, rispondendo a nuove aspettative di velocità e accesso.

Buone notizie sul fronte della digitalizzazione delle PA italiane

Dalle ultime rilevazioni, si osserva oggi una reale maturità del rapporto digitale cittadino – ente: continua infatti ad aumentare il numero di cittadini che utilizzano l'identità digitale per accedere ai servizi online. Nel 2022 gli accessi tramite SPID hanno superato il miliardo, quasi raddoppiando quelli del 2021 (570 milioni), e nell'anno sono state rilasciate (come riporta il Dipartimento per la trasformazione digitale) oltre 6 milioni di identità SPID, raggiungendo così i 33,5 milioni totali. Più di 7 milioni invece le carte di identità elettronica rilasciate nell'anno. Cresciuto anche il numero delle PA che hanno attivato l'autenticazione ai servizi online tramite SPID: è salito di 3.207 unità rispetto all'anno precedente, raggiungendo quota 12.624 (mentre gli enti privati sono passati da 83 a 151).

Risultati importanti anche per l'App IO, che a fine 2022 è stata scaricata 32 milioni di volte. I messaggi inviati ai cittadini sono stati oltre 247 milioni, con una crescita del 117% rispetto al 2021. Con riferimento invece a PagoPA, nel 2022 sono state eseguite circa 332 milioni di transazioni, in aumento del 103% rispetto al 2021, per un valore pari a oltre 61 miliardi di euro (+80% rispetto all'anno precedente). Gli enti che hanno ricevuto almeno una transazione durante l'anno sono stati oltre 19mila, mentre gli utenti attivi mensilmente in media circa 9,6 milioni.

Se consideriamo poi la spinta arrivata dal Piano Nazionale di Ripresa e Resilienza (PNRR) alla digitalizzazione delle PA italiane (con fondi previsti pari a 6,7 miliardi di euro), va considerato che:

- Dal mese di aprile 2022, sono stati pubblicati i primi avvisi pubblici di finanziamento sulla piattaforma "PA Digitale 2026", per favorire le amministrazioni nel fare richiesta di accesso ai fondi e rendicontare l'avanzamento dei progetti.
- A dicembre 2022, entro i tempi stabiliti dal PNRR, oltre il 90% dei Comuni italiani avevano aderito ad almeno uno degli avvisi promossi dalla piattaforma.

- A poco più di anno dalla pubblicazione dei primi avvisi sulla piattaforma erano stati allocati oltre 1,8 miliardi di euro provenienti dal PNRR, con un'adesione che aveva nel frattempo raggiunto il 98% dei Comuni e il 96% delle scuole. Al terzo posto le ASL con un tasso di adesione del 73%. Attraverso la piattaforma sono stati assegnati 1,7 miliardi di euro ai Comuni (79% del totale disponibile), 64 milioni alle scuole (49% del totale disponibile) e 33 milioni ad altri enti (22% del totale disponibile).

In particolare, a giugno di quest'anno, oltre 5mila amministrazioni erano ammesse ai finanziamenti per la migrazione di dati e servizi in cloud, poco meno di 4mila avevano ricevuto risorse per l'estensione delle piattaforme sull'identità digitale, e circa 3mila Comuni avevano avuto accesso ai fondi per l'App IO e a quelli per PagoPA.

Con riferimento al Polo Strategico Nazionale (PSN), la nuova infrastruttura cloud per la PA (partecipata da TIM, Leonardo, Cassa Depositi e Prestiti – attraverso la controllata CDP Equity – e Sogei), operativa dal 21 dicembre 2022, la timeline prevede oggi 2 importanti scadenze:

- entro settembre 2024: almeno 100 PA migrate sulla nuova infrastruttura
- entro giugno 2026: almeno 280 PA migrate sulla nuova infrastruttura.

Gli obiettivi risultano al momento rispettati: a maggio di quest'anno, come riportato dal Dipartimento per la trasformazione digitale, risultava già iniziata la migrazione in cloud verso il PSN di oltre 40 amministrazioni centrali (grazie ai 157 milioni di euro nell'ambito della Misura 1.1 "Infrastrutture digitali" del PNRR).

Con riferimento invece alla Piattaforma Digitale Nazionale Dati (PDND, infrastruttura tecnologica che abilita l'interoperabilità dei sistemi informativi e delle basi di dati delle PA, da realizzare con fondi PNRR – 556 milioni relativi alla misura 1.3.1) la timeline prevede ora 2 importanti scadenze:

- entro dicembre 2024: integrazione di almeno 400 API sul catalogo centrale della PDND;
- entro giugno 2026: integrazione di almeno 1.000 API sul catalogo centrale della PDND.

Obiettivo finale del PNDN è quello di rendere le nostre PA conformi al principio "once-only", in modo che dalla condivisione dei dati, sia possibile una forte semplificazione delle attività per tutti. Dal 21 ottobre 2022, con largo anticipo, la Piattaforma è attiva ed è stato pubblicato un primo avviso da 110 milioni di euro rivolto ai Comuni. Un secondo avviso, da 50 milioni di euro, rivolto questa volta agli enti regionali, è stato invece pubblicato il 22 dicembre 2022.

Risultati conseguiti dalle PA locali, secondo la rilevazione di The Innovation Group e Gruppo Maggioli

La rilevazione di The Innovation Group e Gruppo Maggioli, effettuata tra il 29 giugno e l'8 agosto 2023 su un campione di 207 enti pubblici locali (in prevalenza Comuni, ma anche Regioni e altri enti), offre un quadro approfondito della trasformazione digitale negli Enti pubblici locali italiani, evidenziando alcuni aspetti significativi.

In particolare

- Avanzamento della Cloud Trasformation. Il 27% degli enti locali è già molto avanzato nel processo di migrazione al Cloud, mentre il 28% ha spostato solo parzialmente gli applicativi. Il 32% degli Enti si trova invece nelle prime fasi di avvio del

processo. Con riferimento al PSN, è stato preso in considerazione dalla maggior parte del campione (70%). In particolare, il 6% degli enti pubblici locali aveva a luglio già aderito al PSN, spostando parte di applicazioni e dati, e un ulteriore 23% contava di farlo a breve. Un ulteriore non ha ancora in roadmap il PSN ma 42% prevede di considerarlo a breve: segnale importante di quanto la strategia cloud per la PA sia andata ad offrire la corretta soluzione a esigenze molto diffuse di sicurezza dei dati e affidabilità dei servizi.

- Interoperabilità. L'adesione alla Piattaforma Digitale Nazionale dei Dati (PDND) risulta essere pari al 51%: un ulteriore 47% la prevede (del resto l'adesione sarebbe obbligatoria entro settembre 2023). Questo riflette l'impegno tangibile di tutti gli Enti a conformarsi al principio «once only».
- Servizi digitali e ai percorsi di cittadinanza digitale. Il 45% degli Enti locali si considera «abbastanza» avanzato su questo fronte, dimostrando una chiara consapevolezza dell'importanza di offrire esperienze digitali avanzate ai cittadini, in linea con le attuali tendenze. Gli Enti si stanno concentrando in particolar modo sull'integrazione dei servizi con SPID e CIE (91%) e sull'adozione della piattaforma pagoPA per i pagamenti (79%) principalmente dei servizi tributi (76%) e anagrafe e demografici (74%). La tendenza all'integrazione dei servizi nell'app IO è altrettanto rilevante (68%). I servizi anagrafici e demografici, l'iscrizione alla mensa scolastica, la gestione della TARI e dei tributi IMU stanno emergendo come aree chiave di interesse.

Cosa serve ancora alla PA italiana per vincere la partita per la trasformazione digitale

Prima la pandemia, oggi il PNRR, spingono in questo periodo storico verso una completa digitalizzazione dei processi della PA italiana. Alcuni requisiti generali andrebbero però considerati da subito perché i risultati siano quelli che tutti ci auspichiamo: una PA moderna, efficiente, vicina ai bisogni di cittadini e imprese, volano di competitività del Paese in un'era caratterizzata da elementi come: velocità, qualità, inclusività, rispetto di valori etici e ambiente.

Concentrandoci sugli enti locali, che, come mostrano anche i risultati della nostra indagine (che sarà presentata il prossimo novembre 2023, in occasione del "Digital Italy Summit 2023", dal 14 al 16 novembre a Roma), sono ancora un passo indietro rispetto alle PA centrali per molti aspetti della trasformazione, è importante che, nonostante le loro dimensioni a volta contenute, siano in grado di dotarsi di una visione il più possibile ampia e quindi di una strategia complessiva, che li guidi con un piano articolato e omnicomprensivo in questo percorso.

Serve poi un approccio molto concreto, definire quindi priorità agli interventi da fare, sapendo esattamente quale sarà il punto di approdo finale. Da questo punto di vista, analizzare le scelte di chi è più avanzato può essere una strada molto utile, come anche standardizzare il più possibile processi, soluzioni, tecnologie da adottare.

Storicamente le PA locali hanno rivolto i propri percorsi di digitalizzazione soprattutto verso lo sviluppo di servizi e comunicazioni per i cittadini, quindi, il Front office. La continua pervasività del digitale potrebbe però portare a un ulteriore aumento del numero di servizi digitali offerti, oltre che alla loro progressiva integrazione con le piattaforme nazionali: tutto questo dovrà essere accompagnato da una rinnovata progettazione e da un ripensamento a monte dei modelli di erogazione dei servizi.

Le risorse messe a disposizione dal PNRR rappresentano una fondamentale occasione per tutti gli enti: per quelli con una maturità più bassa, il volano per recuperare i ritardi accumulati. Va tenuto però presente che molti di questi fondi andranno indirizzati agli ambiti che oggi richiedono maggiore attenzione da parte di tutti: la cybersecurity, che è emersa un ambito molto trascurato in passato; la migrazione al cloud, che andrà sostenuta in questo periodo per realizzarla in tempi brevi; l'interoperabilità, che è soltanto all'inizio; l'evoluzione dei servizi online contestualmente a un rafforzamento della gestione delle identità, che deve diventare più sicura ed allineata ai trend recenti, guardando anche alle evoluzioni in corso a livello europeo.

Luigi Iaccarino
Head of Global Cyber Defence and Cybersecurity Italy di Vodafone

Conoscere e prevenire gli incidenti. La ricetta per la cyber resilienza di Vodafone

Roberto Bonino, Research and Content Manager
The Innovation Group

Le cifre che accompagnano le analisi sulla cybersecurity sono impietose. La ricerca "Cyber Risk Management 2023 Survey" di The Innovation Group ha rilevato come il 96% delle aziende italiane abbia osservato almeno un attacco informatico nel corso dell'ultimo anno e il phishing sia la minaccia più ricorrente, persino più del ransomware (che ha comunque interessato il 40% del campione analizzato).

Se la cybersecurity viene perseguita da tempo, seppur con diversi livelli di maturità, da gran parte delle aziende, negli ultimi tempi sembra aver preso piede il concetto di cyber resilienza, che punta l'attenzione sulla capacità di ripresa rapida in caso di incidente informatico, si pone come obiettivo la continuità operativa e genera misure e conoscenze che devono coinvolgere necessariamente tutta l'azienda anche in termini reattivi.

Vodafone è un'azienda che, per la propria natura globale e dimensionale, mette la cyber resilienza al centro delle strategie di prevenzione e reazione ai tentativi di attacco. Per comprendere meglio cosa ispira le scelte corporate e locali della società, abbiamo incontrato Luigi Iaccarino, Head of Global Cyber Defence and Cybersecurity Italy.

Come si declina per voi il concetto di cyber resilienza?

Il tema è molto ampio e abbraccia diversi aspetti, ma in sintesi porta ad avere una postura corretta rispetto alle minacce più importanti che ci troviamo ad affrontare. Una strada maestra è rappresentata dalla creazione di misure preventive per rendere l'azienda meno esposta ai rischi cyber. Va tenuto conto che i threat actor sono quasi sempre aziende a loro volta, quindi più si tiene la barra alta e si eleva a il muro difensivo più si rende la vita difficile a chi vuole attaccare e, magari, lo si convince a desistere. Ma questo non basta, perché è impossibile pensare che non accadano incidenti, per cui la cyber resilienza passa anche per un'accurata azione di detection, mettendo poi in atto le azioni che rendono l'impatto minore possibile. Per questo occorre un mix di azioni automatiche – rapide nell'esecuzione ma più soggette a falsi positivi – e analisi che conducono ad azioni un po' più dilatate nel tempo, ma complessivamente più efficaci.

A questo, naturalmente, si aggiunge poi tutto ciò che ha a che fare con l'ecosistema con il quale l'azienda si confronta.

In questo contesto infrastrutturale, la componente di rilevazione & risposta ha un ruolo determinante?

Siamo una grande azienda e per questo ci siamo dotati di un Security Operations Center (SOC) interno, che opera 24h tutti i giornix7 e del quale io sono responsabile su scala globale. A complemento delle regole definite dai technology player nostri fornitori, abbiamo messo a punto la nostra governance. La Cyber Threat Unit verifica costantemente quali attacchi dobbiamo affrontare e le tecniche utilizzate. Disponiamo anche di team di data hunt, che lavora su dati offline e va più in profondità sugli scenari più tipici del comparto Telco nel quale ci collochiamo.

Quali sono gli elementi che più vi preoccupano in questo scenario?

Mentre nell'ambito delle nostre infrastrutture siamo in grado di effettuare in prima persona controlli preventivi e di monitorare direttamente l'evolversi delle minacce, lavoriamo anche con molti fornitori esterni e lì la nostra capacità di controllo si scontra con limiti oggettivi. Per mitigare il rischio, abbiamo categorizzato i fornitori in base al livello di rischio e al tipo di dati che gestiscono per nostro conto. Questa categorizzazione definisce la tempistica e la metodologia applicata a controlli periodici che effettuiamo per verificare il grado di aderenza ai nostri requisiti, ma riteniamo che l'approccio verso le terze parti debba evolvere in una direzione che renda la riduzione del rischio più sostanziale. Un altro tema rilevante riguarda l'obsolescenza dei sistemi che, su un parco macchine così elevato, è di per sé una sfida. In questo caso le priorità degli interventi sono focalizzate sugli asset più esposti o la cui eventuale compromissione possa comportare conseguenze più gravi. Va da sé che il fattore umano è un altro elemento da tenere presente. Tutte le attività di formazione e consapevolezza che mettiamo in campo vanno nella direzione della minimizzazione dei rischi. Le campagne di test e simulazione su tutta la popolazione aziendale e i conseguenti momenti di approfondimento e feedback con i singoli dipartimenti sono elementi essenziali che mirano a far acquisire a tutti una maggiore consapevolezza sull'importanza del proprio ruolo nella tutela dell'azienda.

PA centrale: il Digitale spinge la competitività del sistema Paese

Arianna Perri, Research Analyst
The Innovation Group

I progressi compiuti dalle Pubbliche Amministrazioni centrali nel loro percorso di trasformazione digitale riguardano sia la fornitura di servizi efficaci e resilienti rivolti ai cittadini e alle imprese, sia l'esplorazione di vari ambiti innovativi, tra cui l'Intelligenza Artificiale e lo sviluppo di nuove competenze. L'analisi di tali percorsi può contribuire a identificare le migliori pratiche, che possono essere applicate con successo anche nel contesto meno avanzato delle PA locali.

Al fine di approfondire queste dinamiche, TIG ha condotto delle interviste individuali in profondità a due figure di spicco coinvolte in questo processo: il Direttore del Dipartimento per lo Sviluppo di Metodi e Tecnologie per la produzione e la diffusione dell'informazione statistica dell'Istat, Massimo Fedeli (nel ruolo di Direttore Centrale per le Tecnologie Informatiche al momento dell'intervista), e Stefano Tomasini Direttore Centrale per l'Organizzazione Digitale dell'Inail.

Verso una visione utente-centrica

Grazie al processo di digitalizzazione, si assiste a un significativo cambiamento di paradigma nella PA centrale: l'orientamento è ora verso una visione centrata sull'utente. In questo contesto, ogni cambiamento organizzativo in favore di una maggiore digitalizzazione tiene conto di coloro che dovranno poi utilizzare i nuovi strumenti e adeguarsi alle nuove logiche, ossia dei dipendenti della PA stessa, da una parte, e i cittadini, dall'altra, a cui si rivolgono i servizi offerti.

Ciò comporta un efficientamento delle operazioni e un ripensamento delle relazioni tra diverse amministrazioni, come ribadito da Massimo Fedeli, Istat: "Il processo di digitalizzazione, che sta accelerando grazie al PNRR, riveste una grande importanza nell'ottica di efficientare le operazioni e creare servizi cross-amministrazione per i cittadini, offrendo notevoli vantaggi sia a loro che alle imprese". Fedeli sottolinea, inoltre, che la creazione di servizi interdipartimentali, mirando all'interoperabilità, contribuisce a potenziare la competitività interna del Paese: "Non possiamo dimenticare che questi cambiamenti in corso rappresentano un fattore di grande competitività per l'Italia. Di conseguenza, non è un caso che la Missione 1 del PNRR includa questo elemento, ovvero la creazione di un vantaggio competitivo per l'intero sistema Paese".

La pandemia come catalizzatore del cambiamento

Il percorso verso la trasformazione digitale è stato notevolmente accelerato dalla pandemia di COVID-19, ha commentato Massimo Fedeli. Durante il periodo critico della pandemia, infatti, Istat è stato costretto a sospendere numerose indagini sul campo, tra cui il censimento della popolazione e

delle imprese. In sostituzione, ha potuto però ricorrere a dati amministrativi delle imprese presenti nei suoi database. Questo processo di trasformazione digitale ha innescato un'evoluzione su vasta scala che ha coinvolto diversi livelli, compreso l'efficientamento interno, come illustrato da Massimo Fedeli: "Il periodo pandemico e la digitalizzazione del processo ci hanno permesso di condurre una serie di indagini che prima richiedevano visite sul campo. Precedentemente chiedevamo direttamente alle imprese tutta una serie di informazioni, come il fatturato, il numero degli addetti eccetera. Ora possiamo acquisire queste informazioni utilizzando i dati amministrativi già a nostra disposizione".

Il Cloud come paradigma

Un altro aspetto cruciale di questa rivoluzione digitale è la migrazione al Cloud. Stefano Tomasini, CIO di Inail, pone l'enfasi sulla prospettiva generale che sta adottando l'Istituto sul tema: "Quando ci riferiamo alla strategia Cloud di Inail, ci concentriamo non tanto sulla mera migrazione, ma piuttosto sull'adozione del Cloud come paradigma fondamentale per la reingegnerizzazione del nostro sistema informatico. Questa transizione verso il Cloud ci offre l'opportunità di rendere scalabili e facilmente integrabili le diverse soluzioni disponibili presso i service cloud provider o presso il Polo Strategico Nazionale". Tomasini rivela che uno dei principali obiettivi dell'Inail per il 2023 è la trasformazione del loro data center in un software-defined data center. Questo significa che l'Istituto sta scommettendo sulla modernizzazione delle applicazioni, adottando il paradigma cloud first e riflettendo sulle modalità con cui erogano i servizi in modo user-centric, come ribadito da Tomasini: "Non parliamo di Lift-and-Shift, ma di Refactoring perché cogliamo l'occasione per un ripensamento, appunto, di tutta l'area dei servizi in ottica utente centrica e in modalità Cloud". L'Inail sta promuovendo, inoltre, l'adozione di soluzioni Cloud pubbliche e private, sia SaaS (Software as a Service) che PaaS (Platform as a Service), che permetteranno di offrire a cittadini e imprese servizi più flessibili e ad alta capacità computazionale, come dimostrato dall'adozione di tecnologie di Intelligenza Artificiale tramite motori Cloud.

Massimo Fedeli rivela che l'Istat ha adottato un approccio cloud native, in cui i nuovi servizi sono avviati direttamente nel Cloud anziché migrare quelli esistenti. Questa decisione è stata guidata dalla convinzione che il Cloud sia un abilitatore chiave per l'innovazione. L'Istituto utilizza anche il Cloud per gestire il proprio contact center, un importante canale di comunicazione con il pubblico e il settore privato che rappresenta un elemento chiave nel mantenere un servizio di alta qualità per i propri stakeholder.

Sicurezza dei dati: un imperativo in un mondo digitalizzato

In un contesto di crescente digitalizzazione del settore pubblico, la sicurezza dei dati emerge come una priorità assoluta, in particolar modo per quanto concerne gli enti della PA centrale in cui la gestione di dati sensibili è parte integrante del loro operato quotidiano.

Tomasini sottolinea che l'Inail ha prestato particolare attenzione agli investimenti per affrontare le minacce cyber, definendo un approccio chiaro alla questione: "Abbiamo individuato tre pilastri fondamentali della resilienza informatica, che comprendono la capacità organizzativa di prevenire, affrontare e risolvere attacchi mantenendo un funzionamento operativo ininterrotto. Pertanto, l'organizzazione, la sicurezza dei sistemi informativi e la continuità operativa costituiscono tre elementi centrali su cui abbiamo fondato il nostro rafforzamento nella sfera della sicurezza cyber". A livello delle misure adottate, elenca l'introduzione della multifactor authentication per utenti interni ed esterni, lo sviluppo di robuste misure di backup multicloud per ripristinare i sistemi in caso di attacco, il potenziamento del proprio SOC (Security Operations Center) e del CERT (Computer Emergency Response Team). Inoltre, l'Inail sta incorporando funzionalità di Intelligenza Artificiale per migliorare l'efficienza ed efficacia delle operazioni di sicurezza.

Ostacoli da superare

Nonostante i progressi, ci sono sfide significative da affrontare. Fedeli

L'opportunità per la PA centrale è quella di sfruttare la transizione digitale per abilitare una governance più efficiente, semplificare le procedure e promuovere una cultura dell'innovazione

identifica due ostacoli principali: il primo riguarda l'attrazione delle competenze giuste e il secondo la burocrazia che rischia di rallentare l'attuazione di programmi come il PNRR. Per affrontare la prima sfida, l'Istat punta a promuovere l'immagine dell'Istituto come parte di un progetto innovativo, come spiega Massimo Fedeli: "Facendo sentire che Istat fa parte di un progetto innovativo, motivando le persone, soprattutto i giovani, a entrare a far parte di questo progetto, a unirsi, quindi, a questa missione di trasformazione digitale".

Tomasini esprime un ulteriore ostacolo da superare in questo processo di trasformazione digitale: l'accelerazione dell'evoluzione tecnologica che talvolta rischia di "lasciare indietro" coloro che hanno un'esperienza professionale consolidata. "Uno dei problemi principali nelle pubbliche amministrazioni, compreso l'Inail" – continua Tomasini – "è rappresentato dalla mancanza di nuove risorse che avrebbero agevolato i processi di transizione e accompagnato sia giovani che meno giovani nei percorsi di cambiamento. La sfida è dunque quella di accompagnare il personale in questo rapido processo di transizione".

L'opportunità per la PA centrale è quella di sfruttare la transizione digitale per abilitare una governance più efficiente, ridefinire i processi interni, semplificare le procedure e promuovere una cultura dell'innovazione. L'obiettivo finale è quello di creare servizi che migliorino la vita di cittadini e imprese e, più in generale, la competitività dell'intero Paese. Superando le sfide, come la ricerca di talenti, la burocrazia e la scarsità di competenze digitali, il tessuto delle Pubbliche Amministrazioni sta aprendo la strada a un futuro digitale più efficiente e innovativo. È necessario però un impegno continuo nella formazione del personale e una maggiore sensibilizzazione all'importanza della sicurezza dei dati e dei servizi.

(Intervento estratto dal contributo di Arianna Perri ed Elena Vaciago per il Rapporto Digital Italy 2023, edizioni Gruppo Maggioli, che sarà presentato in anteprima al Digital Italy Summit 2023)

EU-U.S. Data Privacy Framework: si semplificano i trasferimenti dati verso gli U.S.A. (per ora)

Giulia Rizza, Consultant e PM

Colin & Partners

Il 10 Luglio 2023 la Commissione Europea ha adottato una nuova decisione di adeguatezza stabilendo, ai sensi dell'art. 45 GDPR, che senza necessità di ulteriori verifiche sono legittimi i trasferimenti di dati personali dallo Spazio Economico Europeo verso quei soggetti in U.S.A. che hanno certificato la propria adesione ai principi sanciti dal E.U.-U.S. Data Privacy Framework.

La decisione giunge a seguito della c.d. sentenza "Schrems II" della Corte di Giustizia dell'U.E. (CGUE) che ha invalidato la precedente decisione di adeguatezza con gli U.S.A. (c.d. Privacy Shield che, a sua volta, sostituiva il Safe Harbour, accordo sul trasferimento dati UE/USA decaduto nel 2015 a seguito della decisione c.d. "Schrems" della CGUE): la Corte ha ritenuto che il precedente quadro normativo non garantisse un livello di tutela dei dati personali equivalente a quanto previsto dal GDPR, in particolare in ragione degli ampi margini discrezionali riconosciuti dalla normativa statunitense alle autorità di intelligence per esigenze di sicurezza nazionale. La decisione poneva altresì condizioni per l'applicazione delle clausole contrattuali standard, altro strumento di garanzia del trasferimento previsto dal GDPR ed ampiamente utilizzato nella prassi, tali da comportare una forte incertezza sul punto da entrambi i lati dell'oceano. Basti pensare al Provvedimento del Garante Italiano del 2022, in linea con analoghe decisioni delle autorità francesi ed austriache, con cui è stata ammonita una società italiana per utilizzare Google Analytics, concedendole 90 gg di tempo per adottare adeguate garanzie al trasferimento ed ordinando la cessazione dei flussi illegittimi di dati verso gli U.S.A., scatenando il panico tra i numerosissimi utilizzatori di tale strumento gratuito.

Il DPF ha introdotto nuove garanzie a tutela dei cittadini comunitari e volte a superare i rilievi della CGUE: incorporando i principi di conservazione, minimizzazione, sicurezza ed accuratezza dei dati; rafforzando il rispetto dei principi di necessarietà e proporzionalità nei casi di accesso ai dati da parte dell'intelligence statunitense; introducendo nuovi meccanismi di difesa a tutela degli interessati, tra cui un tribunale di riesame per la protezione dei dati (DPRC) a cui potranno accedere interessati dell'U.E. e che può adottare decisioni correttive vincolanti.

La nuova decisione di adeguatezza è entrata in vigore con la sua adozione il 10 luglio 2023. Un primo riesame della stessa, volto a verificarne l'effettivo funzionamento

nella pratica, avrà luogo entro un anno dall'entrata di vigore. Successivamente, la Commissione, in consultazione con Stati Membri e autorità garanti, deciderà la periodicità dei futuri esami, che avranno luogo almeno ogni quattro anni.

Le aziende interessate, potranno aderire al DPF impegnandosi a rispettare gli obblighi dallo stesso previsti, tra i quali ricordiamo quello di cancellazione dei dati personali una volta esaurita la finalità del trattamento, avanzando la domanda di certificazione al Dipartimento del Commercio statunitense, che si occuperà anche di monitorare il rispetto dei requisiti di certificazione.

I successivi chiarimenti del European Data Protection Board e delle competenti autorità garanti nazionali hanno fornito indicazioni operative per coloro che intendano trasferire dati dall'U.E. verso gli U.S.A.

Laddove si intenda basare il trasferimento di dati personali oltreoceano sulla nuova decisione di adeguatezza, è opportuno verificare preliminarmente sul sito https://www.dataprivacyframework.gov/s/participant-search la sussistenza della certificazione in capo al destinatario dei dati.

Se questi risulta avere una certificazione attiva, il trasferimento può legittimamente basarsi sulla decisione di adeguatezza. Non sarà quindi necessario svolgere ulteriori analisi ed approfondimenti del caso (si pensi, ad esempio, alle valutazioni sulla necessità ed adeguatezza di eventuali misure supplementari alle clausole contrattuali standard). Tuttavia, dovrà essere aggiornata di conseguenza la documentazione in uso (es. informative, Data Processing Agreement, Transfer Impact Assessment, nomine a responsabile), avendo altresì cura di verificare l'allineamento di eventuale documentazione adottata dall'organizzazione statunitense (es. DPA predisposto da Big Tech).
Sul punto, si evidenzia che ad oggi continuiamo a riscontrare casi in cui l'organizzazione, pur risultando certificata DPF, ancora non ha provveduto ad aggiornare la documentazione disciplinante il proprio ruolo di responsabile (es. DPA disponibile sul proprio sito): in tali casi l'invito, anche in ottica accountability, è richiedere aggiornamenti a controparte sul punto ed allineare di conseguenza la documentazione di riferimento.
Permane altresì l'obbligo di verificare, con cadenza quantomeno annuale, la sussistenza della certificazione monitorando il sito https://www.dataprivacyframework.gov.

Se, invece, il destinatario non risulta aver aderito allo schema di certificazione, il trasferimento di dati oltreoceano non potrà basarsi sulla nuova decisione di adeguatezza. Affinchè il trasferimento sia legittimo, dovrà quindi basarsi su un diverso strumento di garanzia di cui all'art. 46 GDPR (es. clausole contrattuali tipo della Commissione o BCR), con tutte le opportune analisi e verifiche del caso.

Dopo un'attesa di 3 anni, la Commissione ha quindi stabilito che gli Stati Uniti garantiscono un adeguato livello di tutela dei dati personali trasferiti dall'U.E. verso quelle organizzazioni negli U.S.A. che sono state incluse nel "Data Privacy framework List" dal Dipartimento del Commercio statunitense.

Tuttavia, Max Schrems e la sua organizzazione Noyb, già all'indomani dell'adozione della decisione, hanno sollevato criticità al riguardo, sostenendo che l'accordo non si basi su cambiamenti sostanziali delle criticità che hanno comportato l'invalidità del Privacy Shield, ma sarebbe una mera espressione degli interessi politici volti a venire incontro alle esigenze delle grandi società statunitensi. Ha quindi già annunciato che la questione tornerà alla Corte di Giustizia entro il prossimo anno.

Cyber Resilienza: strategie di risposta alle minacce cyber

Elena Vaciago, Research Manager
The Innovation Group

Una strategia di cyber resilienza è un approccio complessivo per proteggere la propria organizzazione dalle minacce cyber, nonché per garantire capacità di risposta e ripresa efficace in caso di eventi dannosi. La cyber resilienza si basa, in modalità end-to-end, sulla prevenzione, mitigazione e gestione degli incidenti informatici, al fine di ridurne al minimo l'impatto negativo sulle attività aziendali. In questa intervista con Marcello Fausti, Responsabile della Cybersecurity del Gruppo Italiaonline, approfondiamo le sfide che le odierne organizzazioni incontrano nell'incrementare la propria cyber resilienza e aumentare costantemente le proprie capacità di rilevamento e risposta ad attacchi informatici diventati sempre di più la norma.

Qual è la strategia di Cyber Resilience seguita dalla Sua azienda?

Negli ultimi anni abbiamo fatto un significativo passo in avanti, adeguando strategie, pratiche e tecnologie. Questo è stato relativamente semplice: le difficoltà incontrate sono state soprattutto di natura organizzativa, ossia, riuscire a fare in modo che i processi di sicurezza permeino a regime tutta l'azienda. Il tema della reazione, in materia di resilienza, è molto controverso: non se ne può parlare a "cuor leggero" perché gli impatti potrebbero essere importanti, serve un'organizzazione perfettamente allineata e processi perfettamente recepiti. Questo in moltissime aziende è piuttosto difficile da ottenere. In aggiunta, spesso l'IT operation può offrire un supporto limitato, per problemi banalissimi di capacità, disponibilità di risorse e di tempo per portare a regime i processi. In generale, si investe tanto in tecnologie e poco invece in competenze.

In generale, quali sono gli step per incrementare la Cyber Resilienza?

L'ideale è disporre di un team dedicato al monitoraggio e alla risposta, e puntare ad avere una completa visibilità su dati, applicazioni, sistemi. Bisogna aver predisposto un piano per la gestione di incidenti di cybersecurity, e disporre di soluzioni tecnologiche dedicate, con un forte ricorso all'automazione. Può essere utile utilizzare servizi gestiti di fornitori terzi, avere attività di formazione specifiche per la gestione di incidenti, effettuare periodicamente test/simulazioni di incidenti. Noi stiamo anche collaborando in modo esteso con

Fino a qualche anno fa le aziende non si accorgevano di avere visitatori indesiderati, ora invece, chi ha maturato capacità avanzate di detection, riesce ad accorgersi del momento in cui un attacco sta prendendo forma. L'essenziale è quindi anticipare la fase di detection, possibilmente intercettare un attaccante quanto non è ancora dentro ma quando si sta "avvicinando"

il business in modo da aumentare il controllo, controlliamo la cyber resilienza dei fornitori dell'azienda ed utilizziamo un framework specifico sulla Cyber Resilienza per misurare i nostri risultati e migliorare continuamente.

Parliamo di rilevamento e risposta agli incidenti di sicurezza: quanto è importante il tema secondo la Sua esperienza?

Di recente, abbiamo assistito a un fatto piuttosto importante: l'adozione da parte dell'ACN della tassonomia NIST che è molto orientata all'impatto dell'incidente. Se non si riscontra un impatto, infatti, sostanzialmente non l'incidente non viene registrato. Questa cosa ha effetti positivi (meno lavoro di registrazione e più chiara focalizzazione sull'impatto) ma anche qualche piccolo effetto negativo. In particolare, mi riferisco al fatto che con l'approccio NIST il numero di incidenti registrati rispetto agli anni precedenti diminuisce; non registrando gli incidenti lievi, inoltre, si rischia di perdere informazioni importanti, a volte utili a ricostruire il contesto di un evento malevolo.

Con altre tassonomie (es. Enisa) vengono considerati incidenti anche alcuni eventi di sicurezza importanti (come, ad esempio, un movimento nel darkweb che fa capire che si può essere oggetti di attacco) utili anche a supportare la comunicazione con il management che deve essere messo in grado di valutare questi rischi attraverso una rappresentazione complessiva dei problemi.

Quali sono gli aspetti da perseguire nelle attività di rilevamento e risposta a incidenti cyber?

Fino a qualche anno fa le aziende non si accorgevano di avere visitatori indesiderati, ora invece, chi ha maturato capacità avanzate di detection, riesce ad accorgersi del momento in cui un attacco sta prendendo forma. L'essenziale è quindi anticipare la fase di detection, possibilmente intercettare un attaccante quanto non è ancora dentro ma quando si sta "avvicinando". A questo scopo, la Threat Intelligence è molto efficace, aiutando – ad esempio – ad intercettare i movimenti che ci riguardano nel dark web sia in fonti aperte che in fonti chiuse. L'attività di mitigazione, quindi, può iniziare ben prima che l'attacco sia stato sferrato. Non dimentichiamoci che il tempo di reazione è fondamentale!

Altro tema: gli attaccanti cercano costantemente nel darkweb informazioni su aziende partner o fornitori, perché questi rappresentano un punto di ingresso indiretto molto importante. La gestione della sicurezza delle terze parti è inclusa direttamente nelle clausole contrattuali, ma può essere aiutata con un attento monitoraggio del darkweb.

... e parlando di strumentazione per la detection?

Oggi molti strumenti sono alimentati da AI e machine learning per guardare sia al perimetro aziendale sia al cloud, con strumenti di anomaly detection che funzionano su base statistica e con algoritmi AI, che dopo un training consistente diventano molto efficaci. Tutti gli strumenti di sicurezza (ad es. firewall, sonde IPS) sono una strumentazione utile al monitoraggio che, essendo alimentati da IoC (indicatori di compromissione) inviati tramite la threat intelligence, consentono di riconoscere istantaneamente eventuali movimenti che si verificano.

Un altro tema molto importante da considerare è quello relativo alla protezione del perimetro pubblico. In questo caso, visto che il phishing è una delle minacce più pericolose, è importante monitorare tutti i domini simili a quelli di proprietà della nostra azienda, creati dagli attaccanti a scopo di phishing. Noi, con le attività AI, intercettiamo circa 20 domini al mese, da controllare e, nel caso siano domini creati ad hoc per attività di phishing, chiederne il takedown al service provider e al Registrar.

Quali problemi incontrate nelle attività di rilevamento e risposta a incidenti di sicurezza?

Ormai le attività di rilevamento hanno raggiunto un livello di maturazione piuttosto elevato. In questo ambito, infatti, l'AI ha supportato le aziende nel fare un salto molto importante in termini di efficienza, mantenendo bassi i costi e riducendo il bisogno di ricorrere a una squadra dedicata. Le attività di monitoraggio sono in genere ben rodate, i problemi sorgono invece nelle fasi di remediation, quando emerge una sorta di conflitto di interesse tra sicurezza, velocità di risoluzione ed efficienza del business.

Se ad esempio un incidente comporta la necessità di una modifica architetturale, per motivi di velocità della gestione tecnica del business o per indicazioni del marketing, potrebbe non essere semplice, o addirittura possibile, introdurre le opportune contromisure.

Può accadere che le soluzioni di sicurezza siano – in qualche modo – limitanti: le aziende, però, dovrebbero ragionare su come individuare una corretta via di mezzo. Quindi, una sfida importante è trovare il giusto trade off tra esigenza di business ed esigenze di sicurezza.

Un'ulteriore difficoltà, invece, è legata alla presenza di legacy in azienda. Non è detto che mettere in campo tecnologie sempre nuove sia sempre la strada migliore: se applico la tecnologia solo su progetti nuovi, il legacy rimane non protetto.

L'AI generativa ci obbliga a riflettere su noi stessi

Valentina Bernocco, Web and Content Editor
The Innovation Group

Ripensare alle competenze e imparare a "conoscere il nemico", per portarlo dalla nostra parte. Una strategia possibile per il mondo del lavoro.

L'intelligenza artificiale generativa corre veloce, sia per quanto riguarda le sperimentazioni di sviluppatori e società vendor, sia per i continui ampliamenti di offerta (nuove funzionalità all'interno di software aziendali o nuovi servizi cloud per il training o l'affinamento di algoritmi) e per il numero di aziende che la adottano. I due fronti degli entusiasti e degli scettici o preoccupati sono già schierati, in un dibattito che da ormai circa un anno si dispiega tra ricerche di mercato, comunicati stampa, opinioni di analisti e discussioni da bar (o da social network).

L'impressione di molti è che siamo appena all'inizio di una rivoluzione irreversibile. Bloomberg prevede che il valore dei software e servizi di genAI esploderà nel corso di un decennio, dai 40 miliardi di dollari del 2022 ai 1.300 miliardi stimati per il 2032. Ma oggi sull'AI generativa, o genAI come qualcuno l'ha ribattezzata, pendono ancora molti punti interrogativi, troppi per

> **Oggi sull'AI generativa, o genAI come qualcuno l'ha ribattezzata, pendono ancora molti punti interrogativi**

Immagine creata con AI generativa

riassumerli in un breve articolo. Può diventare un'arma per la disinformazione o per gli attacchi informatici? Cancellerà i confini tra vero, verosimile e falso? Alimenterà pregiudizi e discriminazioni?

La domanda forse più importante per una larga fetta della società riguarda il rapporto fra genAI e occupazione. Con le sue capacità di automazione evoluta e di creazione di contenuti (testi di ogni genere, ma anche immagini simil-fotografiche, opere artistiche, canzoni e chissà che altro in futuro), è assai probabile che questa tecnologia possa sostituire le persone in diverse attività di lavoro quotidiane più o meno tediose o creative. Per i vendor di tecnologia questo sarà un bene: le persone in azienda potranno focalizzarsi su attività a valore aggiunto, intellettualmente più stimolanti della scrittura di un'email, della ricerca di informazioni in un database o della costruzione di una presentazione Power Point. I datori di lavoro raccoglieranno i benefici degli incrementi di produttività ed efficienza. A seconda del punto di vista, però, il quadro cambia.

Uno studio di Goldman Sachs,

pubblicato lo scorso aprile, stima che in un orizzonte di medio periodo l'AI generativa potrebbe spazzar via circa 300 milioni di posti di lavoro (equivalente a tempo pieno), ovvero il 18% degli attuali occupati. Nelle professioni amministrative verrà automatizzato il 46% delle attività, in quelle di ambito legale il 44%, nell'architettura e nell'ingegneria il 37%, mentre sarà più trascurabile l'effetto su professioni che comportano una manualità non standardizzata, come quelle artigiane. L'impatto dell'AI generativa sull'occupazione sarà quindi negativo almeno nel breve o medio termine, ma comunque non troppo diverso da quello di altre tecnologie informatiche che hanno segnato la storia contemporanea, come i computer e Internet. Tecnologie di cui oggi non potremmo più fare a meno e che non vengono generalmente considerate come forze distruttive sull'occupazione.

C'è anche chi, come McKinsey, vede le due facce della medaglia, parlando di una necessità di "transizione" dei lavoratori su nuove attività. Le aziende dovranno farsi carico del problema, aiutando i dipendenti con corsi di formazione affinché sviluppino nuove competenze, e inoltre dovranno "mitigare e controllare" i rischi connessi all'intelligenza artificiale. Se tutto questo sarà gestito correttamente, l'AI generativa potrà "contribuire in modo sostanziale alla crescita economica", scrive McKinsey.

Il tema, ammettiamolo, è ancora controverso e oggi si possono solo fare delle proiezioni. Secondo Ibm, per esempio, il 40% dei dipendenti d'azienda dovrà trovare modi per riqualificarsi da qui a tre anni per mantenere rilevanza di fronte ai progressi dell'AI (il dato è derivato da un'analisi condotta su 3.000 dirigenti di 28 nazioni e 21.000 dipendenti di 22 Paesi). "L'AI non sostituirà le persone, ma le persone che usano l'AI rimpiazzeranno quelle che non la usano", si legge nel report. Insomma, per non perdere opportunità di carriera sarà cruciale restare aggiornati con gli sviluppi dell'informatica, più di quanto non lo sia stato negli ultimi quarant'anni.

Ma che cosa significa imparare a usare l'AI generativa? Come prima cosa significa familiarizzare con un'interfaccia, con i suoi comandi e funzionalità, insomma capire che cosa si possa fare con una data applicazione e come farlo. Questo è però solo il livello di comprensione iniziale e quello più banale: i large language model capiscono il linguaggio naturale e compiono da sé gran parte dello sforzo di comunicazione nel rapporto uomo-macchina. Alle persone e alle aziende sarà semmai richiesto un altro sforzo, quello di restare al passo con le evoluzioni dell'offerta per saper riconoscere le differenze tra una soluzione e l'altra, specie in termini di trattamento dei dati. In terzo luogo, non ci basterà sapere usare un'applicazione come ChatGPT o Bard ma dovremo imparare a usarla bene e responsabilmente, per esempio delimitando il confine tra ciò che possiamo delegare al software e ciò che è meglio continuare a fare nel modo "tradizionale", con la sola creatività e intelligenza umana. In futuro l'AI generativa sarà per qualcuno il migliore alleato per la produttività, per altri un nemico da conoscere per imparare a contrastarlo. In ogni caso, dai Baby Boomer alla Gen Z, nessuno di noi potrà ignorarne l'esistenza.

Rischio Cyber ed evoluzione normativa

Giorgio Grasso

Avv. BTG Legal
Socio ANRA

Il continuo aumento degli attacchi informatici ha spinto il Legislatore europeo ad emanare nuove norme che comportano – da un lato – una maggiore responsabilità dell'alto management (con potenziali impatti anche sulle coperture D&O) e – dall'altro – la necessità di una nuova cultura di risk management aziendale.

Stando alle statistiche, negli ultimi due anni i crimini informatici verso le aziende hanno registrato un incremento esponenziale rispetto al passato. L'utilizzo della tecnologia e l'iperconnettività hanno comportato un cambiamento epocale che ha condotto (o dovrebbe condurre) le imprese a dotarsi di meccanismi di corporate governance sempre più sofisticati, per tutelare non solo gli azionisti, ma anche tutti i soggetti che operano con l'azienda (fornitori, collaboratori, etc) ed il mercato medesimo.

La trasformazione digitale non è però stata accompagnata da un'adeguata consapevolezza e gestione dei rischi informatici, considerando vieppiù che le norme esistenti erano abbastanza frastagliate.

In tale contesto si inseriscono due recenti interventi del Legislatore europeo:

- il Regolamento DORA (Digital Operational Resilience Act) teso ad armonizzare e rafforzare la resilienza operativa dei soggetti che operano nei mercati finanziari (entrato in vigore lo scorso gennaio, ma che prevede un complesso periodo di attuazione di 24 mesi);
- la Direttiva NIS 2 – che sostituisce la precedente Direttiva NIS e prevede un termine di recepimento al 18 ottobre 2024 – volta ad introdurre nuovi obblighi in materia di cybersecurity e nuove categorie di destinatari.

Andiamo per ordine. La portata del Regolamento DORA è molto ampia e impatterà su quasi tutti gli operatori del settore finanziario. Si applicherà, infatti, non solo ad enti finanziari di stampo "tradizionale" (per esempio, banche, imprese di investimento, assicurazioni, grandi broker assicurativi), ma anche ai "nuovi attori" del mercato quali aziende di servizi di cripto-asset e fornitori critici di servizi ICT (es. fornitori di servizi cloud e web).

Saranno da tenere d'occhio altresì le Autorità europee di vigilanza

che dovranno elaborare specifici standard tecnici.

Il Regolamento DORA può essere sintetizzato in quattro pilastri principali:

i) Governance e organizzazione interna (Art. 5)

ii) Risk management (Artt. 6-16)

iii) Incident management e reporting (Artt. 17-23)

iv) Fornitori terzi di servizi ICT (Artt. 28-44)

In poche parole, il Legislatore non solo ha previsto l'obbligo per le entità finanziarie di dotarsi di una governance di cybersecurity interna e di un quadro di controllo tali da garantire una gestione efficace e prudente di tutti i rischi ICT (con conseguente maggiore esposizione in termini di responsabilità civile per gli amministratori), ma ha – inter alia – imposto a tali società di avviare un serio progetto di gestione del rischio cyber solido, completo e ben documentato (unito altresì a piani di reporting e piani di comunicazione nei confronti dei vari stakeholder). Quanto alla Direttiva NIS 2, va subito detto che essa, in sostituzione delle precedenti categorie di cui alla NIS 1, introduce – quale criterio di individuazione dei soggetti destinatari degli obblighi – la distinzione tra:

- "Soggetti Essenziali" (es. Settore energetico, Settore sanitario, Trasporti, Acque e acque di scarico, Infrastrutture digitali, Settore spaziale, etc.), e
- "Soggetti Importanti" (es. Settore postale e di spedizione, Gestione/Trattamento dei rifiuti, Settore chimico, Industrie tecnologiche e ingegneristiche, Servizi digitali, Ricerca scientifica, etc.)

con contestuale applicazione della regola del massimale dimensionale (c.d. " Size-cap ") come canone di accertamento della dimensione medio-grande delle imprese coinvolte.

Ciò premesso, è degno di nota l'approccio di rischio introdotto sottoforma di obbligo verso le imprese interessate, le quali sono chiamate ad implementare un adeguato processo di risk assessment per la gestione degli eventi cyber potenzialmente malevoli, sia interni che esterni.

La Direttiva indica una serie di misure tecniche e organizzative che i destinatari sono chiamati ad applicare (ad es. policy su analisi di rischio e information system; piano di incident response; piano di di Business Continuity e gestione delle crisi; formazione cyber; effettuazione di audit e test di cybersecurity; revisione contratti con i fornitori e service provider).

Infine, la NIS2 introduce novità anche sul fronte sanzionatorio prevedendo ammende tra i 7 e 10 milioni di euro (1,4% -2% del fatturato annuo). Di impatto, forse anche maggiore, la natura interdittiva che potranno assumere le sanzioni.

In conclusione, la nuova legislazione in materia di cybersecurity comporterà la necessità per i destinatari di svolgere una – non sempre agevole – attività di individuazione, mappatura e coordinamento degli obblighi e adempimenti previsti dalle varie fonti normative, nonché la necessità di interfacciarsi con diverse Autorità competenti.

Attività, quelle descritte, che devono procedere necessariamente di pari passo ad un costante awareness program, sia a livello dirigenziale che dell'intera popolazione aziendale. Accrescere la sensibilità verso tali tematiche è fondamentale per comprendere l'importanza di adottare un protocollo di gestione delle minacce cyber e farvi fronte in maniera efficace senza correre il rischio di non riconoscerle o di sottovalutarle.

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