SETTEMBRE 2024

IL CAFFÈ DIGITALE

THE INNOVATION GROUP
NEWSLETTER

AI, LA PREPARAZIONE
PRIMA DELL'UTILIZZO

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Marco Colloredo
Chief Operating Officer
Milano Serravalle

NUMERI E MERCATI

I PC si reinventano e seguono le tracce degli smartphone

DIRITTO ICT IN PILLOLE

Adeguamento AI Act: cosa sapere e cosa fare

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

AI, la preparazione prima dell'utilizzo

Roberto Bonino, Research and Content Manager
TIG

Note e spunti dal Cio Panel di Milano, organizzato da Tig e Cefriel e nel quale oltre trenta di manager tecnologici hanno discusso sulle strategie di implementazione dell'intelligenza artificiale nelle aziende.

Il Cio Panel di Milano, organizzato da Tig e Cefriel, si è concentrato sui principali aspetti che occorre affrontare per prepararsi a una più diffusa e strutturata adozione dell'AI nelle aziende. Il presupposto di partenza è che esista, non solo nell'It, una radicata consapevolezza dell'importanza dei dati come asset fondamentale e volano per il business delle aziende.

Tre sono stati i macrofiloni di discussione trattati dagli oltre trenta Cio (o figure assimilabili) intervenute all'evento milanese. Quello forse più basilare ha riguardato l'evoluzione dello stack tecnologico architetturale e applicativo legato all'adozione di soluzioni costruite sull'AI, soprattutto di tipo generativo. Il quadro di partenza ricavato dalle testimonianze delle aziende intervenute fa capire come oggi la strada maestra per introdurre sperimentazioni sia quella del Proof of Concept, ritenuto necessario per

Il Cio Panel di Milano, organizzato da Tig e Cefriel, si è concentrato sui principali aspetti che occorre affrontare per prepararsi a una più diffusa e strutturata adozione dell'AI nelle aziende.

costruire correttamente gli algoritmi, ma anche per creare conoscenze fra le persone che li dovranno utilizzare. Non si sono ancora fatti particolari investimenti dedicati e, pertanto, si tende a lavorare su quanto già tecnologicamente disponibile in azienda e a fare esplorazioni con le soluzioni di AI integrate nei sistemi It già presenti (Crm, piattaforme di automazione, Mes o altro).

Un secondo macrotema di confronto ha riguardato la governance dei dati e la definizione dei modelli operativi collegati agli sviluppi verso l'AI. Lo scenario di riferimento fa capo ad aziende dove oggi solo in parte largamente minoritaria sono presenti una vera e propria data strategy, un framework di governance completo, iniziative di diffusione di cultura sul dato e processi di continuous improvement. Nella maggior parte dei casi, è stato avviato il presidio solo di alcune delle dimensioni indicate. L'AI Act, di prossima entrata in vigore, dovrebbe dare un supporto in questa direzione, ma per ora il livello di conoscenza della normativa è ancora ritenuto basso e non ci sono nemmeno iniziative di breve termine per migliorare la situazione. In questo contesto, si percepisce come la governance sia un tema molto caldo e come l'AI stia generando nuove complessità, legate alla necessità di sincronizzare quanto già portato avanti negli sviluppi più tradizionali con quelli di nuova implementazione. Nelle aziende è ancora carente la consapevolezza tanto dei vantaggi quanto dei rischi soprattutto collegati a modelli e applicazioni di AI generativa

Infine, la terza macroarea di analisi ha riguardato lo stato dell'arte dei ruoli, degli skill e delle capability necessarie per sviluppare l'AI nelle aziende. Qui ilo panorama, per ora, vede la maggior parte delle aziende procedere con le sperimentazioni facendo leva sulle risorse interne già disponibili, semmai integrate da

collaborazioni esterne con fornitori, consulenti e anche università. Le nuove competenze sarebbero un desiderio di tutti, ma la loro individuazione sul mercato è complessa e anche i budget a disposizione spesso non aiutano. Certamente, gli intervenuti al Cio Panel di Milano hanno convenuto sulla necessità di accrescere le risorse in direzione della conoscenza e dell'integrazione nei processi aziendali, per saper meglio rispondere alle esigenze di business. Dal punto di vista tecnico, ai data scientist si affianca la domanda di gestire progetti e attuare il fine tuning dei modelli di AI. Tra le strade individuate come percorribili per migliorare la situazione, si possono citare la volontà di riqualificare persone senior che vogliano offrire un contributo tecnico e la formazione di data/AI steward da inserire nelle direzioni per garantire qualità del dato, compliance e altro.

Marco Colloredo, Chief Operating Officer, Milano Serravalle

Il digitale corre sulla Milano Serravalle

Roberto Bonino, Research and Content Manager
TIG

Nel complesso del sistema autostradale italiano, 187 km di tratta possono sembrare pochi. Questa è la lunghezza totale gestita dalla società Milano Serravalle – Milano Tangenziali. Come, tuttavia, suggerito dal nome, rientrano sotto la responsabilità della concessionaria non solo il tratto della A7 che parte dal capoluogo lombardo e arriva a Serravalle Scrivia, ma soprattutto le tre tangenziali di Milano, dove si stima che mediamente ogni giorno transitino circa 160mila veicoli.

Le principali incombenze di una concessionaria spaziano dal monitoraggio costante di tutti i percorsi viari alla gestione degli interventi di manutenzione, da un'attenzione agli automobilisti che non può che passare dalla miglior gestione possibile dei flussi di traffico alla qualità del lavoro di chi opera sul campo. Di fatto, in tutti questi processi, oggi, c'è un significativo contributo della tecnologia, nel contesto di un cambiamento culturale più complessivo che negli ultimi anni sta orientando le scelte in direzione del miglioramento tanto dei servizi all'utenza quanto dell'ambiente operativo dei dipendenti.

Dell'apporto che l'innovazione digitale sta offrendo al percorso evolutivo di Milano Serravalle, abbiamo parlato con il chief operating officer Marco Colloredo.

Quali sono le aree dove il contributo della tecnologia si è già consolidata e dove, invece, si notano i più significativi cambiamenti in atto in questo periodo?

Lo scenario complessivo è certamente in evoluzione, ma certamente possiamo considerare più mature attività come la gestione dei pedaggi e quanto direttamente collegato alla strada, ivi compresa la rilevazione della velocità dei veicoli. La tecnologia sta supportando un percorso di semplificazione dei processi aziendali e delle attività operative. Uno degli obiettivi fondamentali del processo di digitalizzazione di Milano Serravalle riguarda la possibilità di integrare le informazioni sulla viabilità con quelle che hanno a che fare con l'asset management stradale, in modo tale da ottenere analisi preventive sull'impatto degli interventi da effettuare e potendo quindi programmarle in momenti a minor impatto. In futuro, vorremmo

riuscire a produrre anche analisi di tipo predittivo.

Quali sfide stanno connotando il vostro percorso di innovazione?

Ci siamo inizialmente concentrati su sistemi che rilevano dati in maniera statica da apparecchiature come radar, fibra ottica o sensori. Ma occorreva prendere in considerazione anche la componente dinamica rappresentata dalle squadre di intervento sulla viabilità, che si trattasse di persone impegnate nella manutenzione vera e propria oppure dedicate al monitoraggio. Per questo. le evoluzioni più recenti sono andate in direzione della possibilità di digitalizzare queste attività, in modo tale che le persone siano in grado di fornire ulteriori dati da convogliare all'interno dell'ecosistema principale. In precedenza, tutto avveniva attraverso documenti cartacei o comunicazioni via radio registrate, mentre la nostra idea evolutiva era di eliminare completamente la carta e trasformare tutto in un sistema digitalizzato che potesse permettere anche una gestione più omogenea dei dati e una loro catalogazione univoca. Abbiamo così proceduto alla catalogazione di tutte le tipologie di interventi, poi inserendole all'interno di un database che i tecnici possono consultare per descrivere in modo standardizzato ogni lavoro svolto, le ragioni che lo hanno reso necessario e lo stato di avanzamento. Oltre ad aver sostituito processi cartacei con omologhi digitali, abbiamo potuto integrare le informazioni all'interno del sistema di gestione del traffico e anche dell'applicazione che si occupa di definire turni e programmazione del lavoro degli operatori.

Come siete organizzati nell'ideazione e successiva implementazione dei vostri progetti di innovazione?

La struttura delle operations che presiedo coordina l'attività di diverse direzioni come quella tecnica, di esercizio e anche l'innovazione. Non abbiamo la figura del Cio, ma un direttore che presiede l'information technology strettamente collegata agli impianti. Il modello che si pone alla base della gestione dei dati descritta in precedenza è stato creato da me e condiviso con le mie persone e con quelle direttamente coinvolte dal punto di vista operativo. Per fortuna, esiste anche un'ampia delega sulle impostazioni, sulle scelte e sulla definizione degli obiettivi, mentre il management condivide con noi i macro-obiettivi, che possono riguardare il raggiungimento dell'efficienza o il processo di digitalizzazione.

Quali sono gli sviluppi sui quali ora state lavorando?

Stiamo concentrando l'attenzione sui sistemi di rilevazione del traffico, con l'implementazione di sistemi a videocamera per la rilevazione delle targhe, utili per determinare così i flussi effettivi di traffico in termini di numero di veicoli, tipologie, velocità media e così via. In parallelo, abbiamo avviato un progetto sperimentale per la rilevazione del numero di veicoli e delle velocità basata sulle vibrazioni della fibra ottica posizionata sulla strada. Il processo di digitalizzazione segue di pari passo questi sviluppi.

Adeguamento AI Act: cosa sapere e cosa fare

Paola Meroni, Global Privacy Manager
Whirlpool Corporation

Il 21 Maggio 2024 il Consiglio Europeo ha formalmente approvato l'EU AI Act, il regolamento europeo sull'Intelligenza Artificiale, che rappresenta un fondamentale precedente normativo, non solo in Europa ma anche a livello globale, nella regolamentazione delle tecnologie basate sull'AI.

L'EU AI Act ha come obiettivo quello di assicurare lo sviluppo, l'uso e l'adozione di soluzioni tecnologiche di Intelligenza Artificiale che possano attivare il potenziale di trasformazione digitale in tutte le regioni dell'Unione ma, allo stesso tempo, possano essere considerate sicure, affidabili, trasparenti, etiche e antropocentriche, in grado di garantire la protezione di interessi pubblici come la salute, la sicurezza e la tutela dei diritti fondamentali come democrazia, Stato di diritto e protezione dell'ambiente.

L'EU AI Act fa parte di un ampio framework regolatorio europeo, come GDPR, NIS2 Directive, Digital Services Act e Digital Markets Act, caratterizzati da un comune approccio risk-based. In questa breve trattazione, proveremo a ripercorrere insieme le tappe fondamentali nell'approvazione della normativa, a descriverne i punti chiave e a delinearne gli impatti operativi sulla governance e sul business delle aziende di oggi e di domani.

EU AI Act: iter approvativo e applicazione

L'EU AI Act o Regolamento 1689/2024 è stato proposto per la prima volta nell'aprile 2021. Una lunga serie di confronti negoziali ha portato al raggiungimento di un accordo politico sul testo nel dicembre del 2023. Il 13 marzo 2024 il Parlamento europeo ha approvato in via definitiva il Regolamento Europeo sull'Intelligenza Artificiale, mentre 21 maggio 2024 l'EU AI Act è stato formalmente approvato dal Consiglio d'Europa, che ne ha sancito l'adozione ufficiale.

Il 12 luglio 2024 il testo finale dell'EU AI Act è stato pubblicato sull'Official Journal dell'Unione Europea ed è entrato in vigore 20 giorni dopo la sua pubblicazione, quindi il 1° agosto 2024. L'applicazione della normativa avverrà a partire dal 2 agosto 2026: nel frattempo verrà adottato un approccio "a fasi": da evidenziare, ad esempio, che il divieto di adozione di soluzioni basate AI che comportino rischi "inaccettabili" sarà applicato già 6 mesi dopo l'entrata in vigore della normativa, quindi dal 2 febbraio 2025.

Sistema sanzionatorio

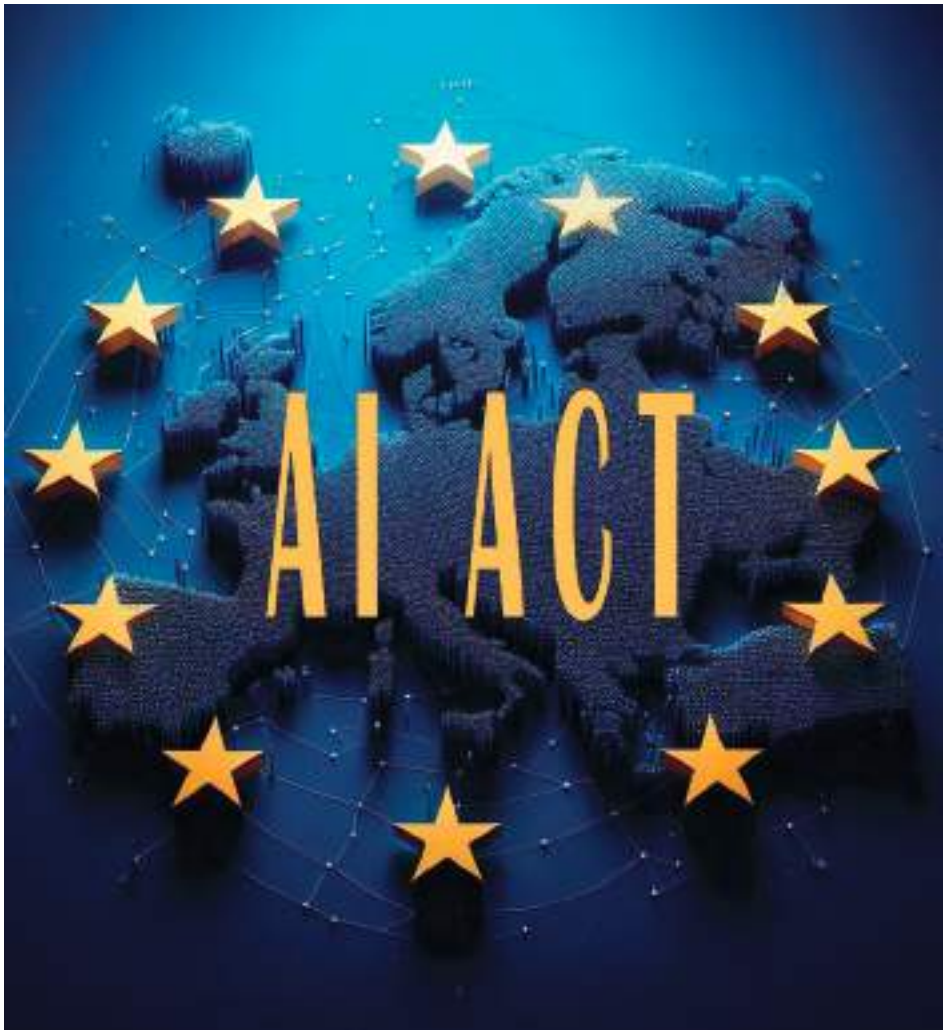
Il sistema sanzionatorio previsto dall'EU AI Act è piuttosto severo: la non conformità al divieto delle pratiche di AI (articolo 5) prevede sanzioni amministrative pecuniarie fino a 35.000.000 di euro o, se l'autore del reato è un'impresa, fino

al 7% del fatturato mondiale totale annuo dell'esercizio precedente, mentre la non conformità alle disposizioni diverse da quanto riportato all'articolo 5 prevedono sanzioni amministrative pecuniarie fino a 15.000.000 di euro o, se l'autore del reato è un'impresa, fino al 3% del fatturato mondiale totale annuo dell'esercizio precedente.

Un po' di terminologia

Secondo l'AI Act, un "AI system" può essere definito come "un sistema automatizzato progettato per funzionare con livelli di autonomia variabili e che può presentare adattabilità dopo la diffusione e che, per obiettivi espliciti o impliciti, deduce dall'input che riceve come generare output quali previsioni, contenuti, raccomandazioni o decisioni che possono influenzare ambienti fisici o virtuali"; in questa definizione rientrano tecniche chiaramente riconducibili all'AI, come deep learning, machine learning, computer vision, natural language processing, reti neurali etc. Va sottolineato che AI Act non si focalizza su sistemi che si basano su software tradizionale, il cui comportamento è fondato sull'applicazione di regole, o genericamente su automatismi per il "decision making" (così come già specificato dal GDPR): il fattore differenziante tra AI e qualunque altra tecnologia è la "capacità inferenziale", cioè riferita al processo di ottenimento degli output e alla capacità dei sistemi di AI di ricavare modelli o algoritmi, o entrambi, da input o dati.

Va inoltre tenuta in considerazione la distinzione tra la definizione di un sistema AI e quella di modello. I modelli, infatti, sono considerati dal Regolamento come componenti essenziali dei sistemi AI ma non possono isolatamente generare output ed essere di per sé considerati come sistemi AI. L'EU AI Act fornisce, comunque, la definizione



di modello general-purpose come riferita alla presenza della "generalità e capacità di svolgere con competenza un'ampia gamma di compiti distinti".

A chi si applica l'EU AI Act

L'EU AI Act si applica ai seguenti operatori nella value chain dell'AI:

Fornitori. Rientrano nell'ambito di applicabilità dell'EU AI Act i fornitori che hanno sviluppato un sistema AI o un modello general-purpose (o lo hanno fatto sviluppare), o lo hanno messo in servizio con il proprio nome o marchio. Tali fornitori sono stabiliti sul territorio dell'Unione o in un paese terzo ma con output dell'AI reso disponibile nell'Unione Europea.

Deployer. I deployer sono persone fisiche o giuridiche, compresi un'autorità pubblica, un'agenzia o un altro organismo, che utilizzano un sistema di AI sotto la propria autorità, ad eccezione del caso in cui il sistema di AI sia utilizzato nel corso di un'attività personale non professionale. I deployer possono avere il loro stabilimento o essere situati all'interno dell'Unione ma sono comunque in scope anche se gli output prodotti dai loro sistemi sono resi disponibili nell'Unione Europea. Gli utilizzatori individuali di sistemi AI, in una logica business-to-consumer, non sono considerati come deployers.

Importatori. Gli importatori hanno il loro stabilimento o sono situati nell'Unione Europea ma mettono sul mercato dell'UE sistemi di intelligenza artificiale che recano il nome o il marchio di persone fisiche o giuridiche con sede in paesi terzi.

Distributori. Questi soggetti rendono i sistemi AI disponibili all'interno dell'Unione Europea come

azione successiva all'importazione.

Produttori. I produttori immettono sul mercato o mettono in servizio un sistema di AI insieme al loro prodotto e con il loro nome o marchio.

Rappresentanti autorizzati. I rappresentanti autorizzati sono stabiliti nell'Unione Europea in rappresentanza di fornitori che sono stabiliti fuori dal territorio europeo.

Un approccio centrato sul rischio

Come si è detto, l'AI Act è basato su un approccio "risk-based" che ritroviamo in molte altre normative, in primis nel GDPR: maggiore è il rischio associato ad una determinata soluzione basata sull'adozione di AI, più rilevanti saranno, ovviamente, le responsabilità in carico agli sviluppatori e agli utilizzatori di quella soluzione. L'AI Act identifica diversi tipi di AI a seconda dei livelli di rischio che ciascuno presenta, in particolare:

- Sistemi AI proibiti, in quanto, per loro natura, presentano un livello di rischio inaccettabile
- Sistemi AI ad alto rischio
- Sistemi AI che presentano rischi relativi alla trasparenza
- Modelli AI che presentano rischi sistemici
- Altri tipi di AI che non rientrano nelle precedenti categorie

Sistemi AI vietati

L'articolo 5 della normativa elenca in modo esauriente le pratiche AI considerate inaccettabili in quanto possono costituire una minaccia per i diritti dei cittadini europei, tra cui:

- sistemi utilizzati per social scoring o basate su tecniche subliminali
- sistemi utilizzati per fini investigativi che prevedano la colpevolezza, o la probabilità che un reato venga commesso, esclusivamente basandosi sulla profilazione fisica o psicologica di un soggetto
- sistemi utilizzati per la raccolta non mirata di immagini facciali da Internet o da filmati CCTV per creare o ampliare database di riconoscimento facciale
- sistemi di riconoscimento delle emozioni sul posto di lavoro e nelle scuole
- sistemi di classificazione biometrica per trarre deduzioni o inferenze in merito a razza, opinioni politiche, appartenenza sindacale, convinzioni religiose o filosofiche, vita sessuale o orientamento sessuale;
- sistemi di identificazione biometrica remota in tempo reale in spazi accessibili al pubblico, ad eccezione del caso in cui vengano utilizzati dalle forze dell'ordine nel corso di specifiche attività investigative o per perseguire reati di particolare gravità che mettano a repentaglio l'incolumità di singoli individui o della collettività.

Sistemi ad alto rischio

I sistemi AI ad alto rischio costituiscono il focus principale del Regolamento. Perché' un sistema AI venga classificato ad alto rischio secondo l'AI Act, questo dovrà:

- essere utilizzato come componente di sicurezza di un prodotto o essere esso stesso un prodotto, soggetto quindi a una valutazione della conformità da parte di terzi ai fini dell'immissione sul mercato o della messa in servizio

oppure

- essere menzionato nell'Annex III, che include i sistemi biometrici, i sistemi utilizzati nel settore delle infrastrutture critiche, dell'istruzione e formazione professionale, della gestione

I sistemi AI ad alto rischio costituiscono il focus principale del Regolamento.

dei lavoratori e per l'accesso al lavoro autonomo, dell'accesso a servizi e a prestazioni pubblici o privati essenziali, dell'attività di contrasto al crimine, della migrazione, asilo e gestione del controllo delle frontiere, dell'amministrazione della giustizia e dei processi democratici.

Eccezioni a queste due condizioni sono contenute nell'articolo 6 (3). La normativa prevede che il provider di una soluzione di AI adotti un sistema per la gestione dei rischi durante il ciclo di vita dell'AI, che offra garanzie di trasparenza, di adeguata qualità dei dati, di robustezza del sistema in termini di protezione da violazioni e minacce cyber e che produca documentazione tecnica in grado di fornire tutte le informazioni necessarie alle autorità per valutare la conformità dei sistemi di AI a tali requisiti. I deployer dovranno essere informati e formati sull'uso del sistema.

Sistemi che presentano rischi relativi alla trasparenza

L'articolo 50 stabilisce obblighi per fornitori e deployer di sistemi il cui utilizzo può comportare rischi in termini di trasparenza, come i sistemi AI che interagiscono direttamente con gli utenti fisici o i sistemi AI che generano contenuti audio, immagine, video o testuali sintetici: in questa

categoria rientrano anche i sistemi di riconoscimento delle emozioni, di categorizzazione biometrica (utilizzati per accertare, prevenire o indagare reati), di generazione o manipolazione di immagini o contenuti audio o video che costituiscono un «deep fake», e, infine, di generazione o manipolazione di testo pubblicato allo scopo di informare il pubblico su questioni di interesse pubblico. In tutti questi casi i sistemi devono essere sviluppati in modo da informare gli utilizzatori del fatto che stanno interagendo o stanno venendo in contatto con contenuti prodotti da AI.

Modelli AI per finalità generali e modelli con rischi sistemici

Questi due tipi di modelli sono descritti nel capitolo V del Regolamento. Un sistema AI per finalità generali ("general purpose") è caratterizzato dall'essere fondato su modelli AI per finalità generali, cioè in grado di servire a vari scopi (direttamente o integrati in altri sistemi AI). Tali modelli sono solitamente addestrati su grandi quantità di dati con diversi metodi, come l'apprendimento auto-supervisionato, non supervisionato o per rinforzo. Un addestramento basato su una grande quantità di dati, con la presenza di almeno un miliardo di parametri, viene considerato come criterio che definisce un modello per finalità generali.

Un sottoinsieme dei modelli AI per finalità generali è costituito dai modelli con rischio sistemico, nel caso in cui questi presentino impatto elevato (o sulla base di una decisione presa dalla Commissione "ex officio" o a seguito di una segnalazione di un gruppo di esperti scientifici). Si intende che un modello di AI per finalità generali abbia capacità di impatto elevato quando la quantità cumulativa di calcolo utilizzata per il suo addestramento, misurata in operazioni in virgola mobile, è superiore a 1025. In questo caso i fornitori dovranno anche effettuare valutazioni atte ad individuare e attenuare il rischio sistemico, documentare e notificare incidenti gravi e garantire elevati standard di cybersicurezza sul modello e sulla sua infrastruttura.

Uno dei principali aspetti operativi che l'azienda dovrà gestire per intraprendere il percorso di adeguamento all'EU AI Act sarà proprio la sistematica classificazione dei sistemi AI sviluppati e/o messi in esercizio, in modo da garantire l'appropriata gestione dei rischi correlati e l'implementazione delle misure tecniche e organizzative necessarie per la mitigazione degli stessi. Qui di seguito forniamo, inoltre, un esempio di supporto operativo all'adeguamento all'AI Act pubblicato dall'IAPP (International Association of Privacy Professionals) basato sulla classificazione dei sistemi AI appena descritta: https://iapp.org/media/pdf/resource_center/eu_ai_act_compliance_matrix_at_a_glance.pdf

La necessaria Governance dell'AI

Le soluzioni basate su Intelligenza Artificiale sono destinate a diffondersi in maniera sempre più integrata e pervasiva nel business delle aziende, così come sempre più acceso si sta facendo il dibattito normativo e regolamentare a livello mondiale su questo tema.

Si rende quindi necessaria una Governance dell'AI, cioè un sistema

di regole, pratiche, processi e strumenti tecnologici usati in modo da assicurare che l'adozione di tecnologie di AI sia aderente alle strategie, agli obiettivi e ai valori dell'organizzazione e, allo stesso tempo, tali da garantire un utilizzo dell'AI etico, responsabile, preciso, affidabile.

Gestione del rischio e data governance

A fronte dello sviluppo velocissimo dell'AI e dei nuovi rischi posti da questa tecnologia, l'adozione di un approccio risk-centrico nella gestione dello sviluppo e dell'utilizzo dell'AI diventa cruciale, in particolare in termini di visione integrata del rischio nelle aree maggiormente investite dall'introduzione di soluzioni basate su AI: marketing, legal/privacy, IT, procurement, IT, R&D, BI.

L'adozione di soluzioni basate su AI all'interno dell'organizzazione esige necessariamente una rivalutazione dell'efficienza dei processi di gestione del rischio già presenti, o la loro introduzione, nel caso fossero addirittura assenti. I rischi, ad esempio, di output non corretti, divergenti rispetto agli obiettivi aziendali, influenzati da bias o discriminatori, non trasparenti/non intelligibili (per fare solo alcuni esempi), in aggiunta ai molteplici rischi tradizionalmente associati al trattamento massivo di grandi quantità di dati personali (data breach, cyber attacks) ma con specifiche declinazioni per gli ambienti AI, solo per limitarci all'ambito Compliance o Cybersecurity, dovranno essere identificati, valutati e monitorati in maniera rigorosa: una gestione responsabile ed efficace del rischio, infatti, costituisce prova evidente dell'accountability nell'utilizzo e sviluppo di soluzioni AI da parte di una organizzazione e nello stabilire un rapporto di fiducia con autorità, fornitori, clienti, partner commerciali e consumatori finali.

Inoltre, una efficace gestione del rischio non può prescindere da una Data Governance in grado di garantire il controllo dei dati aziendali in termini di compliance legale, aderenza agli standard e alle policy interne, nel rispetto di ben identificati ruoli e responsabilità. Una scarsa qualità dei dati o una scarsa visibilità della relazione tra dati e algoritmi può condurre a risultati distorti o inattendibili, con serie ripercussioni sul corretto sviluppo delle soluzioni AI in azienda.

Principi minimi per lo sviluppo o l'utilizzo di sistemi basati su AI

Di seguito riportiamo brevemente alcuni tra i principi minimi fondamentali per lo sviluppo e l'utilizzo di soluzioni AI etico, sicuro e compliant a normative rigorose come l'AI Act:

- Trasparenza e tracciabilità: le logiche che sottendono la produzione di un output devono essere note ad utenti e soggetti coinvolti nello sviluppo, implementazione e utilizzo dell'AI. Il trattamento dei dati personali deve essere chiaro agli utenti, così come i rischi relativi a possibili inaccuratezze. La tracciabilità degli output, in particolare del modo in cui sono stati generati, è fondamentale per garantire agli utenti la possibilità di ricostruire l'esito dei processi di decision making e per finalità di audit.
- Fairness e accuratezza

dell'output: i dati prodotti dall'AI devono essere corretti, affidabili, non affetti da bias, in modo da prevenire effetti discriminatori o comunque impatti negativi sui diritti e le libertà dei soggetti. Il controllo accurato sui dati utilizzati per il training dei sistemi AI è fondamentale per garantire questo principio.

- Accountability: le organizzazioni che operano in ambito AI devono garantire una precisa attribuzione di responsabilità per azioni, decisioni e outcome prodotti dai sistemi AI.
- Data minimization: principio di base della privacy sempre valido, finalizzato a garantire che i dati raccolti e trattati dall'AI siano ridotti allo stretto necessario per gli scopi dichiarati nell'erogazione del servizio e in accordo ai consensi rilasciati.
- Privacy & security by design: rigorosi controlli di sicurezza e privacy devono essere previsti sin dalle primissime fasi di design di una soluzione basata su AI.
- Supply chain: opportune clausole contrattuali dovranno essere previste con i fornitori di soluzioni AI che garantiscano, tra l'altro, la presenza di un processo di gestione dei rischi da parte del fornitore e l'adozione di adeguate misure per la cybersicurezza, e assicurino accuratezza e affidabilità dei modelli forniti.
- Formazione: formazione e informazione sono necessarie per tutti i soggetti coinvolti nell'ecosistema AI (dagli sviluppatori di sistemi AI agli utilizzatori). All'interno di ogni organizzazione che utilizzi soluzioni AI per migliorare l'operatività aziendale, ad esempio, dovranno essere condotte opportune attività di training in modo da consentire un utilizzo dell'AI responsabile e consapevole dei rischi che queste tecnologie possono comportare per i dati aziendali (dai dati personali alla proprietà intellettuale).

Suggeriamo, come utile lettura, tra i moltissimi framework, self-assessment e documentazione disponibili in rete, l'assessment ALTAI (Assessment List for Trustworthy Artificial Intelligence – ALTAI), che propone una possibile metodologia per verificare l'aderenza della propria soluzione AI ai principi generali per una AI affidabile, secondo le linee guida dell'European Commission: https://digital-strategy.ec.europa.eu/it/node/806.

Modelli di Governance dell'AI

Non esiste un unico approccio per implementare una Governance dell'AI in maniera efficace, che consenta alle organizzazioni di garantire la propria compliance all'EU AI Act, e, in linea generale, di assicurare uno sviluppo sano e profittevole del proprio business avvalendosi o fornendo tecnologie basate su AI. È possibile, ad esempio, creare una struttura di Governance specifica per l'AI, oppure modificare le strutture già presenti in modo che possano integrare la gestione dei rischi e dei controlli necessari per governare le tecnologie AI. In ogni caso, è necessario considerare che l'introduzione di tecnologie basate su AI implica la necessità di intervenire non solo sulle strutture organizzative, ma conseguentemente anche su processi, policy, procedure, contratti, informative, consensi, audit interni, assessment di sicurezza, compliance e privacy ecc., in maniera trasversale all'organizzazione.

La costituzione di un comitato costituito dal management e dai professionisti delle tecnologie, dell'area legale, privacy, security, R&D, che collabori in maniera sinergica con le unità di business, può rappresentare un approccio operativamente efficace per la gestione armonica, efficace e non frammentata del complesso ecosistema che si genera attorno all'AI. Va sottolineato, infine, quanto la scelta di adottare una soluzione basata su AI non si riduca semplicemente ad una decisione di carattere tecnologico o di business: l'AI necessariamente sollecita le aziende di oggi, e sempre di più quelle del futuro, a stabilire e a mantenere allineati i propri obiettivi di business con un uso eticamente sostenibile di questa potente tecnologia, nel rispetto dei diritti fondamentali degli individui e in compliance con le normative emergenti, di cui l'AI EU Act è uno dei più autorevoli esempi.

I Pc si reinventano e seguono le tracce degli smartphone

Valentina Bernocco, Web and Content Editor
TIG

E' dello scorso dicembre il documento congiunto dell'Agenzia per la cybersicurezza nazionale (ACN) e del Garante per la protezione dei dati personali relativo alle linee guida in materia di conservazione delle password. Dalla collaborazione tra le due autorità nascono importanti indicazioni rispetto alle misure tecniche da adottare per accrescere il livello di sicurezza sia dei providers di servizi digitali che delle software house.

In risposta all'esponenziale moltiplicazione delle minacce e dei data breach ai danni di imprese ed enti pubblici sempre più spesso connesse alle inefficaci, scarse o inesistenti modalità di protezione delle password di accesso, le Autorità citate hanno messo a fattor comune le reciproche competenze sul tema fornendo informazioni concrete per innalzare e migliorare le misure di sicurezza digitale.

Obiettivo principale delle Linee Guida è quello di prevenire e scongiurare il rischio di violazione delle credenziali di autenticazione che – come insegnano i recenti fatti di cronaca – possano essere

È cominciata una nuova primavera per gli AI Pc, cioè i computer ottimizzati con e per l'intelligenza artificiale, dispositivi dotati di unità di calcolo neurale, o Npu (Neural Processing Unit), un acceleratore hardware che esegue "ragionamenti" simulando il funzionamento di una rete neurale

Un nuovo slancio, ancora una volta. Dopo il boom di domanda del biennio 2020-2021, trainato dalle nuove necessità dello smart working e della didattica a distanza, il mercato dei personal computer aveva subìto una battuta d'arresto, un po' per colpa delle incertezze dell'economia che hanno accomunato Europa, Stati Uniti e Cina (e che certo non hanno invogliato consumatori a fare acquisti di beni voluttuari né le aziende a pianificare investimenti evitabili) e un po' perché quella domanda conseguente alla pandemia era ormai saturata.

Ora però è cominciata una nuova primavera per i Pc, o meglio per gli AI Pc, cioè i computer ottimizzati con e per l'intelligenza artificiale. Tecnicamente, secondo la definizione di Gartner, un AI Pc è un dispositivo dotato di unità di calcolo neurale, o Npu (Neural Processing Unit), cioè un acceleratore hardware che esegue "ragionamenti" simulando il funzionamento di una rete neurale. Microsoft aggiunge alle caratteristiche fondanti anche la presenza di funzioni software di intelligenza artificiale generativa, come quelle del Copilot di Windows, che assiste l'utente in attività di scrittura, ricerca di informazioni, creazione di contenuti, traduzioni simultanee e altro ancora.

Ma un AI Pc, per poter supportare le operazioni di machine learning (appoggiate al cloud e anche in locale) è anche dotato di Cpu e Gpu di ultima generazione e di Ram generose, tutte caratteristiche hardware che lo rendono costoso. Così è stato, almeno, in un primo momento. Ora gli AI Pc stanno uscendo dalla nicchia premium in cui hanno debuttato, anche se ci vorranno ancora un paio di anni prima che diventino il nuovo standard. Si ripeterà, a grandi linee, la dinamica già vissuta nel mercato della telefonia mobile, dove gli smartphone si sono affermati soppiantando gradualmente i "normali" telefoni cellulari e i feature phone con l'allargarsi dell'offerta e della segmentazione di prezzo.

Che questo possa essere anche il destino degli AI Pc è suggerito da vari segnali. Innanzitutto, pur nella varietà dei punti di vista sull'intelligenza artificiale generativa, è quasi unanime il giudizio sulla natura non effimera di questa rivoluzione, che superato l'hype attuale si consoliderà e fonderà con altre tecnologie. Dunque anche i Pc, in quanto primario strumento di lavoro per centinaia di milioni di professionisti in tutto il globo, dovranno inserirsi nell'onda di trasformazione innescata dalla GenAI: in sostanza, dovranno garantire un'esperienza d'uso soddisfacente per tutta una costellazione di applicazioni, da ChatGpt in poi, dall'interrogazione di database alla creazione di contenuti.

Altri segnali sul probabile destino mainstream degli AI Pc ci giungono dagli analisti. All'inizio dell'anno Gartner aveva previsto per gli AI Pc una quota del 22% sul totale dei personal computer commercializzati in tutto il 2024. Ora è la stessa società di ricerca a ridimensionare la stima: la percentuale effettiva sarà, probabilmente, un 17%. Ma da qui in poi si accelera. Complici il rinnovo delle offerte dei principali vendor (Lenovo, Hp, Dell, Acer, Asus, Apple) e il fine vita di molti dispositivi acquistati nel biennio 2020-21, secondo Gartner nel 2025 la quota degli AI Pc salirà al 43%, per un volume di circa 114,2 milioni di unità commercializzate (di cui 102,4 milioni di portatili e 11,8 milioni di sistemi desktop). Canalys, altro autorevole osservatore del mercato, ha fatto previsioni abbastanza sovrapponibili: una quota di AI Pc pari al 19% delle vendite totali di computer del 2024, e che salirà al 37% l'anno prossimo, al 53% nel 2026 e al 60% nel 2027. I numeri cambiano leggermente, ma la sostanza resta la stessa. "La discussione si è spostata dallo speculare su quali Pc potessero includere funzionalità di AI all'attesa che la maggior parte dei Pc, prima o poi, arrivi a integrare capacità di intelligenza artificiale su Npu", ha commentato Ranjit Atwal, senior director analyst di Gartner. "Di fatto, la Npu diventerà una caratteristica standard per i produttori di Pc".

L'estate della Cybersicurezza: come si evolve la normativa europea e l'impatto su enti ed imprese

Valentina Frediani, General Manager
Colin & Partners

Il 2024 si sta confermando l'anno della sicurezza informatica: l'inarrestabile digitalizzazione delle attività ha ampliato in maniera significativa fenomeni di cyber attacchi ai danni di aziende ed Enti

Gli ultimi mesi hanno visto una significativa proliferazione di norme in materia di cybersicurezza. Il 2024 si sta infatti confermando l'anno della sicurezza informatica: l'inarrestabile digitalizzazione delle attività sia in termini di servizi che di settori ha ampliato in maniera significativa fenomeni di cyber attacchi ai danni di aziende ed Enti. Ragione questa che ha imposto alle autorità di dare un impulso decisivo alla regolamentazione del settore con l'introduzione di misure organizzative e di sicurezza tali da garantire il rafforzamento del perimetro di protezione. Una serie di provvedimenti, quelli che hanno visto la luce nelle ultime settimane, accomunati dalla logica secondo cui i possibili rischi connessi alla digitalizzazione devono essere gestiti in ottica di security by design, adottando un approccio multidisciplinare e una visione d'insieme tali da consentire di beneficiare degli indiscutibili vantaggi connessi alle nuove tecnologie e di mitigarne le criticità.

Ma vediamo nella pratica quali sono state le disposizioni normative protagoniste dell'estate.

Prima tra tutti, in ordine di importanza e di impatto, l'attesissima NIS2 che in qualità di Direttiva entrerà in vigore il prossimo 17 ottobre. Ma non solo. Gli ultimi mesi hanno visto anche l'emanazione del provvedimento dell'ACN e Garante Privacy in materia di crittografia delle credenziali e quello del Garante sulla conservazione dei metadati delle e-mail dei dipendenti.

Non ultima la legge pubblicata in Gazzetta Ufficiale lo scorso 28 giugno recante "Disposizioni in materia di rafforzamento della cybersicurezza nazionale e di reati informatici", in vigore dal 17 luglio. E su questa concentreremo la nostra attenzione per non correre il rischio che una normativa da un impatto così significativo possa passare in sordina.

I 24 articoli della versione finale della cosiddetta "Legge sulla Cybersicurezza" contengono una serie di misure destinate al «rafforzamento della cybersicurezza nazionale, resilienza delle pubbliche amministrazioni, personale e funzionamento dell'Agenzia per la

cybersicurezza nazionale, nonché di contratti pubblici di beni e servizi informatici impiegati in un contesto connesso alla tutela degli interessi nazionali strategici», confermando il grande impegno delle autorità – in un momento storico di grande fermento sul fronte della cyber sicurezza – nell'innalzamento del livello di protezione dei sistemi informativi delle organizzazioni, soprattutto pubbliche, attive nel mercato tecnologico e digitale e della resilienza rispetto ai cyber attacchi.

Sul piano operativo, la Legge 90 si muove in varie direzioni, annunciando l'introduzione di nuovi reati, un impianto sanzionatorio di notevole impatto, un focus specifico sul tema dei contratti pubblici di beni e servizi informatici e rilevanti prescrizioni per i soggetti pubblici (principali destinatari delle disposizioni) tra cui l'introduzione – per i soggetti previsti – della figura del Referente per la cibersicurezza. Tale soggetto interverrà a titolo esemplificativo sullo sviluppo delle politiche e le procedure di cybersicurezza interne all'Ente, sulla produzione e l'aggiornamento di sistemi di analisi preventiva di rilevamento e di un piano per la gestione del rischio informatico e sulla produzione e aggiornamento di un piano programmatico per la sicurezza dei dati.

Per quanto concerne l'ambito di applicazione, il provvedimento si rivolge alle pubbliche amministrazioni individuate dalla norma, ai soggetti considerati nel Perimetro di Sicurezza Nazionale Cibernetica, fino a quelli sottoposti alla Direttiva NIS2, comprese le autorità più significative del settore della cybersicurezza, quali il CISR, gli Organismi di Informazione per la Sicurezza, l'ACN e il suo Nucleo per la Cybersicurezza.

Tra i soggetti pubblici destinatari, a titolo esemplificativo sono ricomprese:

- le pubbliche amministrazioni centrali incluse nell'elenco annuale ISTAT delle pubbliche amministrazioni previsto dall'articolo 1, comma 3, della legge di contabilità e finanza pubblica (legge n. 196 del 2009);
- le regioni e le province autonome di Trento e di Bolzano;
- le città metropolitane;

- i comuni con popolazione superiore a 100.000 abitanti;
- i comuni capoluoghi di regione;
- le società di trasporto pubblico urbano con bacino di utenza non inferiore a 100.000 abitanti;
- le società di trasporto pubblico extraurbano operanti nell'ambito delle città metropolitane;
- le aziende sanitarie locali;
- le società in house degli enti fin qui richiamati, qualora siano fornitrici di servizi informatici, dei servizi di trasporto sopra indicati, dei servizi di raccolta, smaltimento o trattamento di acque reflue urbane, domestiche o industriali, ovvero servizi di gestione dei rifiuti.

Da una prima lettura potrebbe sembrare che la legge 90 sia in sovrapposizione o ridondante rispetto alla NIS2. Basti pensare ai soggetti destinatari piuttosto che a disposizioni specifiche come l'obbligo di notifica degli incidenti. Tuttavia, le due cornici normative devono essere lette come due impianti distinti con finalità differenti, nonostante vi siano evidenti aspetti di continuità e vicinanza.

La differenza principale dei due provvedimenti risiede nella ratio che li definisce. La legge 90 obbliga infatti a fare le notifiche in ottica di monitoraggio dell'andamento, delle vulnerabilità e delle minacce per consentire all'autorità di intervenire e di creare una strategia. La NIS2, pur consentendo di raccogliere informazioni al CSIRT, si rivela invece molto più operativa: gap analysis, prevenzione, procedure, supply chain, formazione. La notifica di un incidente, inoltre, nel caso della NIS2, riguarda la continuità operativa, più che il tema del monitoraggio e analisi degli attacchi.

La Legge 90 non introduce degli obblighi rispetto alle misure, come avviene nella NIS2, ma prevede degli obblighi di monitoraggio e rilevazione per enti e PA che gestiscono dati di interesse comune. Per la reiterata inosservanza dell'obbligo di segnalazione il provvedimento prevede ispezioni e possibili sanzioni da 25 a 125.000 euro.

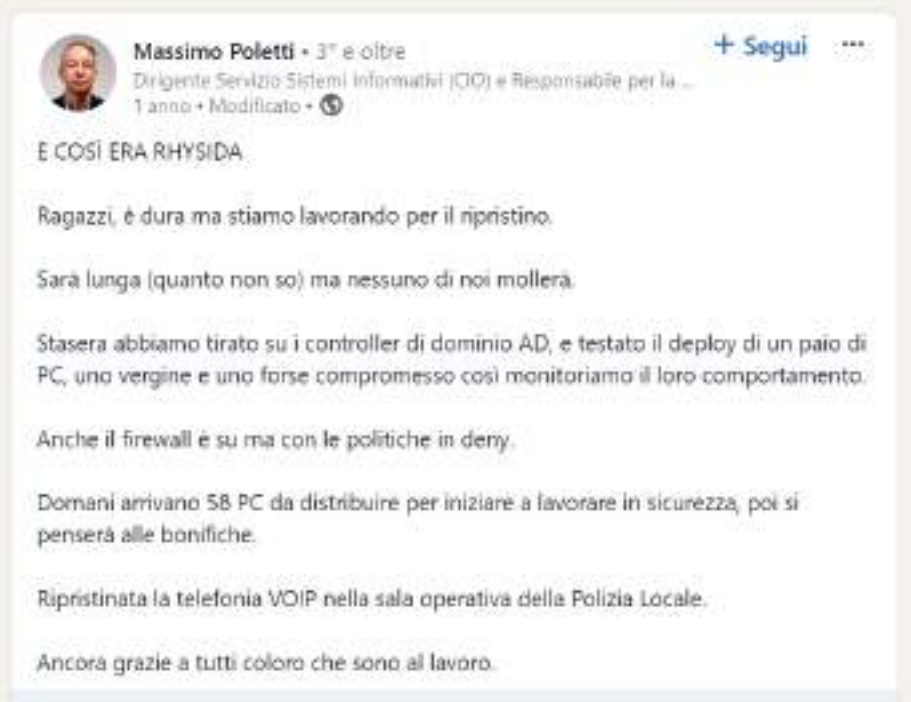
Ma come dicevamo la legge 90 non è una legge isolata – altri paesi si sono mossi in questa direzione – e si inserisce in un quadro europeo estremamente attivo rappresentando un'apripista in posizione preliminare rispetto all'applicazione della strategia della cybersicurezza del nostro Paese. È sintomatica di fatto di come l'attenzione dell'autorità non si focalizzi solo sul settore privato, ma stia spostando la lente dell'obiettivo anche sulla PA, spesso coinvolta in prima linea in attacchi informatici.

Le lezioni apprese dall'attacco ransomware al Comune di Ferrara

Elena Vaciago, Research Manager
TIG

Tra l'11 e il 12 luglio 2023 il Comune di Ferrara subisce un pesante attacco ransomware, distruttivo, mirato, condotto da professionisti che dimostrano di avere una conoscenza approfondita dell'infrastruttura digitale comunale e della rete regionale Lepida[1]. La mattina del 12 luglio esce la notizia sul sito del Comune: le postazioni informatiche e il numero verde sono temporaneamente inattivi a causa di un attacco hacker alla rete internet del Comune. I tecnici informatici impegnati nella "bonifica" dei sistemi ne riferiscono nel corso di una riunione interna in Municipio il giorno successivo, giovedì 13 luglio, e il sindaco della città Alan Fabbri afferma: "Non accetteremo ricatti o minacce, nessun dialogo con i delinquenti".

Nei giorni successivi, una squadra di professionisti, i tecnici del Comune e quelli esterni, in collegamento con la Polizia Postale e l'ACN, si avvicendano nella messa in sicurezza dei sistemi. E Massimo Poletti, Dirigente Servizio Sistemi Informativi (CIO) e Responsabile per la Transizione al Digitale del Comune di Ferrara, pubblica giornalmente sui social la cronistoria dell'attacco informatico e delle attività di ripristino, documentando – dal campo e con assoluta trasparenza – gli sforzi per ripristinare i servizi per i cittadini. Inizia così una vicenda completamente unica: grazie alla totale trasparenza del Comune e dei suoi Dirigenti, le persone interessate seguiranno i fatti via via che questi si verificano, un'esperienza che apre una prospettiva diversa su un attacco di questo tipo e sullo svolgersi nel tempo delle attività di ripristino e ripresa dei servizi informatici.



“Ragazzi, è dura ma stiamo lavorando per il ripristino. Sarà lunga (quanto non so) ma nessuno di noi mollerà”, scrive il 13 luglio il CIO della Comune Massimo Poletti. “Stasera abbiamo tirato su i controller di dominio AD, e testato il deploy di un paio di PC, uno vergine e uno forse compromesso così monitoriamo il loro comportamento. Anche il firewall è su ma con le politiche in deny. Domani arrivano 58 PC da distribuire per iniziare a lavorare in sicurezza, poi si penserà alle bonifiche. Ripristinata la telefonia VOIP nella sala operativa della Polizia Locale” dice Poletti.

Nell’intervista che segue, abbiamo chiesto a Massimo Poletti quali sono le lezioni apprese dall’attacco ransomware che qualunque organizzazione, pubblica o privata, dovrebbe considerare con attenzione.

TIG. Quali sono gli elementi che rendono più efficace la gestione dell’incidente?

Massimo Poletti. Innanzitutto, avere previsto la possibilità di chiamare un numero di telefono per attivare un team di risposta. Non importa la forma contrattuale, ma la reazione deve essere immediata e gestita da professionisti del settore. Poi individuare subito, in relazione alle dimensioni dell’Ente o dell’Azienda, un responsabile tecnico e uno organizzativo-gestionale-comunicativo. Occorre disaccoppiare le attività tecniche, che saranno molto impegnative, da tutte le altre. I tecnici devono lavorare tranquilli senza inutili sollecitazioni. Saranno i due responsabili a parlare tra di loro e scambiarsi le informazioni. Questo perlomeno è il modello che da noi ha funzionato.

Altra cosa è l’atteggiamento: specialmente il responsabile organizzativo, che si andrà a rapportare con i vertici, le dirigenze e l’ufficio stampa/comunicazione/web/social, deve mostrarsi determinato, una persona che sa perfettamente cosa va fatto e come va fatto. Ciò tranquillizza l’organizzazione che, presumibilmente, è in preda al panico. Poi magari dentro di sé non si sentirà così, ma il ruolo va gestito in maniera, passatemi il termine, militare. Segnalerei anche come sia importante avere una squadra motivata (più o meno numerosa) nella quale ognuno metta in gioco con passione le proprie grandi o piccole capacità. Per spiegarmi meglio, nel nostro caso anche persone dell’Amministrazione si sono dedicate a operazioni ripetitive (per ricreare gli utenti di dominio) liberando così i tecnici esperti per lavori più impegnativi.

TIG. Quali sono gli elementi che rendono più onerosa l’attività di ripristino post incidente?

Massimo Poletti. Le attività di ripristino richiedono decisioni rapide e, molto spesso, drastiche. Anzi, spesso sono quest’ultime le più efficaci ma richiedono un notevole impegno in termini di risorse. Nel nostro caso abbiamo deciso di rifare completamente l’infrastruttura di dominio e ciò al fine di costruire un ambiente ripulito da qualsiasi persistenza e dalle tare che i successivi upgrade (a partire dall’originario dominio NT) si sono portati dietro. Quindi si è trattato di fare un’attività che ha comportato l’installazione di un centinaio di PC acquistati sul mercato a cavallo di luglio e agosto, sia per ripristinare al più presto le funzionalità di base dei servizi interni, sia per rottamare gli ultimi Windows 7 rimasti. Ma il grosso è stata la bonifica di circa 900 macchine, processo che impegnava ogni PC in due giorni consecutivi contando un congruo periodo di quarantena.

L’intervento sui PC ha richiesto l’ingaggio di numerosi tecnici esterni, alcuni dei quali per fortuna ci sono stati prestati gratuitamente dall’Università di Ferrara, che ringrazio.

Oltre a quanto richiesto per l’ingaggio dei tecnici esterni i costi più rilevanti a fondo perduto sono stati: l’intervento del Response Team (compresa l’analisi forense), le licenze provvisorie dei software di sicurezza da installare sui mille PC all’atto della installazione o bonifica, gli interventi sistemistici per il rifacimento delle configurazioni di rete e infrastruttura,

specialmente quella virtuale. Inoltre, anche se non immediatamente visibile, non si trascuri il costo di circa 700 ore di straordinario svolte da parte del personale interno. Infine, sono stati rilevanti i costi per la gestione del rapporto con l'Autorità Garante, di cui si accennerà più avanti.

I costi da considerare come investimento sono quelli per l'acquisto dei PC e l'attivazione di licenze e contratti a lungo termine per servizi di gestione della sicurezza, quali la gestione del SOC. Erano costi già previsti per il budget 2024 che sono stati anticipati.

TIG. Collaborazioni e terze parti: quali servono di più nella gestione di un incidente?

Massimo Poletti. Quando succede un episodio di questo genere capisci quanto il fare rete, lo stringere partnership con i fornitori e il creare amicizie con colleghi di altri enti sia utile. Sono rimasto piacevolmente stupito dell'aiuto che ci è stato offerto (vedi UniFE) o della disponibilità di diversi fornitori a lavorare per noi in agosto. E comunque anche coloro che lo facevano per contratto lo hanno fatto con impegno e passione. Naturalmente mi sento di porgere ancora una volta un sentito ringraziamento ai tecnici dell'Agenzia Nazionale per la Cybersicurezza che ci hanno aiutato nel ripristino dei dati. Siamo stati molto fortunati ad avere il loro aiuto, quindi consiglio di fare sempre la segnalazione ad ACN anche nel caso che la normativa non lo preveda. Se hanno un modo per aiutare certamente lo faranno.

TIG. Segnalazioni al Garante? Cosa avete appreso?

Massimo Poletti. Ovviamente in questo caso l'importanza del DPO è fondamentale. Quello che abbiamo appreso è che, al pari dei cittadini, è importante informare anche l'Autorità Garante per la Protezione dei Dati Personali in maniera continua. Come i cittadini, che, tramite una comunicazione accorta ma mai reticente, devono capire che ci sono lavori in corso e l'ente non si barrica dietro al silenzio, anche il Garante deve avere il polso di quello che sta succedendo dal punto di vista del dato. Specialmente quando, come nel nostro caso, c'è stata la pubblicazione di una certa quantità di dati, consistenti in cartelle scelte casualmente dai server cifrati e contenenti dati eterogenei non strutturati. Il DPO ci ha guidati nel complesso e lungo processo di segnalazione, e infatti ne abbiamo fatte ben otto.

Altra cosa appresa è che la gestione delle segnalazioni di dati pubblicati, specie se derivanti da fonti eterogenee, è veramente complicata. L'individuazione puntuale degli interessati per i casi ad alto rischio che richiedevano notifica personalizzata ha richiesto numerosi cicli di elaborazione che sono andati avanti per due mesi. È servita anche una qualificata consulenza legale che aveva già lavorato su casi simili e che ha operato a fianco del DPO. Elaborazione e consulenza hanno avuto un costo non indifferente.

TIG. Quali sono le opportunità da sfruttare nel caso – malaugurato – di un evento di questo tipo?

Massimo Poletti. Il mio consiglio è di sfruttare il momento per rinnovare il più possibile l'infrastruttura liberandoci di mille oggetti legacy insicuri che ci portiamo dietro da anni e non abbiamo mai avuto il tempo (e talvolta la voglia) di dismettere. E mi riferisco a PC e apparati hardware, ma anche a software sia di base che applicativi. Nel nostro caso la ricostruzione totale del dominio ha permesso una pulizia radicale che non sarebbe mai stata possibile in condizioni normali di operatività.

Inoltre, in questi casi è molto probabile che ci sia un allentamento dei cordoni della borsa, notoriamente ben chiusi quando si parla di "infrastrutture", e ciò può permettere di acquisire servizi e strumenti non altrimenti accessibili.

TIG. Quali sono i temi che ancora oggi, con tutto quello che abbiamo visto negli ultimi anni, tendiamo a sottovalutare?

Massimo Poletti. Non solo nella mia esperienza il fattore formazione è spesso sottovalutato. Io punterei ad una formazione continua che unisca il mondo della sicurezza con quello della privacy. Se ci pensiamo solo un attimo le due cose sono strettamente collegate, ma spesso si ritiene che siano solo "affari del CED". Per la privacy piano piano stiamo migliorando, ma sulla sicurezza è proprio così.

Un altro argomento sottovalutato (forse perché considerato solo un costo) è il fatto che le infrastrutture richiedono costanti aggiornamenti negli anni. Forse una metafora che si può usare è l'acquisto di una casa nuova. Per un paio d'anni va tutto bene, poi devi cominciare a sistemare uno scarico, un infisso. Arriva il punto che non basta più verificare la caldaia tutti gli anni, la devi sostituire. E ancora, prima o poi il tetto lo devi sistemare. Ma se non fai niente per vent'anni alla fine la casa ti crolla in testa!

Infine, porrei l'attenzione sul backup. È una infrastruttura che spesso viene presa di mira durante un attacco. Le gang hanno competenze sistemistiche di alto livello e quando scatenano un attacco operano con una preventiva distruzione dei backup. Occorre procedere a più livelli: prevedere innanzitutto un backup principale di tipo immutabile, cosa che non avevamo ancora la possibilità di avere al momento dell'attacco, e ulteriori copie seguendo la regola del 3-2-1.

Ricordiamoci tuttavia che il recupero dal backup non dà la garanzia di avere gli oggetti "puliti", in quanto non sappiamo da quanto tempo gli attaccanti erano all'interno della nostra struttura. Ogni server ripristinato deve servire per recuperare i contenuti da inserire in nuovi server certamente puliti. Ogni dato ripristinato deve essere accuratamente analizzato prima di tornare a disposizione degli utenti.

TIG. Migrazione al Cloud? Quanto la raccomandi, qual è stata la vostra esperienza?

Massimo Poletti. Come Pubblica Amministrazione la migrazione al cloud rientra nei compiti previsti dalla normativa. Noi abbiamo intrapreso il percorso in tempi non sospetti, quando non si parlava né di Covid né (di conseguenza) di PNRR. Abbiamo giustamente aderito al bando PNRR sulla migrazione in Cloud per dare la "botta" finale ma l'obiettivo finale era già in vista. Con la migrazione in cloud SaaS (Software-as-a-Service) abbiamo raggiunto alcuni importanti obiettivi:

spegnimento del datacenter comunale, ormai obsoleto

spostamento completo sui fornitori degli oneri di assistenza sistemistica (quella applicativa lo era già)

oneri di gestione sicurezza in carico ai fornitori in forza della certifica ACN

disaccoppiamento con l'infrastruttura interna.

Ed è stato proprio quest'ultimo punto che ci ha aiutato durante l'incidente: tutto ciò che era in cloud non è stato toccato; quindi, gli sportelli digitali di front office non si sono mai fermati. Se teniamo conto che la quasi totalità dei servizi per l'utenza prevede l'uso dello Sportello Telematico Polifunzionale, ciò ha contribuito a minimizzare i disagi per i cittadini. Ovviamente la parte di back office si era fermata, ma l'abbiamo fatta ripartire in tempi ragionevoli.

TIG. Diffusione di consapevolezza: è massima dopo l'incidente, poi tende a calare nel tempo. Cosa servirebbe invece?

Massimo Poletti. Servirebbe una formazione continua e differenziata che renda tutti, a partire dai vertici fino all'ultimo dei dipendenti, consapevoli che viviamo in un mondo sempre più pericoloso. Se non si procede in questo modo purtroppo l'essere umano tende a dimenticare, e molto in fretta!

[1] Attacco Cyber. Il Comune nella morsa della gang Rhysida https://www.estense.com/2023/1029804/attacco-hacker-agli-uffici-comunali-in-azione-la-cyber-gang-rhysida/

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