GENNAIO - FEBBRAIO 2022

IL CAFFÈ DIGITALE

THE INNOVATION GROUP NEWSLETTER

I DATI DAL CIELO SONO LA NUOVA MANNA

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Alessio Pomasan
Banca Mediolanum

NUMERI E MERCATI

PNRR: gli obiettivi del 2021 e le sfide per il 2022

CANALE ICT

Buoni segnali per l'ecosistema ICT

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

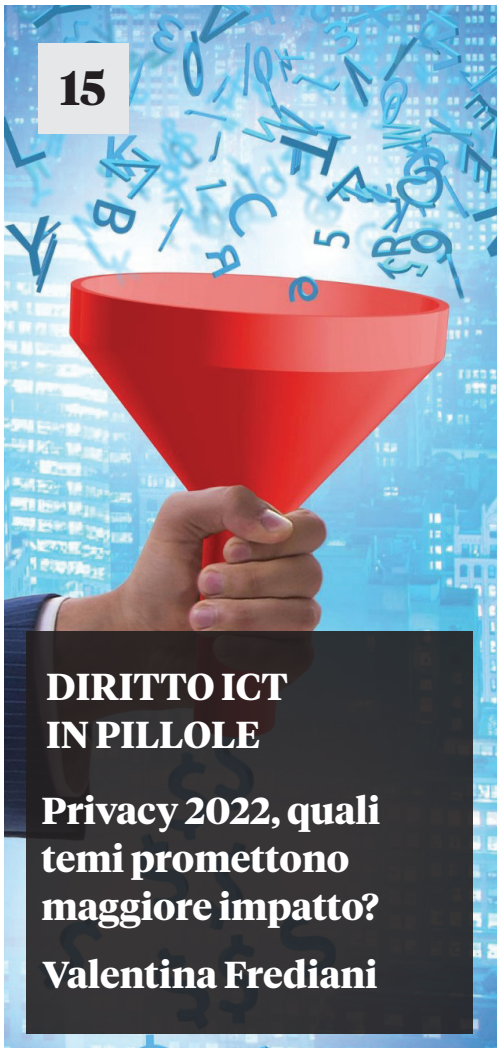
Carmen CAMARCA
Analyst
The Innovation Group

Roberto BONINO
Giornalista, Research and Content Manager
The Innovation Group

Valentina BERNOCCO
Web and Content Editor
The Innovation Group

Loris FREZZATO
Channel Area Manager
The Innovation Group

SOMMARIO



L'EDITORIALE

I dati dal cielo sono la nuova manna

Ezio Viola, Co-Fondatore

The Innovation Group

Non ci sono solo Elon Musk, Jeff Bezos e Richard Branson che fanno la gara a rincorrere il prossimo business legato al turismo spaziale a portare in primo piano l'importanza di quello che alcuni chiamano sia la "nuova economia dello spazio" e che toccherà molti settori direttamente o indirettamente. Il settore privato è stato infatti finora quello più esposto sui media, ma è stato anche il record di investimenti del 2021 di 14,5 miliardi di dollari, il doppio rispetto al 2020. Tra i protagonisti ci sono anche i governi nazionali. Morgan Stanley stima che il settore varrà più di mille miliardi di dollari entro il 2040 quando nel 2016 contava per 350 miliardi. L'Italia può giocare, una parte nella nuova corsa allo spazio? L'Asi, la nostra Agenzia Spaziale ha censito 153 aziende: 21 di grandi dimensioni, 105 piccole e medie imprese, 21 start-up e il comparto ha un fatturato annuo di 1,6 miliardi di euro con circa 6000 persone. E' a livello europeo che si può fare la differenza perché gli occupati sono circa 250.000, per un valore aggiunto stimato tra i 46 e i 54 miliardi di euro. Morgan Stanley individua diversi driver principali: uno è tornare sulla Luna, poi ci sono il lancio e la rete internet dei satelliti, l'esplorazione dello spazio profondo, l'osservazione terrestre, che consente di monitorare clima e maree; l'estrazione mineraria dagli asteroidi, la mappatura e, in prospettiva, lo smaltimento dei detriti e quindi anche il turismo spaziale .

Le applicazioni delle tecnologie sono studiate per lo spazio, ma sono utilissime pure sulla Terra. Le applicazioni relative all'osservazione terrestre sono le più mature e promettenti e sono la principale manna (non gratis) di dati. Infatti, Copernicus è il primo provider al mondo dei cosiddetti «space data», una mole di informazioni che viene utilizzata dal 60% delle aziende attive nell'osservazione terrestre e supporta uno scambio di dati di 16 terabyte al giorno.

Galileo è un sistema di navigazione e posizionamento satellitare dove passa circa il 10% del prodotto interno lordo del continente ed è il "cuore" di due miliardi di dispositivi, in un mondo dove ci orientiamo solo grazie alle mappe del cellulare con una precisione in circolazione di 20 centimetri. L'Ue possiede più di trenta satelliti in orbita e ne monitora 240 in tempo reale.

La space economy è infatti molto ampia e una delle aree più promettenti e dove il digitale è sia un abilitatore che un utilizzatore dei dati prodotti dalle tecnologie spaziali e satellitari è quello della "Osservazione della Terra". A questo segmento l'ESA (Agenzia Spaziale europea) ha previsto circa 1,5 Mld dei 6,5 totali previsti nel 2021 così come a livello nazionale nel piano strategico sono 1,8 Mld su 4,7 totali. L'Italia è il quinto Paese al mondo, secondo in

Europa, per investimenti messi in campo in relazione al Pil nella space economy. I fondi previsti nell'ambito del Pnrr contribuiranno a dare un'ulteriore spinta al mercato: lo stanziamento diretto allo Spazio è pari a 1,49 miliardi di euro e riguarda le linee di intervento: SatCom, Osservazione della Terra, Space factory, Accesso allo Spazio, In-orbit economy e Downstream.

La ricaduta potenziale sulla vita dei cittadini delle applicazioni è molto estesa. Le tecnologie satellitari sono considerate tra i driver rilevanti per raggiungere gli obbiettivi di sostenibilità perché permettono di realizzare le mappe di copertura del suolo per sviluppare modelli climatici o immagini multispettrali e radar per costruire modelli predittivi sulla deforestazione o di creare mappe di suscettibilità sulle zone a rischio frane, di monitorare i livelli di inquinamento o le dune nel deserto Sono alla base, per esempio, dell'agricoltura di precisione, che accresce la produttività del suolo del 10% e consente una riduzione del 20% dei pesticidi. Osservare la Terra significa contrastare il cambiamento climatico, mappando lo scioglimento dei ghiacci, l'innalzamento degli oceani, l'avanzata dei deserti, la deforestazione e gli eventi meteorologici estremi, ma consentirà anche di coordinare meglio le operazioni di soccorso durante inondazioni, incendi, terremoti e uragani. Tutti eventi sempre più frequenti, e più disastrosi. Dello sviluppo tecnologico, poi, beneficiano altri settori come il trasporto pubblico, le «smart cities» di domani, dove l'interconnessione ridurrà gli sprechi della società di oggi e ottimizzerà il riciclo dei rifiuti. Ma avrà un impatto anche sulle energie rinnovabili – basta pensare ai pannelli solari, messi a punto per lo spazio prima della commercializzazione su larga scala – e persino sulla salute, vista la centralità di parametri come la qualità dell'aria o le radiazioni che filtrano dall'atmosfera. Per salvare il pianeta, insomma, bisogna andare in orbita, osservare catturando e generando dati.

Una delle prospettive di sviluppo futuro della Space Economy è rappresentato dall'Internet Satellitare, destinato a diffondersi per coprire le molte aree del mondo non ancora in grado di accedere ad Internet. Il gap tecnologico rispetto all'infrastruttura terrestre (via cavo) potrebbe essere presto colmato, il vero valore aggiunto di Internet via satellite si otterrà usando in modo complementare i due asset e non in competizione,

Un sistema di osservazione della Terra, formato non solo da una costellazione di satelliti, ma anche di una piattaforma integrata di servizi per utenze istituzionali e commerciali, è l'ambizioso progetto che sarà operativo nel 2026 e al quale sta lavorando l'Italia finanziandolo con 1.070 milioni di euro all'interno del Piano Nazionale di Ripresa e Resilienza (Pnrr). Dalle aziende dell'industria spaziale (il cosiddetto upstream), agli IT provider e system integrator (downstream) fino alle imprese utenti finali, è convinzione diffusa che le tecnologie satellitari in combinazione con le tecnologie digitali più avanzate siano oggi un driver fondamentale per l'innovazione e la sostenibilità nei settori più diversi. La space economy può essere dunque un fattore di sviluppo essenziale per l'ecosistema dell'innovazione del nostro Paese.

QUESTO MESE ABBIAMO FATTO COLAZIONE CON...

Alessio Pomasan, Chief Information Officer, Banca Mediolanum

La sicurezza alla radice dei nuovi sviluppi

Roberto Bonino, Research and Content Manager
The Innovation Group

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

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

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

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

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

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

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

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

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

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

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

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

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

Come evolverà la vostra strategia nel prossimo futuro?

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

PNRR: gli obiettivi del 2021 e le sfide per il 2022

Carmen Camarca, Analyst
The Innovation Group

Il 31/12/2021 è scaduto il termine per raggiungere i 51 traguardi e obiettivi del Piano Nazionale di Ripresa e Resilienza (PNRR) concordati con la Commissione Europea, il cui raggiungimento, si ricorda, è propedeutico all'erogazione della prima tranche di finanziamenti (pari a 24,1 miliardi di euro) che fa seguito al prefinanziamento di 24,9 miliardi ricevuto lo scorso agosto. I 51 risultati in scadenza entro il 2021, conseguiti in anticipo rispetto ai tempi stabiliti, si compongono di 27 riforme e 24 investimenti. Di questi si ricorda, in particolare, l'avvio di riforme quali:

- Pubblica Amministrazione,
- quadro legislativo in materia di appalti pubblici,
- processo civile e penale,

e degli investimenti relativi a:

- creazione dell'hub del turismo digitale,
- interventi infrastrutturali dedicati alle Zone Economiche Speciali (ZES),
- ammodernamento del parco tecnologico e digitale ospedaliero.

L'aver conseguito in anticipo rispetto ai tempi previsti tutte le scadenze richieste dalla Commissione Europea rappresenta senz'altro un risultato importante, soprattutto per l'Italia, sin da subito osservata speciale da parte delle istituzioni europee (considerando, da un lato, l'entità delle risorse richieste dal nostro Paese, dall'altro i gravi ritardi e le lentezze procedurali che da tempo caratterizzano l'operare delle amministrazioni pubbliche); tuttavia ci sono alcuni aspetti da prendere in considerazione. Innanzitutto va specificato che gli obiettivi raggiunti finora sono soprattutto di tipo qualitativo (milestone), rappresentando principalmente condizioni abilitanti (individuazione di strategie, assunzione di esperti, entrata in vigore di decreti, pubblicazione di manifestazione di interesse) relative alla necessità di semplificare il percorso per il raggiungimento di obiettivi di maggior complessità (che nel PNRR vengono definiti "target") per cui la scadenza temporale è più lontana (trattandosi, appunto, di attività la cui conclusione richiede maggior tempo a disposizione). Si rileva, dunque, come, almeno in questa prima fase di attuazione del Piano, l'erogazione delle risorse europee sia subordinata alla conclusione di interventi volti principalmente alla preparazione delle condizioni indispensabili per poi procedere, in un secondo momento, all'effettiva realizzazione degli investimenti.

> **Gli obiettivi raggiunti finora sono soprattutto di tipo qualitativo, rappresentando principalmente condizioni abilitanti relative alla necessità di semplificare il percorso per il raggiungimento di obiettivi di maggior complessità per cui la scadenza temporale è più lontana**

In questo contesto, il reale di banco di prova sarà per il 2022, anno decisivo per l'attuazione del Piano in cui i target e le milestone da raggiungere saranno 100 (per ottenere altri 45,9 miliardi di finanziamenti europei). L'anno in corso sarà, inoltre, fondamentale anche per la reale attuazione degli investimenti, una sfida impegnativa per l'Italia che ha più volte dimostrato una scarsa capacità di spesa e di investimento in relazione ai finanziamenti europei[1].

In particolare, quest'anno dovranno essere contabilizzati altri 27,5 miliardi (destinati a 167 progetti), portando la spesa a fine anno a quasi 42 miliardi (anche se non ci sono resoconti ufficiali relativi alla spesa dei 14,2 miliardi previsti per il 2020-2021, sembrerebbe che al momento siano stati impiegati per progetti quali Superbonus, Transizione 4.0 e per le tratte di Alta velocità già in corso).

Il 2022 rappresenta, inoltre, un anno decisivo anche per il contesto macroeconomico in cui dovranno essere sviluppati i progetti, che non pare essere favorevole come quello del 2021: la spinta inflazionistica e il rincaro dei materiali stanno già facendo parlare di una possibile revisione del PNRR italiano, una eventualità prevista anche dall'articolo 21 del regolamento UE 2021/241 che ha istituito il Next Generation EU e che, qualora dovesse effettivamente realizzarsi, apre a diversi interrogativi, quali, ad esempio, l'individuazione dei progetti da ridefinire e le modifiche previste.

Infine, il 2022 suscita particolare attenzione anche per i progetti da avviare. Analizzando soltanto quelli digitali, dopo aver avviato nel 2021 attività per incentivare il rinnovamento tecnologico della filiera autobus, l'ammodernamento del parco tecnologico e digitale ospedaliero e aver pubblicato i bandi relativi al MaaS (Mobility as a Service) e allo sviluppo delle reti ultraveloci, nel 2022 si attende l'avvio di progetti quali:

- cybersecurity,
- digitalizzazione delle grandi amministrazioni centrali,
- interoperabilità,
- green communities,
- rafforzamento smart grid,
- scuola 4.0 e sanità connessa,
- oltre all'avvio del piano per satelliti ed economia spaziale e all'aggiudicazione del bando per la creazione del Polo Strategico Nazionale (PSN) che avrà l'obiettivo di ospitare i dati e i servizi critici e strategici di tutte le amministrazioni centrali.

Si tratta di progetti di notevole rilevanza per cui (anche se in forme e modalità differenti) si attendono significativi investimenti in tecnologia digitale e il cui sviluppo è destinato a creare profonde trasformazioni nei diversi settori produttivi del Paese, oltre che all'interno delle dinamiche con cui attualmente è gestita la Pubblica Amministrazione.

Per l'Italia, dunque, reduce da un ventennio caratterizzato da lenta crescita economica, costante aumento del tasso di disoccupazione e scarsa produttività del lavoro, il PNRR rappresenta un'occasione unica di ripresa economica e sociale. Perché ciò accada bisognerà supportare gli interventi del Piano con adeguati indirizzi di policy, nonché intensificare gli sforzi per adeguare il nostro Paese agli impegni cogenti richiesti dall'Europa: si tratta di una chiamata collettiva che richiede l'impegno di tutti gli stakeholder, dalle amministrazioni pubbliche alle aziende ai cittadini stessi.

Traguardi e obiettivi del PNRR

MISSIONI	TRAGUARDI	OBIETTIVI	TOTALE T&O PER MISSIONE
M1. DIGITALIZZAZIONE, INNOVAZIONE, COMPETITIVITÀ, CULTURA E TURISMO	88	132	220
M2. RIVOLUZIONE VERDE E TRANSIZIONE ECOLOGICA	56	85	141
M3. INFRASTRUTTURE PER UNA MOBILITÀ SOSTENIBILE	17	15	32
M4. ISTRUZIONE E RICERCA	20	32	52
M5. INCLUSIONE E COESIONE	22	32	54
M6. SALUTE	10	18	28
TOTALE	213	314	527

[1] Come si legge in un articolo pubblicato su "La Repubblica" il 2/2/2022, nel biennio 2022-2023 l'Italia è chiamata a spendere quasi 50 miliardi l'anno in progetti europei, contro una media, rilevata per il periodo 2015-2022, di quasi sei miliardi l'anno.

Un'azienda su 4 ha subito un attacco ransomware

Elena Vaciago, Associate Research Manager
The Innovation Group

Nel 2021 la minaccia ransomware ha continuato a crescere in importanza, per il numero degli attacchi andati a segno e per gli importi richiesti. Nel corso dello scorso anno si sono confermate alcune tendenze generali con riferimento al ransomware:

#1 – Una crescita del valore del riscatto. Con la tecnica della doppia estorsione (si minaccia anche di rendere pubbliche le informazioni esfiltrate) e con attacchi molto mirati, sono state raggiunte cifre milionarie legate a singoli incidenti da ransomware.

#2 – Il ransomware è stato utilizzato per attacchi alle Supply Chain, ad esempio, a fornitori di software. In questo modo gli attaccanti sono riusciti a colpire un gran numero di aziende in cascata. Colpendo il fornitore Kaseya, la gang di REvil è arrivata a danneggiare circa 1.500 aziende finali, compromettendo 50 MSP (Managed Services Provider) che utilizzavano questi prodotti e di conseguenze le loro aziende clienti.

#3 – Si sono intensificate le attività degli Stati, per bloccare le gang del ransomware e per intercettare le transazioni legate a pagamenti con criptovaluta. Dopo l'interessamento del Presidente Biden (in seguito all'attacco a Colonial Pipeline) e i suoi colloqui con il Presidente russo Putin, hanno cominciato a muoversi anche le polizie russe. Il 14 gennaio scorso si è saputo, ad esempio, che il Servizio di sicurezza federale russo (FSB) aveva arrestato la famigerata banda del ransomware REvil (Sodinokibi), 14 membri sospettati di far parte del team a Mosca, San Pietroburgo, Leningrado e Lipetsk.

Qual è oggi la probabilità di incorrere in un Ransomware?

Non c'è in pratica più nessuna realtà che possa dirsi del tutto immune dal rischio di incorrere in un incidente informatico con cifratura ed esfiltrazione di dati causato da un attacco ransomware. Durante la pandemia, il ricorso maggiore allo smart working ha ampliato la superfice d'attacco, aprendo agli hacker nuove porte per portare a termine i propri attacchi.

Allo stesso tempo, gli attacchi sono aumentati numericamente, e hanno preso di mira servizi critici come quelli sanitari.

Ciò nonostante, la maggior parte delle aziende pensa ancora che la probabilità di incorrere in un incidente di questo tipo sia bassa. Secondo i risultati della "Cyber Risk Management Survey 2022" di The Innovation Group (sarà presentata il prossimo 10 marzo 2022, nel corso del CYBERSECURITY SUMMIT 2022 di Milano), la probabilità di incorrere in un ransomware è Alta o Altissima per il 28% delle aziende, Media per il 48%, Bassa o Nulla per il 24%.

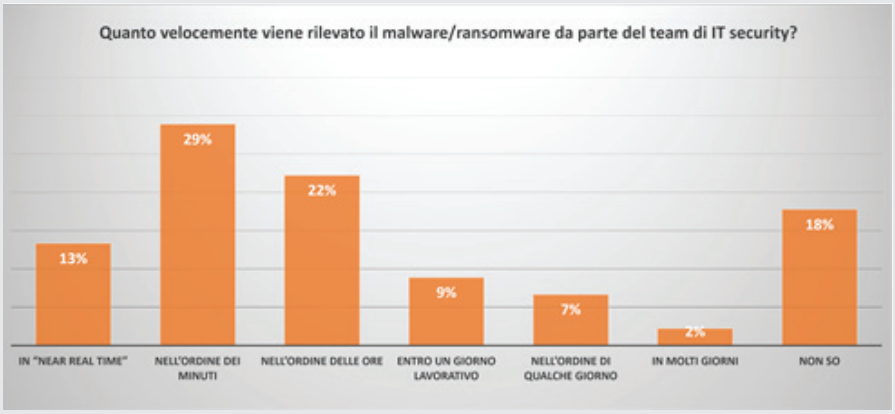
Con riferimento a chi afferma di aver già sofferto in passato per un evento di questo genere (il 26% dei rispondenti, un'azienda su 4) si tratta di realtà dei diversi settori e di diversa dimensione. Aspetto interessante, considerando solo queste aziende, per loro la probabilità di incorrere in ransomware è Alta/Altissima nel 50% dei casi, Media nel 33%, Bassa o Nulla nel 17%: quindi, chi ha già avuto un incidente, ritiene la possibilità di riaverlo più alta rispetto a chi non ne ha mai sofferto.

Come noto, dietro la fragilità delle aziende agli attacchi ransomware ci sono diverse cause: la prima tra tutte è la numerosità delle mail di Phishing, che riguardano oramai ogni realtà, pubblica o privata, business o consumer.

La scarsa educazione degli utenti, la credulità ai messaggi sempre più vicini all'esperienza quotidiana contenuti nel Phishing (o nei metodi simili dello Smishing e del Vishing) induce alcuni a cadere vittima. A questo si aggiunga il fatto che il furto di identità è diventato una pratica molto comune degli attaccanti, per la facilità con cui sono scritte le password e per la grande disponibilità di dati personali come account e password, frutto di precedenti data breach e quindi acquisibili senza difficoltà nel dark web.

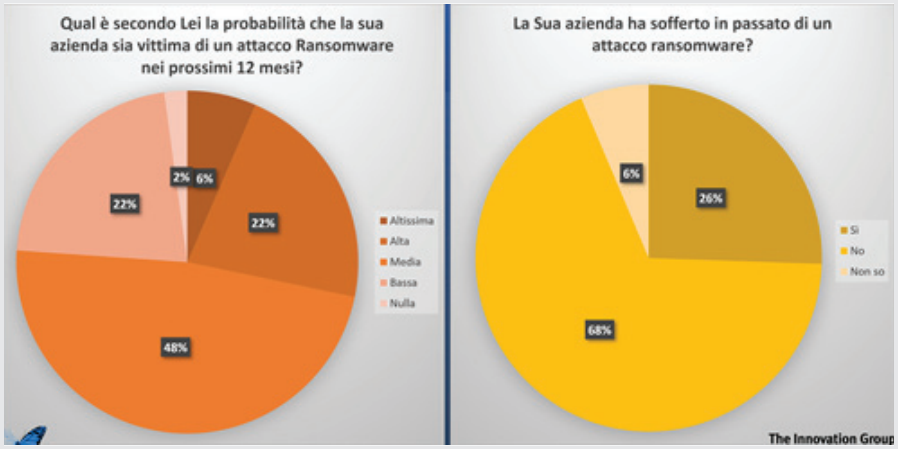
Utilizzando credenziali rubate gli hacker riescono ad entrare nelle reti corporate e a sferrare attacchi ancora più mirati, che si concludono con l'inserimento di ransomware e quindi la cifratura di dati molto sensibili delle aziende.

Il 64% delle aziende riesce a rilevare il malware entro qualche ora, mentre per il 9% servono più giorni



Fonte: TIG, Cyber Risk Management 2022 Survey, Febbraio 2022

Ransomware



Fonte: TIG, Cyber Risk Management 2022 Survey, Febbraio 2022

Secondo i risultati della "Cyber Risk Management Survey 2022" di The Innovation Group (sarà presentata il prossimo 10 marzo 2022, nel corso del CYBERSECURITY SUMMIT 2022 di Milano), la probabilità di incorrere in un ransomware è Alta o Altissima per il 28% delle aziende, Media per il 48%, Bassa o Nulla per il 24%.

Quali le conseguenze quando un attacco ransomware ha successo?

È ben noto che le conseguenze di un attacco ransomware possono essere gravissime. Come ha commentato di recente Stefano Mele (nell'articolo "Sanità veneta vittima di ransomware, per Mele è una minaccia alla sicurezza nazionale" di Formiche.net) "... E' sotto gli occhi di tutti come gli attacchi ransomware siano ormai da alcuni anni in costante crescita soprattutto sul piano "qualitativo" degli obiettivi colpiti e delle tecniche estorsive utilizzate per ottenere il pagamento del riscatto. Questo genere di attacchi, peraltro, causa nella vittima che li subisce non solo un danno immediato, relativo all'impossibilità di utilizzare in maniera efficiente gran parte – se non la totalità – delle infrastrutture tecnologiche, ma contestualmente innesca decisioni di vitale importanza per l'azienda sul piano legale, etico, dei processi e della reputazione, le quali devono anche essere prese nell'arco di pochissime ore".

Per una risposta immediata servono oggi capacità di rilevamento del malware il più possibile efficaci: invece la situazione vede una grande disparità di situazioni nelle aziende italiane, con una minoranza di aziende in grado di rilevare il malware che si infiltra nei sistemi in pochi secondi o minuti (il 35%) e le altre che sono in grado di farlo con tempistiche più lunghe.

Cosa serve quindi per prepararsi a rispondere?

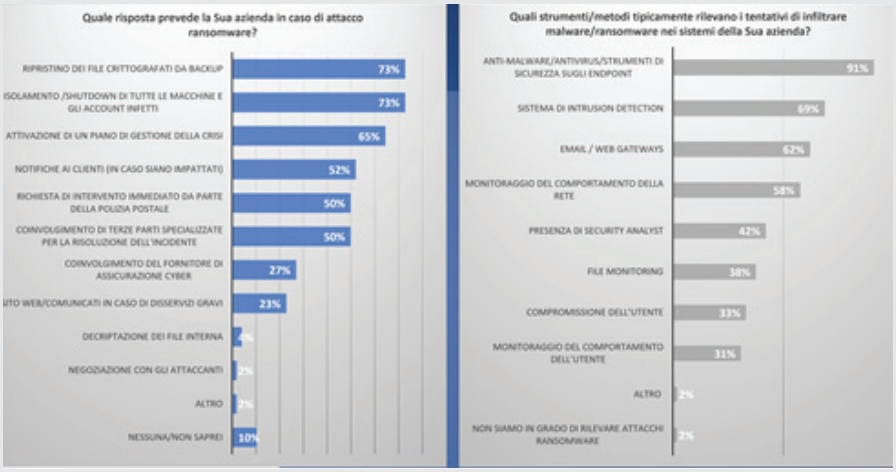
L'indagine ha messo in luce una convergenza su alcuni strumenti e metodi per prepararsi ad affrontare un'emergenza di questo tipo. In ordine di importanza abbiamo:

- Ripristino dei file crittografati tramite backup (73% delle risposte); Isolamento e shutdown delle macchine attaccate e degli account infetti (73%) e Attivazione del piano di crisi (65%).
- Solo un'azienda su 2 si è invece preparata ad affrontare aspetti importanti come: Notifiche ai clienti (52% delle risposte); Richiesta di intervento della Polizia Postale (50%) e Coinvolgimento di terzi specializzati nella risoluzione di incidenti (50%).
- Infine, una minoranza di azienda ha predisposto un'assicurazione cyber (27%) e una procedura per produrre un sito web per la comunicazione a tutti i clienti/ i terzi impattati di un eventuale disservizio (23%).

Con riferimento invece agli strumenti utilizzati per la rilevazione del malware, quelli più diffusi sono gli antimalware a livello di endpoint (in uso nel 91% dei casi) e, a seguire, l'intrusion detection a livello di rete (69%). Email e web gateways e tool specifici per il monitoraggio del comportamento della rete risultano comunque diffusi (rispettivamente, 62% e 58% dei casi) mentre la presenza di un security analyst dedicato è piuttosto bassa (42%), considerando che il campione dell'analisi è composto di aziende medio grandi.

In conclusione, nonostante il tema del ransomware sia oggi considerato un'emergenza nazionale per la velocità con cui si sta diffondendo, per gli importi milionari delle estorsioni e per gli impatti negativi, il blocco dell'operatività e il danno alla reputazione del brand, le misure utilizzate per prevenirlo risultano ancora molto basilari: servirebbe un'attività preventiva più decisa e focalizzata su questo tema.

Risposta al Ransomware



Fonte: TIG, Cyber Risk Management 2022 Survey, Febbraio 2022

Buoni segnali per l'ecosistema ICT

Loris Frezzato, Channel Area Manager
The Innovation Group

Sono tanti i segnali di ripresa e di opportunità di business che si paventano da una situazione generale del mercato in netto miglioramento. Un miglioramento che è concomitante con quella che sembrerebbe essere ormai una evoluzione della pandemia in un fenomeno più gestibile e meno pericoloso di quanto lo sia stato fino a oggi.

C'è fermento e speriamo tutti che sia un fermento positivo, nel senso buono del termine. Il PIL italiano viaggia a velocità maggiori della media europea e le risorse del PNRR stanno iniziando ad essere allocate o almeno pianificate, e l'alta quota da destinare mandatoriamente alla digitalizzazione per una trasformazione e modernizzazione del Paese fa ovviamente ben sperare anche il canale italiano delle terze parti ICT.

Un flusso di denaro e di stimoli alla spesa che magari non investiranno direttamente i system integrator locali della Penisola, se non coloro con le spalle abbastanza grandi da riuscire a gestire le gare per le pesanti richieste di revisione dei processi e di trasformazione digitali innescate dalle Pubbliche Amministrazioni, centrali, locali e derivate.

Ma il canale deve stare all'erta e aspettarsi l'onda indiretta di questo tsunami benefico.

Indirettamente, per canali o rivoli laterali, l'onda arriva. Siamo nell'era degli ecosistemi.

E gli ecosistemi sono tra loro collegati e tra loro interdipendenti.

Vendor, distributori, system Integrator, consulenti e le tante altre forme di operatori specializzati nelle nuove tecnologie digitali che si stanno delineando con una evoluzione veloce, fanno tutti parte dell'Ecosistema ICT, dove al centro c'è il cliente finale, certo non inoperoso come un tempo ma anch'esso parte pensante, formata, operativa e, sempre più spesso, culturalmente avanzata dal punto di vista tecnologico.

E dell'ecosistema ICT si vuole anche quest'anno, con ancor maggiori motivazioni, occuparsi The Innovation Group attraverso un percorso di eventi distribuito nell'intero arco di questo 2022.

Un Summit e ben quattro Web Conferecne tematiche che hanno l'intento di riattivare il confronto tra i fornitori primari di tecnologie e i propri partner del canale e quello spirito di networking, trasferimento di esperienze e di collaborazione che stava iniziando a caratterizzare i rapporti tra i diversi operatori, pratica bruscamente ostacolata dall'arrivo della pandemia.

Il primo appuntamento sarà il 18 e il 19 maggio 2022, con ICT Ecosystem Summit 2022, l'evento annuale dedicato a tutte le figure che compongono il variegato mondo del canale ICT (a questo link i dettagli e il modulo di iscrizione).

Non solo proclami, ma finalmente un ritorno al vero confronto tra gli operatori del canale, con quello spirito di networking che questo evento vuole stimolare. L'edizione 2022 del Summit si svolgerà, infatti, interamente in presenza, proponendo momenti di trasferimento di informazioni, previsioni di mercato, analisi dei trend e delle aspettative dei clienti, ma anche delle opportunità che possono derivare dagli stimoli all'innovazione che arrivano a livello governativo ed europeo.

Contenuti esclusivi che aumenteranno il loro valore dalla possibilità di ritrovarsi finalmente a guardarsi negli occhi di persona, e di confrontarsi direttamente con vendor, distributori, analisti, giornalisti ma, soprattutto, tra altri operatori, per poter rivitalizzare quello spirito di ecosistema necessario per affrontare le enormi opportunità che il mercato sta offrendo.

L'edizione di quest'anno dell'ICT Ecosystem Summit si terrà in due tempi. Un pomeriggio di confronto stretto e riservato tra i maggiori esponenti di vendor e distributori che culminerà in una cena di gala. Il giorno dopo sarà invece interamente dedicato ai contenuti e alle opportunità, con un programma che punta all'operatività e dare segnali concreti su come collaborare insieme per vincere sul mercato.

La mattinata inizierà con una visione del mercato da parte di analisti di respiro internazionali,

che mostreranno le potenzialità, e il confronto, del canale ICT a livello italiano ed europeo. Ci sarà poi modo di ascoltare la voce e le aspettative dei clienti e le opportunità prospettate da istituzioni e associazioni di categoria.

Quindi, via libera alle tavole rotonde tematiche, in cui vendor e distributori, anche insieme ai loro partner, illustreranno le loro strategie e il loro supporto per attivare partnership profittevoli con il canale.

Luglio, Settembre, Ottobre e Novembre saranno poi le altre tappe del percorso ICT Ecosystem proposto da The Innovation Group, dove i system integrator avranno spazio per illustrare al loro pubblico di prospect clienti le proprie soluzioni riguardo i diversi temi che verranno trattati nel corso di questo ciclo di Web Conference.

Questi gli appuntamenti, di cui vi daremo dettagli via via che ci avvicineremo alla data:

5 Luglio – DIREZIONE CLOUD: LA STRADA PIU' VELOCE E SICURA
I percorsi scelti dai vendor e i system integrator che portano alla trasformazione digitale delle imprese

15 Settembre – SICUREZZA IT: UN UNIVERSO COMPLESSO
I system integrator colmano lo skill gap del mercato

27 Ottobre – BUSINESS E CORE APPLICATION GUIDANO LE AZIENDE
Da soluzioni monolitiche a sistemi flessibili

24 Novembre – I DATI PARLANO. LE AZIENDE ASCOLTINO
L'analisi dei dati e l'interpretazione in chiave business stanno ormai mostrando tutte le loro potenzialità

Privacy 2022, quali temi promettono maggiore impatto?

Valentina Frediani, General Manager
Colin & Partners

Il piano ispettivo del Garante offre sempre informazioni importanti rispetto ai focus privacy nel nostro Paese. Per il primo semestre 2022, gli obiettivi riguardano essenzialmente due macrocategorie che investono la maggior parte delle imprese e degli enti.

La prima riguarda accertamenti in merito a profili di interesse generale per categorie di interessati. Sotto la lente i "fornitori di database" e i trattamenti di dati personali che effettuano ma anche piattaforme e siti web in riferimento alla gestione dei cookies. I siti di incontri sono citati in modo esplicito, così come i trattamenti che vengono effettuati nell'ambito – mai dimenticato dal Garante – della cosiddetta "videosorveglianza".

Interesse viene mostrato anche per ambiti e modelli di business più innovativi e in crescita. Si pensi a chi sceglie di abbracciare la "data monetization", un ambito che sta guadagnando rapidamente attenzione per il suo potenziale, sostenuto anche da AI e utilizzo del Cloud. Definito da Gartner come il processo di utilizzo dei dati finalizzato all'ottenimento di un beneficio economico quantificabile, vede nel comparto finance un traino importante, al momento. Tuttavia, è piuttosto intuitivo che, per qualunque settore di business, la disponibilità di dati (interni o esterni) e la loro raccolta e analisi costituisca una base per incrementare le proprie attività.

Interessante, al riguardo, la notizia di una proposta di legge d'Oltreoceano, la Banning Surveillance Advertising Act, promossa da alcuni esponenti democratici. Si tratta, in estrema sintesi, di ribaltare il modello pubblicitario costruito fin qui e basato – per l'appunto – su dati sempre più focalizzati sull'estrema personalizzazione in base a interessi, abitudini di consumo, preferenze, ecc. Insomma, sarebbe un ritorno alle origini abbandonando il paradigma della profilazione che rappresenta croce e delizia per i marketers e la fortuna delle Big Tech fino ad oggi.

Come molti analisti hanno commentato, è difficile che una simile proposta diventi legge. Ha tuttavia il valore di un segnale che, da più parti, chiede un Internet meno invasivo e condizionato, in cui i servizi apparentemente gratuiti (che vengono in realtà remunerati con l'accesso ai dati personali) lasceranno il posto a quelli a pagamento, rivoluzionando nel profondo ogni modello di business basato sulla pubblicità mirata.

D'altra parte, siamo in attesa, proprio in questo 2022, della finalizzazione del Regolamento ePrivacy che, se l'iter verrà rispettato, entrerà in vigore entro due anni dalla sua approvazione. Un asset di regole armonizzate al GDPR e basate su consenso esplicito (e meno laborioso) e sull'estensione della tutela della riservatezza dei dati delle persone fisiche a tutti gli strumenti utilizzati per le comunicazioni elettroniche, comprese telefonate via web e messaggistica. Citando tre macro-temi affrontati nel Regolamento: cookies, soft spam e direct marketing, sarà utile per chi opera in questi settori, o fruisce di servizi simili, prepararsi per tempo aggiornando i propri processi, prima delle soluzioni tecnologiche, in ottica di conformità.

Il GDPR, d'altro canto, ha già costituito una notevole occasione in tal senso. Non stupisce infatti l'attenzione del Garante per i produttori e distributori di smart toys e le realtà che operano attraverso algoritmi e intelligenza artificiale in ambito pubblico e privato. Anche questi settori saranno oggetto di interventi ispettivi che, di certo, terranno conto dei principi di privacy by design e by default che orami abbiamo imparato a conoscere.

La seconda macroarea di accertamenti si rivolgerà a soggetti pubblici e privati allo scopo di verificare la corretta individuazione dei Titolari e dei Responsabili del trattamento, anche in relazione all'utilizzo di app e altri applicativi informatici.

Dato l'incremento dello Smart working negli ultimi due anni, l'acquisizione di informazioni e dati personali da parte di app istallate sugli smartphone suscita particolare interesse; in particolare, il Garante mira ad accertare il corretto trattamento di app diverse da Verifica C19.

Ampliando lo sguardo al di fuori dei nostri confini e dal piano ispettivo del primo semestre, per imprese ed enti, il 2022 sarà un anno intenso sul fronte privacy, soprattutto qualora intervenga la necessità di trasferire dati oltre frontiera. Molti i paesi che stanno costruendo, o hanno in programma di farlo, regolamentazioni più stringenti a tutela dei dati personali "territoriali". In Europa la norma è già delineata, c'è da aspettarsi forse una maggiore attenzione nel farne rispettare le regole. E' di inizio anno la decisione dell'EDPB che, analizzando il sito web del Parlamento Europeo ed i relativi servizi di Google Analytics e di Stripes, ha emesso una reprimenda nei confronti dell'istituzione relativamente ai cookies presenti sul sito che comportano il trasferimento di dati verso gli U.S.A.

Una tendenza, questa, che non deve necessariamente spaventare. È certo, però, che occorra gestire le proprie banche dati con accortezza e lungimiranza, unendo gli aspetti legali e tecnologici in soluzioni abilitanti che non compromettano il successo della propria attività di business.

Questo anche tenendo conto di una, conseguente e logica, maggiore attenzione verso le regole che intervengono in caso di breach di sicurezza.

Perché l'intelligenza non è artificiale

Rita Cucchiara
Professore Ordinario Dipartimento di Ingegneria "Enzo Ferrari"
Università degli Studi di Modena e Reggio Emilia

Articolo tratto dall'intervento di Rita Cucchiara, Professore Ordinario Dipartimento di Ingegneria "Enzo Ferrari" dell'Università degli Studi di Modena e Reggio Emilia, durante la Web Confrerence "L'ARTIFICIAL INTELLIGENCE STA DIVENTANDO REALTA'?" del programma Digital Italy 2021

#LaVisioneDeiLeader

L'intelligenza artificiale non è più un imitation game ma è diventata una forma diversa di intelligenza: oggi, infatti, l'obiettivo non è più quello di realizzare sistemi capaci di emulare il cervello umano (anche se ne condividono le finalità) ma piuttosto dei sistemi che hanno dei comportamenti reagendo con ambiente, gestendo quantità di dati che derivano dal mondo esterno, dall'interazione con l'uomo o da tutti i dati sul web.

L'intelligenza artificiale non è una black box di scarsa comprensione, piuttosto una tecnologia ingegneristicamente concreta che può essere progettata e regolata e che rappresenta un campo in cui la ricerca e l'industria stanno investendo ingenti quantità di denaro. Non va dimenticato, infatti, che l'intelligenza artificiale è ancora soprattutto ricerca, una ricerca che si è sviluppata in modo concreto negli ultimi 10 anni e che necessita di grandissimi investimenti e di grande collaborazione tra sfera pubblica e privata: ciò perché, da un lato, per fare conoscenza serve conoscenza (e quindi la ricerca) e, dall'altro, la ricerca deve essere collegata in maniera diretta al mondo produttivo anche considerando che adesso il time to market tra ricerca e applicazione si è ridotto notevolmente.

La strategia italiana sull'Intelligenza Artificiale

Per sviluppare, dunque, una strategia vincente basata sull'intelligenza artificiale è necessaria la sinergia di 4 grandi entità: mondo della ricerca delle aziende IT (che lavorano e che producono intelligenza artificiale), dell'industria, della Pubblica Amministrazione e della società. Tali aspetti vengono ripresi anche all'interno della Strategia Italiana sull'Intelligenza Artificiale, nata dalla collaborazione tra Ministero dello Sviluppo Economico (MISE), Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) e Ministero Innovazione Tecnologica e Transizione Digitale (MITD) e che si basa appunto su tre grandi pillar: ricerca, talenti e applicazioni sia nel mondo dell'industria sia nella Pubblica Amministrazione. In particolare, in Italia sono stati individuati 13 ambiti applicativi dell'intelligenza artificiale relativi, ad esempio, a tematiche quali industria, agroalimentare, cultura e turismo, salute-benessere, infrastrutture, servizi finanziari (banche e assicurazioni), Pubblica Amministrazione, sicurezza nazionale.

È importante comprendere che l'Italia può ancora vincere la partita sull'intelligenza artificiale, perché l'intelligenza artificiale siamo noi, siamo noi che dobbiamo inserirla con le nostre competenze, con i nostri valori, con la nostra legislazione e soprattutto dal punto di vista tecnico, lavorando in modo transdisciplinare tra esperti informatici e del settore per creare le applicazioni e i sistemi di domani.

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