N. 128

DIRECTION

LE TECNOLOGIE CHE MUOVONO IL BUSINESS

SentinelOne

Protezione multilivello, integrata e guidata dall'AI

Paolo Ardemagni, *Vice President Southern EMEA di SentinelOne*

TECNOLOGIA E BUSINESS
SUPPORTARE I PROCESSI CON **ANALYTICS, CRM, ERP**

INTELLIGENZA ARTIFICIALE
NUTANIX PREPARA L'AI IN A BOX

MERCATI VERTICALI
AGRICOLTURA 4.0, LA TECNOLOGIA C'È

INNOVAZIONE
LA CRESCITA INARRESTABILE DEL **5G**

SPECIALE RANSOMWARE
DIVENTARE RESILIENTI CON **OPENTEXT CYBERSECURITY**

ESET PORTA LA PROTEZIONE VICINO ALL'UTENTE

INDICE

3 **Editoriale**
Cosa ne facciamo del tempo che ci fa guadagnare l'AI?

5 **COVER STORY**
SentinelOne: protezione multilivello, integrata e guidata dall'AI

12 **SPECIALE RANSOMWARE**
Ransomware una minaccia che continua a cambiare pelle
Un baluardo contro il ransomware: le soluzioni di OpenText Cybersecurity
ESET: combattere il ransomware portando la protezione vicino all'utente

22 **MERCATI VERTICALI**
Agricoltura 4.0, la tecnologia c'è, ora tocca agli agricoltori
La tecnologia porta la sostenibilità nei campi
Tracciabilità per garantire il consumatore
Nel futuro, spazio ad aeroponica e idroponica

28 **Scenari**
Pay or consent: il trattamento "con requisiti" è moneta

30 **Data Center**
Un Green Data Center per l'Università di Pisa

32 **FOCUS TECNOLOGIA E BUSINESS**
Supportare i processi aziendali con gli analytics
ERP e CRM aprono la strada al business data-driven

38 **Intelligenza artificiale**
Nutanix integra l'AI e punta al mercato di VMware

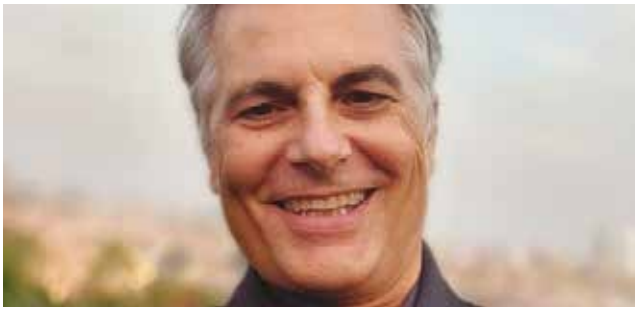
40 **Innovazione**
5G, una crescita inarrestabile

46 **Riflessioni**
Aiuto arriva un messaggio whatsapp

Reportec è una società fondata da Gaetano Di Blasio, Riccardo Florio, Giuseppe Saccardi

DIRECTION
Anno XXI - numero 128
Aprile 2024
Direttore responsabile: Riccardo Florio
Coordinamento editoriale: Paola Rosa
Ha collaborato: Primo Bonacina, Aldo Cattaneo, Maurizio Ferrari, Fabrizio Pincelli, Stefano Uberti Foppa
Redazione: Via Gorizia 35/37 20099 Sesto San Giovanni (MI); Tel 339 3785157; https://reportec.it; redazione@reportec.it

Immagini: Dreamstime.com
Stampa: A.G. Printing Srl Via Milano 3/5; 20068 Peschiera Borromeo (MI)
Editore: Reportec Srl; C.so Italia 50 20122 Milano
Il Sole 24 Ore non ha partecipato alla realizzazione di questo periodico e non ha responsabilità per il suo contenuto
Amministratore unico: Riccardo Florio
Iscrizione al tribunale di Milano n° 212 del 31 marzo 2003
Diffusione cartacea + digitale 32.500 copie



COSA NE FACCIAMO DEL TEMPO **CHE CI FA GUADAGNARE L'AI?**

di Riccardo Florio
• *direttore responsabile* •

L'introduzione dell'intelligenza artificiale nelle nostre vite promette di liberarci da molte attività quotidiane e lavorative, riducendo il tempo necessario per compiti ripetitivi e automatizzabili. Sfrutteremo questa opportunità per migliorare realmente la qualità della nostra vita e della società? Oppure, come sostengono alcuni, l'effetto sarà di ridurre i posti di lavoro e fare lavorare ancora di più quelli che resteranno?

L'AI TOGLIERÀ POSTI DI LAVORO ?

Alcuni sostengono che l'automazione portata dall'AI toglierà posti di lavoro mentre, al contrario, alcuni esperti sostengono che questa tecnologia creerà nuove e migliori opportunità. Secondo un'analisi del World Economic Forum (Future of Jobs Report 2023), entro il 2025 l'automazione e l'intelligenza artificiale provocheranno la perdita di circa 85 milioni di posti di lavoro a livello globale ma ne genereranno circa 97 milioni.

L'impatto però non sarà uguale su tutti i settori e i ceti sociali. L'automazione, infatti, porterà a una riduzione del bisogno di manodopera oggi usata per svolgere compiti ripetitivi, mente per coprire i nuovi lavori del futuro saranno richieste competenze avanzate, per esempio legate alla gestione e manutenzione dell'AI, alla programmazione, alla data analysis e a competenze trasversali come il "problem solving" e il pensiero critico. Tra i settori più a rischio vi sono i trasporti con l'avvento dei veicoli autonomi, alcune componenti del manifatturiero e quello amministrativo con l'automazione degli uffici. Al contrario, settori come la tecnologia dell'informazione, l'ingegneria e la sanità potrebbero beneficiare significativamente dell'AI.

Se è indubbio che l'avanzamento dell'AI richiederà una forza lavoro altamente qualificata ne deriva che, per prepararsi a questi cambiamenti, **il sistema educativo dovrà adattarsi rapidamente**, promuovendo percorsi di formazione che includano competenze digitali avanzate e una continua educazione professionale. Università e istituti di formazione, anche italiani, stanno già introducendo corsi specializzati in intelligenza artificiale, robotica e analisi dei dati.

L'AI MIGLIORERÀ LA NOSTRA VITA SOCIALE E LAVORATIVA?

Invece di focalizzarsi esclusivamente sui posti di lavoro che potrebbero essere perduti, è utile considerare come l'AI possa essere utilizzata per **migliorare la qualità del lavoro umano e creare un**

futuro lavorativo più inclusivo e diversificato. La chiave sta nel gestire la transizione in modo che sia equa e che offra opportunità di riqualificazione a chi ne ha bisogno. Una promessa dell'AI è quella di permettere agli individui di concentrarsi su attività più gratificanti e creative. Teoricamente, meno tempo dedicato a compiti routinari potrebbe tradursi in più tempo per l'educazione continua, l'arte, il volontariato e la cura delle relazioni personali. Tuttavia, la realtà può essere meno idilliaca e la questione centrale diventa come utilizzeremo effettivamente il tempo risparmiato grazie all'AI. L'uso ottimale del tempo guadagnato potrebbe avere un **impatto significativo sul benessere individuale e sulla salute mentale.** Più tempo per attività significative può portare a una maggiore soddisfazione personale e a un equilibrio più armonioso tra lavoro e vita privata. Per le comunità, questo tempo potrebbe essere investito in iniziative che promuovono la coesione sociale e il benessere collettivo. Nonostante queste potenzialità, esistono ostacoli significativi che si frappongono alla realizzazione di questi obiettivi. **La distribuzione diseguale dei benefici dell'AI** può portare a una società dove solo alcuni godono del tempo liberato da queste tecnologie, mentre altri potrebbero trovarsi a dover affrontare una maggiore precarietà lavorativa. Inoltre, senza un cambiamento culturale che riveda il nostro approccio al lavoro e al tempo libero, le ore risparmiate potrebbero non tradursi in un miglioramento qualitativo della vita ma venire assorbite da altre attività meno formativa, come il consumo incrementato di media digitali.
Allo stesso tempo, è fondamentale considerare la **responsabilità individuale nell'uso del tempo guadagnato.** La cultura del "sempre attivi" e la pressione per essere costantemente produttivi possono essere contrapposte da un approccio più bilanciato che valorizza il riposo e il tempo personale come essenziali per il benessere. Gli individui potrebbero beneficiare di un maggiore accesso a risorse che li aiutino a riflettere sulle proprie priorità di vita e a utilizzare il tempo in modo più consapevole e soddisfacente.

L'AI SERVIRÀ SOLO AD AUMENTARE LA PRODUTTIVITÀ?

Una visione pragmatica alternativa è quella di considerare l'AI principalmente come uno strumento di produttività e sviluppo del business privilegiando le motivazioni economiche e focalizzandosi sugli incrementi di efficienza e sui vantaggi competitivi piuttosto che sui potenziali benefici sociali o personali. Se, da un lato, l'accento sulla produttività può stimolare la crescita economica, portare a innovazioni tecnologiche più rapide e migliorare la competitività delle aziende a livello globale, dall'altro lato, questa enfasi può anche acuire le disuguaglianze sociali, poiché i benefici dell'AI potrebbero concentrarsi nelle mani di chi ha già risorse e competenze tecnologiche, lasciando indietro vasti segmenti della popolazione.
Le istituzioni educative, le aziende e i governi dovrebbero collaborare per creare programmi e politiche che non solo indirizzino il tempo liberato verso attività produttive, ma che anche incentivino un approccio più equilibrato tra lavoro e al tempo libero. Per esempio, **la promozione di settimane lavorative più corte** potrebbe essere una risposta al tempo guadagnato, distribuendo più equamente lavoro e tempo libero tra la popolazione e aumentando il benessere generale. Un altro possibile modo per **equilibrare la crescita economica stimolata dall'AI e la distribuzione equa dei suoi benefici** potrebbe essere di includere politiche che incentivino le aziende a reinvestire i guadagni ottenuti attraverso l'AI in programmi di formazione e riqualificazione per i lavoratori oppure in iniziative che promuovano un accesso più ampio e democratico alle tecnologie avanzate. Queste riflessioni indirizzano verso la necessità di predisporre **una visione strategica e di lungo termine** e pongono le basi per un dibattito molto ampio sulla **società che desideriamo costruire nell'era dell'AI**: più equa e sostenibile grazie a un incremento del benessere individuale e collettivo oppure accelerata verso un impulso di produttività e di consumo? Forse un insieme di entrambi gli aspetti; in ogni caso, le decisioni che prenderemo su come impiegare il tempo liberato dall'AI potrebbe definire la qualità della nostra vita e della società futura.

PROTEZIONE MULTILIVELLO, INTEGRATA E GUIDATA DALL'AI

di Riccardo Florio

Fondata nel 2013 e quotata in Borsa dal 2021, SentinelOne si è rapidamente affermata come una delle aziende leader nel settore della cybersecurity. Partendo come startup, l'azienda ha visto una crescita esponenziale per diventare oggi una realtà con oltre 2.500 dipendenti e un fatturato per l'anno fiscale 2024 di oltre 621 milioni di dollari conseguendo un incremento rispetto all'anno precedente del 47% di ricavi e del 39% del reddito annuale ricorrente. Il successo di SentinelOne è, in gran parte, dovuto al proprio approccio strategico alla sicurezza, che si basa su un modello di protezione multilivello che affronta le minacce informatiche in maniera comprensiva, dalla prevenzione al rilevamento e alla risposta. L'azienda ha investito in modo significativo nella propria piattaforma Singularity sviluppata in cloud e potenziata dalla tecnologia di intelligenza artificiale Purple AI, che rappresenta una pietra miliare della sua offerta. Purple AI migliora l'efficacia degli analisti di sicurezza, permettendo loro di elaborare indagini complesse in linguaggio naturale e di ricevere risposte rapide e pertinenti, ottimizzando così il tempo di risposta agli incidenti. L'Italia fa parte della Region Southern EMEA guidata dal manager **Paolo Ardemagni**, che ricopre la carica di Vice President.

SentinelOne

UNA **CRESCITA COSTANTE** GUIDATA DALL'**INNOVAZIONE**

SentinelOne prosegue in un percorso di crescita e innovazione che l'ha portata a essere un'azienda di primo piano nello scenario globale della cybersecurity. Alla base vi è un modello di sicurezza aperto all'integrazione e multilivello che sfrutta l'AI e le più innovative tecnologie disponibili.

La storia di SentinelOne parte poco più di un decennio fa quando il fondatore e attuale CEO, Tomer Weingarten, comprese l'importanza di integrare la protezione degli endpoint (EPP) con le capacità di risposta immediata e a velocità macchina (EDR). Tale intuizione si è rivelata cruciale per affrontare le emergenti sfide della sicurezza informatica. *"Sin dai primi anni, SentinelOne si è distinta per funzionalità avanzate indirizzate non solo al rilevamento delle minacce ma anche a fornire complete opzioni di risposta* - sottolinea **Paolo Ardemagni, Vice President Southern EMEA di SentinelOne** - *come la funzionalità di Rollback che consente di ripristinare rapidamente un sistema allo stato precedente a un attacco; questa caratteristica ha contribuito al crescente apprezzamento verso l'azienda ed è oggi un* ***baluardo per la protezione da attacchi come il Ransomware****. Un ulteriore elemento distintivo delle soluzioni SentinelOne è l'uso dell'****intelligenza artificiale, presente fin dall'inizio*** *e via via potenziata attraverso tecnologie per l'analisi delle anomalie di comportamento"*.

Paolo Ardemagni
Vice President Southern EMEA di SentinelOne

UNA PIATTAFORMA PER L'ANALISI INTEGRATA

Oggi lo sviluppo dell'AI nelle soluzioni di SentinelOne raggiunge un nuovo traguardo con il recente rilascio di **Purple AI una piattaforma di intelligenza artificiale**

che abilita l'integrazione tra molteplici tecnologie di sicurezza, incluse quelle di terze parti, pensata per fornire una capacità di riconoscimento delle minacce più rapida e proattiva e funzionalità di risposta che si estendono a tutti gli ambienti, dispositivi, dati e identità che, insieme, costituiscono l'infrastruttura digitale di un'azienda. In più Purple AI prevede un'intuitiva interfaccia utente interrogabile attraverso il linguaggio naturale che permette anche agli utenti meno esperti di comprendere le dinamiche delle minacce e di acquisire consapevolezza in tempo reale sullo stato della sicurezza.

> UNA DIFESA EFFICACE RICHIEDE L'ORCHESTRAZIONE DI TECNICHE DI PROTEZIONE DIVERSIFICATE, IN GRADO DI COPRIRE TUTTE LE SUPERFICI DI ATTACCO

"In un mondo in cui l'intelligenza artificiale è a disposizione sia dei 'buoni' sia del cybercrimine, per vincere la sfida è indispensabile ***adottare una metodologia di protezione multilivello*** *che non faccia affidamento su un'unica tecnica* - sottolinea il Vice President Southern EMEA di SentinelOne -. *Purple AI rappresenta un punto di svolta nella gestione della sicurezza, offrendo semplicità, automazione e velocità di dection and response senza precedenti. Queste caratteristiche confermano* ***la nostra leadership emersa anche nei benchmark più recenti, incluso il 'MITRE Engenuity ATT&CK 2023: Enterprise'*** *dove nelle valutazioni su attacchi simulati SentinelOne ha ottenuto il 100% del livello di rilevamento e protezione, bloccando tutte le minacce senza ritardi nel rilevamento e senza richiedere modifiche della configurazione."*

UNA CRESCITA CHE NON SI FERMA

Il rilascio di Purple AI costituisce un nuovo tassello che si inserisce in una strategia di crescita alimentata anche da acquisizioni. A inizio 2024 è stata la volta di PingSafe, azienda indiana che ha portato in dote la sua piattaforma per la protezione delle applicazioni in modalità cloud-native, che ha fatto seguito a quella avvenuta nel 2021 di Scalyr, piattaforma, anch'essa cloud-native, per l'analisi dei dati su scala cloud che permette di raccogliere, correlare, ricercare e agire sui dati provenienti da qualsiasi sorgente.

"Queste acquisizioni sono state cruciali per sviluppare una gestione integrata delle minacce - afferma Ardemagni -. *Tutto ciò ci ha permesso di* ***realizzare la piattaforma integrata di rilevamento e risposta alle minacce (XDR) più avanzata del settore*** *capace di estendersi attraverso l'intera reta aziendale inclusi gli ambienti cloud e mobile. In questo contesto la piattaforma Purple AI svolge un ruolo chiave nell'integrazione con le soluzioni di sicurezza di altri fornitori attraverso connettori software o integrazioni di tipo nativo per abilitare l'analisi e la 'pulizia' dei dati provenienti da ogni sorgente."*

La direzione strategica per il futuro è di continuare a integrare le nuove tecnologie emergenti puntando non solo a reagire, ma focalizzandosi sempre più su un'idea di prevenzione.

Si tratta di un obiettivo perseguito attraverso il costante potenziamento delle proprie soluzioni di intrusion prevention, vulnerability assessment, quelle per ridurre la superficie di attacco nelle Active Directory (come Singularity Ranger AD) e per l'IoT (Singularity Ranger Insight) e, non da ultima, un'offerta di servizi gestiti (Vigilance Respond MDR) che mette a disposizione competenze e analisi SOC in modalità 24/7.

"Il valore della nostra proposta trova conferma nei numeri - conclude Ardemagni -. *In dieci anni SentinelOne è diventata un'azienda da oltre 621 milioni di dollari di fatturato, con 2.500 dipendenti in tutto il mondo di cui oltre 500 in Europa e una presenza molto forte nella regione Southern EMEA che raggruppa, oltre all'Italia, anche Paesi come Spagna, Portogallo e soprattutto Francia, dove le nostre soluzioni di sicurezza sono oggi presenti in buona parte delle aziende del CAC 40, il principale indice di Borsa francese"*.

PROTEZIONE MULTILIVELLO PER RANSOMWARE E ALTRE MINACCE

Paolo Cecchi
Sales Director Mediterranean Region di SentinelOne

Il ransomware continua a essere una delle tipologie di attacco più utilizzate dal cyber crimine e l'Italia è saldamente al primo posto in Europa per numero di attacchi di questo tipo.

Secondo **Paolo Cecchi, Sales Director Mediterranean Region di SentinelOne**, questo avviene per due ragioni principali. La prima è che è sempre più facilmente accessibile anche ai non esperti, venendo offerto come servizio dal cyber crimine e con l'AI Generativa che ne consente una facile creazione. La seconda è che continua a essere una delle minacce alle quali è più difficile rispondere perché gli attaccanti trovano sempre un modo per ingannare l'essere umano.

"Il ransomware si è evoluto come tipologia di attacco verso una modaltà "silente" – precisa Cecchi -. *Mentre, in passato, interveniva immediatamente a cifrare i dati non appena entrato nella rete di un'azienda, oggi è guidato da una strategia che prevede preventive azioni di ricognizione all'interno dell'organizzazione per cercare di capire quali sono gli asset e le risorse fondamentali disponibili, puntando a carpire un'identità o crearne una fasulla con privilegi legittimi per ottenere un successivo accesso completo a tutta l'infrastruttura aziendale evitando di venire identificato come un utente non autorizzato".*

L'IMPORTANZA DI PROTEGGERE LE IDENTITÀ

La piattaforma di SentinelOne consente di aiutare le aziende a **fronteggiare la piaga del Ransomware proteggendo, innanzitutto, le identità**. Una protezione che interviene, per esempio, in relazione agli attacchi rivolti all'Active Directory o agli endpoint, attraverso tecnologie di rilevamento e risposta in grado di riconoscere processi in cui credenziali legittime provano a effettuare attività di 'escalation" di privilegi e capaci di bloccarli. Un secondo modo in cui le soluzioni di SentinelOne intervengono per proteggere dagli attacchi ransomware è la possibilità, in caso di cifratura dei file effettata da un ransomware, di ripristinare con tempi estremamente rapidi l'ultimo stato "pulito" attraverso la funzionalità denominata Rollback, disponibile per i sistemi in ambiente Windows.

"Oggi le superfici di attacco, si stanno ampliando – osserva Cecchi - *e chi pensa ancora di poter gestire la sicurezza informatica attraverso soluzioni a silos che intervengono su specifici ambiti e superfici di attacco sta combattendo una battaglia nella quale risulterà perdente.* ***SentinelOne propone un modello basato sull'uso di una piattaforma unificata*** *all'interno della quale è possibile implementare differenti funzionalità in grado di estendere la protezione a tutte le superfici di attacco. Solo in questo modo diventa possibile aumentare la capacità di rilevamento e, di conseguenza, di protezione".*

DATA LAKE: UN UNICO LUOGO PER L'ANALISI DEI DATI

La catena di un attacco oggi è costituita da una serie di passaggi successivi che sfruttano vulnerabilità differenti. Se un attaccante riesce a sfruttare una vulnerabilità per ottenere l'accesso a un sistema, passerà al livello successivo, probabilmente cercando di sfruttare credenziali locali per muoversi lateralmente all'interno dell'azienda e arrivare magari all'Active Directory. Dopo la fase iniziale, il sistema di vulnerability management non avrà più alcun ruolo e non sarà in grado di fornire alcun contributo in relazione al modo con cui sta evolvendo l'attacco.

"Per questo motivo - spiega Cecchi - *serve* ***una piattaforma in grado di fare due cose: proteggere tutte le superfici di attacco*** *(endpoint, vulnerabilità, cloud, identità)* ***e correlare gli eventi di sicurezza associati a ogni aspetto*** *per comporre il puzzle finale in modo da individuare un attacco e scoprire come l'attaccante si sta muovendo all'interno dell'organizzazione. In mancanza di questa capacità di correlare tra loro le diverse tracce all'interno di un'organizzazione, continueremo purtroppo a essere vittime degli attacchi Ransomware".* La soluzione che realizza questo modello si chiama **Singularity Data Lake** pensata proprio per mettere a disposizione un luogo centralizzato dove tutte le informazioni provenienti da molteplici fonti e soluzioni di sicurezza vanno a convergere per essere oggetto di un'analisi centralizzata, in cui il motore di intelligenza artificiale Purple AI analizza, correla e interpreta i dati per aiutare gli analisti a identificare possibili minacce. Si tratta di una soluzione cloud native che, quindi, non ha alcun limite di scalabilità e che, proprio per questo, secondo SentinelOne fornisce prestazioni di analisi dei dati superiori rispetto alle soluzioni on-premise. *"Ciò che noi cerchiamo di fare* - osserva Cecchi - *è guidare i nostri clienti verso un approccio che sia più funzionale per loro dal punto di vista non solo dei costi e del consolidamento delle soluzioni, ma anche da quello delle* ***Security Operations****. Questo è possibile predisponendo un punto unico di aggregazione delle informazioni provenienti non solo dalle nostre soluzioni ma anche da quelli di terze parti, perché non vogliamo creare condizioni di lock-in."*

UN MERCATO ITALIANO MATURO MA POCO REATTIVO

Lo scenario italiano presenta sempre differenze rispetto ad altri Paesi ma, sul tema della sicurezza, secondo Cecchi siamo invece avanti a molti altri.

"Oggi in Italia abbiamo più di 300 clienti che ci permettono di coprire in modo trasversale tutti i mercati – spiega Cecchi -. *Rispetto ad altri Paesi del Mediterraneo come Spagna, Portogallo e Israele* ***dal punto di vista della maturità nell'adozione di soluzioni per la cyber security*** *l'Italia si posiziona a un livello più elevato. Un limite tuttavia resta quello della reticenza a cambiare velocemente le direzioni intraprese ovvero di una certa staticità dal punto di vista dell'innovazione. Per scuotere questa staticità ci avvaliamo anche dei partner che sono una risorsa molto importante per noi".*

SentinelOne fa molto affidamento sui partner e, soprattutto, sui cosiddetti fornitori di servizi gestiti (Managed Service Provider o MSP) che sono l'avanguardia sul territorio in grado di ritagliare al meglio le soluzioni di sicurezza dell'azienda sulle specifiche esigenze del cliente. Tramite i partner SentinelOne veicola servizi di sicurezza gestiti di rilevamento (Managed Detection and Response) e a breve anche inclusivi della componente di risposta (Managed eXtended Detection and Response). *"Il nostro motore di Artificial Intelligence Purple AI viene già utilizzato per i servizi di sicurezza gestiti MDR* – conclude Cecchi - *e quindi abbiamo verificato sul campo come l'****AI permetta di velocizzare le attività di Threat Hunting dell'80% e di ridurre del 60% l'mpegno di risorse richieste****. Sono numeri che evidenziano come l'AI possa migliorare moltissimo tutti i processi legati alle Security Operation."*

PURPLE AI: SICUREZZA PER ENDPOINT, IDENTITÀ E CLOUD

Marco Rottigni
Technical Director per l'Italia di SentinelOne

La rapidità nell'identificare una minaccia è un requisito essenziale. Spesso le aziende impiegano anche centinaia di giorni prima di accorgersi di essere stati violati e, nel caso del Ransomware, anche un breve lasso di tempo richiesto prima di individuarlo e bloccarlo, potrebbe essere sufficiente per rendere inutilizzabili centinaia di file e arrecare un danno all'azienda.
"È cruciale riconoscere che l'efficacia della sicurezza informatica si misura attraverso la sua capacità di servire due principali destinatari - spiega **Marco Rottigni, Technical Director per l'Italia di SentinelOne** -. *Da un lato, troviamo **gli utenti finali**, coloro che subiscono direttamente gli attacchi informatici, le infezioni e le violazioni di sicurezza. Dall'altro, abbiamo **il team addetto di Security Operations** che ha il compito critico di identificare rapidamente la natura di un incidente di sicurezza per attuare strategie volte a ridurre i danni, confinare gli attaccanti e prevenire la perdita di dati significativi, oltre a mitigare le potenziali conseguenze sulla reputazione dell'azienda. Entrambi questi gruppi condividono un fattore critico: **la necessità di agire con estrema velocità** per stare al passo con il livello di automazione che caratterizza oggi sia gli attacchi sia le tecniche di raccolta dati da parte degli aggressori".*

PROTEGGERE PIÙ SUPERFICI DI ATTACCO

Lo sforzo fatto da SentinelOne è stato di predisporre una soluzione in grado di rispondere autonomamente e in modo estremamente rapido, per neutralizzare ogni possibile infezione ai primi segni di minaccia e attivare da subito operazioni di ripristino. Per farlo il vendor ha sviluppato un modello di risposta in grado di abbracciare più superfici di attacco. *"Possiamo identificare almeno tre superfici di attacco differenti* – spiega Rottigni - *endpoint, identità e cloud a cui si potrebbe aggiungere l'ambiente mobile, che qualcuno considera una quarta superficie di attacco mentre altri una "sotto branca" degli endpoint. Le strategie di difesa per ognuna di queste sono differenti. Gli attaccanti oggi tendono a prediligere i furti di identità anziché l'uso di malware avanzato e la strategia di difesa in questo caso è di individuare e reagire. La strategia richiesta per proteggere il cloud parte dal presupposto che sia difficile che un'entità collocata in un cloud AWS, Azure o Google Cloud presenti un bug in modo analogo a quanto avviene per un'applicazione, ma sia più facile che possano insorgere problemi di configurazione inesatta o lacunosa a causa di dimenticanze o inosservanze"*. Per poter affrontare i diversi livelli di protezione SentinelOne ha predisposto una piattaforma in grado di fornire funzionalità di protezione per le superfici d'attacco diverse, aperta facilmente all'integrazione con altre soluzioni di difesa e pensata per aumentare la velocità di analisi e riposta attraverso l'uso dell'intelligenza artificiale. Questa piattaforma è Purple AI e rappresenta il substrato del modello di sicurezza proposto dall'azienda.

"La lotta tra attaccante e difensore è caratterizzata da un'elevata asimmetria in cui l'attaccante ha più tempo, più dedizione e spesso anche più risorse – spiega Rottigni -. *Se inseriamo in questo scenario anche l'intelligenza artificiale questa asimmetria viene ulteriormente accentuata. Ecco perché, se può essere una scelta per l'attaccante trarre beneficio dell'intelligenza artificiale* ***non può essere una scelta per le aziende non dotarsi di strumenti in grado di processare grandi quantità di dati in maniera affidabile.***"

LA PIATTAFORMA PURPLE AI

La piattaforma **Purple AI rappresenta la base per il modello di protezione offerto da SentinelOne, essenziale sia per la sicurezza di endpoint, identità, cloud e mobile, così come per la loro integrazione.** Purple AI fornisce elementi cruciali quali un data lake, l'uniformazione delle informazioni e la capacità di integrarsi con altre piattaforme per potenziare l'analisi degli eventi. Questi servizi, comuni a livello di piattaforma, incrementano l'agilità e la velocità delle operazioni di sicurezza. Inoltre, la piattaforma non trascura l'utente finale, garantendo un livello di protezione superiore e ampliando l'area di sicurezza coperta rispetto al passato.

Purple AI aggrega dati da varie fonti, tra cui e-mail, log di sicurezza, sistemi di sicurezza, Web e sistemi di gestione delle identità. Questi dati vengono poi inseriti all'interno di un collettore chiamato **Singularity Data Lake** dove, utilizzando l'intelligenza artificiale, subiscono un processo di normalizzazione e contestualizzazione. Le operazioni di monitoraggio, analisi e risposta sono rese semplici dall'intelligenza artificiale di SentinelOne, che accetta e restituisce istruzioni in linguaggio naturale.

"Partendo dal presupposto che è improbabile che un vendor da solo riesca a fornire tutti i componenti necessari a qualsiasi azienda per garantire una protezione completa - continua Rottigni - *e che le aziende devono comunque garantire il ritorno degli investimenti sulle scelte già fatte, Purple AI fornisce tutta la protezione estesa di SentinelOne ma è aperta anche all'integrazione e interazione con le soluzioni di sicurezza sviluppate da altri vendor affinché ciascuna di queste possa contribuire a qualificare meglio il contesto di un incidente".*

L'unico requisito richiesto è che le soluzioni delle terze parti rendano disponibile l'interfaccia software necessaria per abilitare questo livello di comunicazione ovvero le cosiddette API (acronimo di Application Programming Interface) cosa, peraltro, oggi molto diffusa.

IL RUOLO DELL'AI NELLA SICUREZZA

L'inconveniente principale che ha penalizzato le soluzioni SIEM deputate a gestire gli eventi di sicurezza è stato quello di generare una mole eccessiva di allarmi di sicurezza che, a causa del loro numero elevato, non potevano essere analizzati tempestivamente.

"In assenza delle attività di normalizzazione e automazione tramite AI i dati di sicurezza non sono più interpretabili - precisa Rottigni -. *L'intelligenza artificiale ha sempre caratterizzato le nostre soluzioni. Oggi però l'AI deve evolvere verso forme di tipo generativo perché il suo ruolo è cambiato:* ***non più semplice difensore che deve individuare un malware ma, invece, un vero e proprio collega degli analisti di sicurezza*** *in grado di partecipare a una riunione esponendo le proprie osservazioni in linguaggio naturale, fornendo suggerimenti su come proseguire nel processo di analisi e apprendendo dalle domande che vengono fatte. Un ultimo aspetto distintivo di Purple AI è la sua capacità non solo di svolgere analisi, ma anche di* ***fornire spiegazioni*** *per esempio sui log di sicurezza contribuendo a sviluppare le competenze degli analisti meno esperti e valorizzando al contempo l'esperienza degli analisti più qualificati rendendosi un vero e proprio alleato nelle security operations".*

Nel processo di interazione tra il cliente e l'intelligenza artificiale i dati degli utenti non vengono usati per addestrare l'intelligenza artificiale né condivisi con terzi.

RANSOMWARE UNA MINACCIA CHE CONTINUA A CAMBIARE PELLE

EVOLUZIONE ED EFFICACIA SONO LE PAROLE CHIAVE DI QUESTO TIPO DI ATTACCO CHE, NEL NOSTRO PAESE, È PIÙ PRESENTE CHE IN ALTRI E LA CUI DIFFUSIONE È FACILITATA ANCHE DA OFFERTE DI RANSOMWARE AS A SERVICE E DALL'AI GENERATIVA. PER MINIMIZZARE I DANNI, IN UN APPROCCIO DI RESILIENZA DEL "NON SE MA QUANDO", SERVONO FORMAZIONE, PREVENZIONE, PROTEZIONE E CAPACITÀ DI RIPRISTINO RAPIDO.

a cura della Redazione

Il Ransomware è oggi la prima minaccia al mondo per diffusione e danno ed è una piaga che colpisce l'Italia in maniera superiore ad altri Paesi. Secondo il report di Trend Micro Research "Stepping ahead of risk" sulle minacce informatiche 2023, infatti, l'Italia risulta il terzo Paese al mondo e il primo in Europa maggiormente colpito dai malware dove il ransomware ricopre un ruolo importante. Secondo la i dati della polizia postale, gli eventi di cyber crime gravi nel 2023 sono stati caratterizzati per il 34% da attacchi di tipo ransomware.

UN ATTACCO CHE BLOCCA, CIFRA, ELIMINA E SOTTRAE

In molti hanno familiarità con la definizione più tradizionale di ransomware che è quella fornita dal NIST che lo descrive come un tipo di attacco malevolo in cui gli aggressori cifrano i dati di un'organizzazione e chiedono un pagamento per ripristinare l'accesso.

In realtà al ransomware si adatta più la definizione di attacco dato che può eseguire quattro azioni fondamentali: **bloccare** l'accesso a una risorsa come uno schermo o una particolare applicazione; **cifrare** un asset rendendolo non più disponibile; **eliminare** un asset, per esempio cancellando il riferimento di un file nel file system oppure riscrivendo i suoi byte senza per forza cifrarlo; **sottrarre** dati e file e assumerne il controllo.

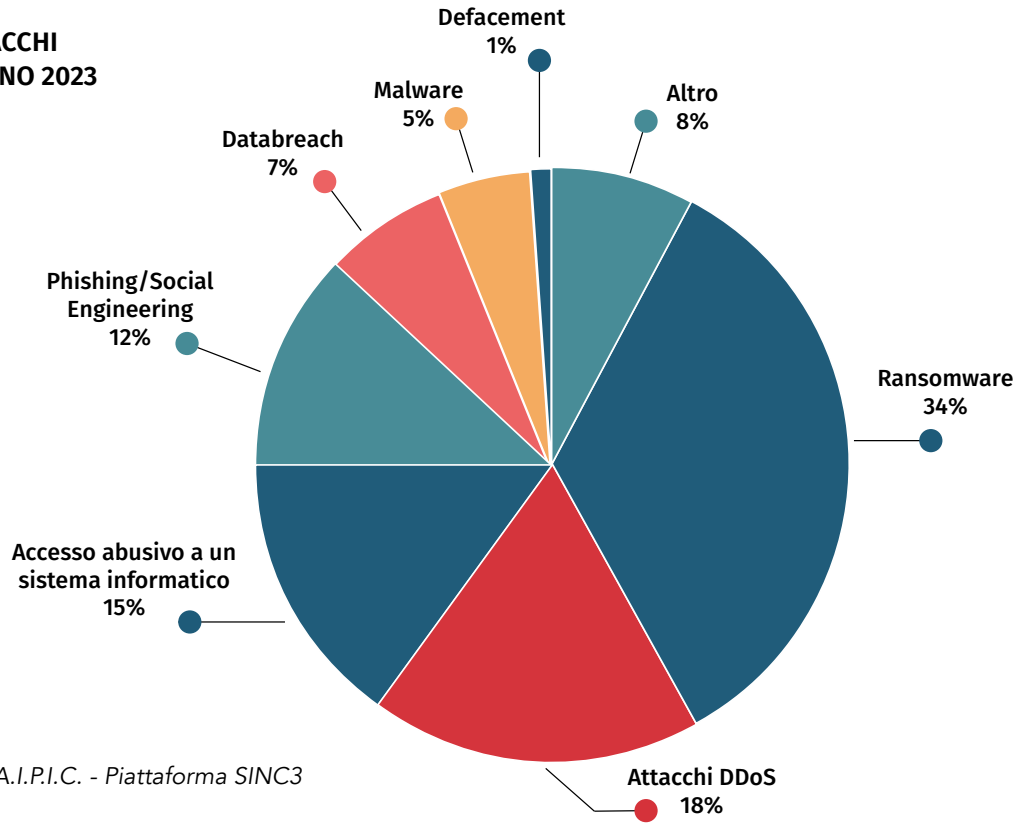
Per svolgere queste attività i ransomware continuano a evolvere adottando strategie di attacco diversificate finalizzate a massimizzare il possibile ritorno in termini di profitto.

TECNICHE EMERGENTI DI DIFFUSIONE

Oggi anche persone prive di competenza hanno la possibilità di affittare **il ransomware come un servizio (RaaS)** messo a disposizione da decine di organizzazioni criminali che operano con criteri analoghi a quelli delle aziende legittime fornendo tool, istruzioni, supporto per individuare target e punti di accesso fino a fornire servizi di assistenza e garanzia di qualità.

È in crescita anche l'attività svolta da operatori indipendenti che ha dato origine a un nuovo fenomeno denominato **Franken-ransomware**. Un termine che descrive la tendenza a mettere insieme nuove

TIPOLOGIE DI ATTACCHI
EVENTI GRAVI - ANNO 2023



© 2024 - Fonte C.N.A.I.P.I.C. - Piattaforma SINC3

varianti di ransomware utilizzando frammenti di codice rubato o divulgato da varie fonti. Il malware ESXiArgs, utilizzato per colpire i sistemi VMware nel 2023 è stato uno di questi esempi, utilizzando la nota di riscatto di un ransomware e lo schema di crittografia di un altro.

Per quanto riguarda i vettori di attacco il predominio degli allegati di posta elettronica utilizzati con i protocolli SMTP e POP3, ha lasciato il posto ai **link URL e alla navigazione sul Web come metodi predominanti per distribuire i ransomware**. A questi si aggiungono lo sfruttamento delle vulnerabilità del software e gli attacchi "forza bruta" sui servizi Remote Desktop Protocol (RDP) in cui vengono utilizzati algoritmi automatizzati per ricavare le credenziali legittime sfruttando l'uso di password deboli, mancanza di un sistema di autenticazione a due fattori o dell'adozione di reti VPN sicure.

NUOVE STRATEGIE DI ATTACCO

In passato, non appena il criminale otteneva l'accesso alla rete aziendale avviava l'attività di cifratura. Oggi invece, un attaccante che è riuscito a entrare all'interno della rete aziendale, anziché rendere immediatamente manifesta la sua presenza, predilige strategie finalizzate a muoversi al suo interno con quelli che vengono denominati spostamenti laterali, per acquisire informazioni sull'azienda, sulla sua struttura, sugli asset che detiene, sul suo stato patrimoniale e sui partner con cui intreccia relazioni commerciali e partnership tecnologiche. In tal modo riesce a valutare meglio come agire e a stabilire con precisione l'importo più alto possibile, ma non inarrivabile, che un'azienda sarebbe in grado di pagare per ritornare in possesso dei suoi dati.

In questo scenario, è frequente il tentativo di **creare identità digitali "legittime"** dotate di privilegi sempre più ampi che consentano di migliorare il livello di esplorazione e nel contempo, che possano risultare invisibili ai sistemi di "detection" tradizionali.

In molti casi l'ingresso nella rete di un'azienda può essere utilizzato per accedere ai suoi clienti.

Per esempio, compromettere l'identità digitale di una piccola software house che lavora per grandi

entità potrebbe permettere agli aggressori di inviare email convincenti e apparentemente legittime, che avrebbero più possibilità di essere aperte, facilitando così l'inserimento di malware.

SINGOLA, DUPLICE, TRIPLICE ESTORSIONE

Le novità non riguardano solo le tecniche di attacco ma anche il livello di estorsione. Le strategie di attacco non sono più di ampia portata ma si sono trasformate in attacchi mirati e personalizzati verso specifiche aziende, che talvolta puntano a riscatti di importi milionari. Tuttavia, non sempre si mira a cifre così elevate; in alcuni casi, le attività rivolte a riscatti di piccola entità possono consentire di ottenere pagamenti in modo più agevole e comportare una minore esposizione pubblica per chi effettua la minaccia.
Si definisce doppio livello di estorsione la situazione in cui alla tradizionale cifratura dei file presenti sulla rete e sui sistemi della vittima si aggiunge la minaccia di copiare questi dati e di divulgarli pubblicamente o persino di venderli nel dark web. Di conseguenza, le vittime sono motivate non solo dal desiderio di recuperare i propri dati, ma anche dalla minaccia della loro possibile diffusione e dalla rivelazione della violazione ai loro clienti e partner.
In altri casi, l'estorsione avviene esclusivamente attraverso il furto di dati, senza imporre alle vittime la cifratura. Questo tipo di estorsione offre numerosi vantaggi ai gruppi di ransomware rispetto agli attacchi basati sulla crittografia: un minore rischio di essere rilevati e la possibilità di generare profitti senza la complessità tecnologica degli attacchi di cifratura. Inoltre, l'estorsione dei dati permette ai criminali informatici di colpire più efficacemente le organizzazioni con infrastrutture critiche, le quali sono generalmente più disposte a pagare riscatti per evitare violazioni dei dati, data l'alta sensibilità e il potenziale danno associato.
A volte, si può verificare anche un terzo livello di estorsione, in cui i cyber criminali prendono di mira i clienti delle aziende compromesse, chiedendo direttamente a loro un riscatto per evitare la diffusione delle informazioni che li riguardano. Questo può servire sia per ampliare ulteriormente il profitto sia per esercitare pressione sull'azienda violata, nel caso in cui si rifiuti di pagare il riscatto richiesto.

RANSOMWARE E AI GENERATIVA

L'impiego dell'intelligenza artificiale generativa nel contesto del ransomware rappresenta un'avanzata significativa nelle tecniche utilizzate dagli attaccanti per rendere i loro attacchi più efficaci e meno riconoscibili. Le capacità dell'AI possono essere sfruttate per personalizzare massivamente gli attacchi di phishing, generando email, messaggi istantanei o comunicazioni sui social media che imitano il tono, lo stile e il contenuto di fonti legittime e familiari all'utente, aumentando notevolmente le probabilità che il destinatario clicchi su un link malevolo o scarichi un allegato infetto.
Inoltre, l'AI generativa può essere impiegata per ottimizzare i payload di ransomware. Per esempio, algoritmi avanzati possono analizzare dati rubati o accessibili pubblicamente per determinare quali tipi di file sono più critici per una specifica organizzazione. Successivamente, possono adattare il ransomware per criptare selettivamente questi file critici, massimizzando così l'impatto e, potenzialmente, aumentando la probabilità che il riscatto venga pagato.
Un altro aspetto preoccupante dell'uso dell'AI generativa nei ransomware è la capacità di questi sistemi di apprendere e adattarsi in continuazione. A mano a mano che i sistemi di sicurezza si evolvono per rilevare e neutralizzare le minacce, l'AI generativa può essere utilizzata per testare la rilevabilità dei nuovi payload di ransomware, modificandoli fino a quando non eludono con successo le misure di sicurezza attuali in un ciclo continuo di test e adattamento.

DANNI A BREVE E LUNGO TERMINE

Un attacco ransomware di successo comporta per l'azienda danni significativi che superano le mere perdite finanziarie e si protraggono oltre il periodo dell'attacco stesso.
Un **danno immediato** riguarda la possibilità di non recuperare i propri file, che possono includere informazioni critiche dei clienti. La legislazione vigente impone di informare i soggetti interessati che, di

conseguenza, potrebbero intraprendere azioni legali e decidere di non avvalersi più dei servizi dell'azienda in questione.
Altri impatti a breve termine includono la diminuzione delle vendite, la riduzione della produttività, i costi di risposta, recupero e ripristino; l'interruzione di processi aziendali critici; la perdita di asset come software, procedure interne e risorse intellettuali **in più** il costo del pagamento del riscatto, qualora l'organizzazione decidesse di cedere alla richiesta di estorsione. I **danni a lungo termine** sono altrettanto gravi. La divulgazione pubblica dei dati dei clienti può non solo causare la perdita di clienti esistenti ma anche precludere la possibilità di acquisirne di nuovi o di stringere partnership strategiche. I danni alla reputazione possono influenzare il personale, che potrebbe essere licenziato o decidere di cambiare azienda, generando una discontinuità nelle operazioni che compromette la stabilità e la continuità operativa dell'azienda. L'immediata riduzione delle entrate, conseguente all'evento, provoca ovviamente anche problemi di flusso di cassa.

PAGARE O NON PAGARE?

È l'eterno dilemma per chi ha subito un attacco di questo tipo. Le motivazioni per decidere di pagare sono diverse e comprendono principalmente il desiderio di evitare perdite di fatturato, accelerare il ripristino operativo e recuperare i dati. Chi deve prendere tale decisione si trova spesso in una situazione critica, necessitando di una soluzione rapida, il che può influenzare la lucidità nel prendere decisioni.
È importante chiarire un punto fondamentale: **non esiste una soluzione tecnologica che permetta di ripristinare i dati cifrati senza avere accesso alla chiave di cifratura** utilizzata dai cybercriminali. I dati cifrati da un ransomware sono, a tutti gli effetti, irrecuperabili se non si possiede la chiave.
Quando un'organizzazione subisce un attacco ransomware, si trova di fronte a **tre possibili scenari**. Il primo è pagare il riscatto nella speranza di recuperare i dati. Il secondo è tentare di ripristinare i dati alla condizione pre-attacco, avendo predisposto un sistema di sicurezza tecnologico capace di duplicare costantemente le risorse e di eliminare quelle compromesse per ripristinare quelle sicure. La terza opzione è quella di accettare la situazione, rimboccarsi le maniche e ripartire, assorbendo la perdita.
Tra queste, la seconda opzione è certamente la più auspicabile, ma anche quella che richiede lungimiranza che troppo spesso manca. Poter ripristinare i dati richiede la certezza che le copie di backup siano libere da codici maligni, il che non è affatto scontato considerando che, secondo i dati di Ponemon Institute, il tempo medio per rilevare una compromissione supera 200 giorni.

COME DIFENDERSI?

Il ransomware spesso entra nelle aziende attraverso azioni inconsapevoli dei dipendenti. Pertanto, **il primo passo consiste nella prevenzione**, che si attua elevando la cultura della sicurezza aziendale. È fondamentale che i dipendenti, di fronte a

email che li esortano a compiere azioni contrarie alle procedure di sicurezza, basate su presunte emergenze, abbiano l'abitudine di consultarsi con il personale addetto prima di intraprendere qualsiasi iniziativa autonoma.

Altri strumenti preventivi includono l'uso di tecnologie di detection capaci di rilevare ogni tipo di malware e intercettare e di bloccare messaggi potenzialmente pericolosi.

Questi strumenti spaziano dai sistemi di filtro antiphishing, ai sistemi di rilevamento di minacce note e attacchi zero day ma solo attraversi sistemi basati su AI è possibile intercettare azioni nocive attraessero l'analisi delle anomalie di comportamento.

Per ridurre il rischio di estorsione attraverso l'esfiltrazione dei dati, è consigliabile cifrare i dati: in questo modo, anche se sottratti, non rappresenteranno alcun valore per il cybercriminale.

Tuttavia, l'esperienza dimostra che la possibilità di un attacco ransomware riuscito, anche in presenza di tecnologie di protezione avanzate, non è mai completamente azzerabile.

La gestione del ransomware, così come altri aspetti della sicurezza IT, dovrebbe quindi essere affrontata con un approccio basato sull'analisi e sulla gestione del rischio, piuttosto che su una mera logica di protezione. Il principio guida è sempre più riconosciuto nel settore: **non si tratta di chiedersi "se" si verificherà una violazione, ma "quando" questa avverrà**, sottolineando l'inevitabilità di essere violati.

La risposta al ransomware non dovrebbe, quindi, consistere nel tentare di costruire un improbabile sistema di sicurezza impenetrabile né nel pagare il riscatto, poiché non vi è garanzia che il pagamento elimini la minaccia o impedisca future aggressioni. Risulta più indicato indirizzarsi verso **un approccio che si sposta dalla sicurezza alla resilienza**. Essere un'azienda resiliente significa essere in grado di affrontare un attacco ransomware con effetti limitati nel tempo, danni minimizzati e un'interruzione delle attività aziendali quasi nulla.

10 buone pratiche per contrastare il ransomware

1. **Formare gli utenti, inclusi quelli di tipo privilegiato, sulle più recenti tendenze del ransomware e alimentare una cultura della sicurezza.**
2. **Eseguire un backup costante di tutti i file critici e dei dati personali e tenerlo costantemente aggiornato, protetto e isolato dalla rete.**
3. **Utilizzare prodotti o servizi di sicurezza, possibilmente dotati di strumenti che utilizzano tecniche di AI per rilevare anomalie e comportamenti insoliti, per monitorare costantemente gli asset e identificare rapidamente possibili minacce.**
4. **Predisporre misure di difesa diversificate adatte a proteggere le molteplici superfici di attacco utilizzate dai criminali informatici.**
5. **Mantenere i dati critici cifrati in modo che, anche in caso di esfiltrazione, risultino inutilizzabili.**
6. **Allineare il più possibile il livello di protezione di partner e fornitori a quello dell'organizzazione.**
7. **Effettuare una valutazione regolare del rischio.**
8. **Predisporre un piano di risposta e ripristino rapido e collaudarlo periodicamente per essere sicuri che sia sempre aggiornato rispetto all'evoluzione del ransomware.**
9. **Gestire le identità e le autorizzazioni di accesso per dispositivi, utenti e processi, seguendo il principio del minimo privilegio e della separazione dei compiti.**
10. **Separare gli ambienti di sviluppo da quelli di produzione.**

UN BALUARDO CONTRO IL RANSOMWARE: LE SOLUZIONI DI **OPENTEXT CYBERSECURITY**

OpenText Cybersecurity rende le aziende resilienti al ransomware combinando tecnologie di intelligenza artificiale con soluzioni che, non solo rilevano le minacce, ma garantiscono anche una ripresa rapida e sicura delle attività aziendali in caso di incidenti

di Riccardo Florio

OpenText Cybersecurity è la divisione dedicata alla sicurezza informatica di OpenText, **una delle prime aziende di software al mondo, con un fatturato in costante crescita** (1,5 miliardi di dollari solo nell'ultimo trimestre 2024). Le soluzioni offerte da OpenText Cybersecurity offrono tecnologie all'avanguardia per il monitoraggio delle minacce, la prevenzione delle vulnerabilità, l'identificazione proattiva di attività sospette e sistemi di risposta rapida agli incidenti.

"In un mercato dove le parole spesso superano i fatti, i numeri di OpenText Cybersecurity parlano da soli - sostiene **Pierpaolo Alì, Director Southern EMEA di OpenText Cybersecurity** -. *Con migliaia di clienti serviti, oltre 95 milioni di dispositivi protetti, innumerevoli Security Operations Centers distribuiti a livello globale per monitorare e rispondere alle minacce informatiche in tempo reale e una gamma completa di soluzioni multilivello, siamo davvero in grado di rendere le organizzazioni di ogni tipo resilienti a ogni genere di minaccia, incluso il Ransomware".*

Pierpaolo Alì
Director Southern EMEA di OpenText Cybersecurity

UN MODELLO INTEGRATO PER ESSERE RESILIENTI AL RANSOMWARE

Il modello di sicurezza di OpenText Cybersecurity è progettato per offrire una **protezione olistica attraverso un approccio di difesa multilivello** basato su diverse famiglie di prodotti software, che lavorano in sinergia per coprire le differenti aree di rischio.

L'approccio di OpenText Cybersecurity oltre a prevenire le minacce assicura che, anche in caso di compromissione, l'organizzazione possa **restare resiliente ovvero mantenere la sua operatività, minimizzando l'impatto sulle operazioni di business**, anche in caso di Ransomware.

L'attuale evoluzione del Ransomware mostra un'intensificazione nei metodi di estorsione che non si limitano più alla semplice cifratura dei dati ma possono anche, per esempio, includere richieste per evitare la divulgazione pubblica di informazioni riservate sottratte. In questo scenario

sempre più complesso, il primo passo verso una difesa efficace è l'adozione di un approccio preventivo che blindi i possibili punti di ingresso nell'infrastruttura aziendale. La famiglia **OpenText ArcSight fornisce monitoraggio in tempo reale e analisi avanzata** per rilevare comportamenti sospetti e potenziali minacce prima che possano causare danni significativi. La **piattaforma di intelligenza artificiale OpenText Cybersecurity Aviator** gioca un ruolo cruciale in questo contesto, utilizzando algoritmi avanzati di machine learning non supervisionato per correlare dati provenienti da fonti diverse e identificare possibili minacce anche attraverso l'analisi di comportamenti anomali di persone e sistemi. Le funzionalità di **sicurezza delle applicazioni di OpenText Fortify** riducono il rischio di inserire vulnerabilità nello sviluppo del codice che potrebbero essere sfruttate dai cybercriminali, mentre le soluzioni per la **gestione sicura di identità e accesso OpenText NetIQ** prevengono gli accessi non autorizzati e impediscono che i cybercriminali possano sottrarre credenziale per ottenere accesso all'infrastruttura aziendale ed eventualmente svolgere attività di ricognizione, cifratura o sottrazione delle informazioni. Le tecnologie di **cifratura avanzata di OpenText Voltage** sono, invece, in grado di proteggere i dati sempre e in qualsiasi ambiente (incluso il cloud) rendendo così le informazioni eventualmente sottratte inutilizzabili e neutralizzando il rischio di una seconda estorsione tramite la minaccia di divulgazione. Un ulteriore baluardo nel fronteggiare il Ransomware è fornito da **OpenText EnCase**, **la soluzione XDR** (eXtended Detection and Response) che permette di rispondere rapidamente agli attacchi.

OPENTEXT ENCASE: L'XDR CHE RISPONDE AL RANSOMWARE

OpenText EnCase è una consolidata soluzione XDR che si distingue nel panorama della sicurezza informatica per le sue capacità di investigazione forense e risposta agli incidenti, rendendola uno strumento efficace per proteggere le infrastrutture aziendali da minacce informatiche e attacchi Ransomware. **EnCase fornisce una visibilità completa su endpoint, rete e cloud**, il che permette alle aziende di rilevare attività sospette in tempo reale. La piattaforma utilizza analisi avanzate e AI per automatizzare la raccolta di prove, l'analisi degli incidenti e la risposta. Uno dei principali vantaggi di EnCase è la sua capacità di ridurre significativamente i tempi di risposta agli incidenti: un aspetto fondamentale quando si affrontano attacchi Ransomware. EnCase aiuta le aziende a contrastare il Ransomware su più fronti. Prima di tutto, la sua **capacità di monitoraggio continuo e la valutazione delle minacce in tempo reale** consentono di intercettare i tentativi di intrusione prima che il malware possa cifrare i dati aziendali. Inoltre, la piattaforma può aiutare a identificare e isolare rapidamente i dispositivi infetti attraverso **azioni di risposta automatizzate**, limitando così la possibile diffusione del Ransomware all'interno della rete. Infine, grazie alle sue **funzionalità forensi**, EnCase permette di investigare a fondo le dinamiche di attacco, favorendo la comprensione delle tecniche degli aggressori e migliorando le strategie di difesa future. Rispetto ad altre soluzioni disponibili sul mercato, EnCase offre un'integrazione più profonda e flessibile con i sistemi esistenti, permettendo una personalizzazione che si adatta alle specifiche esigenze di sicurezza di un'organizzazione. *"Per proteggersi efficacemente, oggi è indispensabile adottare un approccio di difesa basato su una piattaforma integrata* - conclude Pierpaolo Alì -. *Molti vendor concordano su questo punto* ***ma pochi dispongono della ricchezza di soluzioni e risorse di OpenText Cybersecurity.*** *Con tecnologie come ArcSight per la gestione degli eventi di sicurezza, EnCase per la risposta agli incidenti, NetIQ per la gestione dell'accesso, Voltage per la cifratura dei dati, Fortify per la sicurezza delle applicazioni e il sostegno dell'intelligenza artificiale di Cybersecurity Aviator per analizzare e interpretare le minacce in tempo reale, OpenText offre una copertura completa capace di prevenire, riconoscere, arrestare e rimediare ogni possibile rischio e danno legato al Ransomware e non solo".*

COMBATTERE IL RANSOMWARE PORTANDO LA **PROTEZIONE VICINO ALL'UTENTE**

Protezione dell'endpoint, ma non solo, nel modello proposto da ESET che mira a supportare le aziende di ogni dimensione attraverso tecnologie di rilevamento e risposta, di intelligenza artificiale integrata da 30 anni e di servizi erogati tramite il suo SOC italiano.

di Riccardo Florio

Da oltre 30 anni ESET è un protagonista tra i fornitori di soluzioni per la sicurezza IT con un'offerta che ha saputo capitalizzare, nel tempo, i successi del suo noto antivirus (NOD 32) per svilupparsi in linea con l'evoluzione degli scenari di minaccia e approdare ora a un modello di protezione multilivello indirizzato a utenti finali, PMI e realtà enterprise.

Sotto la guida di Fabio Buccigrossi, ESET in Italia ha moltiplicato per 5 il proprio fatturato negli ultimi cinque anni e conta oggi 40 dipendenti con un proprio Security Operations Center anche nel nostro Paese, a Milano.

"ESET è un'azienda storicamente focalizzata sulla protezione degli endpoint e molto presente nel segmento delle piccole e medie imprese - sottolinea **Fabio Buccigrossi, country manager per l'Italia di ESET** -. *Nel mondo odierno sempre più digitalizzato, anche le aziende di queste dimensioni stanno acquisendo la consapevolezza dell'importanza di una protezione H24/7 dei dati aziendali, con la tendenza ad affidarsi a rivenditori specializzati per la mancanza di risorse interne. La complessità degli scenari di minaccia attuali, inclusi gli attacchi Ransomware, sollecita una gestione della sicurezza all'altezza delle nuove sfide ed ESET, insieme ai suoi partner, è in grado di fornire le soluzioni, i servizi e il supporto necessari per affrontarle".*

COMBATTERE IL RANSOMWARE PRESSO L'UTENTE FINALE

Oggi non solo la nostra vita lavorativa ma anche la gestione operativa delle imprese italiane è sempre più dipendente dal digitale; questo significa che un attacco Ransomware non riguarda più solo i dati (comunque importantissimi) ma è in grado di paralizzare la produzione di un'azienda.

"Proteggere i dati oggi richiede di ripensare le modalità di protezione e di metter in conto di incrementare il budget dedicato alla security - sottolinea Buccigrossi -. *Non si tratta solo di adottare nuove tecnologie come l'intelligenza artificiale, ma* **anche di adottare servizi di monitoraggio e gestione delle minacce e di investire sulla formazione interna del personale.** *Aumentare la cultura della sicurezza è un tema fondamentale per contrastare il Ransomware che si diffonde, soprattutto, sfruttando le azioni incaute e superficiali delle persone".*

Se l'antivirus da solo non può esaurire il livello di protezione, tra le nuove tecnologie è sempre più l'intelligenza artificiale ad assumere un ruolo centrale per anticipare e neutralizzare le minacce come il Ransomware. **ESET, sin dal lontano 1995, è pioniere nell'integrare algoritmi di Deep Learning nelle proprie soluzioni di sicurezza**, offrendo una protezione avanzata che va ben oltre i tradizionali antivirus.

Fabio Buccigrossi
country manager per l'Italia di ESET

"Poiché i dati più rilevanti per tutti noi risiedono sui nostri computer e telefoni cellulari, la protezione dell'endpoint assume un ruolo di primaria importanza in termini di sicurezza. Per questa ragione ***ESET si impegna innanzitutto a proteggere i dati presso l'utente finale*** *e aspira a posizionarsi tra i primi tre fornitori a livello globale di soluzioni per la protezione degli endpoint."*
L'insieme di tecnologie e soluzioni software compone **ESET Protect, una piattaforma di cybersecurity XDR "cloud-first"** che integra funzionalità di prevenzione, rilevamento e risposta alle minacce informatiche di nuova generazione, adatta per fronteggiare attacchi Ransomware, minacce zero-day, e-mail fraudolente e altro ancora. Infine, tutte le soluzioni tecnologiche di ESET si combinano con le competenze, i servizi e l'esperienza trentennale che caratterizzano l'azienda per comporre un modello di sicurezza pensato per agire in modo preventivo, reattivo e proattivo.

UN SOC ITALIANO PER UN MONITORAGGIO 24/7

A supporto di questa strategia ESET ha predisposto un efficace sistema di monitoraggio e risposta agli attacchi erogato attraverso un proprio Security Operations Center (SOC) dislocato a Milano dove operano professionisti della sicurezza che analizzano costantemente le infrastrutture delle aziende clienti. Attraverso il SOC vengono erogati servizi gestiti sia per le PMI sia per le grandi aziende. **ESET Managed Detection & Response ed ESET Detection & Response Ultimate sono i servizi di gestione delle minacce operativi 24 ore su 24, 7 giorni su 7**; utilizzano l'intelligenza artificiale e l'esperienza professionale per garantire una protezione da attacchi Ransomware provenienti da qualsiasi parte del mondo, eliminando così la necessità per le aziende di dover assumere tecnici specializzati.
"La decisione di realizzare un SOC in Italia - spiega Buccigrossi - è *stata presa non solo per aumentare l'efficacia di protezione ma anche per aggirare barriere linguistiche e culturali che, soprattutto durante i momenti critici di un attacco informatico, possono inficiare un'efficace difesa. Le strategie di risposta che eroghiamo* ***tramite il nostro SOC prevedono diversi livelli di servizio adattabili alle esigenze specifiche del cliente****: dalla semplice notifica di un attacco, all'intervento diretto immediato fino alla gestione post crisi. In caso di incidente possiamo anche fornire un livello di indagine estremamente approfondito e dettagliato avvalendoci del contributo del nostro team di sicurezza a Bratislava presso la sede della corporate. Possiamo anche mettere a disposizione delle aziende che lo richiedono un gruppo di tecnici esperti dedicati".*

UN VALORE AGGIUNTO FATTO DI PERSONE

In Italia, ESET punta a consolidare la propria presenza, guardando con attenzione crescente verso il mercato enterprise, ma senza per questo trascurare la solida base di clienti del mid-market.
"Le nostre ***soluzioni sono adatte anche alle aziende enterprise*** *e stiamo crescendo anche in questo segmento* - precisa Buccigrossi -. *Questo s****enza mai trascurare la nostra base installata nel mid-market*** *italiano che è ampia e fidelizzata riconoscendo in ESET una caratteristica distintiva: le persone. Un team dedicato e appassionato come il nostro è fondamentale per trasmettere e favorire lo sviluppo di una cultura di sicurezza efficace all'interno delle organizzazioni dei nostri clienti. Noi siamo ancora un vendor capace di sviluppare uno specifico progetto in base al 'commitment' del cliente, puntando a* ***sostenere ogni servizio richiesto con l'intelligenza artificiale ma anche con tanta intelligenza umana.*** *Senza dimenticare il contributo fondamentale dei rivenditori delle nostre tecnologie che, quotidianamente, promuovono la diffusione di questa cultura presso i clienti finali".*

AGRICOLTURA 4.0
LA TECNOLOGIA C'È, ORA TOCCA AGLI AGRICOLTORI

LE SOLUZIONI TECNOLOGICHE PER TRASFORMARE IL COMPARTO AGROALIMENTARE CI SONO, MA SONO POCHE LE REALTÀ VERAMENTE DIGITALI, LA MAGGIOR PARTE DELLE AZIENDE È INDIETRO

di Maurizio Ferrari

Il mondo dell'agricoltura è oggi messo sotto pressione: deve fornire sostentamento a una popolazione sempre più numerosa, deve farlo diventando più sostenibile e deve essere in grado di rispondere in modo efficace ai cambiamenti climatici che negli ultimi anni stanno creando molti problemi. La tecnologia e la ricerca, per fortuna, possono aiutare a trovare delle soluzioni a tutti questi problemi, spingendo il mondo dell'agricoltura, della zootecnia e della trasformazione verso un nuovo modo di lavorare. Purtroppo tutto il comparto fatica a iniziare questo percorso, nonostante gli incentivi che sono stati messi a disposi-

zione con il piano Transizione 4.0 negli ultimi anni. «*Nel 2023* – ha spiegato Andrea Bacchetti, direttore dell'Osservatorio Smart Agrifood del Politecnico di Milano – *abbiamo assistito a una forte crescita del mercato, ma anche a un incremento più modesto della superficie coltivata con tecnologie digitali e delle aziende che applicano concretamente almeno una tecnologia. Chi storicamente ha già investito nel digitale per l'agrifood raggiunge risultati positivi e quindi prosegue a investire in maniera ancora più intensa, ma nuove aziende faticano a fare il primo passo*». Il mercato dell'Agricoltura 4.0 è in crescita, ma dalla ricerca realizzata e presentata poche settimane fa dall'Osservatorio Smart Agrifood e del Laboratorio Rise (Research & Innovation for Smart Enterprises) dell'Università degli Studi di Brescia è emerso che la spesa cresce: ha raggiunto nel 2023 i 2,5 miliardi di euro (+19% rispetto al 2022). Tuttavia gli investimenti non hanno portato a un aumento della superficie coltivata con tecnologie digitali, che continua a essere modesta, ed è passata dall'8% del 2022 al 9% del 2023. **Il 72% delle aziende agrarie italiane utilizza almeno una soluzione di Agricoltura 4.0**, valore rimasto pressoché invariato rispetto al 2022: questo dato conferma che sono pochi i nuovi "adepti".

GLI INVESTIMENTI INSEGUONO GLI INCENTIVI

In questo ultimo anno la distribuzione della spesa è cambiata a causa della riduzione degli incentivi statali su macchinari connessi e sistemi di monitoraggio e controllo dei mezzi: fanno ancora la parte del leone, ma stanno crescendo gli investimenti in soluzioni software che permettono di interconnettere la parte hardware e di analizzare i dati raccolti. In particolare l'11% della spesa è data da software gestionali e Fmis (Farm management information systems), l'8% da piattaforme di integrazione dati, un altro 8% da sistemi di mappatura di coltivazioni e terreni, e il 5% da Dss (Software di supporto alle decisioni). «*Nell'ultimo anno temperature primaverili sotto la media, ondate di calore estive, eventi alluvionali estremi hanno messo a dura prova il settore agricolo* – ha sottolineato Chiara Corbo, direttrice dell'Osservatorio Smart AgriFood –. *In questo contesto, l'innovazione digitale ha continuato a dimostrare il suo ruolo nel rendere più sostenibile, efficiente e competitivo il settore. Abbiamo analizzato diversi casi che lo dimostrano: per esempio, le soluzioni di irrigazione di precisione possono consentire di meglio stimare le esigenze irrigue delle colture aumentando le rese, come si è verificato in un caso in Portogallo dove le rese del mais sono aumentate quasi del 30%. Oppure l'utilizzo dei Dss può consentire di impiegare in maniera più razionale gli input tecnici: in un'applicazione in vigneto in Italia, ad esempio, il risparmio di agrofarmaci è stato del 35% circa*». Dai dati della ricerca emerge un mercato dinamico, specialmente sul fronte delle soluzioni legate ad Agricoltura 4.0 che sono cresciute del 10%, come i provider tecnologici che le offrono (+13%). Sono il 20% le startup che operano in questo settore e queste ultime sono spesso focalizzate su tecnologie di frontiera, come l'Intelligenza Artificiale, Machine Learning e robotica.

COMPARTO AGRICOLO SPACCATO IN TRE SEGMENTI

Però non è tutto oro quel che luccica: solo l'8% delle aziende agricole del campione della ricerca può essere considerata "matura" a livello digitale. Il 50% si trova ancora "in cammino", mentre il restante 42% è in forte ritardo nel percorso di adozione delle soluzioni di Agricoltura 4.0 o addirittura fermo. Da questa ricerca emerge come il mondo dell'agricoltura italiano sia spaccato in tre segmenti: quelli che puntano alla trasformazione digitale, quelli che ci stanno provando e quelli che oltre al minimo indispensabile non fanno nulla. Il rischio reale è di trovarsi spiazzati di fronte a situazioni esterne, in particolare quelle climatiche, o normative che possono stravolgere il mercato: essere capaci di rispondere in modo rapido è fondamentale, specialmente in agricoltura dove la perdita della stagione può avere effetti negativi su tutta la filiera sino ai consumatori.

LA TECNOLOGIA PORTA LA **SOSTENIBILITÀ** NEI CAMPI

Utilizzare in azienda sensori IoT per raccogliere dati agronomici, connettere i mezzi agricoli, sfruttare droni e satelliti con appositi software DSS cambia il mondo di lavorare e lo rende più sostenibile

La sostenibilità è una delle chiavi di volta per l'agricoltura moderna. La sostenibilità, per essere efficace, deve, però, fare rima con **profittabilità, modernità e flessibilità**. Oggi non si tratta di applicare la rotazione dei campi o piantare leguminose per il ciclo dell'azoto; oggi è necessario sfruttare al meglio quello che la tecnologia sta offrendo per l'agricoltura di precisione. Le recenti crisi idriche hanno messo in luce come l'utilizzo di una risorsa finita come l'acqua non sia stato ottimizzato. Oggi gli agricoltori hanno a disposizione tutti gli strumenti che permettono di migliorare e rendere più efficiente l'uso dell'acqua: sensori nei campi, droni e immagini satellitari, software per elaborare questi dati e stabilire le best practice da attuare. **Analizzando con precisione l'umidità e altri dati agronomici si può ottimizzare il prelievo dell'acqua e utilizzarla dove e quando serve**. Con quelle colture che permettono l'utilizzo di sistemi d'irrigazione a goccia, diventa possibile automatizzare l'irrigazione in funzione di parametri pre impostati: riducendo così al minimo l'intervento dell'uomo, ma, soprattutto, usando in modo ottimale l'acqua. La francese **Sencrop ha elaborato un sistema di analisi di previsioni "ultra-locali" grazie alla presenza di sensori installati sul campo** che misurano la radiazione solare, l'umidità, la temperatura, il vento; attraverso i dati raccolti l'app di Sencrop fornisce all'agricoltore indicazioni sullo stato dell'evotraspirazione del terreno, cioè l'acqua persa dalla pianta, che unita ad altri dati meteo e alla disponibilità di acqua presente nel campo stabilisce quando e quanto irrigare.

SERVE IL 5G ANCHE NELLE AREE RURALI

Si tratta di un esempio di IoT applicata all'agricoltura, ma questo tipo di soluzioni ha un limite strutturale: la disponibilità di banda nelle zone rurali.

Per permettere una capillare diffusione di sensori sul campo **è necessario che la rete mobile, 4G e, meglio ancora, 5G, copra tutta la superficie coltivabile.** I moderni trattori dispongono di sensori che analizzano il terreno e li comunicano a specifici software di controllo, grazie a essi possono regolare la pressione degli pneumatici per evitare il fenomeno del compattamento del terreno.
I moduli Gps, inoltre, consentono di guidare il mezzo, trattore o mietitrebbia, ottimizzandone il percorso e automatizzandone la guida: la macchina si muoverà su "binari" con uno scarto di pochi cm, evitando le sovrapposizioni e migliorando la qualità del lavoro.

MATRIMONIO TRA MACCHINE AGRICOLE E STRUMENTI DI SUPPORTO ALLE DECISIONI

Tutti i principali costruttori di macchine agricole offrono agli agricoltori soluzioni per portare le tecnologie nei campi, integrandole all'interno dei propri mezzi e fornendo software in grado di gestire, come detto, i dati raccolti.
L'utilizzo di queste soluzioni porta a sensibili risparmi di carburante e tempo, migliorando al contempo efficienza e produttività. L'adozione di queste applicazioni Dss mette in mano agli agricoltori tutti gli strumenti, dalle analisi dei campi alle immagini satellitari, per gestire nel modo migliore tutte le operazioni: preparazione del terreno, semina, interventi fitosanitari, concimazione, diserbo, irrigazione e raccolta. Questi software sono in grado di gestire sia dati provenienti dai propri mezzi sia da fonti di terze parti, come immagini da droni e satelliti. Forniscono supporto decisionale al responsabile dell'azienda, all'agronomo, a chi opera sul campo, consentendo accessi sia via web sia attraverso app mobili.
Ibf Servizi attraverso Agronica fornisce tutti questi strumenti, e molti altri ancora, per rendere l'agricoltura di precisione alla portata di tutti. Oltre alla gestione del campo e dei mezzi, mette a disposizione della filiera agricola e della zootecnia sensori IoT per rilevare dati agronomici, strumenti informatici e competenze scientifiche. Una azienda agricola, attraverso la soluzione di Agronica, è in grado di migliorare la propria resa di diversi punti percentuali, nel contempo diminuire le emissioni di CO2 e contenere l'utilizzo dei concimi azotati.
Periodicamente **ci sono bandi, come recentemente uno da 26 milioni di euro della Regione Lombardia** appena terminato, che mettono a disposizione fondi per il rinnovamento del parco macchine e l'adozione di tecnologie per aumentare la diffusione dell'agricoltura di precisione.
Questa "evoluzione" è vista da molti stakeholder come uno dei punti fondamentali per rendere l'attuale sistema agricolo sostenibile e idoneo ad affrontare le sfide del futuro

TRACCIABILITÀ PER GARANTIRE IL CONSUMATORE

Gli stakeholder richiedono trasparenza: bisogna adottare soluzioni per rintracciare la filiera dei prodotti. La tecnologia offre l'aiuto necessario.

La tecnologia entra a gamba tesa nella gestione di diversi processi in ambito agroalimentare. È fondamentale per quanto riguarda la tracciabilità e rintracciabilità degli alimenti. Molti degli interventi delle forze dell'ordine riguardano proprio la presenza in ristoranti, negozi e magazzini di confezioni con prodotti di cui non risulta possibile stabilire l'origine e la rintracciabilità delle filiera. La normativa del 2006, il cosiddetto "pacchetto igiene", parla chiaro: **è necessario poter risalire a qualsiasi prodotto in ognuna delle fasi del ciclo produttivo.** Utilizzare la Blockchain per garantire la tracciabilità è forse la soluzione migliore, proprio per come nasce questa tecnologia.

IL NOSTRO PAESE CREDE NELLA TRACCIABILITÀ

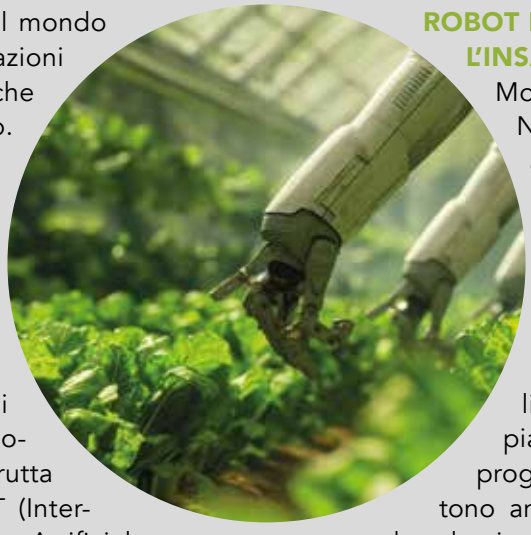
L'Italia è all'avanguardia in questo segmento del mercato, secondo gli Osservatori del Politecnico di Milano ci sono nel nostro Paese il 10% dei progetti Blockchain per la tracciabilità alimentare al mondo. Ibm è una delle società più attive in questo settore, con la sua **Ibm Sterling Supply Chain Intelligence Suite Food Trust** mette a disposizione del mondo dell'agroalimentare i benefici della Blockchain. Si tratta di una soluzione in grado di garantire l'immutabilità dei dati, protetti nella Blockchain di Ibm, e **per il consumatore finale significa avere accesso a tutte le informazioni relative al prodotto e alla sua filiera**, con la sicurezza di non incorrere in frodi. In questo mercato opera anche la francese **Connecting Food** che ha realizzato una soluzione per la tracciabilità basata su Blockchain; con i servizi proposti ha dato vita a una piattaforma di "Fiducia alimentare" pensata per garantire la trasparenza totale, acquisendo e gestendo tutte le informazioni legate all'intero ciclo di vita di un prodotto agroalimentare o zootecnico. Le fonti dei dati possono essere innumerevoli, da sensori IoT a lettori di codici a barre o etichette Rfid: ci pensa il software a gestire queste informazioni per gli adempimenti burocratici e per consentire a tutti di accedere alla filiera in modo trasparente.

IL MERCATO APPREZZA LA TRASPARENZA

Trasparenza che è molto apprezzata dai consumatori: inquadrando un Qr Code presente sulle confezioni è possibile controllare tutta la filiera di quel prodotto: origine, lavorazioni, confezionamento. Garantire tracciabilità e rintracciabilità di quello che si trova nei negozi è importante per l'agroalimentare italiano da sempre soggetto a falsificazioni e frodi, specialmente sui mercati internazionali. La trasparenza diventa sinonimo di qualità.

NEL FUTURO, SPAZIO A **AEROPONICA E IDROPONICA**

Grazie all'utilizzo di sensori IoT, software specifico e robotica si aprono nuove opportunità con colture che non consumano suolo



Una nuova frontiera per il mondo agricolo sono le coltivazioni urbane o in strutture che non consumano ulteriore suolo. Il **vertical farming, l'idroponica e l'aeroponica** permettono di sfruttare al meglio vecchi container, recuperare aree industriali dismesse e spazi urbani periferici e non solo. Si tratta di soluzioni per coltivare un'ampia varietà di vegetali in un ambiente tecnologicamente avanzato, che sfrutta le potenzialità dei sensori IoT (Internet of Things), dell'Intelligenza Artificiale e della robotica.

La startup torinese **Agricooltur ha progettato e brevettato Aerofresh, un sistema di agricoltura aeroponica**. Si tratta di una soluzione **capace di ridurre molto il consumo idrico, irrorando quando è necessario le radici** delle piante con miscele nutritive. Vengono coltivati tipicamente degli ortaggi (diversi tipi di insalate), erbe aromatiche, fragole e così via.

Questa soluzione sarà oggetto di studio dagli studenti del Ciofs-Fp Piemonte, scuola che ha aderito al progetto Edu Farm di Agricooltur.

Nelle sedi di Nizza Monferrato (Asti), Casale Monferrato e Tortona (Alessandria), gli alunni potranno scoprire e conoscere gli strumenti e le tecniche necessarie per conoscere l'agricoltura aeroponica.

ROBOT PER CURARE L'INSALATA

Molte realtà, specialmente nel Nord Europa, stanno lavorando a questo tipo di soluzioni che grazie a una rete di **sensori IoT consente di controllare tutti i parametri necessari alla crescita delle piante**, come l'illuminazione, l'umidità ambientale, l'acqua utilizzata, il posizionamento delle piante nella struttura. Ci sono progetti di idroponica che permettono anche la pescicoltura nei canali dove le piastre di coltivazione sono inserite.

L'utilizzo di robot, specialmente in strutture di certe dimensioni, permette di automatizzare molte delle operazioni, come l'irrorazione delle radici o lo spostamento delle piastre nelle posizioni richieste per la crescita ottimale e la raccolta. La danese **Seasony ha creato Watney, un robot modulare che permette diverse operazioni logistiche** all'interno delle vertical farming in modo autonomo, inoltre è pensato per raccogliere dati e immagini da inviare a sistemi di AI che gestiscono e controllano l'andamento della crescita. L'italiana Vdn sta sperimentando molte soluzioni in questo ambito e sta collaborando con diversi istituti e università per **creare figure tecniche** in grado di sfruttare al meglio queste soluzioni nel prossimo futuro perché l'agricoltore di domani deve avere anche competenze IT.

PAY OR CONSENT
IL TRATTAMENTO "CON REQUISITI" È MONETA

Una guida per il business digitale nella cessione di servizi digitali.
In primo piano l'alternativa tra pagare o abbonarsi, sullo sfondo anche i dati per l'intelligenza artificiale.

di Leo Sorge

Non solo nuovi modelli di business, ma modelli essenziali nell'oggi. Acquisire sensibilità ai termini della conversazione giuridica in atto è essenziale per orientarsi nella compliance delle numerose norme esistenti e future.

Ammissibilità del modello pay or consent: tra rivoluzione economica digitale e modernizzazione della protezione dei dati è un documento redatto dall'Istituto italiano per la Privacy e la valorizzazione dei dati. Uno degli estensori, Luca Bolognini, lo ha discusso insieme a Giovanni Maria Riccio (Studio E-Lex), Marco Scialdone (Euroconsumers), Laura Liguori (Studio Portolano Cavallo), Stefano Fratta (Meta) Guido Scorza (Componente del Garante per la protezione dei dati personali).

Parlare di un modello di business e di quale sia l'ambito regolativo nel quale si muove è essenziale per indirizzare la politica di qualsiasi azienda si muova nei contenuti: Netflix e i social network stanno sulla stessa barca, secondo un parallelo ormai accettato.

Il pay or consent prevede quindi di remunerare un servizio o con denaro, oppure cedendo il diritto all'uso dei propri dati e metadati, abilitando la relativa pubblicità personalizzata.

Va rimarcato che il dato personale è un diritto e non può essere usato come moneta. Invece **il trattamento dei dati può essere usato come moneta di scambio**, magari dettagliando -per quanto possibile- quali dati vanno a quali attori e per quanto tempo.

Questo approccio, a lungo oggetto di discussione per liceità e valore, è stato ormai accettato (prima in UE e poi in Italia): è un **modello di business di tipo contratto, "legittimo ma con requisiti".**

Per quanto riguarda le dimensioni dell'azienda che li applica si devono considerare due livelli, basso e alto. Al livello alto troviamo chi ha dimensioni ragguardevoli nei confronti dell'utente per esempio la Pubblica amministrazione o un monopolista. Al livello basso ci sono gli operatori normali, con obblighi diversi. Ma bisogna fare attenzione, perché raggruppamenti di piccoli che possano comunque raggiungere grandi dimensioni andrebbero considerati al livello alto.

Tutto risolto? No, certo, perché ci sono svariati modelli di business digitali, ciascuno con la sua interpretazione a seconda delle numerose norme che bisogna conoscere per portare avanti l'attività senza intoppi.

È lunga la lista delle tante normative: le specifiche GDPR, Direttiva CE 770/2019 e 2019/2161, le Carte (dalla Costituzione italiana ai Diritti fondamentali EU). Molti anche i pronunciamenti: in particolare, quello della Corte europea di giustizia riguardante Meta nel 2023 (CJEU C-252/21).
È quindi possibile tracciare un percorso minimo che il manager aziendale che si occupa di questo settore del business deve seguire.
Innanzitutto bisogna fare attenzione con la definizione di consenso, perché potrebbe presentarsi in modo diverso tra GDPR, ePrivacy e DMA (Digital Market Act). Si passa poi alla questione centrale, ovvero **la natura del mercato: consenso, contratto o legittimo interesse?**
Se il pay per consent è un contratto con requisiti, **nei dati per gli algoritmi di AI sta vincendo il legittimo interesse**, un tipo di accordo senza il quale non ci sarebbe proprio l'intelligenza artificiale.
Serve ora identificare i requisiti -verrebbe da dire minimi- per poter definitivamente inquadrare la cessione del trattamento come contratto. I tre principali sono oggi la fungibilità, il prezzo e l'applicabilità (definita in ePrivacy e DMA).
La fungibilità risponde a una semplice domanda: posso farne a meno di quel servizio, oppure è essenziale? La risposta cambia a secondo dei contesti: Instagram o le chat di gruppo sono oggi essenziali per i giovani, ma non per tutte le persone.
Una nota a parte la merita il problema del prezzo. In termini assoluti il valore dei dati personali (e del relativo trattamento) è molto alto, ma in termini di percepito o di mercato il valore è molto ridotto. Inoltre ciascuno assegna alle cose il valore-soglia che crede. E se la legge suggerisce ragionevolezza, il diritto non tutela gli stupidi.

UN **GREEN DATA CENTER** PER L'UNIVERSITÀ DI PISA

Si amplia e potenzia il data center dell'Università di Pisa, realizzato con il supporto di Vertiv, raggiungendo un primato di eccellenza tra le università italiane per prestazioni ed efficienza energetica

di Riccardo Florio

Fondata nel 1343, l'Università di Pisa è tra le più longeve d'Europa ed è oggi è una realtà organizzati in 20 Dipartimenti in cui orbitano 45mila studenti, 1700 docenti e 1500 tecnici amministrativi. L'Università di Pisa è stata sempre un punto di riferimento nel panorama scientifico italiano, in particolare per quanto riguarda le tecnologie informatiche grazie a un approccio costantemente rivolto alla ricerca e all'innovazione.

UN CONTRIBUTO IMPORTANTE ALLA STORIA DELL'IT ITALIANO E NON SOLO

La città della Torre pendente e di Galileo Galilei ha fornito un contributo importante alla storia dell'IT italiano. I fondatori del **primo corso di laurea in Informatica** in Italia furono due matematici dell'Università di Pisa, che stabilirono il corso oltre cinquanta anni fa, nel 1969. A Pisa fu **costruito il primo calcolatore elettronico italiano, il CEP (Calcolatrice Elettronica Pisana)**, progettato da Enrico Fermi e inaugurato nel 1961 dal presidente della Repubblica Giovanni Gronchi. Nel 1969, sulla scia di questo progetto, fu istituito il più importante centro nazionale di calcolo elettronico del paese (il CNUCE, che in seguito divenne parte del CNR) e il primo Istituto per l'Informatica (ISI) precursori dell'attuale Dipartimento di Informatica. Insieme a questi, fu fondato anche il primo corso di laurea italiano in Informatica e, successivamente, nel 1983, il primo dottorato in Italia in Informatica. Nel 1986, **la prima connessione Internet in Italia** fu realizzata anch'essa a Pisa, motivo per cui la città ospita ancora oggi il Registro dei domini nazionali .it. A partire dagli anni '90 l'università pisana ha fornito anche un contributo significativo alle reti di comunicazione con lo sviluppo della rete metropolitana di Pisa che ora serve circa 100mila utenti e contribuendo alla creazione della rete nazionale a banda ultra larga dedicata alla comunità di insegnamento e ricerca (GARR). Nel 2016 una nuova tappa importante di questo percorso è la creazione di un **Green Data Center realizzato utilizzando l'infrastruttura di Vertiv,** che oggi fa un segnare un ulteriore passo in avanti nell'innovazione tecnologica con un ampliamento che lo porta a essere uno dei centri di elaborazione dati più avanzati d'Europa, dotato delle ultime tecnologie per garantire efficienza energetica, sicurezza dei dati e scalabilità. Ancora una volta il partner di riferimento è Vertiv, che ha fornito le soluzioni di alimentazione, raffreddamento, rack, collegamento in rete e l'assistenza.

Giordano Albertazzi,
Chief Executive Officer di Vertiv

UN DATA CENTER ALL'AVANGUARDIA

Con la nuova espansione il Green Data Center dell'Università di Pisa arriva ad alloggiare 104 rack e si affianca ad altri 3 data center operati dall'università e collegati attraverso la rete a fibra otica dell'Università di Pisa che si estende fino a Livorno con oltre 90 Km di canalizzazione: un data center "core" per il collegamento alla rete GARR e altri due piccoli data center utilizzati per garantire il disaster recovery. Il Green Data Center si caratteristica per una vocazione "universitaria" ed è stato progettato per essere aperto; viene utilizzato per il 70% a supporto dell'attività di ricerca e per il 30% degli altri servizi. Ospiterà le ultimissime tecnologie di calcolo ad alte prestazioni (HPC) e i più avanzati sistemi di accelerazione grafica (GPU) di Nvidia utili per le innovative applicazioni di Intelligenza artificiale. *"Il data center aveva raggiunto la saturazione e, per questo motivo, ne abbiamo pianificato il rafforzamento tecnologico e l'ampliamento* - spiega **Giuseppe Anastasi, professore presso il Dipartimento di Ingegneria dell'Informazione dell'Università di Pisa** e Direttore esecutivo del CrossLab per le Industrie 4.0 -, *che siamo riusciti a realizzare in tempi sorprendentemente brevi grazie anche al supporto di Vertiv. Con questo progetto siamo l'unica università italiana ad avere un data center di questa livello tecnologico. Il data center sarà equipaggiato con sistemi di raffreddamento e alimentazione di ultima generazione, progettati per massimizzare la sostenibilità ambientale e ridurre il consumo energetico. La scelta di Vertiv come partner riflette l'impegno dell'Università di Pisa verso soluzioni che non solo avanzano la ricerca e l'educazione, ma promuovono anche una tecnologia responsabile e rispettosa dell'ambiente".*

UN MODELLO DI EFFICIENZA ENERGETICA

Il Green Data Center dell'Università di Pisa emerge come un modello di efficienza energetica. Il **Power Usage Effectiveness (PUE) è l'indice che misura l'efficienza energetica dei data center**, espresso come rapporto tra l'energia totale consumata da un data center e l'energia effettivamente utilizzata per le operazioni computazionali. Un PUE ottimale si avvicina a 1, indicando che la totalità dell'energia è utilizzata per l'elaborazione dei dati.

"Il sistema di raffreddamento ha un impatto che varia dal 30 al 50% sui costi dell'energia del data center e anche in questo siamo riusciti a essere all'avanguardia grazie alle soluzioni di Vertiv – spiega Anastasi –. ***Abbiamo un PUE medio compreso tra 1,15 e 1,20*** *che in inverno arriva a scendere fino a 1,05. Questo risultato non solo migliora l'impatto ambientale ma garantisce anche una significativa riduzione dei costi operativi, consolidando l'impegno dell'università verso l'innovazione e la responsabilità ecologica".* Il nuovo data center non solo rafforzerà la capacità di ricerca dell'Università di Pisa, permettendo di elaborare quantità enormi di dati con maggiore velocità e sicurezza, ma servirà anche come un punto di riferimento per le aziende e le istituzioni che operano in ambiti critici, offrendo loro accesso a risorse computazionali di primo livello.

"Vertiv è un leader nel mercato delle infrastruttura critiche - precisa **Giordano Albertazzi, Chief Executive Officer di Vertiv** - *e abbiamo una presenza importantissima nel mondo del data center che rappresenta il 75% delle nostre vendite. Il nostro impegno è globale ma diamo anche grande attenzione alle realtà locali nei paesi in cui operiamo come l'Italia, dove abbiamo centri di centri di eccellenza per le tecnologie di raffreddamento e alimentazione elettrica. Il Green Data Center dell'Università di Pisa è il risultato di una partnership che prosegue ormai da otto anni e prevede un'infrastruttura molto avanzata che lo rende pronto per supportare i workload del futuro e, nel contempo, che lo pone come modello di riferimento per l'efficienza energetica".*

SUPPORTARE I PROCESSI AZIENDALI CON GLI ANALYTICS

OGGI LE IMPRESE DEVONO SAPER ADATTARE LE PROPRIE ATTIVITÀ ALLE RICHIESTE DI UN MERCATO IN CONTINUA EVOLUZIONE. SERVONO PROCESSI AGILI E LA CAPACITÀ DI PRENDERE DECISIONI NON PIÙ BASATE SU INTUIZIONI MA SU ELEMENTI CONCRETI. LA RISPOSTA A QUESTE ESIGENZE STA TUTTA NEI DATI AZIENDALI

di Fabrizio Pincelli

È assodato che i dati che possiede un'azienda rappresentano un bene prezioso. Questo perché da tali dati si possono ottenere utili indicazioni per migliorare le attività e i processi aziendali a tutto beneficio del business. Infatti, analizzando in modo adeguato i big data prodotti da sistemi come CRM (Customer Relationship Management) o ERP (Enterprise Resource Planning) le aziende possono ricavare informazioni utilizzabili per perfezionare il marketing, la pubblicità e le promozioni così da aumentare il coinvolgimento dei clienti e i tassi di conversione. Analytics di dati storici e in tempo reale consentono di valutare l'evoluzione delle preferenze dei consumatori o dei buyer aziendali, permettendo di rispondere meglio ai loro desideri e alle loro esigenze. Alla base di questo risultato ci sono processi ottimizzati, produzioni più mirate e costi più contenuti. In so-

stanza, l'analisi dei big data può davvero fornire un supporto strategico al business. E grazie all'intelligenza artificiale e all'apprendimento automatico si può avere un riscontro in tempi sempre più brevi e con una precisione e un'efficacia sempre maggiori, guadagnando in competitività.
C'è però un problema: i dati devono essere "di qualità", altrimenti il risultato ottenuto attraverso gli analytics non solo è ben lontano dalle aspettative ma le indicazioni potrebbero anche essere fuorvianti e quindi nocive per il business. Ma cosa significa dati di qualità? Vediamolo assieme.

COSA SONO I BIG DATA

I big data sono una combinazione di dati strutturati (transazioni, database fogli di calcolo), semi-strutturati (log di server web, file XML e dati dei sensori IoT) e non strutturati (e-mail, video, file multimediali) che le organizzazioni raccolgono, analizzano ed estraggono per ottenere informazioni e insight. Il termine big data, che è stato coniato nel 2001 dall'analista Douglas Laney di Meta Group, ma è stato reso popolare da Gartner nel 2005 dopo che ha acquisito la stessa Meta Group, e si basava su tre caratteristiche, definite le tre "v": volume, varietà e velocità.
Pur non stabilendo una dimensione precisa, quando si parla di big data si intende un gran volume di informazioni dell'ordine dei terabyte o dei petabyte, ma in alcuni casi si arriva sino agli exabyte.
Riguardo la varietà, i big data provengono da molteplici fonti, tra cui i database dei clienti, i documenti, le e-mail, i log del flusso di clic su Internet, le app mobili e i social network. Vanno inclusi anche i dati generati dai dispositivi IT, come i file di log di reti, e i dati dei sensori provenienti da macchine di produzione, apparecchiature industriali e dispositivi dell'Internet of Things (IoT).
Spesso sono inclusi anche set di dati che non possono essere integrati a priori. Per esempio, un progetto di big data analytics potrebbe tentare di prevedere le vendite di un prodotto correlando i dati sulle vendite passate, sui resi, sulle recensioni online e sulle chiamate al servizio clienti.
La terza caratteristica, la velocità con cui i dati sono generati, elaborati e analizzati, è un aspetto che assume sempre più importanza. Sempre più di frequente, i set di big data sono aggiornati in tempo reale o quasi, invece che giornalmente, settimanalmente o mensilmente come accade con i data warehouse tradizionali. E la gestione della velocità diventa sempre più rilevante man mano che l'analisi si estende verso l'apprendimento automatico e l'intelligenza artificiale, dove i processi analitici individuano automaticamente gli schemi nei dati e li utilizzano per ottenere degli insight.

GESTIRE E ANALIZZARE I BIG DATA

I dati devono essere accurati e affidabili. In pratica, devono essere di qualità, perché dati grezzi raccolti da varie fonti possono causare problemi di coerenza che potrebbero essere difficili da individuare. Si deve evitare che tali problemi si verifichino operando procedure di "pulizia": dati errati provocano imprecisioni nelle analisi che possono compromettere il valore delle iniziative di business analytics.
Un discorso analogo vale per la variabilità: i big data vanno normalizzati in quanto possono avere molteplici significati o essere formattati in modo diverso in funzione delle fonti da cui sono stati estratti. Tutti questi fattori possono complicare la gestione e l'analisi.
Non solo. Avere dati di qualità significa anche assicurarsi di avere a disposizione un numero sufficiente di informazioni per produrre risultati validi.
In tal senso, va precisato che non tutti i dati raccolti hanno il medesimo valore per gli analytics. Di conseguenza, bisogna essere certi che tali dati si riferiscano ad aspetti rilevanti per i propri obiettivi prima di utilizzarli.
Per "archiviare" i big data si tende a preferire i data lake ai data warehouse. Questi ultimi, infatti, sono solitamente costruiti su database relazionali e contengono solo dati strutturati, mentre i data lake possono supportare vari tipi di dati.
Tuttavia, molti ambienti di big data combinano più sistemi all'interno di un'architettura distribuita. Per

esempio, un data lake centrale può essere integrato con altre piattaforme, tra cui database relazionali o un data warehouse.
Va da sé che per l'elaborazione dei big data serve un'adeguata infrastruttura IT. Ottenere questo tipo di capacità di elaborazione on premise limitando i costi solitamente non è semplice. Perciò, la soluzione più frequentemente adottata è di effettuare le elaborazioni nel cloud. Le aziende possono implementare sistemi propri in cloud oppure avvalersi di offerte di big data-as-a-service. In questo modo, si può scalare il numero di server in funzione delle esigenze, usandoli solo per il tempo necessario a completare i progetti di analytics. Si paga unicamente lo storage dei dati e il tempo di calcolo realmente sfruttati.

I QUATTRO MODELLI DI BIG DATA ANALYTICS

Esistono quattro tipi principali di big data analytics: descrittivo, diagnostico, prescrittivo e predittivo. Ciascuno dei quali può portare precisi vantaggi nel supporto dei processi aziendali.

Analisi descrittiva
È una delle forme più comuni di analisi che le aziende usano per rimanere aggiornate sulle tendenze attuali e sulle proprie prestazioni operative. È una delle prime fasi dell'analisi, con la quale si cerca di rispondere alla domanda "Cosa è successo?". Dopo aver identificato tendenze e intuizioni con l'analisi descrittiva, è possibile utilizzare gli altri tipi di analisi per approfondire le cause di tali tendenze.

Analisi diagnostica
È uno dei tipi più avanzati di big data analytics utilizzabili per indagare su dati e contenuti. Attraverso questo tipo di analisi, si utilizzano le informazioni acquisite per rispondere alla domanda "Perché è successo?". Esaminando i dati, è possibile comprendere le ragioni di determinati comportamenti ed eventi relativi ad azienda, clienti, dipendenti, prodotti e altro ancora.

Analisi predittiva
Come suggerisce il nome, questo tipo di big data analytics consiste nell'effettuare previsioni sui risultati futuri in base alle intuizioni ricavate dai dati. Per ottenere i migliori risultati, utilizza strumenti e modelli predittivi sofisticati, come l'apprendimento automatico e la modellazione statistica. L'analisi predittiva è oggi uno dei tipi di analisi più utilizzati.
Grazie alle previsioni effettuate con questo tipo di analisi, le aziende possono trovare modi per risparmiare e guadagnare denaro, gestire la logistica e tenere sotto controllo l'inventario. L'utilizzo dell'analisi predittiva nel reparto marketing può aiutare le aziende ad attrarre nuovi clienti e a conservare quelli esistenti. Analizzando i dati dei clienti o le tendenze attuali, le aziende possono anticipare le loro esigenze.

Analisi prescrittiva
L'analisi prescrittiva considera i risultati dell'analisi descrittiva e predittiva e individua soluzioni per ottimizzare le pratiche aziendali attraverso diverse simulazioni e tecniche. Utilizza le intuizioni ricavate dai dati per suggerire quale sarebbe il miglior passo successivo per l'azienda.

Le aziende raccolgono ogni giorno enormi quantità di dati (da clienti, dipendenti, collaboratori e così via). Tuttavia, questi dati non valgono nulla se non si sa come estrarre informazioni da essi. Le organizzazioni più grandi utilizzano i big data analytics per supportare i processi aziendali e far crescere le propria attività. Un buon motivo per seguire l'esempio e diventare un'impresa data-driven.

ERP E CRM APRONO LA STRADA AL **BUSINESS DATA-DRIVEN**

LA CAPACITÀ DI GESTIRE E SFRUTTARE I PROPRI DATI CONSENTE ALLE AZIENDE DI PRENDERE DECISIONI CONSAPEVOLI E DI OTTENERE UN NOTEVOLE VANTAGGIO COMPETITIVO. TUTTAVIA, NONOSTANTE LE AVANZATE FUNZIONALITÀ DEI SOFTWARE CRM E ERP E LA POSSIBILITÀ DI SFRUTTARE L'INTELLIGENZA ARTIFICIALE, MOLTE IMPRESE SI AFFIDANO ANCORA AI FOGLI DI CALCOLO

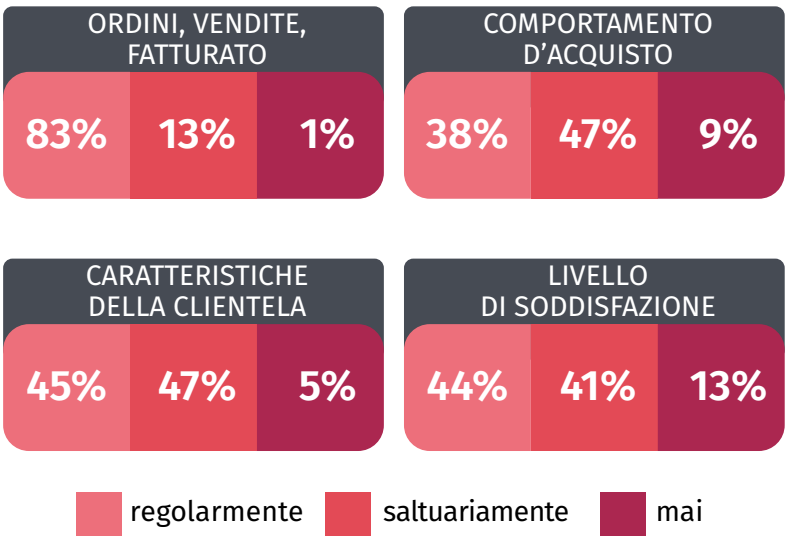
I software per il CRM (Customer Relationship Management) e l'ERP (Enterprise Resource Planning) sono strumenti utilizzati dalla gran parte delle aziende perché consentono di gestire in modo efficace due aspetti fondamentali: le relazioni con i clienti e tutti i processi core delle attività quotidiane, dal magazzino alle vendite, dagli acquisti alla finanza. E sia per il CRM sia per l'ERP, i dati sono la base dell'efficacia del loro supporto al business.

DA ARCHIVIO DATI A STRUMENTO STRATEGICO

Sono più di 30 anni che nelle aziende si usano applicativi per tenere traccia delle interazioni che la forza vendita ha con i clienti.

Proprio per questo per lungo tempo si è parlato di software per la Sales Force Automation, ma si trattava essenzialmente di contenitori dove inserire una serie di informazioni. Solo con l'arrivo di funzionalità di analisi avanzata dei dati in tempi recenti si è iniziato a parlare di CRM, ovvero di **applicazioni in grado di offrire una visione a tutto tondo delle relazioni con i clienti** e che consentono di sfruttare i dati disponibili per strutturare attività di marketing, pubblicità e promozioni così

DATI DELLA CUSTOMER BASE **MONITORATI**



Dati Osservatorio CRM

da soddisfare al meglio i clienti esistenti e anche attirarne di nuovi.
La disponibilità di big data che includono informazioni su gusti, preferenze, acquisiti, comportamenti, dati demografici e anche giudizi o desideri espressi sui social permette di conoscere in modo dettagliato la propria customer base e le sue aspettative. L'analisi di queste informazioni consente di ottenere utili indicazioni per prendere decisioni consapevoli, risultando sempre più competitivi.
Un aspetto importante, se si considera quanto emerso da un recente studio effettuato dall'**Osservatorio CRM**. Infatti, tale studio ha evidenziato che il 67% delle aziende ritiene di avere un buona oppure ottima conoscenza dei propri clienti. Tuttavia, solo il 54% analizza i dati regolarmente. E la percentuale scende ancora se si entra più nel dettaglio: il 38% controlla il comportamento d'acquisto, il 45% le caratteristiche della clientela e il 44% il suo livello di soddisfazione.
In sostanza, i dati ci sono, ma sono ancora poco consultati. Non stupisce quindi se il 72% delle aziende dice di prendere ancora le decisioni basandosi sull'esperienza e sulle intuizioni del management e nel 53% dei casi sui feedback e sulle opinioni della rete di vendita. Si è ben lontani da un modello data-driven, dove le scelte strategiche non sono basate sulle intuizioni ma su precisi insight ricavati dai dati. Soprattutto, si fa fatica ad abbandonare uno strumento consolidato come Excel, che ancora oggi nel 76% è il più usato per la gestione del cliente.
Affrontare un mercato complicato come quello attuale basandosi sui risultati ottenuti dalle elaborazioni consentite da un foglio di calcolo invece che sfruttare gli analytics avanzati dei big data, che oggi sono praticamente alla portata di tutti, significa porsi in una situazione di svantaggio rispetto ai concorrenti. Ancor più se si considera che **un terzo delle aziende italiane sta già investendo nell'intelligenza artificiale quale supporto all'analisi dei dati** potendo così disporre non solo di un sistema più efficiente, ma anche che fornisce risposte più precise che migliorano nel tempo. Ne beneficiano le campagne marketing, le vendite e anche i customer service dove si possono addestrare chatbot in grado di rispondere in modo preciso e puntuale alla maggior parte delle richieste senza l'intervento umano e con una copertura 24/7 per tutto l'anno. In pratica, ne beneficia il business nel suo complesso.

OTTIMIZZARE LE OPERAZIONI E CAPITALIZZARE LE OPPORTUNITÀ

In modo analogo a quanto accade per i sistemi CRM, anche i moderni software per l'ERP hanno un impatto radicale nel modo in cui sono gestiti i processi aziendali. I sistemi ERP tradizionali sono stati fondamentali per snellire le operazioni, ridurre i costi e migliorare l'efficienza. Hanno fornito un quadro centralizzato per la gestione dei dati,

garantendo coerenza e accuratezza tra i vari reparti. Questa centralizzazione ha facilitato la pianificazione, l'allocazione delle risorse e il processo decisionale, poiché tutte le informazioni pertinenti erano riunite in un sistema unificato. Inoltre, i sistemi ERP hanno automatizzato molte attività di routine, liberando tempo ai dipendenti che hanno potuto concentrarsi su iniziative più strategiche.

Tuttavia, nel tempo, il volume, la varietà e la velocità dei dati generati dalle aziende sono esplosi. Ciò ha determinato un **cambiamento significativo nel panorama ERP con l'integrazione di big data e analytics.** Questa integrazione ha segnato una fase di trasformazione dei sistemi ERP, trascendendo le loro funzionalità tradizionali. Sfruttando la potenza dei big data, **i sistemi ERP** attuali non sono più solo depositi di informazioni, ma **sono diventati strumenti intelligenti in grado di fornire approfondimenti e analisi predittive**.

Questa integrazione ha dato il via a un cambiamento di paradigma, migliorando in modo significativo le loro capacità in vari ambiti. Uno degli effetti più di rilievo si osserva nel campo del processo decisionale. Grazie all'analisi dei dati in tempo reale, i sistemi ERP si sono trasformati da piattaforme di archiviazione a strumenti dinamici che offrono approfondimenti praticabili nel momento in cui si verificano gli eventi.

Questa analisi in tempo reale consente alle aziende di rispondere rapidamente ai cambiamenti del mercato, ai comportamenti dei clienti e alle sfide operative. **Sfruttando i big data, i sistemi ERP possono elaborare e analizzare grandi volumi di dati** provenienti da fonti diverse, fornendo una visione olistica del panorama aziendale. Ciò consente ai responsabili delle decisioni di basare le proprie strategie e risposte su informazioni complete e aggiornate, portando a decisioni più accurate ed efficaci.

Nell'ambito della previsione e della pianificazione, l'influenza dei big data è altrettanto trasformativa. Le analisi predittive, alimentate da **sofisticati algoritmi e tecniche di apprendimento automatico, analizzano i dati storici per prevedere le tendenze e i risultati futuri.** Questo offre un prezioso supporto ai processi in vari ambiti aziendali, come la previsione della domanda, la gestione delle scorte o la pianificazione finanziaria.

Prevedendo accuratamente le tendenze e i modelli futuri, le aziende possono ottimizzare le loro operazioni, ridurre gli sprechi e capitalizzare le opportunità di mercato. Questo approccio, che è facilitato dall'integrazione dei big data nei sistemi ERP, aiuta le aziende a stare al passo con i tempi, assicurando che siano preparate a molteplici scenari di mercato.

NUTANIX INTEGRA L'AI E PUNTA AL MERCATO DI VMWARE

Nutanix continua a crescere capitalizzando sulla sua piattaforma multicloud ibrida a cui oggi si aggiungono servizi a supporto dell'AI. Si rafforza anche la partnership con Cisco con la volontà di sfruttare le opportunità di ridefinizione del mercato aperte dall'acquisizione di VMware.

di Riccardo Florio

Nutanix è stata la prima azienda a proporre, nel 2011, un modello di infrastruttura iperconvergente (HCI) che consente di gestire l'intero stack tecnologico attraverso un'unica piattaforma software in accordo al modello del software-defined. Un'altra tappa miliare nella storia dell'azienda con sede a San Jose (California) è il 2015, con il rilascio di Nutanix Acropolis Operating System che ha introdotto un sistema operativo dedicato in grado non solo di integrare storage, networking e computazione ma capace di supportare molteplici hypervisor per la virtualizzazione, inclusi VMware ESXi, Microsoft Hyper-V e, naturalmente, il proprio Acropolis Hypervisor (AHV).

UN'UNICA PIATTAFORMA PER IL MULTICLOUD IBRIDO

Da allora l'azienda non ha smesso di crescere e svilupparsi e oggi l'offerta di Nutanix ruota attorno alla **Nutanix Cloud Platform, una piattaforma per il multicloud ibrido** che mette a disposizione servizi di storage unificato, database e desktop corredata di tutti i tasselli di tipo infrastrutturale e gestionale che includono interfaccia di controllo unificata, API unificate, funzioni di sicurezza e gestione del ciclo di vita di dati e applicazioni esteso attraverso ambienti Core, edge e multicloud.

Benjamin Jolivet, country manager per l'Italia di Nutanix, può a ragione mostrare soddisfazione per gli ultimi risultati finanziari.

"Siamo spinti da un vento favorevole del mercato - sottolinea Jolivet -. *Nel nostro secondo trimestre per l'anno fiscale 2024 abbiamo ottenuto un fatturato di 565 milioni di dollari corrispondente a un incremento del 16% rispetto al medesimo periodo dell'anno precedente, mentre le entrate ricorrenti annuali (ARR) si sono attestate a 1,74 miliardi di dollari con un aumento del 26%. Un risultato che conferma il valore della nostra piattaforma e l'attenzione dei nostri clienti che ci assegnano un NPS (Net Promoter Score, l'indicatore che misura la soddisfazione dei clienti - N.d.R.) altissimo pari a 90. Inoltre il nostro hypervisor Nutanix AHV continua costantemente a crescere e viene utilizzato oggi dal 70% dei nostri clienti".*

NUTANIX GPT-IN-A-BOX PER L'INTELLIGENZA ARTIFICIALE

La partnership con Cisco rappresenta un tema strategico e abilitante per l'erogazione delle componenti di networking, elaborazione e storage all'interno della soluzione iperconvergente di Nutanix. È in questo contesto che si inserisce l'ulteriore rafforzamento della collaborazione tecnologica tra i due vendor all'insegna di quello che è il tema del momento: l'intelligenza artificiale.

"Uno studio di Vanson Bourne condotto per Nutanix rileva che il 90% delle aziende ha fatto dell'AI una priorità – precisa Jolivet – *e gli analisti di Gartner hanno recentemente dichiarato durante il loro Symposium che il 51% dei CEO si aspetta che il CIO guidi la propria strategia di intelligenza artificiale.* ***Spetta dunque ai CxO in ambito tecnologico garantire il successo dell'AI*** *e Nutanix ha sviluppato una soluzione che permette di sfruttare i benefici offerti da queste tecnologie attraverso un'unica piattaforma che abilita l'esecuzione di applicazioni, dati e AI senza soluzione di continuità dal core all'edge."*

Quella citata da Jolivet è **Nutanix GPT-in-a-Box, una soluzione software-defined chiavi in mano progettata per integrare senza problemi le applicazioni AI e AI/ML** generative all'interno delle organizzazioni, mantenendo i dati e le applicazioni sotto controllo.

GPT-in-a-Box mette a disposizione all'interno della piattaforma cloud di Nutanix nodi abilitati con acceleratori grafici GPU, infrastruttura di calcolo in rete, hypervisor AHV, orchestrazione Kubernetes e storage sia a file sia a oggetti, insieme a workshop e servizi di pianificazione, progettazione e distribuzione dello stack AI.

"La componente di elaborazione in rete è fondamentale sul multicloud e lo diverrà ancor di più con lo sviluppo dell'AI - sostiene Jolivet -. *Nutanix GPT-in-a-Box fornisce già oggi tutti i componenti tecnologici abilitanti in termini di stack per supportare l'implementazione di un set personalizzato di Large Language Model (LLM) utilizzando i principali framework di intelligenza artificiale di tipo open source e per rilasciarlo ovunque: da un ambiente edge su piccola scala a un cloud privato su scala enterprise. Il nostro intento è di arrivare, a breve, a poter consentire di generare e rilasciare un sistema AI sul nostro ambiente digitale con un solo click".*

Benjamin Jolivet
country manager per l'Italia di Nutanix

ALL'ATTACCO DI VMWARE

C'è un ulteriore obiettivo che anima la collaborazione tra le Nutanix e Cisco e che ha come oggetto il fermento di mercato causato dall'acquisizione di VMware da parte di Broadcom, che si è completata lo scorso novembre 2023 per 61 miliardi di dollari.

"L'acquisizione d VMware ha creato un periodo di incertezza sul mercato - afferma **Thomas Giudici, sales manager per il nord Italia di Nutanix** - *a cui noi siamo in grado di rispondere con strumenti idonei e un ecosistema forte che si avvale del supporto di partner importanti quali, per esempio, Cisco. Dopo l'acquisizione di VMware i nostri clienti vengono da noi con due approcci. Alcuni intendono effettuare un cambiamento completo dell'infrastruttura entro un anno mentre altri vogliono approntare una strategia "dual vendor" per dotarsi di una piattaforma alternativa su cui eventualmente migrare i workflow che erano appoggiati su tecnologia VMware."*

In questo scenario che evolve di giorno in giorno, Nutanix evidenzia l'importanza non solo dei partner tecnologici ma anche di quelli di Canale.

"Oggi la componente di incertezza riguarda anche gli operatori del Canale - sottolinea Giudici - *che per la mancanza di un partner program chiaro di VMware si trovano in difficoltà nel rispondere alle richieste dei loro clienti. Per questo stiamo incontrando i clienti che vogliono trovare un alternativa insieme sia ai nostri partner di Canale sia ai vendor che collaborano con Nutanix".*

5G
UNA CRESCITA INARRESTABILE

L'ULTIMO STANDARD PER LA CONNESSIONE MOBILE AD ALTA VELOCITÀ STA ALLARGANDO LA SUA PRESENZA SIA IN TERMINI DI COPERTURA DELLA RETE A LIVELLO GLOBALE SIA DI APPARATI VENDUTI. GRAZIE ALLE LORO PRESTAZIONI UNICHE ELEVATISSIME, LE RETI MOBILI DI QUINTA GENERAZIONE POSSONO RIVOLUZIONARE IL MODO DI FARE BUSINESS E ACCELERARE LA DIGITALIZZAZIONE DI NUMEROSI SETTORI, DALL'INDUSTRIA ALL'ECONOMIA. ECCO A CHE PUNTO SIAMO E QUALI SCENARI SI APRONO

di Aldo Cattaneo

Il 5G si sta diffondendo sempre più rapidamente nel mondo. Secondo l'ultimo report di Ericsson alla fine del 2023 almeno una linea mobile su cinque ne faceva uso. Nel dettaglio la ricerca evidenzia che rispetto al 2022 si è registrato un **incremento dei clienti 5G del 63%** (ovvero più di 610 milioni), toccando quindi quota 1,6 miliardi (cioè il 18% del totale), circa 100 milioni in più rispetto alle previsioni precedenti. L'ultimo **Ericsson Mobility Report** presenta inoltre una nuova linea temporale di riferimento per le previsioni statistiche, che passa dal 2028 al 2029. In linea con le ultime edizioni, il nuovo Mobility Report conferma che la banda larga mobile potenziata, il Fixed Wireless Access, i giochi e i servizi basati su AR/VR/ sono i primi casi d'uso più comuni per il 5G destinati ai consumatori.

A livello regionale, la diffusione degli abbonamenti 5G in Nord America continua a essere forte: entro la fine del 2023 si prevede che la regione avrà la più alta penetrazione di abbonamenti 5G a livello globale, con il 61%. La crescita degli abbonamenti 5G è stata forte anche in India durante tutto il 2023. Alla fine dell'anno – appena quattordici mesi dopo il lancio commerciale – si prevede che la penetrazione del 5G in India avrà superato l'11%.

Nell'arco di sei anni, tra la fine del 2023 e il 2029, l'Ericsson Mobility Report prevede che gli abbonamenti globali al 5G aumenteranno di oltre il 330%, passando da 1,6 miliardi a 5,3 miliardi. Si prevede inoltre che la copertura 5G sarà disponibile per oltre il 45% della popolazione mondiale entro la fine del 2023 e per l'85% entro la fine del 2029, dove il Nord America e il Consiglio di Cooperazione del Golfo, con il 92%, avranno i tassi di penetrazione 5G. L'Europa occidentale seguirà con l'85%.

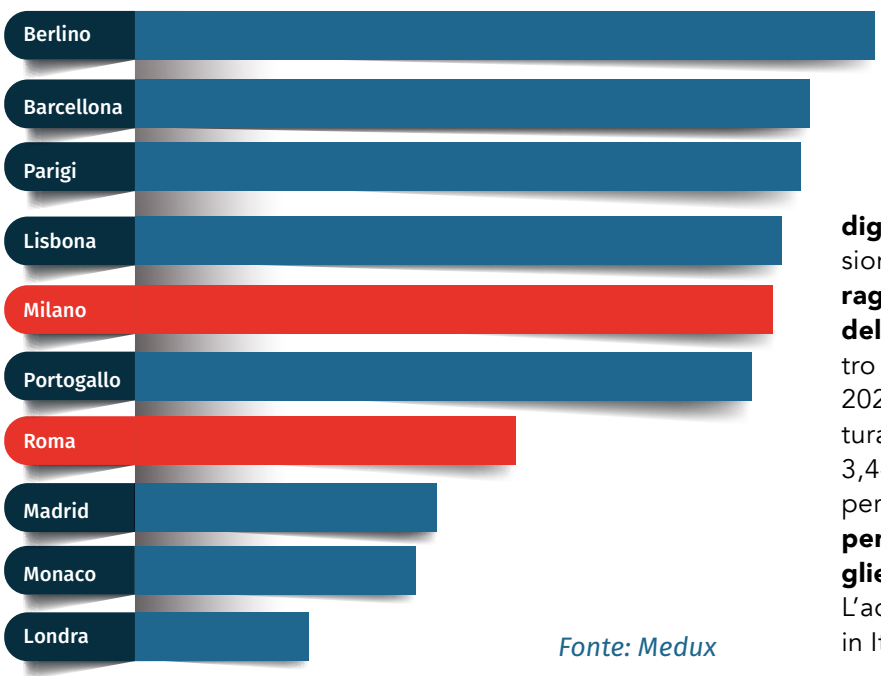
ITALIA TRA LUCI E OMBRE

Il consumo medio globale di dati per smartphone continua a crescere. L'Ericsson Mobility Report stima che il traffico dati mobile totale triplicherà tra la fine del 2023 e la fine del 2029, grazie a fattori quali il miglioramento delle funzionalità dei dispositivi, l'aumento di contenuti ad alta intensità di dati e il continuo miglioramento delle prestazioni delle reti disponibili.

Secondo il primo **Rapporto sullo Stato del Decennio digitale**, pubblicato dalla Commissione europea a fine 2023, **l'Italia ha raggiunto una copertura nazionale del 5G nel 2021** e il 93% dello spettro armonizzato è stato assegnato nel 2023. Per quanto riguarda la copertura del 5G sulla banda di frequenza 3,4-3,8 GHz, che è molto importante per abilitare applicazioni avanzate, **la percentuale complessiva di famiglie coperte è dell'80%**.

L'adozione della banda larga mobile in Italia è inferiore alla media dell'Ue,

Ranking dell'esperienza mobile 5G in Europa



Fonte: Medux

nonostante un aumento del 10% tra il 2018 e il 2021 (dal 70% all'80%). Alcuni attori del settore hanno evidenziato che problemi strutturali probabilmente ritarderanno i progressi verso gli obiettivi di connettività del Decennio digitale in Italia. Tra questi si includono il peso degli oneri amministrativi e burocratici sugli operatori, in particolare i permessi di costruzione, e altre questioni impreviste, come l'aumento dei prezzi dovuto all'inflazione.

COSA C'È DA SAPERE SUL 5G

È vero che il termine 5G è ormai entrato nel linguaggio comune come sinonimo di rete mobile di ultima generazione ad alta velocità, ma i vantaggi apportati da questo step tecnologico delle telecomunicazioni sono diversi e con applicazioni numerose sia in ambito consumer ma soprattutto in quello business. Certamente l'ultima generazione di connessione mobile **offre una velocità di trasmissione dei dati fino a 100 volte superiore di quella del 4G.** In condizioni ottimali il nuovo standard promette una velocità massima di 20 Gbps (Giga bit per secondo) che permette di scaricare rapidamente grandi quantità di dati.

A questo aspetto si unisce il **risparmio energetico:** le celle (antenne) 5G hanno un consumo energetico più contenuto anche quando operano sotto carico e sono dotate di una modalità di risparmio energetico quando sono in stand by.

Un elemento di grande interesse per l'industria è quello della **latenza minima garantita**: con questa connessione il tempo che trascorre tra l'invio del segnale e la sua ricezione per il 5G è da 30 a 50 volte inferiore al 4G.

Una latenza così contenuta permette di comandare e monitorare a distanza praticamente in tempo reale veicoli, dispositivi, apparecchi e lo stato delle infrastrutture connesse.

Infine non dobbiamo dimenticare la maggiore densità dispositivi connessi consentita, infatti il 5G permette di collegare fino a un milione di apparecchiature per km2, 100 volte di più rispetto al 4G, senza compromettere la velocità di connessione.

I VANTAGGI DEL 5G IN PILLOLE

Ecco una tabella riassuntiva di quale sia l'upgrade che il 5G ha portato rispetto alla tecnologia precedente.

Velocità: il 5G ha una velocità di trasmissione dei dati fino a 100 volte superiore di quella del 4G. In condizioni ottimali il nuovo standard promette una velocità massima di 20 Gbps (Giga bit per secondo) che permette di scaricare rapidamente grandi quantità di dati.

Risparmio energetico: le celle (antenne) 5G hanno un consumo energetico più contenuto anche quando operano sotto carico e sono dotate di una modalità di risparmio energetico quando sono in stand by.

Latenza minima: il tempo che trascorre tra l'invio del segnale e la sua ricezione per il 5G è da 30 a 50 volte inferiore al 4G. Una latenza così contenuta permette di comandare e monitorare a distanza praticamente in tempo reale veicoli, dispositivi, apparecchi e lo stato delle infrastrutture connesse.

Densità dispositivi connessi: il 5G permette di collegare fino a un milione di apparecchiature per km2, 100 volte di più rispetto al 4G, senza compromettere la velocità di connessione.

UN IMPORTANTE **STRUMENTO PER IL BUSINESS**

L'USO DEL 5G IN AMBITO BUSINESS OFFRE NUMEROSI VANTAGGI PER L'EFFICIENZA OPERATIVA, L'INNOVAZIONE E LA COMPETITIVITÀ.
DALL'IOT ALL'AUTOMAZIONE INDUSTRIALE, DALLA REALTÀ AUMENTA ALLO SMART WORKING, LE PRESTAZIONI DI QUESTO STANDARD SONO UN FATTORE ABILITANTE E DI ACCELERAZIONE DI MOLTE TECNOLOGIE A SERVIZIO DELLE ATTIVITÀ PRODUTTIVE, MA NON SOLO.

La diffusione del 5G, con un elevata velocità, latenza ridotta e alte prestazioni che il 4G non poteva garantire e che si avvicinano a quelle della fibra, offre una vasta gamma di opportunità per vari livelli del tessuto produttivo del paese. È facile quindi pensare che nessun settore come sanità, istruzione, agricoltura, manufacturing, logistica, trasporti e entertainment è o sarà escluso dalla rivoluzione abilitata dalle reti 5G. Ma vediamo su quali aspetti impatterà la nuova tecnologia: alcuni già in fase di sviluppo avanzata mentre altri con forti potenzialità che potranno essere liberate proprio dalla nuova tecnologia.

L'IMPATTO DEL 5G SUL BUSINESS

Il 5G consentirà una connettività più rapida, affidabile e a bassa latenza per un numero sempre maggiore di **dispositivi IoT**, permettendo l'implementazione su larga scala di soluzioni IoT in settori come **manifatturiero, agricoltura, salute, trasporti e logistica**.
Anche i processi di automazione industriale con le reti mobili di quinta generazione disporranno di comunicazione ultra-veloce e affidabile tra macchine, robot e sistemi di controllo, aprendo la strada alla trasformazione digitale e all'automazione avanzata nei settori manifatturiero e industriale. Non solo: rimanendo nell'ambito della robotica, **il 5G consentirà l'utilizzo di robot collaborativi** senza l'utilizzo della tecnologia via cavo (attualmente quella più utilizzata per la realizzazione di queste iniziative), permettendo una maggiore flessibilità del layout dell'ambiente lavorativo. Le prime applicazioni sviluppate in tale ambito riguardano

VENEZIA DIVENTA UNA SMART CITY GRAZIE AL 5G

Venezia si è trasformata in una smart city grazie a TIM Urban Genius, una piattaforma di "intelligenza urbana" realizzata da TIM Enterprise che impiega il 5G e le più innovative tecnologie, quali l'Intelligenza Artificiale e i Big Data, per l'analisi dei dati di campo e offrire un supporto decisionale nella gestione di un sistema complesso come quello di una città. Raccogliendo i dati con l'ultra velocità del 5G questa piattaforma permette di offrire informazioni e previsioni in tempo reale, a supporto dei decisori istituzionali, per il monitoraggio e la misura dello stato della città, della mobilità e del traffico stradale e acqueo, per governare i flussi e per assistere alla mobilità dei cittadini. La piattaforma promette di intervenire rapidamente (o di anticipare l'intervento) in situazioni di bisogno e di migliorare la pianificazione dei servizi.

robot umanoidi per fornire informazioni alla clientela o robot in fabbrica che automatizzano le operazioni più semplici.

UN FATTORE ACCELERANTE PER SANITÀ E MOBILITÀ

Negli anni passati si è molto parlato di veicoli autonomi e mobilità connessa. Il 5G fornirà la connettività con le prestazioni necessarie per abilitare i **veicoli autonomi e la comunicazione tra veicoli e infrastrutture,** migliorando la sicurezza stradale e ottimizzando il traffico. Qualche anno fa, agli albori delle reti di quinta generazione, Ericsson aveva fatto un test dimostrativo in collaborazione con Einride, nel quale aveva fatto guidare senza problemi un TIR che si trovava in Svezia da una postazione ubicata in Spagna. Per non parlare delle prime sperimentazioni sull'utilizzo di mezzi per effettuare consegne di prodotti in città (riducendo sensibilmente l'impatto di inquinamento e traffico) o per l'agricoltura di precisione. Ma non solo: il nuovo standard potrebbe portare innovazione anche in ambito **smart car**, con il miglioramento della sicurezza del guidatore e l'intrattenimento a bordo veicolo. Tra le soluzioni in ambito automotive volte a migliorare la tutela dell'automobilista troviamo sistemi per ampliare il campo visivo nei sorpassi, o l'utilizzo di smart sensor in grado di monitorare lo stato del manto stradale e facilitare lo scambio di informazioni con gli altri veicoli connessi.

Anche i settore della **sanità sta ottenendo benefici dalla connessione ultra veloce** che permette di trasmettere grandi quantità di dati medici in tempo reale, consentendo servizi come la telemedicina, la chirurgia remota, il monitoraggio dei pazienti e la gestione degli ospedali in modo più efficiente ed efficace. Pochi anni fa Vodafone, insieme all'Ospedale San Raffaele di Milano, aveva iniziato una sperimentazione per effettuare operazioni chirurgiche da remoto che ha ottenuto risultati incoraggianti.

A BARI IL PRIMO INTERVENTO ALLA CORNEA DA REMOTO CON CONNESSIONE 5G

Nel settembre 2023 l'equipe del Policlinico di Bari ha effettuato il primo intervento oculistico al mondo da remoto con il 5G di Tim. Il direttore del dipartimento di oculistica dell'ospedale, Gianni Alessio, ha operato dalla sede della direzione clinica oculistica controllando il laser a distanza, mentre il paziente era sdraiato in sala operatoria assistito da una equipe chirurgica di controllo. Nel dettaglio, il medico ha indossato un sistema di visione 3D ad alta definizione, monitorandolo e indirizzandolo a distanza per effettuare l'operazione di telechirurgia. TIM ha fornito al Policlinico di Bari l'infrastruttura necessaria a garantire la connessione 5G con latenza di trasmissione dati inferiore a 50 millisecondi tra la iVis Remote Control Station ed il laser iRes 2KHz. L'infrastruttura fornita da TIM ha previsto due moduli radio 5G installati all'interno della sala del Prof. Alessio e nella sala operatoria presso il reparto di oculistica, che hanno reso possibile il collegamento ad Internet via radio grazie all'utilizzo di appositi Router 5G. I moduli radio sono stati interconnessi direttamente alla Core Network di TIM attraverso un accesso in fibra ottica a 10Gbps.

SMART CITY, SMART RETAIL E SMART WORKING

La velocità di connessione e di volumi di dati "trasportabili" garantiti dal 5G possono svolgere un ruolo fondamentale nello **sviluppo delle smart city**, consentendo una migliore gestione dell'amministrazione della città: dai trasporti all'energia, dai rifiuti ai servizi pubblici attraverso l'Internet delle cose e l'analisi dei dati in tempo reale.

Anche il settore del retail può percorrere nuove strade di sviluppo: le reti di quinta generazione consentono l'implementazione di **esperienze di shopping personalizzate**, pagamenti contact less più rapidi, automazione dei processi di inventario e analisi avanzata dei dati di acquisto o dei percorsi all'interno del punto vendita, per comprendere meglio i comportamenti dei consumatori e adottare strategie ad hoc.

Infine una pratica trasversale a diverse attività produttive, cioè lo **smart working**, può ottenere enormi benefici da una connessione 5G, in quanto può migliorare la qualità delle call con streaming ad alta definizione, fornendo la possibilità di implementare i collegamenti tra azienda e dipendenti con contenuti interattivi e accesso a dati online più avanzate.

In sintesi, il 5G offre un'enorme potenzialità per l'innovazione e la trasformazione digitale in una vasta gamma di settori, creando nuove opportunità di business e migliorando l'efficienza, la produttività e l'esperienza del cliente.

AIUTO ARRIVA UN MESSAGGIO **WHATSAPP**

I messaggi istantanei sono diventati oggi strumenti indispensabili ma anche fonte di distrazioni e truffe. Gruppi WhatsApp insieme a spam e a comunicazioni non prioritarie, possano soffocare l'utilità dei sistemi di messaggistica.

di Primo Bonacina

L'attenzione di tutti noi è una risorsa scarsa, spesso insufficiente. Le decisioni di ogni giorno sono difficili e la vita richiede impegno. Per questo, strumenti che ci aiutino nel lavoro o tempo libero sono sempre i benvenuti. Per parecchio tempo gli SMS (oggi sostituiti da WhatsApp e similari, ma il concetto rimane) sono stati un mezzo potente, quasi indispensabile. Sentiamo un beep o una vibrazione nelle tasche. È sicuramente qualcosa di urgente che richiede risposta altrettanto sollecita:

- *"Sono in ritardo di 20 minuti. Aspettami"* è un messaggio breve, utile, informativo;
- *"Ok, ti attendo dentro il bar di Piazza Garibaldi"* è una risposta altrettanto sintetica ed efficace.

Come tutti i media che funzionano, il messaggio ha un potente effetto rete. **Quando qualcuno ti invia un messaggio, devi inviarne uno in risposta. È quasi una regola.** E, come tutti i sistemi di gruppo o rete, funziona meglio se tutti adottano lo stesso comportamento. Non a caso, nel 2014, WhatsApp ha introdotto la spunta blu. Non potete più nemmeno accampare la scusa *"Non l'avevo visto …"*.

MA ANCHE QUESTO SMETTE DI FUNZIONARE

Utili i messaggi ma poi è facile degenerare. Non mancano gli spammer malintenzionati che cercano di sfruttare lo strumento **in-**

viando messaggi subdoli e fingendo di conoscervi: *"vuoi giocare a calcetto domani?"* oppure *"tua moglie mi ha detto che stavi vendendo la casa…"*. E mentre scrivo, ho sotto gli occhi un articolo di giornale di un quarantenne ligure che ha pagato 50.000 euro credendo di acquistare da Angelina Jolie un suo fuoristrada ma, facile ora a dirsi, era una truffa. Questo episodio è solo l'ultimo degli **innumerevoli casi di truffe informatiche in costante aumento.** Le frodi vanno dai falsi investimenti nel trading online al più comune phishing per ottenere dati bancari fino ai metodi più ingegnosi, come questo. Vi contatta online una sedicente Angelina Jolie che si comporta proprio come immaginate che si comporterebbe lei. A un certo punto vi propone di vendervi la propria autovettura, mandando anche un video dell'imbarco sulla nave che l'avrebbe recapitata in Italia. E voi abboccate.

Ma a parte casi particolari come questo, i sistemi di messaggistica si corrompono a causa di persone niente affatto malvagie, ma che, semplicemente, hanno un senso dello strumento diverso dal vostro. **E quindi messaggi con 20 persone in copia.** Non conoscete la maggior parte di loro, quindi tutto ciò che vedete sono dei numeri di telefono. E ciò richiede che interrompiate ciò che state facendo. E ovviamente, se qualcuno dà seguito, tutti riceveranno la risposta. E, magari, una di quelle persone decide di approfittarne e dire a tutti gli altri di quell'evento o di quella svendita. Alla fine si esce dal gruppo o lo si silenzia e il valore della messaggistica istantanea va a morire. E, anche se non si esce dal gruppo, ben presto, i messaggi si accumulano. Poi arrivano i vocali interminabili (mi confermate che sopra i 5 minuti siamo nel penale?) e cominciate ad ascoltarli a velocità 2x (modalità Paperino). Alla fine, scoprite che avete ricevuto 5-10 messaggi all'ora, in un mix tra urgente, importante, non urgente, non importante. E, la prossima volta che arriva un messaggio decisivo, magari verrà ignorato o almeno sottovalutato. Salvo eccezioni (sto aspettando una persona, ho un'urgenza …), **sempre più persone si sono imposte di non controllare immediatamente i messaggi** per non venire continuamente interrotti.

L'ASSENZA DI PRIORITÀ

Il vero fattore è che **i messaggi sono LIFO** (Last In First Out). **L'ultimo finisce in testa e viene visto o servito per primo.** Non ci sono sfumature, nessuna lista di priorità. Spetta a ogni persona che conoscete di proteggere la vostra attenzione, spetta a ognuno di loro essere generoso, discreto e di non farvi perdere tempo. Però il costo di fare semplicemente quello che fanno molti altri è così basso che il tutto inevitabilmente degenera.

Forse l'Intelligenza Artificiale riuscirà ad aiutarci in futuro inserendo filtri (probabilmente imperfetti), ma il problema è così difficile da risolvere a posteriori da non essere particolarmente ottimisti. Eppure i messaggi sono utili e importanti. Non ne possiamo più fare a meno. **WhatsApp, la mail, il telefono sono strumenti irrinunciabili.** La regola è allora piuttosto semplice: in tutti i mezzi di comunicazione il rumore di fondo sopprime facilmente il segnale utile. L'opportunità che vi propongo, tra di voi e verso i vostri clienti e fornitori, è quella di lottare contro questo fenomeno perverso e di essere vigili nel mantenere intatta la magia che ha reso utile questi strumenti.

BASTA QUINDI CON SPAM E COLD CALLING!

Tutti i giorni ricevo offerte da parte di agenzie che mi vogliono vendere un servizio di presa appuntamenti, basato sostanzialmente su messaggi automatizzati e ripetitivi di vario tipo, che cercheranno di ingaggiare a freddo potenziali contatti. Pensateci bene. È così che volete che i vostri potenziali clienti vi vedano? Come uno spammer? Come uno che fa pesca a strascico in modo automatizzato sperando che resti attaccato qualcosa? O invece piuttosto come un professionista o azienda competente che vi contatta in modo mirato quando ha qualcosa di valido e personalizzato da proporre?

bizIT.it

MAGAZINE ONLINE DI ICT E TECNOLOGIA

INFORMATION COMMUNICATION TECHNOLOGY

bizzIT.it è la rivista online che ti aggiorna con notizie, analisi, report, approfondimenti, interviste e case history dedicati all'ICT e alla tecnologia.

Continua a seguirci su:
https://bizzit.it/

Iscriviti alla nostra newsletter https://bizzit.it/