

DIRECTION

Reportec

LA DIGITAL ECONOMY AL SUPPORTO DEL BUSINESS

La Smart Economy

**Automazione,
servizi, infrastrutture
e soluzioni sicure per
il business**

OAD: Osservatorio Attacchi Digitali in Italia

L'OAD, Osservatorio Attacchi Digitali, è l'unica iniziativa in Italia per l'analisi sugli attacchi intenzionali ai sistemi informatici delle aziende e degli enti pubblici in Italia, basata sui dati raccolti attraverso un questionario compilabile anonimamente on line.

Obiettivo principale di OAD è fornire reali e concrete indicazioni sugli attacchi ai sistemi informatici che possano essere di riferimento nazionale, autorevole e indipendente, per la sicurezza ICT in Italia e per l'analisi dei rischi ICT. La disponibilità di un'indagine sugli attacchi digitali indipendente, autorevole e sistematicamente aggiornata (su base annuale) costituisce una indispensabile base per contestualizzare l'analisi dei rischi digitali, richiesta ora da numerose certificazioni e normative, ultima delle quali il nuovo regolamento europeo sulla privacy, GDPR.

La pubblicazione dei rapporti OAD aiutano in maniera concreta all'azione di sensibilizzazione sulla sicurezza digitale del personale a tutti i livelli, dai decisori di vertice agli utenti.

OAD è la continuazione del precedente OAI, Osservatorio Attacchi Informatici in Italia, che ha iniziato le indagini sugli attacchi digitali dal 2008. In occasione del decennale OAD, in termini di anni considerati nelle indagini sono state introdotte numerose innovazioni per l'iniziativa, che includono:

- sito ad hoc come punto di riferimento per OAD e come repository, anno per anno, di tutta la documentazione pubblicata sull'iniziativa OAD-OAI: <https://www.oadweb.it>
- visibilità di OAD nei principali social network: pagina facebook @OADweb, in LinkedIn il Gruppo OAD <https://www.linkedin.com/groups/3862308>
- realizzazione di webinar gratuiti sugli attacchi agli applicativi: il primo, sugli attacchi agli applicativi, è in <https://aipsi.thinkific.com/courses/attacchi-applicativi-italia>
- questionario OAD 2018 con chiara separazione tra che cosa si attacca rispetto alle tecniche di attacco, con nuove domande su attacchi a IoT, a sistemi di automazione industriale e a sistemi basati sulla block chain
- omaggio del numero di gennaio 2018 della rivista ISSA Journal e di un libro di Reportec sulla sicurezza digitale ai rispondenti al questionario OAD 2018
- ampliamento del bacino dei potenziali rispondenti al questionario con accordi di patrocinio con Associazioni ed Ordini di categoria, quali ad esempio il Consiglio Nazionale Forense con i vari Ordini degli Avvocati territoriali
- Reportec come nuovo Publisher e Media Partner
- collaborazione con Polizia Postale ed AgID (in attesa di conferma).



INDICE

- 4 Le soluzioni che diventano smart
- 7 L'Artificial Intelligence per l'invecchiamento di successo
- 8 Dal produttore al consumatore, come portare AI nell'impresa
- 10 Smart working: in Italia crescono i consensi e la cultura
- 12 Metaenergia investe nell'IT per crescere
- 13 L'economia digitale ha bisogno di una smart city

- 16 Smart Economy: servono relazioni "trusted" tra le entità
- 19 Data Governance e GDPR in Ubi Banca
- 20 Per la Smart Economy serve un ambiente "trusted"
- 22 I data center prefabbricati e modulari aprono la strada alla Smart Economy

- 24 Per una Smart Industry servono reti e dispositivi IoT efficienti e sicuri
- 27 Reti sicure per l'Industry 4.0
- 28 La Hyper-Availability è la chiave di volta per la Smart Economy
- 30 Flash, iperconvergenza e cloud aprono la strada alla Smart Economy

Direttore responsabile: Gaetano Di Blasio
In redazione: Giuseppe Saccardi,
Gaetano Di Blasio, Paola Saccardi,
Edmondo Espa
Grafica: Airmone Bolliger
Immagini da: Dreamstime.com
Redazione:
via Marco Aurelio, 8 - 20127 Milano
Tel 0236580441 - fax 0236580444
www.reportec.it
redazione@reportec.it

Direction Reportec • anno XV - numero 104

Stampa:
Media Print Srl, via Brenta 7,
37057, S.Giovanni Lupatoto (VR)

Editore: Reportec Srl, via Marco Aurelio 8,
20127 Milano

*Il Sole 24 Ore non ha partecipato alla
realizzazione di questo periodico e non
ha responsabilità per il suo contenuto*

Presidente del C.d.A.: Giuseppe Saccardi
Iscrizione al tribunale di Milano
n° 212 del 31 marzo 2003
Diffusione (cartaceo ed elettronico)
50.000 copie
Tutti i diritti sono riservati;
Tutti i marchi sono registrati e di proprietà
delle relative società.

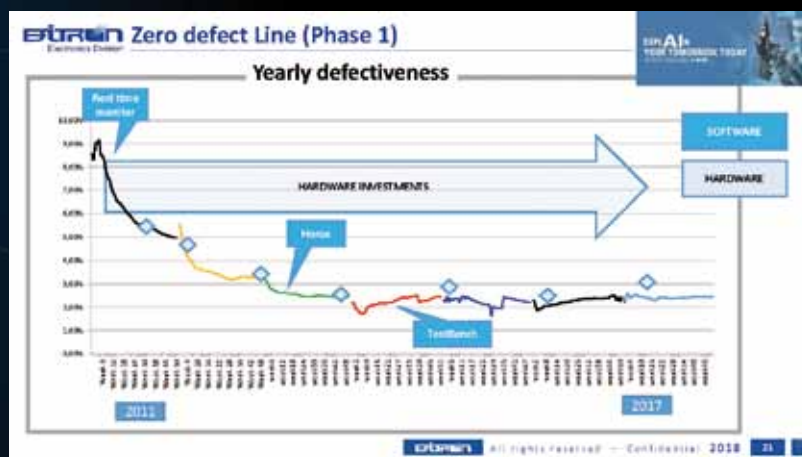
Le soluzioni che diventano smart

Le nuove tecnologie di intelligenza artificiale migliorano i processi e accelerano l'automazione

Non esiste settore economico che non possa sfruttare la potenza dei dati per rinnovare i processi, inventare nuovi modelli di business, aprire scenari inesplorati di sviluppo delle nuove tecnologie.

"Loro multicolore" del terzo millennio è rappresentato dagli algoritmi, che consentono di affinare le informazioni "decodificate" dagli advanced analytics, per alimentare motori di machine learning e deep learning, in altre parole gli strumenti per l'intelligenza artificiale, che l'immaginario collettivo, aiutato dalla letteratura e il cinema, continua a visualizzare in forme antropomorfe, ma che sta entrando nelle nostre case, con le prime applicazioni di smart home o di personal assistant, come i software di Apple, Amazon e Google, ma anche molte app che siamo abituati a usare con i dispositivi mobili.

Sembra non esserci un limite alla tipologie di soluzioni che possono sfruttare l'artificial intelligence per rinnovare processi aziendali e soluzioni o crearne di nuovi. Di fatto, sono anni che si studiano algoritmi e si sviluppano idee, ma a fare la differenza è la disponibilità dei dati e la capacità di elaborazione degli stessi in



gran quantità, fino ad arrivare al "tempo reale". Altro punto importante è l'affinamento degli algoritmi, una fase che vede protagonista ancora l'uomo, la cui intelligenza serve a interpretare i risultati delle elaborazioni.

Tra i settori più avanzati spiccano la medicina, l'industria, lo sport, il finanziario, l'energia e le telecomunicazioni. Con gli operatori che potrebbero divenire i distributori "naturali" di molti servizi disponibili online.

Alto il tasso di startup in crescita.

Di seguito elenchiamo alcuni esempi di smart solutions che abbiamo raccolto in diverse occasioni.

Per esempio nell'ambito della medicina si usano gli analytics da sempre per misurare l'efficacia delle cure, e grazie allo sviluppo dell'AI si stanno raggiungendo traguardi impensabili. È chiaro che la ricerca della longevità è una spinta primordiale e il settore è ovviamente in fermento. In effetti, la startup più finanziata, non solo in ambito medico è iCarbonx, che punta a realizzare "avatar" virtuali

per testare le terapie senza mettere a rischio i pazienti.

Uno studio con finalità analoghe sfrutta le potenzialità dei sistemi di imaging che, attraverso una videocamera, sono in grado di identificare un cancro alla pelle. Il sistema si è dimostrato molto più preciso di dermatologi esperti. Continuando con l'affinamento degli algoritmi si prevede che si possa arrivare a diagnosticare questo tipo di tumore senza bisogno di effettuare una biopsia (si approfondisca a pagina 7).

Lo sport e i manager

L'analisi delle prestazioni degli sportivi è stata utilizzata già ai tempi del Milan di Ancelotti, in particolare per ridurre il rischio infortuni, che sfruttava le analisi effettuate sugli atleti nel Milan Lab, fortemente voluto da Daniele Tognaccini, il preparatore atletico che aveva una visione scientifica dello sport. Dopo varie vittorie il Milan chiuse il laboratorio e solo più recentemente si è osservata una ripresa delle analisi che oltre al calcio interessano diversi altri sport.

Paolo del Bene, direttore sportivo di Luiss Sport Academy, illustra i molti passi avanti sul fronte delle analisi legate alle prestazioni e alle condizioni fisiche degli atleti. Laddove gli interessi economici sono alti è più facile trovare finanziamenti, ma alla Luiss si occupano di

analizzare anche i risvolti sul rendimento nello studio, e non solo, e i risultati si misurano dalle medaglie: non è un caso se o molti degli studenti della Luiss sono diventati campioni olimpionici, come Gregorio Paltrinieri, Chiara Mormile, Giorgia Pelacchi, Matteo Stefanini, Angelica Impronta, Giorgio Avola, Filippo Tortu.

Ma gli studi non si fermano al benessere e ai meriti sportivi. Ci sono, infatti, importanti parallelismi tra le strategie, le dinamiche di pensiero e quelle di esecuzione di uno sportivo e le stesse dinamiche di un manager, che deve appunto prendere decisioni, studiare e applicare strategie.

Proprio di questo si occupano presso il nel Neuroplass Lab, cui si appoggiano diverse società di calcio, compresi Milan e Chievo Verona. Le neuro scienze sono in parallelo studiate per i manager.

Diverso, invece l'insieme dei dati analizzati da Adriano Bacconi, allenatore e giornalista, nonché esperto in match analysis, che ipotizza diversi strumenti per supportare allenatori e società sportive.



La salute in casa

Se l'aria delle città è inquinata, peggiore è la situazione all'interno. Si tende a non ricambiare l'area, ma negli appartamenti, tra esalazioni provenienti dai mobili, dai sistemi di climatizzazione, dai fumi della cucina e così via, l'aria che respiriamo in casa, in ufficio e altri ambienti chiusi è 5 volte più inquinata di quella esterna, come spiega Paolo Ganis, co-fondatore di Clairry, azienda italiana con finanziamenti statunitensi ed europei. In Clairry hanno quindi ideato Natede, un dispositivo attivo che analizza l'ambiente ed effettua le dovute "correzioni", eliminando, a detta dei giovani ideatori, il 93% degli agenti organici volatili (tra cui diversi composti chimici formati da molecole dotate di gruppi funzionali diversi, aventi comportamenti fisici e chimici differenti) e il 99% dei batteri.

Un caso industry 4.0 è quello di Bitron, che ha investito, oltre che per mantenere le fabbriche in Italia e per aprirne all'estero, per migliorare la qualità del prodotto e ottimizzare i processi. Federico Perrero, Plant manager di Bitron Electronics, ha ottenuto una notevole riduzione dei pezzi difettosi, puntando alla "Zero Defect Line", grazie al monitoraggio dei dati. ❁



THE PLAYER: A COMPLEX MACHINE



L'Artificial Intelligence per l'invecchiamento di successo

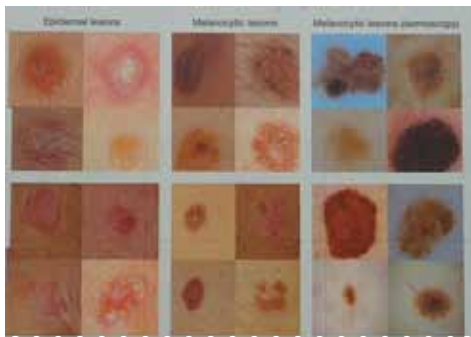
di
Gaetano
Di Blasio

Il machine learning assicura diagnosi accurate e apre nuovi fronti di ricerca in ambito medicale

Resa possibile dalle nuove tecnologie di imaging, la Radiomica è una nuova branca di analisi medica. Finora il radiologo, per valutare una diagnosi, ha avuto a disposizione una lastra, oggi può osservare un'immagine digitale a elevata risoluzione, che gli consente di essere più accurato. «Ma un'immagine digitale non è altro che un insieme di dati - ci spiega Enzo Grossi, direttore Scientifico della Fondazione Villa Santa Maria e ricercatore di Bracco -, quindi quello che "osserva" sono dati».

In effetti a "osservare" nel dettaglio i dati è appunto la radiomica, che si prefigge di estrarre informazioni matematiche dalle immagini. Tali informazioni, attraverso una progressiva raffinazione algoritmica, forniscono parametri che permettono di effettuare una diagnosi.

«Non solo una diagnosi, perché l'analisi dei dati consente di modellizzare il futuro di quella particolare diagnosi» afferma Grossi, continuando: «Si prospetta di poter fare a meno delle biopsie, una volta che addestreremo i sistemi radiomici a dare un'idea della composizione genetica della lesione



Per il tumore della pelle non occorrerà più la biopsia

rappresentata dall'immagine». Il livello raggiunto è già alto, tanto che, nei test, la macchina si è sempre mostrata più precisa dei dermatologi.

La radiologia acquisisce così sistemi molto potenti, ma le nuove soluzioni di imaging, consentono anche di "vedere" diversi elementi potenzialmente critici, come un restringimento arterioso in una gamba invisibile per gli strumenti attuali.

Con l'età media che cresce, sarà sempre più importante prevenire, per puntare a quello che Grossi definisce "invecchiamento di successo", perché tutti vogliono vivere a lungo, ma non trasformandosi in un vegetale e qui si aprono tanti altri fronti d'investigazione, per esempio sul microbiota o l'epigenetica.

Know how italiano

Quanto rapidamente si arriverà a questo futuro dipende soprattutto dagli investimenti necessari, ma ci sono diverse università che mettono a disposizione risorse, in particolare di calcolo, oltre a comunità open source.

Grossi, tra l'altro, è ricercatore associato nella onlus Semeion, fondata nel 1985, con personalità giuridica riconosciuta dal 1991 dal Miur (il ministero dell'Istruzione), che sviluppa sistemi d'intelligenza artificiale proprietari da oltre 25 anni. «Abbiamo dimostrato come questi sistemi siano in grado di rispondere a domande che, prima, non si credeva neanche di poter porre: per esempio riuscire a fare diagnosi a livello individuale ottenendo la statistica del singolo individuo».

Quello che sembra un ossimoro è il frutto di analisi con tassi di accuratezza molto elevati, che vengono ripetuti da diversi sistemi, ciascuno addestrato a un punto di vista differente. È la filosofia dei "molteplici giudici", cioè un ribaltamento dell'approccio che tende ad analizzare un campione statistico. Avendo un solo individuo si moltiplicano le statistiche. Questi sistemi di assistenza decisionale sono stati forniti a diversi medici che li hanno "testati" sul campo. ✱

Dal produttore al consumatore, come portare AI nell'impresa

Raccogliere i dati per trasformarli in azioni. Alessandro de Bartolo, country general manager di Lenovo Data Center Group Italia, ci spiega come sfruttare l'artificial intelligence per sviluppare il business aziendale

"Come il cibo per gli esseri umani, i dati sono la risorsa che alimenta diversi aspetti della vita aziendale. Quindi, analogamente al ciclo naturale, che permette di produrre gli alimenti, dalla semina al raccolto fino alla combinazione, il condimento e alla preparazione di un pasto, anche i dati devono essere utilizzati al meglio traendone il massimo vantaggio per sfamare e irrobustire l'azienda e farla crescere."

Con questa metafora, Alessandro de Bartolo, country general manager di Lenovo Data Center Group Italia, introduce l'importante questione del come si possono raccogliere i dati per ricavarne informazioni da tradurre in azioni.

Afferma il manager: «I dati, in genere, rimangono nel luogo dove sono creati, tendono ad attirare dati simili nelle loro vicinanze e in alcuni casi sono confinati all'interno di specifici limiti. Le imprese stanno quindi cercando di trarre valore dai dati già presenti nei loro sistemi e da quelli che continuamente vi entrano».

Da qui, continua de Bartolo, nasce l'esigenza di avere a disposizione una potenza di calcolo sufficientemente elevata da consentire l'estrazione di valore. «Mantenendo l'analogia con il cibo, questi dati rappresentano la produzione locale, il chilometro zero, per così dire». Le tecnologie IT per abilitare la raccolta e la preparazione dei dati, come per ogni nuova tecnologia necessitano di specifici passi da compiere, così come in cucina si devono impiegare le tecniche per la preparazione del piatto: «La formazione e la valutazione dei modelli di Machine Learning (ML) e Deep Learning (DL) sono simili alla preparazione di una ricetta di cucina, mentre la messa in opera di modelli formati in determinate applicazioni è analoga all'impiattamento e al servizio» esemplifica il manager, che continua: «Guardando alle diverse fasi del flusso di lavoro, è sempre utile capire quali siano i blocchi di tecnologia da utilizzare in ciascuna fase, la prima inizia con la raccolta dei dati non elaborati, che richiede capacità di immagazzinamento, trasformazione e storage».



Alessandro de Bartolo,
general manager di
Lenovo Data Center
Group Italia

In questa fase è di importanza fondamentale gestire il volume, la varietà e la velocità dei dati con un'infrastruttura adatta. I dati strutturati sono poi inseriti nei database e nelle data warehouse, mentre i dati non strutturati entrano nei cluster Hadoop. I dati specialistici semistrutturati possono essere immagazzinati ora in un tipo ora nell'altro di questi depositi. Collettivamente, i dati sono incorporati in un'architettura cosiddetta di enterprise data lake. Occorre poi disporre tutti i dati, che porta alla possibilità di estrarli preparando data set specifici. Questi possono essere utilizzati per formare i modelli ML e DL. È qui che entra in gioco il data scientist, che fornisce gli strumenti adeguati per ripulire e curare i dati in modo da renderli utilizzabili, esattamente come gli ingredienti da adoperare in una ricetta di cucina, ci spiega sempre de Bartolo. Un'altra fase importante prevede la formazione e la valutazione dei modelli, che è l'altra responsabilità del data scientist, e richiede la capacità di creare test di calcolo con diversi gradi di variabilità in termini di modelli, parametri, data set e metriche di risultato. «È necessaria molta sperimentazione per arrivare al giusto

equilibrio fra infrastrutture scalabili, tool di orchestrazione e gestione facili da usare, framework potenti e ambienti di programmazione che consentano di selezionare i giusti modelli», sottolinea il manager italiano, che aggiunge: «Dopo aver selezionato i modelli, si può iniziare a fare delle deduzioni. Questa è la fase in cui il modello è incorporato nel software applicativo, che adotterà le analitiche di nuova generazione per fornire una visione migliore e sostenere un processo decisionale più produttivo».

Attenzione agli errori del passato

Alessandro de Bartolo ci mette in guardia: «L'adozione dell'AI nell'impresa deve partire dall'esperienza dei processi di adozione delle nuove tecnologie del passato, per esempio il cloud 6-8 anni fa o i Big Data 3-4 anni fa. Una delle lezioni più importanti di quelle esperienze è di evitare di fare progetti autonomi, in quanto più di tre quarti di questi è fallito. Non è solo una questione di tecnologia, infatti se non si affrontano anche i cambiamenti di processo e cultura all'interno dell'azienda, anche la migliore tecnologia diventa una semplice curiosità che rischia di non essere utilizzata al meglio». È pertanto opportuno, afferma ancora il manager, scegliere una funzione aziendale per sperimentare l'adozione dell'AI con un progetto pilota e selezionare il software applicativo che la implementa e abilita. «Questo passaggio è paragonabile

a scegliere un tipo di cucina. Lanciare un programma pilota, acquisire e preparare i dati, esplorare con la formazione e il benchmarking i modelli più adatti per gli algoritmi ML e DL; questo è come selezionare le ricette e i menu. Selezionare i modelli migliori e incorporarli nell'applicazione è, invece, la consumazione. Naturalmente la continua raffinazione dei modelli sulla base del feedback ricevuto dall'uso continuo è necessaria per rimanere al passo con l'evoluzione del mercato».

Una volta che la fase pilota è completa e il processo è entrato in produzione, si può ripetere con l'applicazione successiva, e così via.

«Vi sono altre necessità -», avverte inoltre de Bartolo - Chiedere consiglio e coinvolgere persone con le giuste competenze è fondamentale. Esplorare i modelli ML/DL può essere di per sé un progetto. È importante concentrare lo sforzo sul dominio applicativo da abilitare con funzioni AI».

Conclude quindi il manager: «Portare l'AI nell'impresa può sembrare un lavoro complesso, così come cucinare può essere uno stress per chi non si sa destreggiare ai fornelli. Chi sta imparando probabilmente prenderà lezioni da uno chef e allo stesso modo Lenovo Data Center Group può fornire l'infrastruttura, gli strumenti associati e l'esperienza di ecosistemi che possano rendere questo viaggio nell'Intelligenza artificiale un viaggio che vale la pena di fare».✱

Smart working: in Italia crescono i consensi e la cultura

Un'indagine commissionata da Citrix mostra quanto è apprezzato il lavoro flessibile, soprattutto quando la tecnologia migliora la user experience e garantisce la sicurezza

Lo smart working si fonda essenzialmente su due aspetti: una cultura organizzativa innovativa e la tecnologia. La prima è fondamentale, perché è evidente come un approccio tradizionale che misura il lavoro in "ore passate in ufficio" sia incompatibile con il concetto di flessibilità. La seconda è altrettanto basilare, perché serve ad abilitare l'operatività all'esterno dell'ufficio. Dosando bene questi ingredienti i risultati arrivano e sono sorprendenti.

Una ricerca (commissionata da Citrix all'istituto di ricerca OnePoll e condotta online su un campione di 500 persone tra i 18 e 55 anni di età, occupati e residenti in Italia, distribuite tra Nord, Centro e Sud) mostra come gli italiani stanno vivendo questo cambiamento culturale che propone di sostituire il tradizionale ufficio con un ambiente di lavoro virtuale.

Non solo lo smart working non è più percepito come una minaccia per la carriera, né considerato dispersivo (il 91% degli intervistati ritiene che migliori la produttività), ma per il 70% è un'opportunità e il 50% lo ritiene la modalità di lavoro del futuro.

Questo entusiasmo deriva in massima parte dalla tecnologia, ci spiega Benjamin Jolivet, country manager di Citrix per Italia: «La diffusione dei device mobili ha reso più accessibile la tecnologia che evolve verso forme di fruizione sempre più semplici, basti pensare ai recenti annunci di Apple che portano a una maggiore condivisione».

Per contro, mette in guardia il manager: «Il management aziendale e il dipartimento delle risorse umane devono favorire questo cambiamento se vogliono coglierne i frutti». L'organizzazione del lavoro è critica per il successo dello

Il vero fattore abilitante è la tecnologia, che decide, in ultima analisi, della produttività di chi lavora

smart working. Occorre, infatti, impostare i processi per facilitare i lavoratori, che andranno motivati e giudicati per obiettivi, possibilmente in strutture gerarchiche molto orizzontali, che favoriscono l'autonomia con una catena decisionale corta.

La tecnologia determina la produttività

L'appunto del manager, peraltro, riguarda alcuni dati negativi come il 44,6% degli intervistati che ritiene di non disporre ancora degli strumenti adeguati.

Più precisamente, coloro i quali non si sentono supportati dalla tecnologia nello svolgere il proprio lavoro rivendicano il bisogno di tool più efficaci per la condivisione e la sincronizzazione (per il 50% del campione), una connessione a Internet non sufficientemente veloce (31,82%), strumenti di messaggistica istantanea o sistemi di videoconferenza migliori (13,64%). Sono note dolenti, evidenzia Jolivet, perché quando si lavora in remoto, si devono poter utilizzare gli strumenti di lavoro appieno, altrimenti si rischia di perdere la produttività. Le imprese devono garantire un'esperienza di lavoro unificata, afferma il manager, il quale concorda che lo smart working fa risparmiare sui costi dell'affitto, ma rimarca: «i benefici sono soprattutto altrove, a patto di essere supportati dalla tecnologia, in particolare per quanto riguarda la sicurezza».

A tal proposito, Citrix ha recentemente annunciato Citrix Workspace, «la postazione di lavoro digitale



più completa e integrata, che consente di accedere in maniera sicura a tutte le app, ai desktop e ai file, da qualsiasi dispositivo e da qualsiasi luogo», dichiara Jolivet che chiarisce: «Citrix ha sviluppato un "security perimeter", che è in grado di centrare la sicurezza sul singolo utente, verificando da dove opera, che azioni sta effettuando



La ricerca, commissionata a Citrix dall'Istituto di ricerca OnePoll, è stata condotta online su un campione di 100 persone tra i 18 e 55 anni di età, occupati e residenti in Italia distribuiti tra Nord, Centro e Sud.

eccetera, per applicare tutte le policy di sicurezza adeguate».

Una resistenza pericolosa

La sicurezza è importante anche per fronteggiare un rischio crescente generato da un'impostazione troppo rigida delle modalità di lavoro. Sempre in base ai dati di OnePoll, infatti, per il 74% del campione, l'azienda rimane la sede abituale di lavoro, tant'è che solo il 23% degli intervistati può lavorare in modalità smart tutti i giorni (cioè almeno per qualche ora). Il 22,4% lavora da remoto almeno una volta a settimana, il 10,4% si limita a una volta ogni due settimane, il 5,8% a una volta al mese, e ben l'11,6% lavora in smart working meno di una volta al mese, comunque più di quel 26,4% di persone le cui imprese non permettono il lavoro "agile".

Si tratta di una resistenza destinata a cadere, anche perché la ricerca rivela che diversi singoli utenti agiscono di propria iniziativa: il 28% del campione si è dotato individualmente di una tecnologia migliore di quella messa a disposizione dall'azienda e oltre il 41% degli utenti ha migliorato la propria esperienza d'uso. Qui, però, sorge il rischio del cosiddetto shadow IT, cioè proprio l'introduzione in azienda di tecnologia non controllata, che rappresenta una vulnerabilità sfruttabile da hacker malintenzionati. Con Citrix Workspace è possibile identificare immediatamente l'utilizzo di software o servizi online non autorizzati ed eventualmente inserirli nel perimetro di sicurezza. ❁

Metaenergia investe nell'IT per crescere

La società sceglie la piattaforma di Citrix per abilitare lo smart working, risolvere il problema dello shadow IT e conformarsi al GDPR

di P.S.

Metaenergia è la capofila di un gruppo di cinque società che operano dal 2009 nel mercato libero, per fornire energia elettrica, gas naturale e piani di efficientamento energetico ai segmenti corporate, business e domestico. In Italia Metaenergia ha il suo quartier generale a Roma dove si trovano gli uffici di backoffice e dell'IT mentre a Milano è presente la parte commerciale.

Gli obiettivi di espansione internazionale (con la recente apertura di una sede a Londra) e una maggiore flessibilità operativa per rendere possibile lo smart working sono le ragioni che hanno spinto la società a cercare una soluzione «che ci permettesse di rendere operativi nuovi uffici abbattendo i costi - spiega Claudio

Paganelli, CIO e CISO di Metaenergia - e che consentisse alle nostre persone di lavorare nell'arco di tutte le 24 ore e da qualsiasi luogo con gli stessi livelli di produttività che poteva sperimentare in sede».

Metaenergia ha pertanto deciso di affidarsi a Citrix, per implementare la virtualizzazione di applicazioni e desktop, argomentando che le soluzioni precedenti come la tecnologia VPN, non garantivano la sufficiente flessibilità

e limitavano troppo l'accesso alle applicazioni.

Più flessibilità e meno shadow IT

Metaenergia per decidere a chi affidarsi ha condotto innanzitutto uno studio per capire quale tipo di tecnologia potesse soddisfare al meglio le esigenze di flessibilità, sicurezza ed efficienza operativa che stava cercando.

La virtualizzazione delle applicazioni e del desktop di Citrix sono risultate ideali per rispondere ai requisiti della società perché consentono sia di centralizzare il controllo sia di ottimizzare la banda trasmissiva e le risorse. «Avevamo già provato la tecnologia Citrix con NetScaler - chiarisce Paganelli - e con XenApp siamo riusciti a creare un ambiente di lavoro virtuale che ha consentito già dal primo giorno ai nostri dipendenti di lavorare da casa con la stessa efficienza e sicurezza di cui potevano godere in ufficio».

Un altro aspetto importante per Metaenergia era quello di



abbattere il più possibile il fenomeno dello shadow IT, ossia l'utilizzo "nascosto" di applicazioni da parte dei dipendenti sui propri device o sui device aziendali senza il consenso dell'IT centrale.

«La piattaforma Citrix - prosegue Paganelli - non ci ha solo consentito di implementare un vero smart working e di pianificare un'espansione del nostro gruppo a costi infrastrutturali più sostenibili, ma ci ha anche permesso di centralizzare il rilascio e la gestione delle applicazioni».

GDPR senza affanni

Mentre Metaenergia pianificava la nuova infrastruttura, è subentrata anche l'esigenza di rispettare le nuove normative del GDPR.

Grazie alla tecnologia di virtualizzazione di Citrix, Metaenergia ha potuto archiviare i dati aziendali esclusivamente nel suo data center e fornire un accesso sicuro a tutti gli utenti a prescindere da dove si collegino. Paganelli spiega: «riusciamo a operare con un call center esterno (partecipato dal nostro gruppo) senza che nessun dato esca dai nostri server». ❁



L'economia digitale ha bisogno di una smart city

di
Giuseppe
Saccardi

Smart Economy e smart city sono un connubio indissolubile in cui idee, mobilità, collaborazione e gestione intelligente dell'ambiente pongono le basi per il mondo business del futuro

Quando si affronta il tema della Smart Economy e di cosa si intende con questo termine una considerazione iniziale si impone al fine di inquadrare senza eccessive enfattizzazioni il tema.

Innanzitutto va considerato che l'ambiente in cui l'economia avanzata, a partire dall'epoca delle prime città stato, è iniziata nei centri urbani a seguito dell'aggregazione di capacità manifatturiere e dei servizi, di capitali imprenditoriali e mercantili, l'accesso al credito, la facilità di reperimento di risorse e il controllo del territorio.

In sostanza, quando si parla di smart economy e di smart city va osservato che una città è già di per sé il risultato di migliaia di anni di evoluzione della storia umana. Le prime città sorte in Anatolia, in Siria, in Mesopotamia o in Giordania datano a 10.000 anni fa, il che non implica che già prima non ve ne fossero, solo che non si sono ancora ritrovate.

Una città è sempre stata una struttura economica organizzata e vitale, con una sua amministrazione, un perimetro, strade di collegamento per facilitare lo spostamento delle persone, dei mezzi e delle merci, magazzini, centri di conservazione di alimenti e di combustibili, sistemi di distribuzione dell'acqua potabile e così via.

In pratica, un'organizzazione urbana sotto forma di città, cosa diversa dal villaggio o dall'agglomerato rurale, pur autosufficiente sotto numerosi aspetti, poteva essere definita con giusta ragione "intelligente" già migliaia di anni fa dai suoi amministratori ed abitanti in quanto l'obiettivo della sua costituzione e sviluppo era proprio quello di aggiungere servizi a quanto possibile al singolo e in tal modo semplificare la sua esistenza e attività professionale, così come rendere la sua vita più sicura.

La tecnologia digitale e il suo impatto

Quello che differenzia una "smart city" attuale da quelle dell'età del bronzo non è il concetto di base ma più semplicemente la tecnologia disponibile per far fare ad una città un ulteriore passo in avanti, con la creazione di servizi o la smaterializzazione di attività che in precedenza richiedevano più fatica, spostamento fisico e investimenti cospicui in risorse umane. In fondo il noleggio di un animale da trasporto concettualmente non differiva dall'attuale noleggio di una smart car o di una bicicletta a pedalata assistita oggi così diffuse, solo che per prenotarlo non si usava lo smartphone e per trovarlo la funzione di geolocalizzazione, ma si doveva recarsi in loco e i servizi di sicurezza al cittadino non venivano assicurati con videocamere gestite da remoto, ma con guardiani appostati nei crocicchi delle strade o nelle piazze.

Se si analizza in generale quello che si intende per "smart" in generale o correlato ad una città emerge quindi che il fattore tecnologico è del tutto predominante nella sua incarnazione attuale come visione evolutiva.

Nell'attuale concetto di città e di economia Intelligente intervengono poi altri aspetti che si propongono come strategia quello di mettere a fattor comune aspetti urbanistici, sociali, di pianificazione del territorio, di un nuovo approccio ai servizi pubblici, di modalità di fruizione del tempo del cittadino che ne favoriscano la socialità e ne migliorino il rapporto

con il proprio lavoro, per giungere sino al miglioramento ambientale, al risparmio energetico, alla razionalizzazione dei trasporti e così via.

Una definizione di cosa si può intendere per città intelligente la si trova in Wikipedia: «Una città può essere definita intelligente, o smart city, quando gli investimenti effettuati in infrastrutture di comunicazione, tradizionali (trasporti) e moderne (TLC), riferite al capitale umano e sociale, assicurano uno sviluppo economico sostenibile e un'alta qualità della vita, una gestione sapiente delle risorse

naturali, attraverso l'impegno e l'azione partecipativa».

Ne esistono decine di altre, generalmente caratterizzate dagli interessi professionali, sociali, politici, tecnologici dell'estensore della definizione.

L'importanza dell'aspetto amministrativo, gestionale e del coinvolgimento del cittadino è stato però rimarcato anche dall'economista spagnolo Gildo Seisdedos Domínguez, professore di marketing alla IE Business School, secondo il quale il concetto di smart city è centrato sull'efficienza, a sua volta basata sulla gestione manageriale,

sull'integrazione delle telecomunicazioni e sulla partecipazione e il coinvolgimento dei cittadini alla gestione della città, cosa che necessita di un nuovo approccio alla governance che ne permetta il coinvolgimento effettivo.

Cercando però per semplificare di raggruppare in un numero limitato di insieme le attività svolte per una smart city e facendo riferimento a studi sia nazionali sia comunitari, si possono definire quattro aree di intervento che, pur diverse, presentano qualche area di sovrapposizione. In pratica le tre aree sono riferibili come la smart city, la green city, la digital city.

A queste se ne può aggiungere una quarta riferibile come "sustainable city", relativa a una città che fa ampio uso di tecnologie al fine di rendere l'ambiente "eco-friendly" e ridurre l'impatto ambientale delle attività umane sia produttive che sociali.

In questa declinazione la digital city utilizza tecnologie informatiche e di comunicazione per generare, raccogliere ed elaborare informazioni dai cittadini verso le istituzioni e viceversa nonché abilitare canali di comunicazione tra imprese e tra queste e i cittadini in modo da ridurre l'impatto sulle strutture urbane e l'ambiente in genere, per esempio tramite

iniziative di lavoro agile o smart.

La green city è, invece, da vedere come l'insieme di iniziative che si pone come obiettivo quello di creare infrastrutture urbane, gestire gli spazi e i servizi in modo che abbiano il minimo impatto possibile sull'ambiente.

Infine la smart city è la città che utilizza la tecnologia con l'obiettivo primario di migliorare la qualità sia degli spazi sia della vita del cittadino.

Per estensione del termine, e per una semplificazione nella comunicazione da parte del marketing e della stampa, quello di smart city ha finito con l'inglobare tutti o quasi gli altri e comprendere anche quanto più correttamente riferibile come green.

In primis la connettività

La rete a larghissima banda e l'accesso ubiquo sono innanzitutto due aspetti indispensabili per una città e un'industria digitale e smart, sia perché permettono di diffondere lo smart working, di limitare gli spostamenti grazie all'uso di tecnologie di comunicazione e collaborazione, sia per le possibilità che apre nello sviluppo dell'IoT (Internet of Things), strumento chiave per l'Industry 4.0.

Una città digitale e smart, infatti, ha significato solo se si è in presenza di una infrastruttura che permetta di collegare i dispositivi e i sensori elettronici che ne regolano il funzionamento, dai semafori ai sistemi di controllo del territorio, dal riscaldamento a sapere dove è reperibile un particolare mezzo di trasporto.

Tutti questi oggetti, intelligenti in modo nativo o controllati da dispositivi locali dotati di intelligenza, necessitano poi di una rete di comunicazione ad alte prestazioni per poter essere rilevati, controllati e gestiti. sullo strato connettivo di base rappresentato da una rete a larghissima banda fissa e mobile che, come con le sinapsi e i neuroni del cervello umano, viaggiano i segnali che raccolti ed elaborati permettono di trasformare una città in smart city e in una città digitale. Sotto questo aspetto una città digitale coinvolge temi quali:

- La rete a larga banda, la rete d'accesso, l'accesso a Internet.
- I dispositivi per i servizi (ad esempio i punti di accesso wireless, i dispositivi di videosorveglianza, eccetera).
- I dispositivi per il controllo e la rilevazione. Sono riferibili come IoT (o Internet of Things) e provvedono alla rilevazione di dati sul territorio o all'interno degli edifici e a inviarli al centro di gestione.
- I servizi e le applicazioni di utente.

Il forte contributo ai progetti "smart" apportato dall'IoT e dall'IIoT appare evidente se si considera che, stante i dati di mercato, alla data, tre su quattro dei progetti in corso fa leva proprio su tecnologie IoT. ✱



Smart Economy: servono relazioni "trusted" tra le entità

Per la Smart Economy sono necessarie relazioni tra le parti che siano trusted e che i servizi erogati da e tra aziende siano sempre disponibili

Sul tema Smart Economy i dibattiti sono numerosi e generalmente vertono sul come e cosa fa diventare Smart una società o un ambiente di lavoro. Ma cosa fa sì che la relazione tra aziende inserite in una filiera di partnership industriale o commerciale, sia produttiva ed efficace?

Se si va al nocciolo della questione quello che rende tutto questo possibile è che in un qualche modo si viene a stabilire una fiducia negli strumenti che si usano e che permettono di accedere in modo certo e continuo a servizi, a dialogare con macchine, a scambiare valore e a produrlo in modo digitale senza sperimentare disservizi.

In pratica, l'evoluzione verso un ambiente smart è legata in modo indissolubile al concetto di "always-on" e di "trusted", quindi nell'assoluta fiducia in quello che si usa e si fa perché lo si fa in modo sicuro, riservato, protetto sia da strumenti sia dalle normative di legge e garantito da tecnologie in grado di erogare servizi su base continuativa e zero tempi di fuori servizio. Il problema è come creare questa fiducia e soprattutto come mantenerla in una fase in cui i confini fisici aziendali si dissolvono e diventano sempre più liquidi.

Ma, innanzitutto, le aziende avviate lungo il percorso della Smart Economy, cosa stanno facendo per creare relazioni che siano realmente trusted? Non sempre quello che dovrebbero.

Secondo un rapporto di CyberArk, società specializzata nella sicurezza di endpoint privilegiati e quotata ai primissimi posti in una classifica di 500 aziende operanti nella security, mentre le organizzazioni affrontano minacce di cyber security diversificate e dinamiche molte persistono nell'inerzia e uno dei fattori alla base di questa situazione deriva proprio dal liquefarsi dei confini aziendali e dalla loro progressiva "smartizzazione" e connessione in rete.

Smart Economy e cloud

Uno dei fattori critici in questa fase di trasformazione digitale è il cloud, ma non per il concetto in sé, che si è rivelato dopo una prima fase incerta un fattore trainante dello sviluppo economico e industriale, ma bensì per l'uso non corretto che

sovente ne viene fatto. Un ambiente smart e trusted, infatti, è tale in quanto si ha la certezza, come evidenziato, che quanto ha a che fare col business e i dati coinvolti, si trovino in un ambiente sicuro.

Ma se la continuità del servizio, l'always-on, è garantito dall'adozione di tecnologie di business continuity e di data recovery, il problema è che i processi automatizzati insiti negli ambienti cloud possono essere i responsabili della proliferazione di segreti e credenziali privilegiate.

Se compromesse, possono fornire agli attaccanti di un sistema o di un'intera infrastruttura logistica, o di public utilities, un punto di partenza per ottenere accesso laterale su reti, dati e applicazioni, sia nel cloud sia in locale.

Considerando che quando si tratta di infrastrutture di public utilities i danni conseguenti alla mancanza di sicurezza possono avere conseguenze molto serie, deve mettere in allarme il fatto che, si evince nello studio, quasi la metà degli intervistati per la sua realizzazione abbia dichiarato di non avere una strategia di sicurezza degli account privilegiati per il cloud,

account che per la loro importanza possono avere accesso a strumenti, a dati o a impianti produttivi e tecnologici anche molto critici.

Mentre la protezione della console di amministrazione cloud è un'attività che i team di sicurezza svolgono senza difficoltà, l'importanza della protezione di ambienti dinamici non sembra essere altrettanto ben recepita. Cosa ancor più critica se si considera che nove su dieci degli intervistati ha ammesso che l'infrastruttura IT e i dati critici non sono interamente protetti se non sono protetti anche gli account privilegiati e le credenziali, ma che ciononostante una parte significativa di poco meno del trenta per cento afferma che la propria organizzazione non ha ancora implementato una soluzione per la sicurezza degli account privilegiati per archiviare e gestire le password privilegiate e/o amministrative.

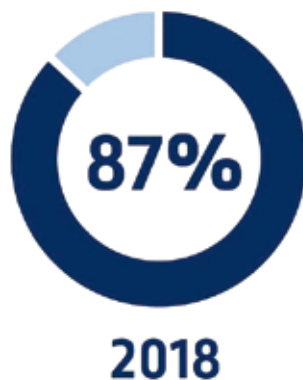
La relazione con il cloud in un mondo sempre più smart sembra però essere interessata contemporaneamente da un sentimento di attrazione e prudente repulsione. Se numerose sono le organizzazioni che ritengono che il cloud

pubblico sia abbastanza sicuro per i propri dati più preziosi, la maggior parte di esse cita almeno una problematica di sicurezza. I rischi maggiori includono per esempio il riutilizzo delle credenziali (47%), le chiavi di accesso API (Application Program Interface) compromesse (42%), le password e le credenziali utilizzate dalle applicazioni e dagli strumenti di automazione (41%).

Dove intervenire per un ambiente che sia smart e trusted?

Come osservato, un ambiente più è intelligente e interconnesso più si rivela critico, e più si espande e aumentano le entità periferiche (end-point), più aumenta la probabilità che qualcosa o qualcuno di essi non si comporti come dovrebbe. Il dato di fatto confermato da continui casi è che molti degli attacchi più dannosi che minano la fiducia in un mondo Smart iniziano proprio da un endpoint, sia esso un tablet o uno smart phone o un dispositivo IoT. Due delle tre minacce principali citate dai professionisti della sicurezza, lo spear phishing e il ransomware/malware, trovano infatti una via di accesso proprio tramite gli endpoint.

È quindi essenziale, suggerisce CyberArk e di certo si può essere d'accordo con i suoi esperti di sicurezza, che le organizzazioni rafforzino la sicurezza degli endpoint per impedire e, cosa ancora più importante, interrompere, il furto e l'escalation delle credenziali negli attacchi mirati e opportunistici. Le misure per arginare il furto di credenziali includono (o





perlomeno dovrebbero) una combinazione di processi di base come l'applicazione di patch, tecnologie come l'autenticazione a più fattori e principi come quello dei privilegi minimi.

Si tratta più che altro di misure di buon senso che tutte le organizzazioni dovrebbero già avere adottato. Invece, la realtà è che circa il 60% è la percentuale di professionisti della sicurezza che si assicura che l'antivirus sia aggiornato e poco oltre il cinquanta quello che mantengono aggiornati i sistemi operativi e le patch. Ma non è tutto. Solo un terzo asserisce di applicare il principio dei privilegi minimi, mentre una percentuale inferiore di circa il trenta per cento impiega controlli delle applicazioni basati sulle classiche whitelist. Non migliora di certo la situazione un altro aspetto critico ai fini di un sistema Smart. Stante ai coinvolti nello studio e operanti nella sicurezza IT, la percentuale di utenti che hanno privilegi di

amministratore locale nei dispositivi endpoint è passata da poco più del 60% del 2016 all'attuale poco meno del 90%, un incremento che sovrverte alla radice uno dei principi fondamentali della sicurezza degli endpoint: impedire e limitare al massimo il novero degli utenti che dispongono di privilegi amministrativi.

Se la fiducia tra le parti è essenziale per la Smart Economy, lo stesso si può dire se dalla sicurezza

di dati e applicazioni si passa a considerare il problema della loro disponibilità e della loro iper-disponibilità, e cioè con tempi di fuori servizio nulli o contenuti a pochi secondi annui. La protezione e la iper-disponibilità del dato, è stato osservato da Veeam Software, società specializzata proprio nel garantirlo, in un suo recente convegno, va oramai considerata un elemento strategico.

Ma non è solo questione di robustezza dei sistemi. Per iper-disponibilità si intende anche l'applicazione di algoritmi di intelligenza artificiale che permettano al dato di gestirsi in modo autonomo e operare in modo proattivo e non puramente reattivo. L'esigenza di modificare in profondità l'approccio adottato sino ad ora nella gestione del dato, passando ad uno proattivo basato sull'AI e relativi analytics, è conseguenza diretta dell'evoluzione del mondo produttivo e delle modalità da parte delle aziende e dei privati di fruire delle applicazioni IT, sempre più basate su ambienti multi-cloud. ❁



Data Governance e GDPR in Ubi Banca

di Gaetano
Di Blasio

UBISS utilizza una soluzione automatica di data mining per mappare i dati sensibili che vanno protetti di Gaetano Di Blasio



Filippo Finocchiaro è Head of IT Data Governance e Big Data & Analytics di UBISS. In questa veste è responsabile per il gruppo Ubi Banca della gestione del dato, che significa tutelare i diritti dell'interessato relativamente ai propri dati.

Da questo punto di vista, il GDPR punta i riflettori sui dati personali e sensibili di tre tipologie di attori: i clienti della banca, i fornitori e i dipendenti.

Vista la varietà di servizi che la banca offre, per esempio mettendo a disposizione dei clienti canali digitali piuttosto che fisici, come le filiali o gli ATM (cioè i Bancomat), visti i rapporti da curare con i molteplici fornitori e i dipendenti, il parco applicativo della banca risulta particolarmente ampio e variegato.

«Per questo ci siamo preoccupati di capire dove risiedono tutti questi dati, che sono stati catalogati in poco più di 50 tipologie, dal sesso di un cliente al codice fiscale di un fornitore e così via, e abbiamo deciso di dotarci di un sistema di discovery automatico, che, attraverso una trentina di regole parametrizzate, trova i dati in questione all'interno di circa 500 applicazioni».

Il risultato della discovery, innanzitutto, permette ai responsabili dei sistemi informatici innanzitutto di capire su quali sistemi risiedono o transitano i dati e ottenere, così, la mappatura dei sistemi, o porzioni degli stessi, da proteggere.

«Dall'altro lato, sapendo dove sono i dati, siamo in grado di rispondere alle eventuali richieste provenienti da fornitori, clienti o dai dipendenti stessi, riguardanti i loro diritti sui dati. Per esempio, possono chiedere quali dati la banca possiede, che uso ne viene fatto, eccetera e noi sappiamo identificarle ed estrarle all'occorrenza».

Altro aspetto fondamentale è che questi sforzi effettuati per il GDPR sono complementari a quelli che la banca è impegnata a svolgere nella propria roadmap di data governance. La suddetta discovery consente, in altre parole, di arricchire le informazioni già mappate aggiungendo nuovi attributi ai dati stessi. Per esempio, un

operatore può più facilmente vedere per quanto tempo può utilizzare un determinato dato, perché il record ne riporta anche il valore di redemption.

Certamente questi diritti erano già previsti e gestiti, ma con il GDPR e le sanzioni previste si sta assumendo una maggiore rigidità e gli stessi clienti sono più esigenti.

Poiché i sistemi che li utilizzano, i servizi proposti dalla banca e i proprietari diretti dei dati stessi sono un insieme variabile, è necessario che la discovery sia effettuata periodicamente per mantenere aggiornata la mappatura dei dati e dei sistemi da proteggere e per essere il più rapidi possibili nel soddisfare le richieste degli interessati aventi diritto.

Uno dei vantaggi della soluzione è l'automaticità, che consente di scoprire i dati "nascosti" in vecchi applicativi, magari quelli di cui manca la documentazione e manca la memoria storica di addetti che hanno lasciato l'azienda. *

Per la Smart Economy serve un ambiente "trusted"

Nell'economia digitale servono relazioni tra le parti che siano trusted e le informazioni protette. I suggerimenti di CyberArk per una Smart Economy trusted

Smart Office, Smart Factory e Smart Home sono termini che oramai fanno parte del vocabolario di ampia parte dei manager. Ma cosa fa sì che il nuovo modo di lavorare e produrre che sta dietro il significato di queste parole sia veramente efficace?

Se si va al nocciolo della questione tutto ciò è possibile se si viene a stabilire una fiducia negli strumenti che si usano e che permettono di accedere a servizi, dialogare con le macchine, scambiare informazioni e fruirne in modo digitale. In pratica, l'evoluzione verso un ambiente smart è strettamente connessa al concetto di fiducia e sicurezza negli strumenti IT che si usano e che quello che si fa avvenga in modo riservato e protetto sia da strumenti sia dalle normative di legge.

Questo però non sempre avviene o non avviene come dovrebbe, osserva CyberArk, azienda di livello mondiale attiva nello sviluppo di soluzioni per garantire la sicurezza di dati dispositivi e ambienti cloud, e quotata ai primissimi posti in una classifica di 500 aziende operanti nel campo della sicurezza. Secondo un suo recente studio sono ancora molte le organizzazioni che persistono nell'inerzia e uno dei fattori alla base di questa situazione deriva dal liquefarsi dei confini di aziende "Smart" rispetto a quelli fisici di un ufficio o di una fabbrica.

La criticità degli account privilegiati

Le possibili vie di compromissione delle aziende, mette in guardia CyberArk, sono in continua espansione trasversale negli ambienti, inclusi gli endpoint, i sistemi on-premise, i servizi cloud, gli ambienti ibridi e DevOps. È un'espansione che può minare, e in molti casi è già avvenuto, la fiducia delle aziende nella trasformazione digitale e rallentare l'evoluzione verso una Smart Economy.

Il problema è in sé semplice. I cambiamenti a livello di infrastruttura, tecnologie e prassi determinano la creazione di numerosi account privilegiati che, se compromessi, potrebbero consentire il libero accesso laterale a reti, dati e applicazioni. «Questo risulta evidente dal nostro Report, in cui l'89% dei professionisti della

sicurezza IT intervistati riconosce che l'infrastruttura IT e i dati critici non sono completamente protetti se non sono protetti anche gli account privilegiati e le credenziali», ha commentato CyberArk.

In sostanza, bloccare gli account privilegiati appare fondamentale, ma nonostante ciò quasi un terzo (28%) dei professionisti della sicurezza IT afferma che la propria azienda non ha ancora implementato una soluzione per la sicurezza degli account privilegiati per archiviare e gestire le password privilegiate e/o amministrative. Ulteriori esempi di cattive prassi sono rappresentati anche dal fatto che le credenziali amministrative sono archiviate in documenti di Word o Excel nei pc aziendali (36%), in server condivisi o unità USB (34%) o su documenti cartacei conservati in archivi fisici (19%). Di certo non un buon viatico per creare un ambiente di lavoro e condiviso smart.

Il fattore cloud

Il cloud è uno dei principali abilitatori della Smart Economy e la sua adozione cresce costantemente a seguito di fattori quali una maggiore efficienza e affidabilità, l'accesso a computing on-demand, prezzi flessibili e una gamma di servizi sempre più ampia messa a disposizione dai fornitori di piattaforme cloud.

Agli effetti dirompenti del cloud, tuttavia, osserva CyberArk, attiva

nello sviluppo di adeguate contromisure, si accompagnano nuovi rischi derivanti dalla proliferazione di account privilegiati non gestiti e non protetti.

Quasi tutti i partecipanti del comparto sicurezza (94%) hanno dichiarato che le proprie organizzazioni archiviano e accedono a dati utilizzando servizi cloud pubblici e sono sempre più propensi ad affidare ai provider cloud un volume di dati sensibili nettamente più consistente rispetto al passato. Molte organizzazioni ritengono

che il cloud pubblico sia



abbastanza sicuro per i propri dati più preziosi, ma la maggior parte di esse cita almeno una problematica di sicurezza. «Abbiamo riscontrato che tra i partecipanti la cui organizzazione attualmente archivia/distribuisce informazioni nel cloud, oltre due terzi (68%) dei professionisti della sicurezza afferma di fare affidamento in una certa misura sulle funzionalità di sicurezza integrate

di un vendor cloud. Inoltre, il 38% dichiara che la sicurezza del fornitore cloud non fornisce una protezione adeguata», ha osservato CyberArk evidenziando come si sia ancora lontani dal raggiungere una fiducia che sia ampiamente condivisa nel cloud in quanto motore sicuro per la Smart Economy e la digital transformation di imprese e ambienti produttivi.

Un ambiente smart inizia dagli endpoint

Il dato di fatto, osserva CyberArk, è che molti degli attacchi odierni più dannosi iniziano da un endpoint. È quindi essenziale che le organizzazioni rafforzino la sicurezza degli endpoint per impedire e, cosa ancora più importante, interrompere il furto e l'escalation delle credenziali negli attacchi mirati e opportunistici che possono azzerare la fiducia degli utilizzatori di strumenti informatici e causare seri danni economici o di brand a un'intera organizzazione.

Le misure per arginare il furto di credenziali e non incrinare la fiducia negli strumenti per la digital transformation e nel cloud includono una combinazione di processi di base come l'applicazione di patch, tecnologie come l'autenticazione a più fattori e principi come quello dei privilegi minimi, e sono tutte misure facilmente attuabili tramite soluzioni del portfolio CyberArk, ha evidenziato la società. *

I data center prefabbricati e modulari aprono la strada alla Smart Economy

Vertiv, già Emerson Network Power, definisce le potenzialità dei data center prefabbricati e realizza uno dei maggiori data center modulari di T-Systems

Attualmente i fattori propulsivi del mercato, rappresentati dalle nuove tendenze dell'economia digitale, rendono tutte le imprese dipendenti in modo incondizionato dalla tecnologia indispensabile sia per l'attività quotidiana sia per le attività critiche, nonché per la protezione dei dati sensibili.

Fattori critici di successo sono la velocità di realizzazione, la tecnologia impiegata per gestire i bisogni di oggi e anticipare la variabilità futura rispettando i criteri più stringenti in termini di qualità e conoscenza realizzativa.

Progettare, costruire, distribuire e gestire infrastrutture critiche non è cosa semplice, soprattutto perché il numero di talenti qualificati, esperti e adeguatamente formati secondo i requisiti dei nuovi data center sono risorsa scarsa, e non solo in Italia.

Come far fronte a tali reali limitazioni senza rallentare la velocità richiesta dal business? Vertiv ha iniziato a rispondere a questa domanda sin dai primi anni 2000, quando iniziò a fornire installazioni modulari, costruite in fabbrica, testate e poi spedite negli angoli più remoti del mondo dove diversamente sarebbe stato impossibile realizzare simili soluzioni.

Inizialmente era una questione di ambienti particolarmente difficili da servire o di assenza di risorse locali. Successivamente, verso il 2010, si iniziò con i data center modulari in alternativa ai modelli convenzionali per poter governare l'intera catena tecnologica direttamente in fabbrica e demandare le attività di sito all'assemblaggio dei macro moduli e allo startup.

Questa è sempre più una tendenza e Vertiv, così come altri player, è impegnata a farvi fronte offrendo soluzioni sempre più competitive e innovative capaci di adattarsi a uno scenario dove la pianificazione è subordinata a eventi esterni e la variabilità è altrettanto alta: basti pensare alle recenti variazioni introdotte dalle architetture edge, alle evoluzioni dei cablaggi in fibra ottica (FTTH), alle tecnologie prossime venture del 5G, alla migrazione degli enterprise data center verso il mondo del colocation, all'attenzione sempre maggiore verso la protezione dei



Stefano Mozzato, country manager di Vertiv

dati sensibili e così via.

«Favorire lo sviluppo dell'industria dei data center è stato naturale all'interno di un'azienda come la nostra che progetta, realizza e fornisce servizi alle infrastrutture critiche - sottolinea Stefano Mozzato, country manager di Vertiv in Italia -. A tal fine, Vertiv si è indirizzata ormai da tempo verso le tecniche di realizzazione modulari e prefabbricate dei data center che ci permettono, insieme ad altre innovazioni, di progettare e costruire data center aziendali in loco, di colocation e hyperscale che possono essere distribuiti in tutto il mondo con costi e tempi di pianificazione ottimali per le aziende».

Dal data center monolitico al modulare

Una soluzione modulare permette di risolvere la maggior parte, se non la totalità, dei problemi legati ai data center tradizionali: con approcci modulari e prefabbricati, il data center può essere realizzato in fabbrica con tutta l'impiantistica, con i cablaggi elettrici e strutturati sia in rame sia in fibra ottica. Il sito completo viene infatti ingegnerizzato il primo giorno per lo stato finale del progetto. Inoltre, le condutture per i cavi, i collegamenti elettrici, le misure antincendio, la sicurezza, il controllo degli accessi, i corridoi caldi e freddi, anche i rack IT e IDF possono essere incorporati all'interno del data center fin da subito.

Attraverso questo nuovo metodo di produzione, la realizzazione modulare si è rivelata la soluzione

ideale per garantire rapidamente ed efficacemente un'elevata scalabilità che assicuri alle aziende la possibilità di portare a compimento investimenti pianificati e nuovi progetti di espansione.

per la struttura possono essere personalizzati, smontati e rimontati in una diversa ubicazione per far fronte ad eventuali cambiamenti. Infine, ultimo ma non per importanza, c'è stato il fattore del



Il data center di T-Systems a Barcellona

Il caso T-Systems

Questo è quanto ha fatto T-Systems, società di consulenze e servizi IT globali, affidandosi a Vertiv per la realizzazione del data center Cerdanyola del Vallès a Barcellona. T-Systems ha scelto di implementare un data center twincore di classe Tier III per rispondere con tempestività ed efficienza ai suoi obiettivi strategici.

La struttura modulare si è dimostrata la soluzione in assoluto migliore per Barcellona sia per i tempi di consegna (9 mesi contro i 20-24 mesi stimati per una soluzione convenzionale) sia per i costi e gli specifici parametri strutturali. La velocità, dunque, è sicuramente stato il primo dei vantaggi chiave della costruzione modulare, che permette un risparmio di tempo pari ad oltre il 50%, rispetto ai data center tradizionali. Il secondo fattore chiave è stato la flessibilità: i moduli progettati appositamente

capitale e delle spese operative che possono essere commisurati alle effettive esigenze.

Sulla base di questi elementi, Vertiv ha lavorato per la progettazione, fornitura, consegna dei moduli, ma anche integrazione e assemblaggio del data center Cerdanyola con professionalità e lavoro di squadra. Progettato ad hoc e costruito nello stabilimento dedicato Integrated Modular Solutions in Croazia e trasferito poi a Barcellona, questo data center è costituito da 38 moduli integrati, con una capacità di carico IT di 1.1 MW, scalabile in futuro fino a 5 MW. Questa infrastruttura include inoltre l'isolamento, la protezione antincendio, il monitoraggio e il controllo di sicurezza degli accessi, oltre al fatto che il progetto ad alta efficienza garantisce una Power Usage Effectiveness (PUE) di 1,3 e consente a T-Systems di ridurre il consumo elettrico totale del 30 %.



di
Giuseppe
Saccardi

Per una Smart Industry servono reti e dispositivi IoT efficienti e sicuri

Il passaggio verso un'azienda intelligente e in linea con i dettami dell'Industry 4.0 richiede reti sicure e dispositivi periferici gestibili e protetti

L'Industrial Internet of Things (in letteratura abbreviato in IIoT) rappresenta un fattore abilitante e un elemento chiave della trasformazione digitale del settore industriale giunto alla sua quarta fase di sviluppo, ed è uno dei componenti basilari della Smart Economy, nonché di quanto inerente le infrastrutture di settori critici distribuiti su territori urbani, regionali e nazionali quali quelli costituenti le smart grid energetiche, le reti dei trasporti su strada o ferrovia, della sicurezza pubblica e del controllo del territorio o della sanità nelle sue diverse espressioni.

Le cifre in gioco in termini economici sono già consistenti e si preannunciano molto corpose e tali da giustificare l'interesse crescente degli operatori del settore e la continua entrata in campo di nuove aziende sia nel settore dei dispositivi fisici sia delle applicazioni software a supporto, come quelle per la gestione o per

gli analytics. Si stima che entro il 2020, quindi tra poco più di due anni, il mercato dell'IloT arriverà a totalizzare la consistente cifra di 225 miliardi di dollari di giro di affari coinvolgendo milioni e milioni di dispositivi intelligenti distribuiti sul territorio.

Virtualmente non manca settore, dalle utilities all'Industry o alle smart city, che non verrà massicciamente coinvolto e interessato da una diffusione dell'IloT e dalla sua trasformazione in chiave Smart. È una trasformazione che a livello industriale e sociale presenterà numerosi problemi, e non solo tecnologici, a causa dell'impatto che potrebbe avere sulla forza lavoro.

Quella che si preannuncia e che appare essere solo ai suoi pro-dromi iniziale è quindi - come evidenziano le società coinvolte nel favorire a livello tecnologico questa trasformazione e la cui vision è esaminata in altri articoli - una rivoluzione industriale quale non si era mai sperimentata per tempi, metodi e tecnologie coinvolte nel processo di rapida trasformazione come quello in atto.

Ed è, se la si osserva nel suo complesso e itinere, una rivoluzione che sta spostando sempre più il focus dell'interesse del mondo produttivo sul lato dell'incremento di efficienza e della riduzione dei costi tramite dispositivi di edge (quelli utilizzati in periferia di una rete per accedere alla grande velocità delle dorsali trasmissive su fibra ottica) e soluzioni di analytics applicate ai big data generati dai dispositivi IloT e smart.

La medaglia e il suo rovescio

Se i benefici derivanti dall'evolvere verso una Smart Economy appaiono indubbi, fatto salvo il gestire adeguatamente l'impatto sociale che ne potrebbe derivare, ed è prevedibile che nel giro di un decennio l'intero mondo produttivo globale ne uscirà profondamente trasformato, l'evoluzione e l'adozione su larga scala nel mondo industriale e dei servizi delle tecnologie IloT nell'ambito del processo verso l'Industry 4.0 non si preannuncia però senza problemi e di fatto è una rosa con delle spine, osserva per esempio RAD.

Ci sono di certo dei punti critici che ne rappresentano il rovescio della medaglia e che vanno considerati in fase di migrazione da datate seppur consolidate infrastrutture a nuove infrastrutture che vogliono far leva su una forte digitalizzazione degli impianti. Di seguito se ne esaminano alcuni che potrebbero impattare sulle performance di un'infrastruttura o sulla sua sicurezza, due aspetti chiave nel migrare verso soluzioni smart e in modo progressivo dotate di propria intelligenza e capacità auto-adattativa alle esigenze della produzione e del mercato.

Il problema rete

Un elemento critico è, in primis, quello della sicurezza degli impianti. A fase industriale ancora ampiamente diffusa prevede in buona parte soluzioni SCADA e una scarsa interconnessione locale o geografica dei dispositivi di produzione. Con l'Industry 4.0 tutto

ciò si modifica profondamente.

L'IloT, per esempio, ha come componente importante l'Intelligenza Artificiale, ma purtroppo intelligenza non è di per sé un sinonimo di sicurezza e certe volte l'eccesso incontrollato di intelligenza in un sistema può risultare molto pericoloso.

Un vulnus a un impianto o a una rete erogante servizi privati o pubblici può derivare per esempio dalla connessione di dispositivi IloT a un centro di controllo o di aggregazione dei dati attraverso reti pubbliche non sicure, ad esempio la stessa Internet o cloud privi di funzionalità di elevata sicurezza. E di certo non mancano casi anche recenti ampiamente trattati a livello giornalistico e dei media a sostegno di questo assunto.

Ciò può essere la causa di numerosi punti di vulnerabilità da cui hacker esterni o interni potrebbero infiltrarsi nella rete e da qui risalire agli endpoint (per esempio una macchina a controllo numerico) e/o diffondersi lateralmente nella rete e tra i dispositivi ad essa connessi, utilizzandoli in modo improprio o, ancor peggio se si tratta di oggetti che controllano impianti critici come pozzi petroliferi o reti di energia o di controllo stradale (semafori, illuminazione e così via), causandone un funzionamento anomalo. In entrambi i casi il disastro sarebbe a un passo di distanza.

La complessità della simulazione

Un secondo punto critico è fornito dalla complessità stessa di un impianto e dalla distribuzione



degli oggetti in gioco. Un conto è verificare il funzionamento e la manutenzione di un dispositivo in laboratorio o in un impianto pilota di test di poche unità concentrato in un'area ristretta, un'altra è quando migliaia e migliaia di dispositivi, aper esempio pali dei sistemi di illuminazione extraurbani, sono distribuiti su scala regionale o nazionale, in luoghi impervi difficilmente raggiungibili e con il personale di manutenzione a ore di distanza.

Il fattore dei costi operativi e di manutenzione è quindi un fattore che deve essere evidenziato e affrontato in fase di progetto.

Gestione dei dati e l'edge computing

Un terzo potenziale vulnus è fornito dai dati stessi generati da dispositivi IIoT e da come vengono e devono essere correlati per

fornire informazioni che risultino congruenti tra loro e con le aspettative progettuali e di business.

Dispositivi distribuiti, non sempre possono essere connessi con reti fisse o mobili che presentano le medesime caratteristiche in termini di velocità, delay o latenza.

Quello che funziona in un campus dove gli apparati di produzione possono essere connessi in fibra ottica e ad altissima velocità non sempre funziona con le medesime prestazioni anche su una ampia rete geografica.

Punti remoti possono essere raggiungibili con connessioni di rete fissa o mobile a bassa velocità, altri possono fruire di reti a larga e larghissima banda perché vicini a punti di accesso di dorsali, così come possono dover ricorrere a connessioni via satellite e in quanto tali soggette ai disturbi atmosferici.

Forti differenze nel raggiungere i centri di raccolta e aggregazione ed elaborazione in tempo reale dei dati sono in questi casi sicure.

La soluzione che è stata ideata a livello architetturale e allo stesso tempo concettuale, evidenzia per esempio RAD, è quella che viene riferita usualmente in letteratura come "Edge Computing", che consiste in pratica nello spostare la capacità elaborativa presso un determinato bacino di dispositivi IIoT in modo da ridurre fortemente i disequilibri insiti nella rete di connessione. Sarà poi l'elaboratore locale che esaminerà i dati, li marcherà temporalmente, li aggrenderà in base ad analytics, li selezionerà e ne invierà il risultato all'entità centrale, che potrà dal proprio canto fornire analitiche aggregate al massimo livello e particolareggiate in base al singolo fruitore e alle sue specifiche esigenze.

Se ciò mitiga il problema pur tuttavia non è però la panacea universale, per il semplice motivo che distribuire la capacità di calcolo presenta pur sempre un suo costo aggiuntivo, riduce la sicurezza rispetto a un sistema centrale più facilmente gestibile e controllabile e a sua volta si presta a problemi di gestione e manutenzione, con personale locale e infrastrutture a supporto adeguate.

Il trovare il giusto equilibrio tra edge/cloud/network in sede di progettazione, è quindi un elemento chiave al fine di ottimizzare costi e prestazioni di un'infrastruttura IIoT e garantire l'evoluzione verso una Smart Industry realmente efficace. ❁

Reti sicure per l'Industry 4.0

Le soluzioni di rete per l'IIoT di RAD distribuite da CIE Telematica mettono al sicuro dati ed impianti e le infrastrutture per la Smart Economy

di Giuseppe Saccardi

Con il termine Industry 4.0 ci si riferisce all'automazione della produzione e all'utilizzo di dispositivi IIoT per la connessione di apparati e la fruizione dei dati da essi generati per il controllo automatico dei processi, oppure per il controllo di infrastrutture critiche quali quelli delle smart grid energetiche, dei trasporti, della sicurezza pubblica o della Sanità. Pur tuttavia, osserva Luigi Meregalli, general manager di CIE Telematica, che rappresenta in Italia RAD, società specializzata nelle reti di accesso sia per applicazioni business sia industriali, i problemi non mancano. Tra questi, quello della sicurezza degli impianti se le reti di connessione non sono sicure.

Reti per l'Industry 4.0 e ambienti smart al sicuro con SecFlow

Per garantire la sicurezza, RAD ha sviluppato un portfolio che comprende gli elementi chiave di una soluzione IIoT e che è stato ideato per far fronte alle esigenze di reti in settori quali per esempio le Smart City, la Smart Transportation, la Smart Energy e garantire l'installazione veloce e sicura di migliaia di dispositivi IIoT in siti anche remoti e dove sia richiesta una disponibilità always-on.

Tre gli elementi di base della soluzione: la famiglia SecFlow di dispositivi rugged "SCADA aware" che implementano la funzione di gateway/switch/router; il dispositivo Security Gateway che opera da aggregatore VPN, router e firewall; il sistema di management RAD-view che abilita la gestione della rete e di configurazione dei firewall.

Connessioni al sicuro, duplicate e certificate

A livello di rete di accesso SecFlow opera da punto di connessione dei dispositivi



Luigi Meregalli -
General manager CIE Telematica

IIoT, realizza la trasmissione sicura su reti pubbliche tramite il protocollo IPSec, fa da firewall "SCADA aware" ed effettua la cifratura dei dati. La sicurezza comprende anche l'intrusion prevention, il controllo e il logging di comandi SCADA.

A livello di rete i dispositivi permettono di realizzare connessioni con media che vanno dalla fibra ottica a reti private wireless o cellulari, compreso LTE e le tecnologie 5G. La realizzazione fisica "rugged" permette di installare gli apparati anche in ambienti esterni e critici per quanto riguarda l'ambiente atmosferico.

Sulla rete i dati vengono trasportati in modo trasparente tramite la conversione automatica del protocollo SCADA. La delivery delle informazioni è anche garantita da una funzione di dual homing che prevede la ridondanza delle connessioni di rete realizzata tramite un dual modem e una dual SIM, oltre che ad altre funzioni di ridondanza interne.

Ampie sono anche le funzioni per la gestione e il controllo dei dispositivi IIoT. Tra queste l'installazione e il provisioning automatico dei dispositivi, la collezione degli eventi con una rappresentazione geografica delle sorgenti di attacchi, e la disponibilità di un database RAD che contiene informazioni sulla sicurezza. *

La Hyper-Availability è la chiave di volta per la Smart Economy

Veeam ha delineato una vision strategica per rendere i dati sempre disponibili e garantire un'azienda always-on e pronta per la Smart Economy

L'affermazione della Smart Economy ha portato all'attenzione di aziende ed utilizzatori di servizi IT l'importanza della disponibilità di dati e applicazioni, e il come garantirla. Ma in un contesto esteso e senza confini aziendali fisici come quello attuale è profondamente mutato il modo in cui questo può essere fatto.

L'esigenza di modificare in profondità l'approccio adottato sino ad ora nella gestione del dato, passando ad uno proattivo basato sull'AI (artificial intelligence) e gli analytics è conseguenza diretta, osserva Albert Zammar, responsabile per il Sud EMEA di Veeam Software, dell'evoluzione del mondo produttivo e delle modalità con cui aziende e privati fruiscono delle applicazioni IT, un modo sempre più basato su ambienti multi-cloud.

Si tratta di realtà che, si parli di reti di sensori IoT inerenti infrastrutture di tipo sanitario, dei trasporti, di grid, richiedono di essere orchestrate e garantite sia per quanto concerne la loro disponibilità sia per i tempi in cui rispondono in termine di latenza e velocità alle richieste inoltrate.

La risposta la si trova nel nuovo paradigma riferito come Hyper Availability. Obiettivo chiave delle soluzioni per la Hyper-Availability è in sostanza quello di facilitare una data orchestration behavior-driven su infrastrutture multi-cloud di grandi dimensioni.

«La Hyper-Availability è la nuova frontiera nel trattamento del dato e nella sua fruizione per il business. La Hyper-Availability Platform di Veeam, già utilizzata da numerose grandi aziende ed operatori mondiali e italiani è una soluzione molto ampia di Intelligent Data Management che permette di sviluppare e fornire rapidamente e in modo sicuro servizi digitali innovativi», ha evidenziato Zammar.

La Hyper Availability è la via obbligata per la Smart Economy

La protezione e la gestione dei dati pensata come salvaguardia attraverso policy reattive è in sostanza superata e nella vision di Veeam deve trasformarsi in un

sistema che fornisca in modo proattivo valore di business, cosa che per la Hyper-Availabile Enterprise prevede di attuare in cinque fasi con un portfolio ad hoc.

La prima riguarda il “Backup” ed è inerente al backup di tutti i workload, assicurandosi che siano sempre ripristinabili.

La seconda è relativa all’“Aggregazione” ed è volta a garantire la protezione e la disponibilità dei dati in ambienti multi-cloud.

Il terzo elemento chiave è la “Visibilità”, con soluzioni che permettono di migliorare la gestione dei dati in ambienti multi-cloud grazie a un controllo unificato dell’utilizzo, delle prestazioni e operatività, a cui aggiunge monitoraggio, ottimizzazione delle risorse, capacity planning e intelligenza integrata. Il quarto punto è la “Orchestrizzazione”, che tramite un motore di orchestrazione sposta i dati all’interno degli ambienti multi-cloud senza interruzioni per garantire la continuità del business, la compliance, la sicurezza e l’utilizzo ottimale delle risorse.

L’ultimo e quinto punto è l’“Automazione”, con i dati che, tramite la pattern recognition e il machine learning, si auto-gestiscono, imparando a duplicarsi, spostarsi verso il sito più adatto in base alle esigenze di business, proteggersi in caso di attività anomale e ripristinarsi in modo istantaneo.

«Per iper disponibilità in Veeam si intende l’applicazione di algoritmi di intelligenza artificiale che permettano al dato di gestirsi in modo autonomo e operare in modo proattivo e non puramente reattivo,

e questo al fine di garantire la disponibilità dei dati in un contesto in cui il fuori servizio anche di poche decine di secondi è considerato sempre più inaccettabile. Questo perché la vita e le relazioni tra cittadini e tra enti sono sempre più digitali e in questo rapporto digitale i dati costituiscono l’elemento ipercritico. La mission di Veeam e delle sue soluzioni per la Hyper Availability è proprio quella di abilitare il passaggio verso la Smart Economy e un ambiente in cui il dato, tramite l’AI, abbia sempre più valore per le aziende e il cittadino» ha osservato Zammar.

Veeam DataLabs: dall’idea alla produzione

Garantire la sopravvivenza e la disponibilità del dato, tramite il ricorso all’intelligenza artificiale, osserva Zammar, è solo una delle componenti dell’equazione che porta ad una smart economy e a un’azienda always-on. L’altro fattore da considerare è il “tempo” correlato ai processi produttivi e



Albert Zammar, responsabile Sud EMEA di Veeam Software

a cosa necessita a livello di dati per passare dalla formulazione di un’idea al suo rapido passaggio in produzione, sia che si tratti di un bene materiale sia di un servizio immateriale.

Un aiuto concreto Veeam si è proposta di darlo con lo sviluppo della piattaforma per l’alta disponibilità Veeam DataLabs, una soluzione per la gestione delle copie che permette alle aziende di creare rapidamente e on-demand nuove istanze dei propri ambienti di produzione. La soluzione, osserva la società, abilita casi d’uso che vanno oltre i classici scenari di protezione dei dati, come DevTest, DevOps e DevSecOps, e include test di sicurezza e di analisi forense e sandbox on-demand per le operations IT. In sostanza, rende disponibile un contesto per sperimentare e accelerare l’innovazione, migliorare l’efficienza operativa, ridurre i rischi e ottimizzare le risorse.

«Quello che abbiamo intrapreso è un percorso per consentire alle aziende e agli enti pubblici e privati di perseguire in modo rapido e sicuro una trasformazione che abiliti la smart economy, sia che si tratti di garantire l’always-on di una semplice macchina virtuale sia di un intero data center o di un ambiente multi-cloud. Questo è quello che serve oggi alle aziende e che ci chiedono per creare quella confidenza e fiducia nella trasformazione digitale che ha come condizione sine qua non che servizi, infrastrutture e dati siano sempre disponibili» ha spiegato il manager della società. ❁

Flash, iperconvergenza e cloud aprono la strada alla Smart

di
Giuseppe
Saccardi

Economy

Analytics, Artificial Intelligence e Deep Analysis, alla base della digital transformation, richiedono elevate prestazioni storage. La risposta nei tre pillar della strategia di NetApp

Quale sarà la tecnologia del futuro che supporterà l'evoluzione aziendale, le applicazioni di Artificial Intelligence, deep analysis o di business analytics, e in un futuro anche immediato?

Il tema lo ha approfondito Marco Pozzoni, country manager di NetApp, facendo il punto sui nuovi paradigmi tecnologici e architetturali che sono a disposizione dei manager aziendali alle prese con la crescente necessità di analizzare moli consistenti di dati per trarne indicazioni su come pianificare, sviluppare e adeguare il proprio business o le modalità di produzione nello scenario della Smart Economy che si consolida.

Per affrontare il problema a livello tecnologico e architetturale si possono identificare tre pillar che sono fondamentali, ha osservato Pozzoni, tre aspetti su cui si fonda la strategia NetApp per far sì che AI e Analytics possano costituire per le aziende e i loro manager un'effettiva e praticabile risorsa.

Il primo punto è la velocità. La mole di dati da analizzare è

tale che le tecnologie di elaborazione attuali hanno finito con il trovare nello storage e nella sua velocità di I/O un serio vincolo per l'effettiva utilità di pur sofisticate applicazioni di analytics.

La risposta è stata lo sviluppo di tecnologie storage all flash che hanno permesso a NetApp di mettere a disposizione delle aziende e dei provider apparati che consentono di analizzare volumi di dati con una velocità sino ad ora inimmaginabile.

Il secondo pilastro è l'iperconvergenza, intendendo con questo una piattaforma che abbina in un unico sistema capacità di calcolo e di storage e costituisce quello che è a tutti gli effetti una soluzione di cloud privata, soluzione che può poi essere gestita, messa in relazione e interagire con cloud pubblici di provider quali Amazon, Microsoft Google mantenendo il controllo complessivo e la sicurezza dei dati.



Marco Pozzoni, country manager di NetApp

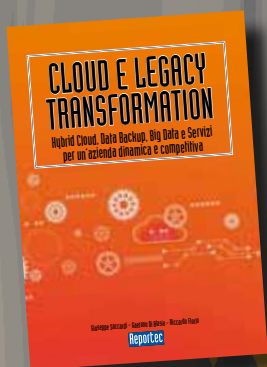
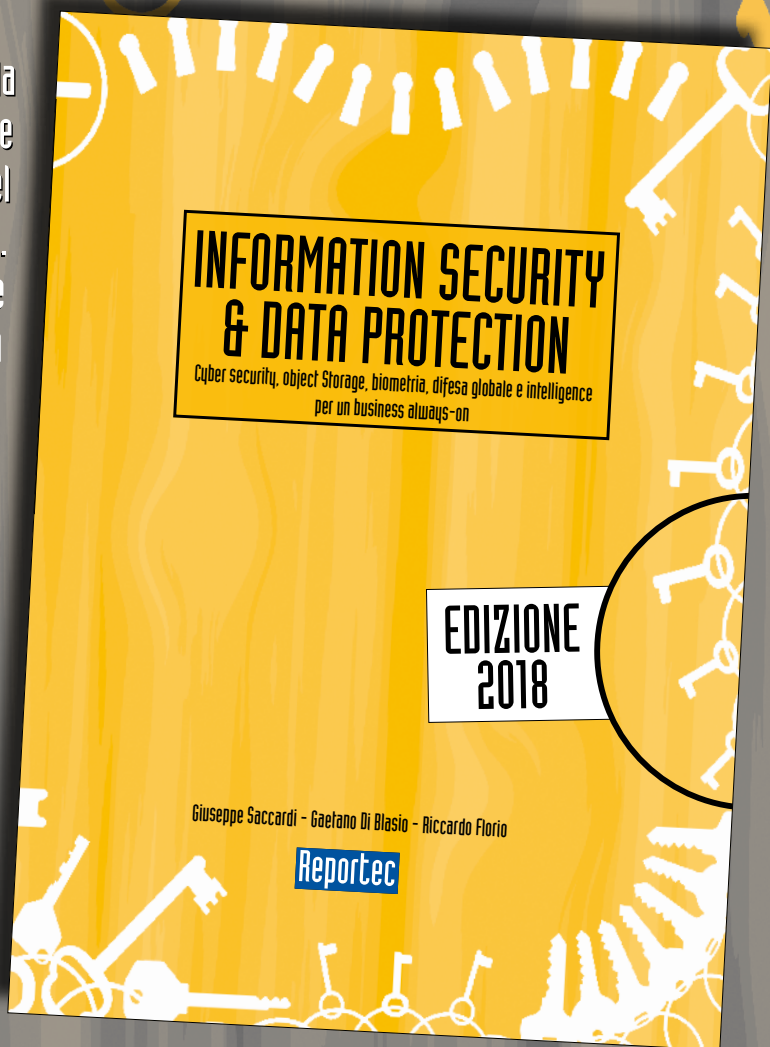
Il terzo pilastro della vision di NetApp è il cloud. Oltre alla citata soluzione iperconvergente per realizzare un cloud privato, la chiave di volta della strategia NetApp è costituita da accordi strate-

gici con i principali fornitori di servizi cloud e, in particolare, quelli che ha in corso da tempo con Amazon Web Services e con Microsoft Azure, e a cui da poco si è aggiunta Google. L'accordo con i tre big del cloud, evidenzia Pozzoni, permette alle aziende di distribuire i propri dati tra la soluzione cloud privata e quelle pubbliche, di movimentare i dati in modo trasparente dall'una all'altra o di riportare i dati in casa una volta completato il compito per il quale ci si era rivolti al cloud pubblico.

Il ricorso a un cloud in parte pubblico può, per esempio, rendersi necessario per l'analisi di grossi volumi di dati quando non si dispone in-house dello storage nella quantità e qualità necessaria, o per far girare sui medesimi analytics, oppure per eseguire il test di applicazioni prima di metterle in produzione. ❁

È disponibile il nuovo libro **SICUREZZA E PROTEZIONE DEI DATI**

In oltre 200 pagine il punto sulla situazione della cybersecurity e sulle dinamiche aziendali nella protezione del dato e della continuità del business. Una tematica sempre più vitale per le imprese, le quali devono mettere in conto che saranno attaccate. Ormai esistono sistemi automatici e pressioni da parte dei cybercriminali, tali per cui nessuno può sentirsi al sicuro: chi non è ancora stato attaccato lo sarà e, se non subirà danni gravi, sarà solo perché chi l'ha assalito cercava qualcos'altro.



È disponibili anche
CLOUD E LEGACY TRANSFORMATION

Il libro è acquistabile al prezzo di 48 euro (più IVA 22%) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444

ThinkSystem ThinkAgile

Il Data Center del futuro è già qui!

Different innovates better

Scopri di più su
lenovo.com

Lenovo™



Processore Platinum Intel® Xeon®

Ultrabook, Celeron, Celeron Inside, Core Inside, Intel, il logo Intel, Intel Atom, Intel Atom Inside, Intel Core, Intel Inside, il logo Intel Inside, Intel vPro, Itanium, Itanium Inside, Pentium, Pentium Inside, vPro Inside, Xeon, Xeon Phi, Xeon Inside e Intel Optane sono marchi di Intel Corporation o di società controllate da Intel negli Stati Uniti e/o in altri Paesi.