

## Economia &amp; Imprese

## Cyber difesa delle imprese, conto da 1,3 miliardi

## ECONOMIA DIGITALE

Una grande azienda su due aumenta gli investimenti ma fatica a trovare le figure

Quest'anno le Pmi non prevedono di aumentare i budget

Enrico Netti

«La sicurezza informatica è un elemento fondamentale per il successo di ogni business ed è confermato dal crescente interesse in termini di investimenti e di attenzione che ci aspettiamo proseguano anche quest'anno. Accanto alla specializzazione delle difese con strumenti allo stato dell'arte ora emerge la necessità di sviluppare cultura e consapevolezza, costituire centri di competenza strutturati e creare meccanismi di coordinamento e contaminazione, lavorando in una prospettiva trasversale che coinvolge l'intera organizzazione aziendale». Questa è la premessa di Alessandro Piva, direttore dell'Osservatorio Information Security & Privacy del Politecnico di Milano, commentando l'evol-

uzione degli investimenti per la difesa digitale delle imprese italiane. Oggi presenterà l'Osservatorio «Security-enabled transformation: la resa dei conti» che fotografa l'evoluzione dell'attività delle aziende sul fronte caldo della difesa digitale.

La aziende italiane da parte loro continuano ad investire. Lo scorso anno sono stati spesi in cyber sicurezza poco più di 1,3 miliardi, +11% sull'anno precedente. Una grande azienda su due nel periodo ha aumentato il budget mentre le Pmi, nonostante il sostanziale ritardo soffrono per le risorse limitate e si fermano alle difese essenziali come, per esempio, l'antivirus e l'antispam. «Una Pmi su due non prevede investimenti di miglioramento di queste tecnologie nel 2020» rimarca Gabriele Faggioli, responsabile scientifico dell'Osservatorio.

Alla fine dello scorso anno poco più di una azienda italiana su due, evidenzia l'Osservatorio, aveva completato il processo di adeguamento al Regolamento generale sulla protezione dei dati (Gdpr) contro il 24% del 2018. Il 45% delle imprese ha aumentato gli investimenti in quest'area e quasi i due terzi dispone al proprio interno del Data protection officer. Sono invece ancora da quantificare le ricadute del Cybersecurity act, certifi-

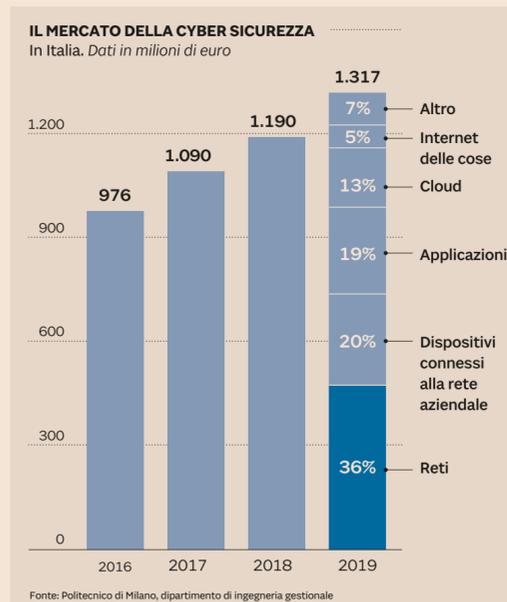
cazione a livello europeo che dovrebbe innalzare la soglia della difesa. Ma le aziende scontano un altro handicap: l'endemica carenza di figure specializzate. Tra le grandi aziende quattro su dieci sono alla ricerca di nuove figure professionali come, per esempio, architect e security analyst.

In ambiente industriale il rischio maggiore è quello del blocco della produzione causata da attacchi ai robot collaborativi e macchinari, ma si teme anche la modifica dell'output e il furto dei dati sensibili. Qui le contromisure adottate in quasi due casi su tre sono soluzioni specifiche per gli ambiti produttivi.

Un'altra via percorsa dalle imprese è il ricorso al mercato, per il momento in fase di sviluppo, delle polizze assicurative contro i rischi cyber. Solo un terzo del campione delle aziende osservate dal team del Politecnico ricorre già a queste polizze mentre quasi il 40% sta valutando l'opportunità.

Tra le aziende c'è una maggiore sensibilità e attenzione verso la protezione dei dati, la sicurezza delle informazioni aziendali, la sensibilizzazione del personale e il coinvolgimento del top management. Quest'anno tra le priorità continua a spiccare la difesa dei dati e delle reti aziendali, la gestione del rischio che conquistano il secondo posto alle

## Lo scenario



## LE PRIORITÀ D'INVESTIMENTO DELLE GRANDI AZIENDE ITALIANE

- 1 Big data & business intelligence
- 2 Sicurezza delle informazioni, rispetto delle norme, gestione del rischio
- 3 Sviluppo e rinnovo della gestione dei processi aziendali
- 4 Sviluppo e rinnovo delle soluzioni per gestire il rapporto con i clienti
- 5 Data center, gestione delle informazioni, virtualizzazione
- 6 Mobile business

Fonte: Politecnico di Milano, dipartimento di ingegneria gestionale

spalle della business intelligence e dei big data. Questo exploit è dettato dai processi di trasformazione digitale avviati dalle imprese: tra i vertici aziendali cresce la consapevolezza che la sicurezza è un fattore chiave, anzi strategico per perseguire il successo e che i dati e la loro protezione sono irrinunciabili. Ma a mettere a rischio questi asset tangibili molto spesso c'è il fattore umano. «Al primo posto tra le priorità emergono l'importanza di sensibilizzare i dipendenti sulle problematiche di sicurezza - aggiunge Piva -. Lo scorso anno il fattore umano è stata la principale fonte di vulnerabilità». Qui opportune politiche di formazione possono fare la differenza. In questi giorni, per esempio, gli hacker fanno leva della paura per il coronavirus inviando mail "esca" che se attivate permettono agli attaccanti di accedere ai dati sensibili come quelli bancari. Il tutto sfruttando le vulnerabilità dei sistemi e la disattenzione del dipendente. Insomma resta ancora molto da fare sul fronte della formazione. A questi sforzi partecipa anche la Commissione Europea che ha istituito e promuove la «giornata mondiale per la sicurezza in rete». La prossima giornata di sensibilizzazione sarà martedì.

enrico.netti@ilssole24ore.com

© RIPRODUZIONE RISERVATA

## TORNA CONNEXT

Il grande network Confindustria fa crescere il tuo business: entra nella community, vivi da protagonista due giornate uniche di confronto e sviluppo!

MiCo Milano, 27-28 febbraio

Dopo il successo della prima edizione, un altro appuntamento ad alto impatto per l'ecosistema delle imprese. Un concentrato di opportunità:

- 4 driver tematici
- Piccole e grandi imprese, startup, università, manager, istituzioni
- Matching B2B e messaggistica istantanea
- Guru internazionali per guardare insieme alle sfide di domani
- Laboratori tematici e prodotti flagship
- Una piattaforma di networking attiva anche dopo l'evento

connexf.confindustria.it/2020



## INTERNATIONAL DATA SPACES ASSOCIATION

## Dati sicuri, Cefriel e Engineering guidano l'hub italiano di Idsa

L'associazione definisce regole e standard certificati per condividere informazioni

Definire regole e standard certificati per permettere ad aziende, enti pubblici e privati di condividere dati e informazioni in modo sicuro e interoperabile all'interno di ecosistemi. È la missione dell'International data spaces association (Idsa), associazione che lavora a fianco di aziende, Governi nazionali e Commissione europea e che ora ha anche un hub italiano.

Per sviluppare l'Idsa nel nostro Paese è stato infatti scelto Cefriel, centro di innovazione digitale fondato nel 1988 dal Politecnico di Milano. Mentre Engineering, società specializzata in prodotti e servizi digitali tra i primi associati a livello internazionale, è promotrice in Italia dell'associazione. Dario Avallone, R&D director di Engineering, è tra l'altro l'unico italiano presente nel board di Idsa.

«L'investitura da parte di Idsa - spiega Alfonso Fuggetta, amministratore delegato di Cefriel - è per noi un importante riconoscimento. Attraverso l'hub - continua Fuggetta - Cefriel si farà capofila dell'ecosistema italiano, supportando Idsa nella definizione di regole condivise e ap-

procci da proporre alle aziende che possano semplificare, così come è già stato fatto con il progetto "Ecosistema Digitale 015", la condivisione di dati in modo sicuro». Le aziende italiane interessate a questo tipo di supporto possono ora aderire direttamente all'hub nazionale di Idsa.

La condivisione sicura di dati nell'ecosistema digitale globale è oggi il principale fattore abilitante per la digitalizzazione di processi industriali,



**DARIO AVALLONE**  
R&D director  
di Engineering

modelli di business, prodotti e servizi. Una leva capace di dare una spinta alla trasformazione digitale, permettendole di attuarsi pienamente, ma anche di frenarla o impedirli.

Il tema è presente nell'agenda digitale dell'Unione europea, che sta promuovendo con ruolo attivo la trasformazione di settori "guida" come automotive, domotica, logistica e sanità. Con l'obiettivo di creare l'ambiente favorevole alla nascita di campioni europei del digitale.

«Engineering - spiega Avallone - in linea con la propria missione di guidare le aziende e le organizzazioni attraverso la trasformazione digitale traendo i massimi benefici dalle informazioni contenute nei dati, si muove nella convinzione che piattaforme ed ecosistemi possano amplificare il valore generato dal dato». Ma i benefici non devono contemplare rischi per il business. «Per noi - aggiunge Avallone - è prioritario far sì che le aziende che accompagniamo nell'adozione e adesione di queste piattaforme, tecnologie ed ecosistemi possano farlo nella garanzia di una totale protezione del loro patrimonio di informazioni».

I dati non custodiscono solo importanti informazioni sulla privacy di utenti e clienti, ma possono anche rivelare aspetti riservati di processi industriali e alterare posizioni di vantaggio competitivo tra aziende, o tra aziende e piattaforme. «Non offrire la garanzia di protezione di tale patrimonio definendo una chiara sovranità dei dati - conclude l'R&D director di Engineering - significa alimentare timori e sfiducia nelle imprese, rallentare l'innovazione e gli investimenti e, in definitiva, frenare la competitività».

— A. Lar.

© RIPRODUZIONE RISERVATA

Sensori e connessioni ultraveloci  
A Roma i test 5G di Fastweb e Zte

## TLC

Anche l'università dell'Aquila nella sperimentazione per il monitoraggio di edifici

Andrea Biondi

Il 5G al servizio del monitoraggio degli edifici, in tempo reale. Fastweb, Zte e l'università dell'Aquila hanno presentato ieri a Roma la sperimentazione per il monitoraggio strutturale degli edifici in 5G attraverso una rete di sensori di nuova generazione attivata in due sale dei Musei Capitolini.

Si tratta di una sperimentazione, ma anche di una soluzione commerciale già pronta di Fastweb e Zte, con l'idea di tutelare edifici storici grazie a sensori e alle connessioni ultraveloci garantite dal 5G su cui far viaggiare l'analisi di parametri strutturali come variazioni di umidità, deformazioni e temperatura. Risultato? La possibilità di avere dati in tempo reale, se

non anche predittivi pur se non di tantissimo, su anomalie e criticità. E questo in condizioni di emergenza come un terremoto, ma non solo.

«Siamo aperti ad accogliere questo uso intelligente della tecnologia che ci aiuterà a gestire i nostri beni storici», spiega Luca Bergamo, vicesindaco con delega alla Crescita Culturale. Del resto la sperimentazione rientra nel progetto #Roma5G, presentato dalla giunta capitolina a settembre 2017, nato dalla collaborazione con Ericsson e Fastweb e cui nel tempo si sono uniti altri partner come Atac e il vendor Zte.

Nello specifico caso presentato ieri l'infrastruttura 5G è stata fornita da Zte, le frequenze da Fastweb e il sistema di raccolta ed elaborazione dei dati è stato sviluppato dall'università dell'Aquila. «La rete di quinta generazione è pronta a rivoluzionare il modo di vivere la tecnologia, abilitando servizi prima solo immaginabili a beneficio dei cittadini, delle imprese e della pubblica amministrazione», commenta Andrea Lasagna,

Chief Technology Officer di Fastweb. «Questa collaborazione con Fastweb e Univaq è motivo di soddisfazione in quanto ha portato a questa importante sperimentazione nel cuore del Comune di Roma. Un perfetto connubio tra la nuova tecnologia e il patrimonio storico», afferma dal canto suo Kun Hu, presidente Europa Occidentale di Zte e ceo di Zte Italia.

Il passaggio di ieri a Roma è indubbiamente un'ulteriore testimonianza di quanto il 5G possa impattare nella quotidianità, ma anche in qualche modo sul business delle compagnie telefoniche, ora chiamate a realizzare le proprie reti con le frequenze 5G a disposizione. In tal senso Fastweb - che ha in corso la gara per scegliere il vendor per la sua rete - ha siglato un'intesa con Wind Tre per fare sinergie nella realizzazione delle rispettive reti. Telecom e Vodafone stanno lavorando per mettere in comune i propri asset, da far confluire in una Inwit compartecipata. Con la partita del 5G che entra nel vivo.

© RIPRODUZIONE RISERVATA