

DIRECTION

Reportec

LA DIGITAL ECONOMY AL SUPPORTO DEL BUSINESS



**Le
imprese
epiche
contro
Covid e
cybercrime**

Distribuito gratuitamente con "Il Sole 24 Ore"

OAD 2020

L'iniziativa OAD, Osservatorio Attacchi Digitali in Italia, con il 2020 è alla 12° edizione, con 12 anni consecutivi di indagini sugli attacchi digitali intenzionali ad aziende ed enti pubblici in Italia.

OAD è l'unica iniziativa in Italia per l'analisi sugli attacchi, realizzata tramite una indagine anonima con un questionario compilabile on line, indirizzata a tutte le aziende e alle Pubbliche Amministrazioni di ogni settore merceologico e dimensione. OAD collabora con la Polizia Postale e delle Comunicazioni, che fornisce significativi dati sugli attacchi digitali che costituiscono crimini informatici. 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 dati "locali all'Italia" sugli attacchi digitali intenzionali rilevati, sulla tipologia e sull'ampiezza del fenomeno è fondamentale anche per le organizzazioni di piccole e piccolissime dimensioni per valutare i possibili rischi e attivare le misure più idonee di prevenzione e protezione, così come richiesto da numerose normative nazionali ed internazionali, non ultimo il GDPR, il regolamento europeo sulla privacy. OAD, con la sua indagine e con lo stretto supporto di AIPSI, Associazione Italiana Professionisti Sicurezza Digitale (Capitolo italiano della mondiale ISSA), intende inoltre contribuire alla sensibilizzazione e alla consapevolezza, in Italia, sulla sicurezza digitale del personale a tutti i livelli, dai decisori di vertice agli utenti. Quest'ultimo obiettivo è particolarmente importante per creare una più diffusa cultura in materia di sicurezza digitale, che va oltre il mondo tecnico-informatico e toc-

ca anche i vertici dell'organizzazione e tutti coloro che decidono requisiti e budget della sicurezza digitale nei processi organizzativi delle proprie strutture.

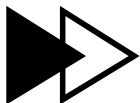
Per la prima volta nell'edizione 2020, chi completa il questionario on line avrà anche in tempo reale una valutazione di sintesi di come le misure di sicurezza digitale indicate rispondano effettivamente alle esigenze di sicurezza digitale indicate per l'azienda/ente ed il suo sistema informatico: una macro valutazione qualitativa (e gratuita) del livello di sicurezza digitale del sistema informatico oggetto delle risposte fornite provè nel rispondere al questionario.

Per motivare il rispondente, a conclusione delle risposte fornite al questionario on line, oltre alla valutazione di cui sopra, è possibile scaricare gratuitamente il numero di maggio 2020 di ISSA Journal, la rivista mensile riservata ai soci AIPSI-ISSA, che tratta la crittografia quantistica, e l'intero volume "Information Security e Data Protection", pubblicato da Reportec, che è anche Publisher e Media Partner per OAD.

Il Rapporto finale di OAD 2020 è previsto per fine novembre 2020, e sarà scaricabile gratuitamente da parte di tutti gli interessati. Più compilazioni del questionario si avranno, provenienti dai vari settori merceologici e dalle Pubbliche Amministrazioni Centrali e Locali, più analitico, dettagliato, accurato e autorevole potrà essere il rapporto finale.

Si prega pertanto il lettore di questa nota di compilare, o di far compilare dai suoi tecnici, il questionario on line disponibile alla pagina: <https://www.oadweb.it/lime-survey2020/index.php/574592?lang=it>





INDICE

Direttore responsabile

Gaetano Di Blasio

In redazione

Gaetano Di Blasio
Paola Saccardi
Edmondo Espa

Ha collaborato

Giancarlo Lanzetti

Grafica

Aimone Bolliger

Immagini

Dreamstime.com

Redazione

via Marco Aurelio, 8
20127 Milano
Tel 0236580441
fax 0236580444
www.reportec.it
redazione@reportec.it

Stampa

A.G.Printing Srl
via Milano 3/5
20068 Peschiera Borromeo (MI)

Editore

Reportec Srl
C.so Italia 50
20122 Milano

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

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.

7 TESEO UCCIDE UN CENTAURO

8 RSA tutela la sicurezza nel lavoro da remoto

10 BenQ Instashow è la soluzione plug & play
ideale per l'ufficio e non solo

12 Soluzioni di sicurezza per la cyber resilienza

14 L'innovazione che nasce dalle applicazioni creando servizi

16 Il supporto di Westcon

17 Una piattaforma per assicurare la continuità del business

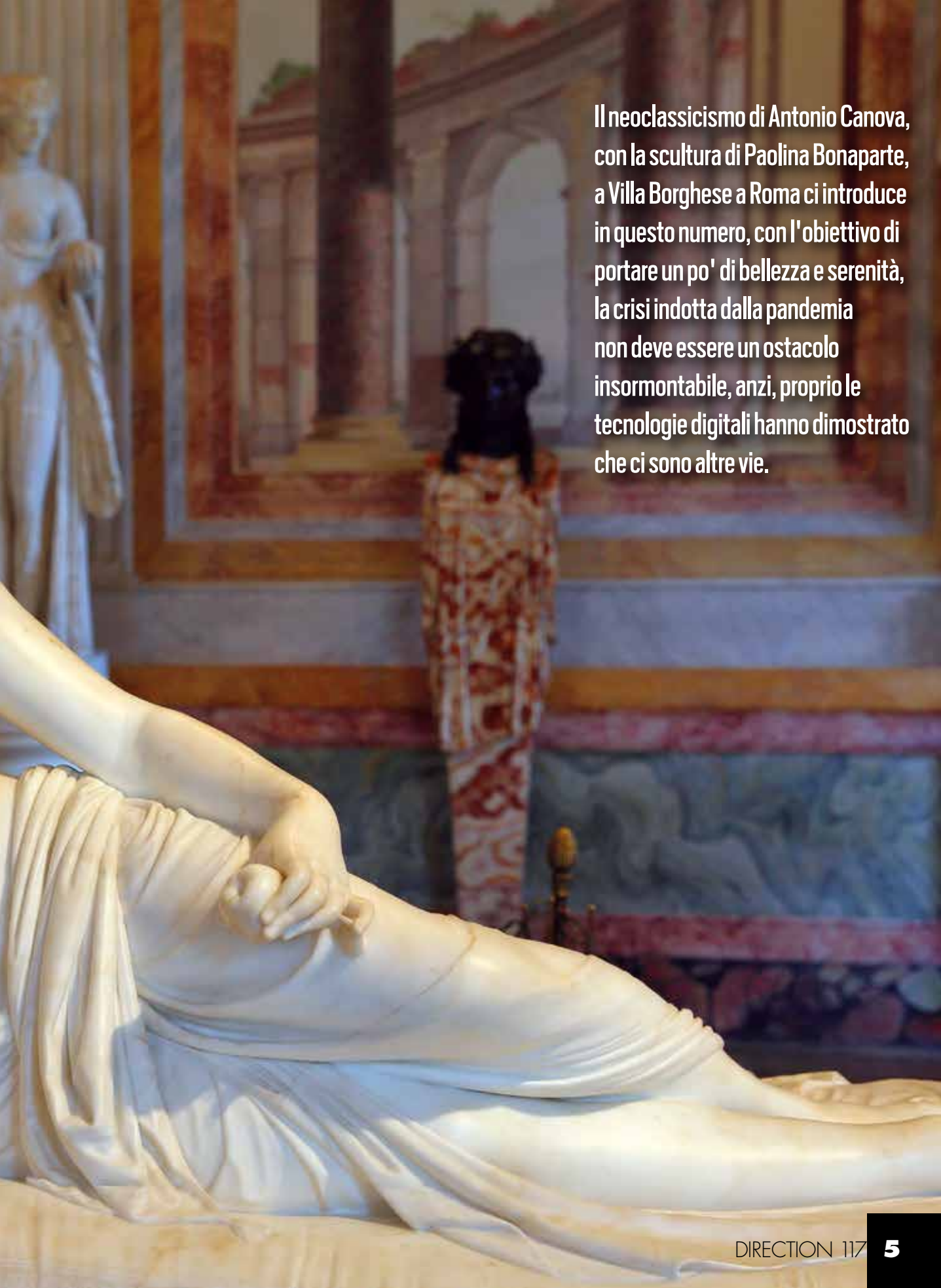
20 Il retail nel prossimo futuro

26 I rischi che le aziende temono di più nel 2021

28 Il BEUC chiede regole europee per l'intelligenza artificiale

31 Cresce e si consolida il crowdfunding di Backtework





Il neoclassicismo di Antonio Canova, con la scultura di Paolina Bonaparte, a Villa Borghese a Roma ci introduce in questo numero, con l'obiettivo di portare un po' di bellezza e serenità, la crisi indotta dalla pandemia non deve essere un ostacolo insormontabile, anzi, proprio le tecnologie digitali hanno dimostrato che ci sono altre vie.



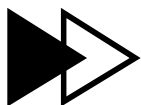
A marble sculpture by Antonio Canova depicting the mythological hero Theseus slaying a Centaur. The Centaur is shown in a crouching, defensive posture, while Theseus stands over it, ready to strike. The sculpture is set against a dark, textured background, possibly a wall or a large panel.

Teseo uccide un Centauro

opera di Antonio Canova, esposta al museo storico di Vienna

Vita o morte. Può sembrare eccessivo, ma una paziente è deceduta perché cyber criminali hanno bloccato le apparecchiature mediche.

La sicurezza informatica non è mai stata così critica, per il business e per la salvaguardia della vita umana



RSA tutela la sicurezza nel lavoro da remoto

La pandemia ha velocizzato il processo di trasformazione digitale e spinto l'adozione del lavoro da remoto, spesso sottovalutando i rischi alla sicurezza informatica

di Gaetano Di Blasio

La sicurezza in RSA, società storica del settore, parte dal concetto di digital risk che, ci spiega Roberto Branz, Channel Account Executive di RSA Security Italia rispetto ai rischi di business cui sono avvezzi i top manager, presenta due fattori differenzianti, la velocità con cui si concretizzano i fenomeni collegati ai rischi e si modificano nel tempo e i volumi che li caratterizzano.

A causa della pandemia si è accelerato il percorso delle aziende verso il digitale, ma non tutti sono stati al passo adottando tecnologie e modelli operativi corrispondenti.

Se, da un lato, il digitale amplia le potenzialità del business, dall'altro accresce in modo esponenziale il rischio: «*La trasformazione digitale amplia il perimetro delle aziende e velocizza il commercio e i processi interni incrementando, i relativi rischi alla sicurezza dei dati* - sottolinea Branz, che aggiunge - *RSA aiuta a riconoscere per tempo questi rischi, a monitorarli e tenerne traccia, per mitigarli, fornendo le evidenze di quanto è accaduto. Questo è il nostro leit motif che cerchiamo di diffondere nelle aziende in modo di coinvolgere tre entità: l'IT tradizionale, il team che si occupa di audit & compliance e i responsabili della security. Tutti insieme devono aiutare il Board nel prendere le decisioni giuste per la trasformazione digitale, a patto di condividere tali decisioni in modo corretto con il management*».



Roberto Branz, Channel Account Executive di RSA Security Italia

Le priorità di sicurezza del 2021

Il manager evidenzia come le imprese nel 2020 abbiano cercato di mitigare la crisi indotta dal Coronavirus, usando la tecnologia e lavorando da casa. Sono state, così più disponibili a mettere contenuti in cloud, sia per i dipendenti sia per i clienti, aumentando il livello di digitalizzazione, superando vetuste impostazioni a silos, migliorando i propri prodotti e servizi, anche estendendosi al di fuori dei confini nazionali. Chi era preparato, dal punto di vista delle soluzioni di sicurezza già adottate, è cresciuto anche in questo, aumentando, per esempio, il numero di utenti cui è stato elevato il livello di sicurezza. Tutto ciò è accaduto in modo piuttosto rapido, afferma Branz.

In sostanza si è visto che il nuovo modello di smart working funziona e che sarà possibile accrescere la sicurezza



inquadra per approfondimenti online

assegnando una identità digitale sicura che certifichi l'ingresso digitale in azienda di chi è colui o colei che dice di essere.

L'identità della persona diventa il primo punto da proteggere anche perché le identità aziendali sono spesso collegate con quelle personali. Una buona pratica richiederebbe che a ogni utente siano assegnati specifici privilegi, pur considerando che in troppe realtà non si controlla nemmeno che vengano cancellate le credenziali di un dipendente che lascia l'azienda.

Cresce l'importanza dell'identità digitale

In molte aziende nel prossimo anno si tornerà in ufficio, ma nulla sarà come prima, perché in tanti hanno sperimentato il lavoro da remoto con successo. Molti, a rotazione resteranno casa, per ottimizzare e risparmiare tempi di spostamento e costi. In tali contesti si troveranno ambienti di lavoro variegati con un perimetro esteso e sarà fondamentale certificare l'identità digitale delle persone perché ognuno dovrà conservare i propri privilegi all'interno del perimetro aziendale, senza che persone malintenzionate possano accedere a ogni contenitore d'informazioni.

Quindi certificare l'identità digitale delle persone è prioritario, perché molti attacchi si rivolgono all'utente come persona, il che si porta dietro un bagaglio digitale. *«I cyber criminali possono accedere facilmente alle informazioni e a questo rischio - spiega Branz - poche aziende hanno pensato, perché la priorità era tornare al lavoro».*

Un'altra fonte di rischio sono le frodi innescate dalla curiosità verso i temi attuali, che spesso nascondono contenuti malevoli, ma ci sono anche casi

di persone che si presentano in una azienda spacciandosi per qualcun altro. Ognuno deve valutare la propria esposizione. Una possibilità interessante per numerose imprese è dotarsi di un sistema per il controllo dei rischi aziendali.

Le soluzioni di RSA Security

Soluzione storica di RSA, SecurID si occupa dell'identità digitale e la sua evoluzione ha allargato il concetto alla Identity Assurance. È disponibile un'ampia gamma di "autenticator" multifactor per soddisfare esigenze adatte a variegate applicazioni. Si va dal classico token, proseguendo alle impronte digitali, oppure una semplice operazione come accettare un messaggio o scuotere lo smartphone per dimostrare di possedere quello smartphone. In RSA, oltre a questo hanno anche lavorato per semplificare l'utilizzo di queste tecnologie di authentication per gli utenti.

«La migliore tecnologia è quella che fa il lavoro in modo silenzioso. Noi monitoriamo il comportamento degli utenti e interveniamo soltanto quando c'è un fattore di rischio e chiediamo un'informazione in più per certificare l'utente - spiega Branz, che aggiunge - Se l'operazione che stai facendo è regolare, ti stai collegando da casa tua, col tuo pc e indirizzo, come fai tutti i giorni non ti chiediamo nessuna autenticazione agevolandoti nel tuo lavoro».

A questo si aggiunge una soluzione di Identity Governance per gestire persone e diritti in azienda e un sistema SIEM (Security Information and Event Management) evoluto, tra i più recenti strumenti di RSA, per il controllo di tutto quello che accade sull'infrastruttura, NetWitness. Raccogliendo molte

informazioni, oltre a controllare, la soluzione è in grado di apportare i rimedi necessari usando le suddette informazioni e applicando modelli matematici ad hoc, fornendo un servizio di Detection e response in ambito esteso: *«Ci spingiamo fino a proteggere le nuove reti basate su servizi e prodotti IoT che sono sempre più pervasive»*, sottolinea Branz.

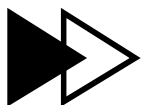
Fraud&Risk affronta i temi antifrode insieme a NetWitness, monitorando la presenza sul web di siti con pagine social non ufficiali, quindi se qualcuno tentasse di registrare siti fake simili a quelli di un'azienda, RSA riesce a monitorarli ed, eventualmente, a bloccarli, grazie alle relazioni e alla expertise di RSA, producendo tutta la documentazione che dimostra la frode.

La storica suite Archer di RSA fornisce una piattaforma tecnologica per la gestione dei rischi e della conformità nel contesto del business.

50mila utenti in smart working nella PA

In RSA, durante il primo lockdown sono riusciti a implementare il lavoro da remoto su un perimetro di 50mila utenti. Il tutto in pochissimi giorni usando una app per l'autenticazione. Il progetto era già in corso, ma è stato inevitabilmente accelerato dall'emergenza sanitaria

Alle piccole e medie imprese, invece, è stato fornito un sistema di sicurezza gratuitamente per sei mesi. Qui la difficoltà è stata quella di superare le preoccupazioni degli IT manager, che non si fidano delle capacità dei loro stessi utenti, nel gestire lo strumento di autenticazione. La impossibilità di incontrarsi ci ha permesso di automatizzare molti dei processi per la sicurezza, come quelli per l'auditing. ❁



BenQ Instashow è la soluzione plug & play ideale per l'ufficio e non solo

Tecnologia evoluta
a prova di utente,
senza dimenticare la
sicurezza e la salute
nell'ambiente di
lavoro

di Gaetano Di Blasio



Mai come in questo momento è importante per le aziende operare in un contesto digitalmente al passo con i cambiamenti e soprattutto sicuro. Queste esigenze, che riguardano sia il lavoro in presenza che lo smart working, hanno messo in evidenza le soluzioni proposte da BenQ, il cui core business in Italia si rivolge ai segmenti monitor e videoproiettori, sia per il consumatore finale che per i settori business ed education.

Le proposte del brand taiwanese si distinguono per il design di prodotto e la semplicità di utilizzo: non sono necessarie competenze tecniche per collegare dispositivi wireless Plug & Play, come ci spiega con soddisfazione Giacomo Rocchi, Sales and Marketing Director di BenQ Italy: «Basta una breve dimostrazione per comprendere l'utilizzo di tutti i nostri prodotti pensati per il settore Business, dai display interattivi ai videoproiettori smart, senza dimenticare i sistemi di wireless presentation. Per esempio, il BenQ Instashow» sottolinea Rocchi, «un dispositivo WPS (Wireless Presentation System) che consente di organizzare una riunione in pochi semplici passi, eliminando il fastidioso problema del cavo da collegare al PC. Basta premere un pulsante per far sì che uno dei partecipanti alla riunione abbia la possibilità di presentare utilizzando il proprio PC, il tutto wireless.



inquadrare per approfondimenti online



inquadrare per approfondimenti online



Non servono cavi ne' alcun software da installare».

Questo piccolo dettaglio non è un caso, bensì l'applicazione della filosofia stessa di BenQ, il cui nome deriva dall'acronimo della promessa del marchio "Bringing Enjoyment 'n Quality to life": la tecnologia, anche la più complessa, deve avvicinarsi agli utenti garantendo la massima semplicità di utilizzo.

Tecnologia e sicurezza con Instashow

Fra le diverse proposte B2B fornite da BenQ, ci soffermiamo proprio sulla soluzione Instashow, che unisce la semplicità della tecnologia wireless a complessi sistemi che garantiscono la totale sicurezza dei dati.

Instashow è composto da due button e un host centrale dotato di porte HDMI, LAN, USB, più il relativo contenitore cradle. Il sistema è conforme HDMI 1.4 con HDCP e può quindi essere connesso con facilità a qualsiasi PC/notebook e riprodurre video DVD/Blu-ray. Non solo: consente di condividere contemporaneamente fino a quattro presentazioni diverse, suddividendo lo schermo in 4 quadranti.

La semplicità di utilizzo di Instashow, tuttavia, non pone in secondo piano la totale sicurezza dei dati, garantita dalla protezione WPA2-PSK con crittografia AES a 128 bit.

In virtù di queste caratteristiche,

evidenzia Giacomo Rocchi, InstaShow è stato certificato CVSS - Common Vulnerability Security System e ha ottenuto la certificazione ISO27001 per i sistemi di gestione della sicurezza delle informazioni (ISMS), a dimostrazione delle sue funzioni, che garantiscono la totale sicurezza dei dati e protezione della privacy degli utenti.

Garantire la tutela della salute nell'ambiente di lavoro

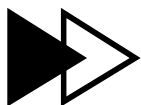
Oltre alla sicurezza dei dati, un altro pilastro della filosofia BenQ è sicuramente quello legato alla salute e al benessere dei suoi utenti. Ad esempio, sullo schermo dei display interattivi IFP (Interactive Flat Panels) viene applicato uno strato nanoionico d'argento, che li rende antibatterici e diminuisce così il rischio di diffusione dei germi.

Di fatto, la pandemia cambierà per sempre le abitudini dei lavoratori, sostiene Rocchi. Anche quando sarà superata, le aziende dovranno confrontarsi con le sue conseguenze e già molte si stanno interrogando sulla questione della sicurezza nelle sale riunioni e negli open space. Uno dei problemi principali riguarda la ventilazione

e la nebulizzazione negli spazi chiusi. L'OMS afferma che soprattutto le stanze con scarsa ventilazione corrono un rischio elevato: mantenere una buona qualità dell'aria e ridurre la trasmissione di germi è fondamentale per fornire un ambiente di lavoro sicuro e anche più produttivo.

A questo proposito, i display interattivi IFP BenQ sono dotati di sensori di controllo per la qualità dell'aria: i sensori integrati forniscono dati in tempo reale sui parametri ambientali circostanti, rilevando la temperatura e l'umidità e monitorando il livello di concentrazione di PM 2,5, PM 10 e CO2. In questo modo sarà più facile controllare la qualità dell'aria circostante, così da adottare le contromisure giuste per favorire un ambiente di lavoro o studio più sano. Conclude infine Rocchi con un ultimo accenno alla tecnologia Eye-care presente in tutti i Display Interattivi di BenQ: *«I nostri schermi garantiscono un livello minimo di emissione di luce blu e offrono la tecnologia anti sfarfallio, riducendo così l'affaticamento e l'irritazione degli occhi e migliorando notevolmente il comfort visivo».* ✨





Soluzioni di sicurezza per la cyber resilienza

Micro Focus propone
un insieme di
prodotti e tecnologie
per rispondere
alle minacce in
modo intelligente,
adattabile e
proattivo e per
garantire la business
continuity anche in
caso di attacco

di Riccardo Florio

Conseguire la cyber resilienza significa predisporre le condizioni per avere un'infrastruttura IT in grado di continuare a svolgere le principali attività di business anche in caso di attacco informatico e mantenere l'accesso agli strumenti necessari per avviare procedure di salvataggio dei dati, di eliminazione delle minacce e di ripristino così da minimizzare i danni e accelerare la ripresa.

Per il conseguimento di questo obiettivo Micro Focus ha sviluppato un modello di "resilient security" che fornisce tutti gli strumenti per predisporre un livello di protezione completo ed efficace, adattabile in modo intelligente e dinamico all'evoluzione delle minacce.

Una strategia per la cyber resilienza

Micro Focus abilita la cyber resilienza attraverso un'ampia gamma di soluzioni e tecnologie integrate, organizzate in famiglie specifiche e guidate da una strategia comune incentrata su tre principi fondamentali.

Il primo è di aumentare il livello di protezione attraverso soluzioni pensate per la sicurezza delle identità digitali, delle applicazioni e dei dati. A ciò si affianca l'integrazione della sicurezza all'interno dei modelli di sviluppo come DevOps. L'ultimo tassello è un percorso costante di evoluzione basato su intelligenza artificiale e machine learning che permette di individuare costantemente le minacce, di determinare chi ha accesso a quali risorse e di adattarsi dinamicamente alle nuove condizioni.

«L'insieme delle soluzioni di resilient security di Micro Focus fornisce gli elementi per implementare una protezione efficace, predittiva e intelligente necessaria per garantire la cyber resilienza richiesta dal nuovo mondo digitale - spiega Pierpaolo Ali, Director CyberSecurity Southern Europe di Micro Focus - Le soluzioni software di Micro Focus sono organizzate in famiglie specifiche, integrabili tra loro e con soluzioni di terze parti, che abilitano un approccio di sicurezza efficace favorendo, nel contempo, un percorso di aggiornamento che garantisce la protezione degli investimenti già effettuati».

Protezione intelligente e governance della sicurezza

Un tassello importante nel modello di cyber resilienza proposto da Micro Focus è svolto da **ArcSight Intelligence** (in



*Pierpaolo Ali, Director
CyberSecurity Southern
Europe di Micro Focus*

precedenza Intersect), un software per l'analisi di sicurezza di tipo predittivo che utilizza tecnologie di machine learning non supervisionato per effettuare analisi comportamentale degli utenti e delle entità. ArcSight Intelligence dispone di un motore di analytics che integra oltre 200 algoritmi ed è stato sviluppato sulla base dell'analisi di casi reali. Questa soluzione è completamente integrata con Enterprise Security Manager di ArcSight, che permette di analizzare in tempo reale grossi flussi di dati per un'analisi completa degli eventi di sicurezza e una protezione in tempo reale contro attacchi noti e sconosciuti. Ad accelerare ulteriormente il rilevamento e la risposta efficace alle minacce concorre **ArcSight SOAR**, la piattaforma di Security Orchestration, Automation and Response che consente di radunare centralmente gli avvisi sulle minacce, riducendo i tempi di indagine a pochi minuti e attivando automaticamente azioni di risposta e ripristino. La tecnologia SOAR è integrata e inclusa gratuitamente nella soluzione SIEM di ArcSight.

Soluzioni per proteggere identità, dati e applicazioni

Nell'attuale modello di azienda aperta e delocalizzata, dove il nuovo perimetro aziendale è definito dalle identità digitali degli utenti, la cyber resilienza richiede la predisposizione di una gestione centralizzata di identità e accesso che copra utenti, dispositivi, cose e servizi. A questa esigenza Micro Focus indirizza la famiglia NetIQ con cui è possibile gestire il "chi" (dipendenti, clienti) e il "cosa" (dispositivi, servizi) accede a sistemi e dati. Conoscere i modelli normali di queste

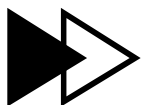
identità rende più facile identificare la comparsa di modelli anormali di comportamento.

La famiglia di prodotti NetIQ favorisce la predisposizione di un modello di sicurezza Zero Trust verso cui tutti si stanno orientando e basato sul principio che non esistano situazioni, sistemi o utenti che possano essere considerati affidabili a priori. In un modello Zero Trust tutte le attività devono essere monitorate, il livello di accesso fornito deve essere sempre quello minimo necessario allo svolgimento del proprio compito e si devono monitorare costantemente anche gli utenti con privilegi come, per esempio, l'amministratore delegato.

La famiglia **Voltage SecureData** di Micro Focus mette a disposizione una serie di tecnologie innovative e brevettate di cifratura e di accesso sicuro per la protezione dei dati sia strutturati sia destrutturati. Alla base di queste soluzioni vi è un modello di sicurezza che prevede di implementare il meccanismo di difesa e protezione direttamente sul dato o sui sistemi che lo trattano. Con le soluzioni Voltage SecureData i dati restano sempre cifrati

dal momento della loro creazione fino alla loro cancellazione sicura. Persino durante l'utilizzo, grazie a tecniche di mascheramento brevettate e uniche sul mercato, le soluzioni Micro Focus permettono di mantenere cifrati i dati anche all'operatore che li sta trattando. La sicurezza delle applicazioni deve partire dalla fase di sviluppo integrando strumenti di controllo e test di sicurezza direttamente nelle piattaforme di sviluppo per poi estendersi all'intero ciclo di vita. Alla protezione delle applicazioni Micro Focus indirizza la consolidata gamma di soluzioni Fortify giunta alla ventesima release e inserita per il settimo anno consecutivo tra i leader nel Gartner Magic Quadrant for Application Security Testing oltre a figurare al primo posto nel rapporto 2020 Gartner Critical Capabilities for Application Security Testing per i casi d'uso Enterprise e Mobile and Client. Le soluzioni Fortify abilitano test di sicurezza delle applicazioni in modalità statica sul codice sorgente, in modalità dinamica mentre sono in esecuzione e in ambiente mobile. Sono disponibili anche come servizio in cloud (Fortify on Demand). ❁





L'innovazione che nasce dalle applicazioni creando servizi

La sicurezza alla base del processo di realizzazione di app e servizi

di Gaetano Di Blasio

In F5 l'importanza delle applicazioni è da sempre il fulcro di una strategia aziendale di lungo termine; lo dimostrano i grandi investimenti degli ultimi quattro anni, volti a potenziare l'offerta sul fronte delle applicazioni cloud native: come evidenza Maurizio Desiderio, Country Manager Italia e Malta, l'acquisizione di NGINX, la piattaforma di application delivery più utilizzata a livello mondiale, è forse il segno più chiaro di questa strategia che mantiene alta l'attenzione anche sul fenomeno del software Open Source.

Poter contare sulla solidità del supporto di F5 in tanti ambiti, compreso il settore pubblico, è una forte garanzia per tutte le imprese che stanno incrementando sempre di più l'utilizzo dei canali digitali.

Ma la strategia di lungo termine di F5 non si è fermata all'application delivery: con il recente investimento da un miliardo di dollari per l'acquisizione della soluzione Shape Security, basata principalmente su soluzioni di machine learning e AI, F5 punta a cambiare le modalità di identificazione dei rischi informatici, riuscendo a identificare un altissimo numero di tipologie d'attacco.

Queste acquisizioni rispondono alle esigenze di un mercato oggi pronto a sviluppare applicazioni con nuove modalità di sviluppo, in grado di supportare i bisogni dei clienti finali, senza rinunciare a adeguati livelli di sicurezza applicativa.

Rispetto al passato, quando lo sviluppo e il rilascio di nuove versioni delle applicazioni aziendali richiedeva dai sei mesi in su, oggi la rapidità del time to market è cruciale: l'adozione dei cloud e l'impiego di moderne metodologie di sviluppo sono la risposta. «Oggi, grazie alle nostre soluzioni di application delivery e security, siamo in grado di fornire un servizio che cresce con gli utenti, aumentando la user experience di ognuna delle app da essi utilizzate», afferma Desiderio.

È naturale chiedersi come si sia potuto raggiungere questo risultato e quali criticità si possano incontrare: «Il tutto è stato reso possibile dall'evoluzione della programmazione, che non richiede più di scrivere linee e linee di codice, ma consente di usare degli elementi che funzionano come i mattoncini di Lego, che possono essere assemblati facilmente, con cui creare varie funzionalità aggiuntive. Tra i primi esempi di questo approccio», aggiunge Desiderio, «possiamo ricordare le tecnologie come Javascript, ma il cambiamento è stato soprattutto nell'impulso a condividere



Maurizio Desiderio, Country Manager Italia e Malta di F5

inquadratura per approfondimenti online



le esperienze e gli stessi "mattoncini di Lego", in pieno spirito Open Source». Senza entrare nel tecnico, le API hanno rappresentato e rappresentano un chiaro esempio di questa evoluzione: esse sono un passo fondamentale nella semplificazione e nella trasparenza dello sviluppo applicativo moderno, ma se non adeguatamente protette con sistemi dedicati di sicurezza possono causare grossi danni a causa della possibile perdita di messaggi, degli errori di "traduzione" dei vari linguaggi di programmazione o della consegna dei messaggi in mani sbagliate. Come sottolinea Desiderio, «Le API sono oggi una delle basi fondamentali dello sviluppo applicativo, ma posso facilmente diventare anche il punto più debole della sicurezza nelle applicazioni». Per tutti questi motivi, F5 ha sviluppato e introdotto tecnologie che proteggono le API dalle principali minacce di sicurezza: il country manager italiano sostiene infatti che «siamo gli unici, da sempre, a porre le applicazioni al centro del business. Anche se oggi tutte le aziende che propongono soluzioni di sicurezza stanno correndo ai ripari per "mettersi al pari" sul fronte della protezione delle applicazioni». Questo "involucro" di sicurezza attorno all'applicazione deve però essere necessariamente trasparente agli utenti, che vogliono interagire con applicazioni semplici, intuitive ed efficaci e agli operatori, che devono preoccuparsi solo degli aspetti logistici o economici nello scegliere dove mettere le proprie applicazioni, avendo molto spesso a disposizione un ambiente multi-cloud o hybrid-cloud. Da parte di F5, evidenzia il country manager italiano, c'è l'impegno a essere sempre all'avanguardia per

garantire che la protezione e gli altri servizi costruiti intorno all'app siano costantemente aggiornati, nonché per estendere la sicurezza ad altre piattaforme in una logica multicloud.

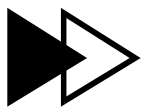
Prestazioni sotto controllo con le performance proattive

Un ulteriore livello di affidabilità e sicurezza sarà aggiunto presto, ci svela Desiderio, grazie a un motore di analytics che consentirà di monitorare il funzionamento delle applicazioni, rendendo possibile mostrare, per esempio, quale esatto elemento di una architettura a microservizi presenta bassi livelli di prestazione.

L'obiettivo è l'ottimizzazione generale delle performance con una logica proattiva.

Come sottolinea il country manager, si tratta di un risultato importante non solo per la sicurezza, ma, in generale, per tutto ciò che riguarda le prestazioni delle applicazioni, «il cui diffuso utilizzo fa in modo che esse siano sempre più indispensabili per gli utenti che, di conseguenza, hanno un livello di pazienza molto bassa e la situazione andrà peggiorando. Il rischio è perdere il cliente che, grazie all'ampia offerta di mercato, ha la possibilità di passare velocemente a un servizio della concorrenza». Tale aspetto è ulteriormente critico nel caso dei managed service provider, non necessariamente fornitori legati alla sicurezza, che devono gestire al meglio il cliente, rispettando come minimo le SLA (Service Level Agreement). Per questo molti managed service provider che utilizzano le tecnologie di F5 troveranno un vantaggio importante con i nuovi analytics. «La stessa cosa», sostiene Desiderio, «vale per il

Public Cloud, poiché ogni fornitore ha logiche commerciali e logistiche che determinano un impatto sulle SLA. I controlli forniti da F5 sono un'ulteriore garanzia, anche nello specifico della sicurezza, rispetto alle credenziali e ai privilegi degli utenti». Un altro vantaggio dell'adozione di soluzioni di machine learning, infatti, consisterà nella capacità dei sistemi di autenticazione di definire un profilo abbinato all'utente. Tipicamente ciascuno di noi opera allo stesso modo: non solo possiamo capire se un utente "torna" sul nostro servizio, ma gli scostamenti dal profilo sono sospetti e meritano un approfondimento con operazioni preventive. Si tratta di logiche già applicate, per esempio, dalle banche sulle transazioni con carte di credito, che avvisano se si sta effettuando un prelievo più alto del solito. In sostanza, scatta un controllo quando si verifica un'anomalia. In tal senso gli strumenti di machine learning sono fondamentali, perché non è umanamente possibile prevedere quali minacce possano nascondere grandi quantità di transazioni generate attraverso bot. Inoltre, è noto che persiste una carenza di tecnici specializzati nella sicurezza e ancora meno sono quelli che possono vantare grande esperienza. Il manager ci lascia con un caso di successo: «Abbiamo realizzato un progetto con centinaia di utenti in una realtà italiana che ha scelto F5. Il suo sviluppo è stato emblematico perché ha permesso di evidenziare l'efficienza del modello a microservizi sia nella parte di progettazione sia in quella di messa in esercizio. Il progetto iniziale, infatti, è stato completamente rivoluzionato e non per rispondere alle esigenze tecniche di F5, bensì per migliorarlo a vantaggio del cliente». ❁



Il supporto di Westcon

La relazione, il supporto e la formazione

di Gaetano Di Blasio

inquadra per approfondimenti online



Alessandro Della Negra,
Country Sales Director Italy,
Greece, Cyprus, Malta and
Adriatics di Westcon



Westcon-Comstor è un distributore globale di soluzioni e sistemi digitali, in grado di offrire una conoscenza profonda delle tecnologie proposte: si tratta di un elemento cruciale, che parte dall'istruzione, fondamentale per l'adozione della tecnologia. Di questo si occupa Westcon, che garantisce la formazione di tecnici e utenti finali accreditati che possono ottenere le competenze e l'esperienza necessarie per fornire un'implementazione senza soluzione di continuità, per massimizzare l'utilizzo.

Come distributore di F5, Westcon ha diversi ruoli. «Certamente l'innovazione è il nostro pane quotidiano, per questo sono fondamentali l'informazione sulle nuove tecnologie e, soprattutto, la capacità di trasmettere le stesse in termini di formazione», afferma Alessandro Della Negra, Country Sales Director Italy, Greece, Cyprus, Malta and Adriatics di Westcon, che aggiunge, «a ciò si abbina il supporto in affiancamento alle risorse già formate. Più in dettaglio, la componente di Accademy, che vede per altro Westcon come l'unico Authorized Training Center di F5 in Italia, è certamente al centro delle importanti attività legate all'erogazione dei training ufficiali».

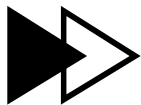
In quanto realtà internazionale, inoltre, i partner possono attingere alle competenze globali dei partner del distributore. «Per esempio, ricordo un episodio che mi è personalmente capitato»,

racconta Della Negra: «Un nostro partner italiano aveva bisogno di supporto relativamente a funzionalità particolari di NGINX e si è potuto appoggiare a un partner europeo con notevole esperienza specifica per realizzare, degli script appositi».

Più in generale emergono le potenzialità di abilitazione per i partner.

Westcon si occupa della soluzione di tutti i paradigmi tipici della filiera operativa che dal distributore arriva fino all'utente finale, in un contesto da gestire che è ben diverso dal rivendere hardware che è sempre più software defined, mentre queste nuove soluzioni si basano su micro-servizi, quindi su licenze. Dinamiche che prevedono gestioni degli approvvigionamenti diversi e così via.

Inoltre, Westcon si è dotata di una piattaforma cloud ad hoc per la gestione degli ordini di fulfillment delle risorse intangibili, ottimizzando la fatturazione ricorsiva, la gestione delle licenze multiple e multifornitore, il pagamento nel corso di utilizzo delle licenze anche nel caso non sia direttamente gestito dal fornitore, in un'ottica di semplificazione per il partner e per l'utente finale. Grazie ad un servizio di intelligent demand progettato dal distributore è possibile analizzare l'utilizzo delle soluzioni per prevedere quale potrà essere l'evoluzione tecnica e le esigenze che i partner e i loro clienti potrebbero avere in futuro, in modo da agevolare e accelerare lo sviluppo. Infine, il distributore fornisce altre tecnologie complementari a F5 fornendo al canale un unico punto di riferimento progettuale. ❄



Una piattaforma per assicurare la continuità del business

La visione della sicurezza 2020 con Trend Micro

di Gaetano Di Blasio

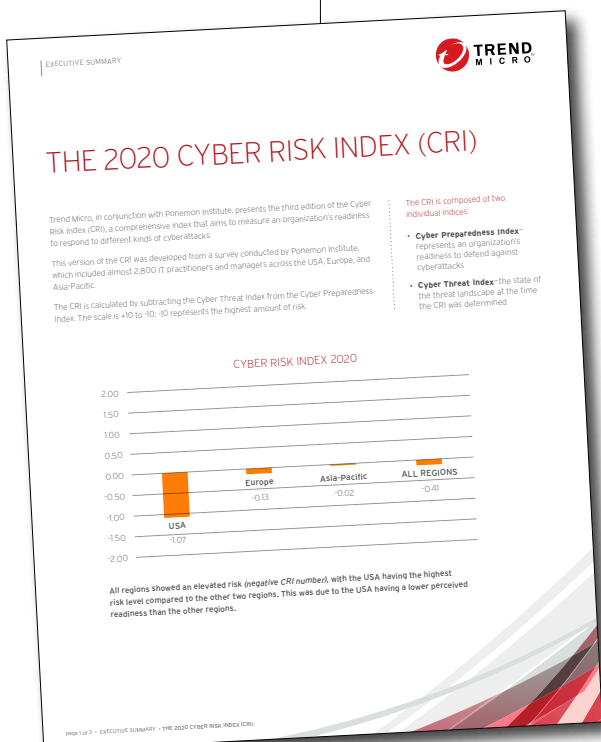
Nel 2020 abbiamo assistito a una corsa per la digitalizzazione scatenatesi per il bisogno di utilizzare lo smart working o l'home working, a causa delle limitazioni indotte dalla pandemia. Una indagine realizzata da Trend Micro con l'istituto Ponemon, mostra che L'88% delle aziende ha accelerato l'aggiornamento del digitale. Un riscontro in tal senso arriva anche dal boom degli acquisti in dispositivi, servizi e applicazioni in cloud.

Ma tutto ciò, ancorché positivo, si limita in parte a spostare confusamente risorse in cloud senza attenzione per la sicurezza né una reale consapevolezza del cloud, afferma Alessandro Fontana Head of Sales Trend Micro Italia, commentando: «Basti pensare alla scarsa consapevolezza del concetto stesso di share responsibility, che implica la messa in sicurezza di quanto è "in the cloud"».

Il manager continua, riprendendo i dati dell'indagine: «A dimostrazione della mancanza di consapevolezza, solo il 55% degli intervistati ha previsto di implementare strumenti di protezione. Ciò è ancora più grave, poiché il cloud prevede un processo continuo e infinito che impone capacità di automazione».

Sul fronte degli attacchi la pressione resta alta, come dimostrano i dati della Smart Protection Network di Trend Micro. Covid 19 è tuttora l'escsa del momento, in varie declinazioni: malware, phishing, attacchi mirati e così via presentano quasi sempre la parola Covid, hanno osservato in Trend Micro.

Tornando ai dati della ricerca Ponemon, il 51% degli intervistati sostiene di aver capito che occorre investire di più in



Inquadra per approfondimenti online



sicurezza, l'87% ritiene di avere il pieno controllo, l'83% è fiducioso di poter gestire la sicurezza nell'immediato futuro. In generale, cresce una certa consapevolezza. D'altro canto, resiste un 45% di rispondenti che considera la sicurezza un ostacolo. Eppure, basterebbe un metodo critico, come suggerito nel GDPR, che impone semplicemente di considerare la security, monitorare e valutare il da farsi. In questo non si è soli: l'utente finale è normalmente supportato da un system integrator: *«Il nostro approccio - evidenzia Fontana - non parte dal voler vendere un prodotto, ma dall'aiutare il cliente e supportarlo a tutto tondo. Sappiamo quali sono le preoccupazioni delle aziende, come, per esempio, la coerenza delle policy, le applicazioni delle patch, la protezione dei flussi network, così come pure la privacy e la compliance. Oggi non esiste un perimetro aziendale, non ci sono confini, pertanto l'obiettivo è supportare il cliente al 100%».*

Attenzione al cloud

Come accennato, spiega il manager c'è stata una rincorsa al cloud confusa e occorre fare attenzione, mette in guardia l'Head of Sales di Trend Micro: «Noi abbiamo una piattaforma di cloud ibrido in grado di soddisfare le esigenze dei nostri clienti. Non tutti sono pronti a gestire le complessità, senza strumenti

di automazione è impossibile e gli ICT manager tornano a preoccuparsi per la sicurezza.

Le aziende, sottolinea Fontana devono comprendere che la continuità del business dipende dalla sicurezza informatica, perché un attacco informatico blocca l'azienda, cioè il business.

Sul mercato ci sono tante aziende e startup di security e altre ne arriveranno ma poche possono vantare trent'anni di storia, durante i quali c'è stato, sottolinea Fontana, un costante

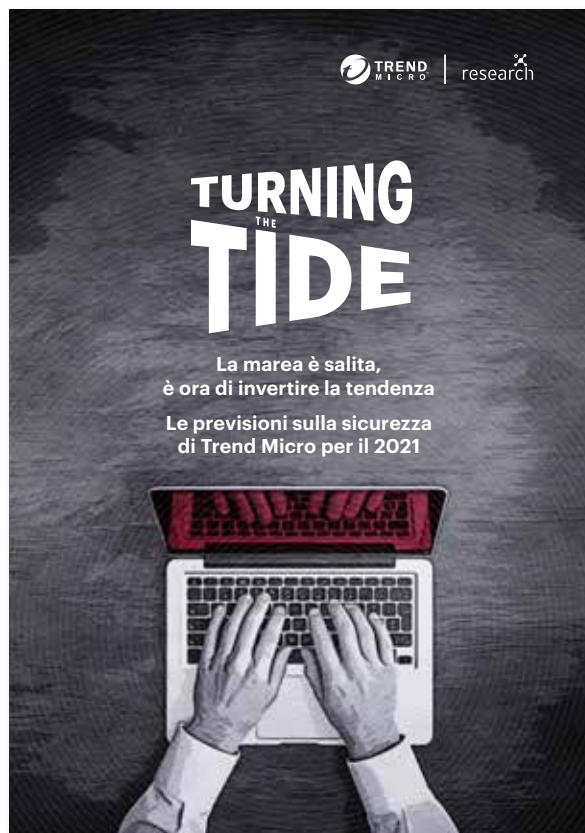


*Alessandro Fontana Head of Sales
Trend Micro Italia*

rinnovamento. Il manager ricorda come prima del cloud fosse stato necessario aggiungere la sicurezza della rete e altro ancora. Ora è il momento della Endpoint Detection and Response, ma si tratta "solo" di un altro pezzo di un progetto di sicurezza, mentre è necessario riuscire a vedere l'insieme. In altre parole, la visione di Trend Micro presume la capacità di Detection and Response non sull'end point, ma sull'intero progetto di sicurezza, che sia on premise, presso un cloud privato, pubblico o ibrido. Non si può perdere la visibilità del progetto di sicurezza. Si deve proteggere il dato che si trova su Office 365 come i servizi dei vari fornitori come Google o altri, sottolinea Fontana, aggiungendo *«Ci sono poi altri aspetti che devono essere considerati: per esempio c'è chi pensa di poter mettere in esercizio un data lake in cloud, trascurando i vincoli, come quelli imposti dall'amministrazione pubblica, rispetto alla movimentazione di tutta una serie di dati».*

Un'altra situazione critica è quella di una tecnologia che è fisicamente on premise, ma si avvale di un sistema di controllo in cloud. In questi casi, di fatto, il problema è il poter garantire sia la privacy che la compliance.

Nel cloud ci si espone a delle minacce, perché non siamo soli, ma condividiamo spazi. come sottolineato pocanzi.



Questi aspetti si allacciano a quelli della privacy, della formazione e della compliance. Senza una share responsibility ci si espone a delle minacce. L'event configuration di Trend Micro, permette di comprendere cosa realmente accade nel cloud.

È fondamentale che questo sia basato su: progetto, servizi e formazione per garantire la propria privacy,

e quella dei dipendenti e di ciò che si fa entrare nel cloud. Serve una visione accurata.

La pressione degli attacchi è notevole come dimostra il rapporto sulle previsioni per la cybersecurity nel 2021, realizzato dagli esperti dell'azienda, che si aspettano un massiccio attacco all'home working.

Cresce l'esigenza del management detection and response, cioè esperti che hanno una visione dall'alto grazie a strumenti per prevedere le minacce. In termini di prevenzione, Fontana ricorda anche le soluzioni di awareness che Trend Micro regala ai propri clienti per diffondere la conoscenza dei rischi e per educare alla protezione.

Per questo in Trend Micro hanno realizzato uno strumento per simulare attacchi in ufficio, in modo da far comprendere come possa essere facile

sbagliare. Con un po' di conoscenza e attenzione si rende più difficile l'azione malevola.

A tal proposito, tornando al cloud è importante verificare l'aggiornamento delle applicazioni. Queste ultime, se non "aggiornate" possono compromettere un sistema: *«È più facile per un hacker sfruttare una vulnerabilità, piuttosto che creare un attacco zero day. D'altro canto, è pressoché impossibile stare al passo col patching, senza automatismi. Con le soluzioni di Trend Micro è possibile effettuare una scansione delle vulnerabilità e verificare quando è il momento migliore per applicarle virtualmente, cioè, precisa il manager, senza che possano generare conflitti, anche perché nulla viene installato sulla macchina.*

Sono diversi gli esempi di business continuity risolti dagli esperti di Trend

Micro, come il caso che ha coinvolto un cliente con 40mila utenti che per ragioni di compliance non potevano utilizzare dispositivi personali, ma dovevano usufruire di tutti i contenuti da lunedì al venerdì.

In generale osserviamo che l'approccio di Trend Micro è basato sul concetto di platform company, che abbraccia l'intera azienda, in sostanza, ci spiega Lisa Dolcini, Head of Marketing di Trend Micro Italia "L'obiettivo è fornire una piattaforma di sicurezza condividendo una base comune, che consiste nel sistema di Threats intelligence e nelle analisi condivise con i ricercatori di Trend Micro, oltre che in un'infrastruttura comune. importante è molto importante anche la nostra capacità di integrazione con altri fornitori, che arricchisce l'intero ecosistema". ❁

Inquadra per approfondimenti online





Il retail nel prossimo futuro

Anche nel retail niente sarà più come prima. La pandemia sta cambiando regole e paradigmi.

Non è ancora del tutto chiaro dove si andrà: forse la sola certezza del momento è che la tecnologia giocherà un ruolo chiave nel ridefinire i nuovi modelli commerciali

di Gian Carlo Lanzetti



Del futuro del retail si è discusso in occasione dell'evento digitale del Sole 24 Ore "Retail transformation summit", svoltosi a Milano lo scorso 24 novembre.

In uno scenario in continua evoluzione, ha esordito Fabio Tamburini, direttore Il Sole 24 Ore, in cui cambiano velocemente i comportamenti di acquisto e di consumo, sono molteplici le sfide con cui si devono e dovranno confrontare gli operatori del retail. Lo sforzo attuale sta nel capire quale sarà la strada migliore da percorrere. Il 2020 si ricorderà come l'anno zero del settore, cosa peraltro che si evince anche dalla nuova grammatura coniata per descrivere i cambiamenti in atto nel settore dei consumi).

«Le aziende dei beni di consumo devono continuare a competere puntando alla distintività e alla qualità dei prodotti - ha commentato Alessandro d'Este, Presidente IBC, Presidente e Amministratore Delegato Ferrero Commerciale Italia -. Quindi sia sul piano locale sia su quello internazionale questa è una delle sfide che le aziende devono vincere. Fondamentalmente dobbiamo continuare a lavorare sugli elementi di distinzione dei prodotti italiani e far leva su quella che è l'immagine del nostro Paese. Allo stesso tempo bisogna continuare a investire, in modo particolare su ricerca, sviluppo e innovazione».

Tutti omniscustomer?

Una cosa quasi certa è l'affermazione del concetto di omnicanalità e quindi della ibridizzazione delle modalità di acquisto. «Questo cambiamento - ha sottolineato **Massimo Curcio, Associate Partner KPMG Advisory** -, richiederà una profonda analisi di tutti i dati a disposizione e quindi l'impiego

di tecnologie come i big data. Sarà sempre più importante trasferire tutti i dati sull'acquirente dal canale digitale e quello fisico, implementando in questo modo la cosiddetta booking economy, per tendere all'acquisto il più possibile personalizzato. Parallelamente si andranno anche sviluppando nuove forme di consegna, anche in questo caso con priorità verso la personalizzazione. In altri termini il cliente andrà sempre maggiormente curato e assistito in modo sia proattivo che reattivo».

E' questa una delle ragioni per cui KPMG ha sponsorizzato con il Politecnico di Milano l'Osservatorio sulla Multicanalità che ha già messo in evidenza come i cambiamenti in corso hanno già prodotto seri impatti all'interno del settore retail, tra cui appunto la nascita dell'omniscustomer, come risultato dello spostamento del processo di acquisto verso la sua digitalizzazione. Ma c'è ancora molto da fare.

A questo riguardo Curcio ha citato un report di Mediobanca, secondo cui per ora solo il 22% dei consumatori possiede competenze digitali avanzate e che sempre più la casa si va trasformando in un hub di servizi, di socializzazione ma anche di acquisto. I dati sullo sviluppo del commercio elettronico sono una dimostrazione, che vale sia per il retail in senso stretto sia per il grocery. Nuovi modelli di relazioni sono all'orizzonte e avranno riflessi significativi non solo sullo sviluppo delle vendite e dei profitti dei retailer ma pure sulla sostenibilità del business. «Bisognerà quindi fare in modo - ha spiegato l'esperto - che l'esperienza digitale venga resa accessibile a tutti i consumatori. Sarà questa una delle missioni dei retailer, nella ricerca del ricompattamento dei servizi; solo quelli che si impegneranno

anche nella alfabetizzazione digitale avranno la certezza di ritagliarsi un futuro di successo.»

Più innovazione distintiva

Bisognerà pertanto investire in innovazione. A questo riguardo **Alessandro d'Este, presidente e amministratore delegato di Ferrero Commerciale Italia** ha parlato di una innovazione distintiva. «La distintività non sarà solo nella qualità dei prodotti ma anche nei servizi offerti a sostegno degli stessi. Andremo verso un retail a più alto contenuto di servizi, parallelamente a quanto sta facendo l'industria. Il rischio è quello della polarizzazione del sistema distributivo».

In uno scenario di questo tipo il posizionamento sul pricing potrebbe non bastare più. Ne è convinto **Enrico Galasso, amministratore delegato Birra Peroni**, che ha annunciato per l'anno prossimo la tracciabilità in blockchain: «Così ciascun consumatore saprà da dove proviene l'orzo utilizzato per la nostra birra». Galasso ha ricordato le perdite - 15% in volumi - dovute al crollo dei consumi e ha lanciato un appello alla distribuzione perché investa in un valore sostenibile nel tempo. Peroni attualmente vanta già una filiera di circa 1500 agricoltori che coltivano le materie prime di cui ha bisogno. Una pratica che accentua il valore del made in Italy, destinato appunto ad essere accentuato ancora di più con l'iniziativa del blockchain di cui si è detto prima.

In vista una polarizzazione dei consumi?

A proposito della possibile polarizzazione dei consumi, ossia della creazione di una fascia premium, in



contrapposizione a una fetta di popolazione sempre maggiore che si orienta sul risparmio, **Marco Pedroni, presidente di ADM** (distribuzione moderna), ha evidenziato che: «La sfida più importante, non solo per la grande distribuzione, ma per tutta la filiera, è offrire prodotti di buona qualità a tutti, altrimenti dovremo adottare un modello americano, che prevede il doppio binario per ricchi e poveri. Si tratterebbe per l'Italia e l'Europa di un cambiamento epocale che farebbe tanti morti e feriti, con evidenti vantaggi per chi è in grado di correre più velocemente sulla strada della digitalizzazione e investire in innovazione in modo corretto e sostenibile».

Un caso è quello della Lidl, azienda tedesca impegnata in Italia a investire della estensione della rete, con aperture di una cinquantina di punti vendita all'anno, e in contemporanea nei servizi. Con la creazione di una media di 2000 posti di lavoro l'anno, ha precisato

Massimiliano Silvestri, presidente di Lidl. «In queste situazioni lo storytelling, ha aggiunto, diventa uno strumento operativo importante all'interno della nostra strategia di vendere prodotti di qualità a un prezzo accessibile a tutti».

«Siamo di fronte a una nuova forma di povertà», ha aggiunto anche **Mario Resca, presidente Confindustria**, che ha aggiunto: «Il bilancio dei consumi ci porta ad un calo del 30-40% su molti settori come l'abbigliamento e gli accessori. Molte aziende stanno chiudendo, anche perché arriviamo da un 2019 che non era brillante. Il bollettino di guerra quotidiano con 500 morti al giorno ha spaventato i consumatori. L'aumento del risparmio nelle banche è il frutto di una grande incertezza per il futuro. Il consumo è alla ricerca di una sua rinascita e l'innovazione tecnologica e organizzativa costituisce una delle fondamenta».

Verso una maggiore tracciabilità dei prodotti

Intervenendo al "Retail transformation summit" **Francesco Pugliese, presidente di Gs1 Italy** (si occupa di standardizzazione, rappresenta circa 35mila aziende) ha detto: «Ogni anno si producono centinaia di bilanci di sostenibilità: Gs1 Italy sta lavorando per la condivisione di strumenti di misurazione che siano certificati, altrimenti ciascuno dice la sua. Abbiamo coinvolto anche il Ministero dell'Ambiente: ho chiesto loro di lavorare insieme per identificare standard di misurazione, altrimenti tutto si riconduce a misure che hanno più a che fare con il marketing, che con la trasparenza». Per Pugliese standardizzazione vuol dire avere dati comuni e omogenei, soprattutto in una filiera così complessa, come quella agricola. Il risultato consentirà di uscire dalla babele in cui viviamo e di avere processi più efficienti. C'è quindi ancora molto da fare per arrivare a un

linguaggio comune in tutto il settore. Sono tre per Pugliese i passaggi da fare: offrire standard tecnologicamente evoluti che vadano oltre il codice a barre, digitalizzare le informazioni di ogni singolo prodotto e garantire la circolarità in quanto fattore di tracciabilità.

«Le imprese che si sono dimostrate più resilienti di fronte all'emergenza sono quelle che avevano già avviato il proprio percorso di digitalizzazione - ha affermato **Donato Di Nella, Head of Corporate Sales di Vodafone Italia**

- La trasformazione digitale in atto è ancor più evidente nel mondo retail. Basti pensare che in questi mesi si sono avvicinati per la prima volta all'e-Commerce 1,3 milioni di utilizzatori e lo smartphone è diventato il primo canale di generazione della domanda e-commerce. Le imprese devono poter contare su un'infrastruttura sicura e scalabile, integrata con soluzioni digitali end-to-end, e su piattaforme di analytics in grado di trasformare

la mole di dati in informazioni utili su cui basare le proprie decisioni. Devono inoltre poter contare su un partner tecnologico, che li accompagni nel proprio percorso di digitalizzazione per abilitare nuovi modelli di business e nuove esperienze per i clienti, che saranno sempre più semplici, interattive, immersive ed efficaci anche grazie allo sviluppo e alla diffusione della rete di ultima generazione».

Blockchain e big data, ma non solo

Che la tecnologia sia il fattore abilitante della trasformazione in corso nel retail è stato ribadito anche da Massimo Visconti, Value Chain Strategist Visconti Lab per il quale non è da escludere che la nuova normalità porti ad una riedizione dei negozi del vicinato, adeguatamente rinnovati rispetto a ieri, stante la ritrosia dei consumatori ad abbandonare l'ultimo miglio. «Il Covid ha impresso un'accelerazione alla

trasformazione e anche allo sviluppo di una nuova Supply (Value) Chain sostenibile e durevole. In questo contesto l'Ict e in particolare le reti di Tlc avranno un peso fondamentale, come già stanno dimostrando le reti 5G e le tecnologie AI e blockchain.

Ma ci sono altre tecnologie destinate ad emergere nel settore, ha detto **Giorgio Palazzo, partner expense Reduction Analysts**. «Una di queste, ha puntualizzato, è la realtà aumentata, che sta maturando velocemente e diventando sempre più accessibile anche economicamente. La cosa importante è avere chiari gli obiettivi verso cui tendere e fissare anche dei target sul ritorno degli investimenti. Ad esempio Casanova, che ha investito molto sulla multicanalità che parte dal negozio virtuale per interagire con il negozio fisico, sta raccogliendo i frutti. Oggi anche le aziende piccole possono accedere a queste tecnologie grazie alla modalità as a service».





Soluzioni specifiche e personalizzate

Anche per **Leonardo Comelli, Chief Marketing & Product Officer di M-Cube**: «La digital transformation sta cambiando sempre di più l'esperienza d'acquisto e le aziende hanno bisogno di essere accompagnate in questo percorso con un'attenzione sempre maggiore al cliente e alla sua soddisfazione finale. Per questo ci siamo alleati con Lenovo per affrontare le prossime frontiere che aspettano sia aziende sia consumatori. Il periodo che stiamo vivendo può essere di grande fervore per quanto riguarda le nuove tecnologie e le loro applicazioni nel retail, per portare l'esperienza virtuale di vendita a un livello ancora più alto e di maggiore soddisfazione per il cliente».

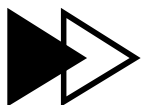
Da parte sua **Davide Patrini, Oem Solutions Sales Executive Lenovo**,

ha aggiunto che: «Con la creazione di questa nuova Divisione la sua azienda si propone di offrire ai clienti Oem non solo prodotti Lenovo ma anche di terze parti per implementare programmi specifici per il retail e per gestire al meglio il ciclo di vita dei prodotti, ovvero soluzioni verticali appositamente studiate e customizzate».

«Le imprese che si sono dimostrate più resilienti di fronte all'emergenza sono quelle che avevano già avviato il proprio percorso di digitalizzazione - ha affermato **Donato Di Nella, Head of Corporate Sales di Vodafone Italia** -. La trasformazione digitale in atto è ancor più evidente nel mondo retail. Basti pensare che in questi mesi si sono avvicinati per la prima volta all'e-commerce 1,3 milioni di utilizzatori e lo smartphone è diventato il primo canale di generazione della domanda e-commerce. Le

imprese devono poter contare su un'infrastruttura sicura e scalabile, integrata con soluzioni digitali end-to-end, e su piattaforme di analytics in grado di trasformare la mole di dati in informazioni utili su cui basare le proprie decisioni. Devono inoltre poter contare su un partner tecnologico, che li accompagni nel proprio percorso di digitalizzazione per abilitare nuovi modelli di business e nuove esperienze per i clienti, che saranno sempre più semplici, interattive, immersive ed efficaci anche grazie allo sviluppo e alla diffusione della rete di ultima generazione».

Infine **Francesco Morace, presidente Future Concept Lab** (sociologia del consumo), ha concluso sostenendo che sia i retailer sia i consumatori alla resa dei conti esprimeranno molta gratitudine al digitale. ❁



I rischi che le aziende temono di più nel 2021



L'Allianz Risk Barometer di quest'anno mostra i cambiamenti in atto nella percezione da parte delle aziende dei rischi che minacciano il business. A livello mondiale, la pandemia sale dal 17° al 2° posto, dopo l'interruzione delle attività

di Paola Saccardi

Il 2020 è stato un anno che sicuramente resterà nella storia per l'impatto che la diffusione del virus Covid-19 ha avuto a livello mondiale in diversi ambiti, da quello sanitario, a quello sociale ed economico.

La pandemia è stato un evento non prevedibile, seppur già accaduto in passato, che ha ricordato a tutti quanto possa essere difficile fare previsioni sul futuro e sui rischi che si corrono. Basta pensare che all'interno dell'Allianz Risk Barometer, l'indagine annuale sui rischi aziendali globali di Allianz Global Corporate & Specialty (AGCS), lo scorso anno la pandemia occupava il 17° posto e quest'anno è risalita al 2°.

Joachim Müller, CEO di AGCS, a tal proposito ha affermato: «La pandemia di coronavirus ci ricorda che non tutto è assicurabile, perciò la gestione del rischio insieme a quella dei Business Continuity Plan deve evolvere per aiutare le aziende a fronteggiare e superare situazioni estreme. Con la pandemia che persiste in tutto il mondo, dobbiamo essere pronti ad affrontare più frequenti scenari catastrofici "estremi", come un'interruzione del cloud su scala globale o un attacco informatico, disastri naturali causati dal cambiamento climatico o anche un'altra epidemia».

Un rischio chiaramente sottovalutato in passato, considerando che prima del 2021 non aveva mai superato il 16° posto in 10 anni di Allianz Risk Barometer. Invece, nel 2021, rappresenta in modo evidente il rischio principale in 16 Paesi e rimane fra i tre maggiori rischi in tutti i continenti e in 35 dei 38 Paesi selezionati per i quali è stata fatta un'analisi dei principali 10 rischi. Giappone, Corea del Sud e Ghana sono le uniche eccezioni.

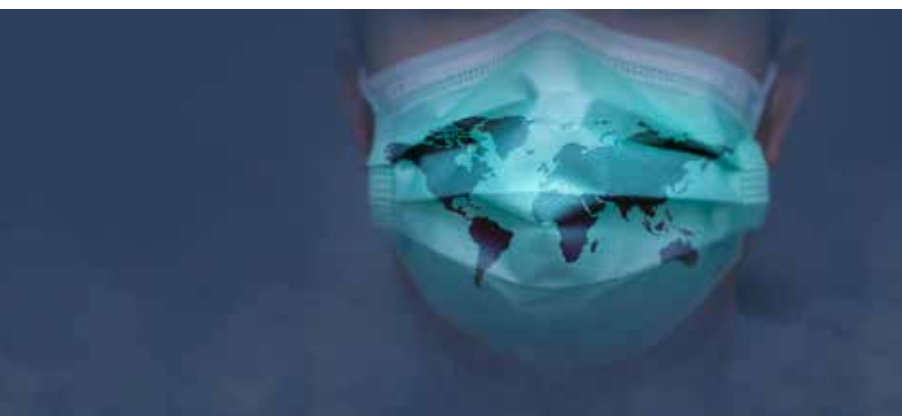
Quest'anno nella classifica dei rischi percepiti dalle aziende l'interruzione di attività risulta al primo posto con 41%

La top 10 dei rischi in Italia

Le risposte rappresentano la frequenza con cui un rischio è stato selezionato come percentuale di tutte le risposte per un determinato Paese – rispondenti:69

1	Rischi informatici (crimini informatici, violazione dei dati, guasti IT)	54%
2	Interruzione di attività (anche alla supply chain)	45%
3	Pandemia	28%
4	Catastrofi naturali (tempeste, inondazioni, terremoti)	25%
5	Cambiamenti nei mercati (volatilità, aumento della competizione/arrivo di nuovi operatori, fusioni e acquisizioni, stagnazione e fluttuazione del mercato)	22%
6	Cambiamenti nello scenario legislativo e regolamentare	20%
7	Cambiamento climatico/instabilità metereologica	19%
8	Danno reputazione o d'immagine	13%
9	Incendio, esplosioni	10%
10	Blackout energetici	9%

Fonte: *Allianza Global Corporate & Socialty*



delle risposte e a seguire la pandemia al secondo con il 40%. I rischi informatici occupano la terza posizione nella classifica mondiale.

Gli altri rischi che sono saliti nella classifica dell'Allianz Risk Barometer 2021, sono i cambiamenti nei mercati (n°4 con il 19%), i cambiamenti macroeconomici (n°8 con il 13%) e i rischi politici (n°10 con l'11%) che sono in gran parte scenari legati all'epidemia di Coronavirus.

Tra i rischi in discesa figurano, invece, i cambiamenti nello scenario legislativo e regolamentare (n°5 con il 19%), le catastrofi naturali (n°6 con il 17%), gli incendi/esplosioni (n°7 con il 16%)

e il cambiamento climatico (n°9 con il 13%), che sono stati superati a seguito dalle preoccupazioni legate alla pandemia.

La percezione dei rischi in Italia

In Italia, a differenza della classifica su scala globale, emerge che per la prima volta in assoluto, gli incidenti informatici si classificano come il più importante rischio per le aziende a livello locale. Al secondo posto vengono indicati i rischi legati alle interruzioni di attività (business interruption - BI), mentre la pandemia si posiziona quest'anno direttamente al 3° posto.

Rischio interruzione di attività

La pandemia in corso ha avuto un impatto molto forte, oltre che nell'ambito sanitario, anche in quello economico, dimostrando purtroppo che gli eventi estremi di Business Interruption su scala globale non sono meramente teorici, ma possono verificarsi realmente e inaspettatamente, causando perdite di ricavi e interruzioni della produzione, delle attività e delle supply chain.

Prima dell'epidemia di Covid-19, l'interruzione di attività si era già classificata per sette volte al vertice dell'Allianz Risk Barometer ma ora torna al primo posto che aveva ceduto agli incidenti informatici nel 2020.

Il 59% degli intervistati ha segnalato la pandemia come causa principale della BI nel 2021, seguita dagli Incidenti informatici (46%) e dalle catastrofi naturali e incendi ed esplosioni (circa il 30% ciascuno).

«Le conseguenze della pandemia, come la digitalizzazione più ampia, l'aumento del lavoro da remoto e la crescente dipendenza di aziende e società dalle tecnologie informatiche, aumenteranno probabilmente i rischi di BI nei prossimi anni - commenta Philip Beblo, del Global Property underwriting team di AGCS -. Tuttavia, i rischi tradizionali non scompariranno e devono rimanere nell'agenda della gestione del rischio. Catastrofi naturali, fenomeni meteorologici estremi o incendi rimangono le cause principali di interruzione dell'attività per molti settori e nel tempo continuiamo a notare una tendenza all'aggravarsi delle perdite a loro relative».

La risposta delle aziende alla vulnerabilità dovuta a eventi di business interruption le ha portate a costruire attività

più resilienti e a ridurre il rischio nelle loro supply chain. Secondo gli intervistati dell'Allianz Risk Barometer, il miglioramento dei piani di business continuity è l'azione principale che le aziende stanno intraprendendo (62%), seguita dallo sviluppo di contratti con fornitori alternativi o multipli (45%), dall'investimento in supply chain digitali (32%) e dal miglioramento della selezione e dell'auditing dei fornitori (31%).

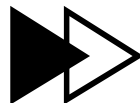
Crescono gli incidenti informatici

La pandemia sta contribuendo ad accelerare nelle aziende l'adozione del lavoro da remoto così come la trasformazione digitale e spesso la velocità resa necessaria dalla situazione di emergenza non consente di valutare attentamente anche il correlato aumento delle vulnerabilità IT.

Sebbene emerge dalla classifica globale che gli incidenti informatici siano scesi al 3° posto, si osserva che rimangono un rischio fondamentale per un certo numero di intervistati superiore a quello del 2020, e si collocano ancora tra i primi tre rischi in molti Paesi,

tra questi: Brasile, Francia, Germania, India, Italia, Giappone, Sudafrica, Spagna, Regno Unito e Stati Uniti.

Gli incidenti di ransomware, che già erano frequenti, stanno diventando più gravi poiché prendono sempre più di mira le grandi imprese con attacchi sofisticati e ingenti casi di estorsione, come risulta da un altro rapporto di AGCS "cyber risk trends". «Il Covid-19 ha dimostrato la rapidità con cui i criminali informatici sono in grado di adattarsi. L'ondata di digitalizzazione provocata dalla pandemia ha creato opportunità di intrusione con nuovi scenari di rischio che emergono costantemente» ha precisato Catharina Richter, Global Head of the Allianz Cyber Center of Competence di AGCS. ✨



Il BEUC chiede regole europee per l'intelligenza artificiale



L'associazione dei consumatori appartenenti alla Unione Europea ha espresso, in un sondaggio preoccupazione sull'uso della automazione senza limiti

di Gaetano Di Blasio





L'intelligenza artificiale è un tema basilare che nasce insieme all'uomo stesso o, almeno, sin dai tempi della Magna Grecia. Non vogliamo "disturbare Platone e ci limitiamo a partire dai primi calcolatori che hanno suscitato grandi entusiasmi per l'impulso innovativo e portato a questioni fondamentali sul piano tecnologico e su quello filosofico.

Il nostro punto di vista di editore specializzato nella tecnologia ci fa ritenere che l'artificial Intelligence sia fondamentale per lo sviluppo dell'innovazione e il miglioramento del modo di lavorare e accrescere la produttività. Ciò non toglie che il tema etico sia fondamentale, sia quando si pensa ai replicanti di "Blade runner" sia quando si progetta un'auto a guida autonoma, oppure quando si devono sintetizzare molecole per creare vaccini. In ogni applicazione la creazione dell'algoritmo è il punto critico dove possono insorgere errori. Gli ambiti di utilizzo sono molteplici in fervente crescita, nonché già utilizzati in numerosi prodotti e servizi: per esempio l'intelligenza artificiale viene impiegata nelle assicurazioni, per calcolare una polizza e decidere se concederla e a quali condizioni, è utilizzata per erogare servizi di assistenza dai

call center con una "chat bot" e sta sviluppando il promettente mercato degli assistenti domestici intelligenti, come quelli progettati dall'Istituto Italiano di Tecnologia a Genova.

In buona sostanza è corretto dire che l'intelligenza artificiale trasformerà la società e la vita dei consumatori.

A tal riguardo, Ursula Pahl, vicedirettore generale del BEUC, l'Organizzazione europea dei consumatori, afferma: «A causa dell'impatto a volte drastico e onnicomprensivo che l'intelligenza artificiale avrà probabilmente sui nostri mercati e sulla nostra società, i responsabili politici hanno iniziato a valutare le opzioni su se e come regolamentarla. Per noi, il punto di partenza del dibattito normativo è duplice: esaminare se i diritti dei consumatori possono essere applicati in modo efficace all'IA e comprendere meglio la consapevolezza, le preoccupazioni e le aspettative dei consumatori nei suoi confronti».

Il BEUC, insieme ad altre organizzazioni aderenti, ha condotto un'indagine tra novembre e dicembre 2019 in Belgio, Danimarca, Francia, Germania, Italia, Polonia, Portogallo, Spagna e Svezia. La sintesi dei risultati, in estrema sostanza: «I consumatori vedono il potenziale dell'intelligenza artificiale, ma sollevano serie preoccupazioni. In effetti, il potenziale esiste sicuramente:

il 91% degli intervistati ritiene che l'IA sia utile, per esempio nel prevenire gli incidenti stradali (91%) o per prevedere la loro salute (87%) problemi finanziari (81%). Il peraltro nell'assegnare un voto ai servizi di intelligenza artificiale che le persone hanno risposto non hanno dati voti elevati. Il 45% ad esempio afferma che l'intelligenza artificiale negli assistenti virtuali a domicilio non offre alcun valore aggiunto».

Nel Libro bianco pubblicato nel febbraio 2020 la Commissione europea ha individuato due elementi indispensabili per aiutare l'IA a progredire: l'eccellenza e la fiducia. Continua, quindi Ursula, «considerando il lato fiducia i risultati del nostro sondaggio non sono rassicuranti. In Belgio, Italia, Portogallo e Spagna la maggior parte delle persone (64%) concordano fortemente sul fatto che le aziende utilizzano l'IA per manipolare le decisioni dei consumatori. In Francia, Danimarca, Germania, Polonia e Svezia il 52% degli intervistati (fortemente) è d'accordo. L'IA sta trasformando il rapporto tra consumatori e aziende, un rapporto in cui il trader ha il sopravvento».

Tradizionalmente, il diritto dei consumatori è stato stabilito per correggere questo squilibrio. Ciò ha comportato, per esempio, obblighi di informazione o l'elaborazione di un elenco di pratiche commerciali sleali vietate. Il punto cruciale dell'IA, tuttavia, è che i consumatori di prodotti o servizi si trovano di fronte a cambiamenti man mano che l'algoritmo si adatta. Allo stesso modo, un trader potrebbe non essere in grado

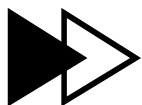
di prevedere ciò che il suo chat bot potrebbe raccomandare a un consumatore in una determinata situazione.

È pertanto essenziale effettuare un'approfondita valutazione del rischio prima di immettere sul mercato un prodotto IA e mettere in atto procedure di monitoraggio e gestione del rischio per tutta la vita. La supervisione umana è essenziale, così come la capacità delle autorità di effettuare controlli di conformità. A tal riguardo si sono espressi vari personaggi, come James Killian, professore di Economia del MIT e altre "autorità del campo sul forum "L'automazione non dovrebbe mai essere automatica". La sintesi della questione sta nell'esigenza di aggiornare l'attuale quadro giuridico. Pahl sostiene: «Riteniamo che tutto il nostro quadro giuridico per proteggere i consumatori debba adattarsi a questo ambiente in evoluzione. Sono necessari obblighi giuridici per regolamentare lo sviluppo e l'uso dell'IA per garantire che rispetti i diritti e i valori fondamentali dei consumatori dell'UE. Uno di questi obblighi giuridici sarebbe quello di dare ai consumatori la possibilità di rifiutare le decisioni prese in merito sulla base della intelligenza artificiale»

I consumatori sono d'accordo, spiega il rappresentante dei consumatori interpellati, che con una netta maggioranza ritengono di avere il diritto di dire "no" al processo decisionale automatizzato. In dettaglio lo affermano il 78% in Italia e Portogallo e l'80% in Spagna. La Commissione europea proporrà norme sull'IA nel 2021. Nondimeno, è in corso un acceso dibattito sul tipo di intelligenza artificiale da modificare e sugli obblighi che tali norme dovrebbero introdurre o se sono necessarie norme. Quest'ultima è l'opzione preferita per

coloro che sostengono che altrimenti le imprese dell'UE potrebbero essere in ritardo rispetto agli Stati Uniti e alla Cina. In questo contesto, è bene sapere cosa ne pensano i consumatori. La nostra indagine ha messo in luce che in Belgio, Italia, Portogallo e Spagna più della metà degli intervistati (51%) non sono d'accordo o sono fortemente in disaccordo sul fatto che l'attuale regolamentazione non sia adeguata a regolamentare in modo efficiente l'IA. In tutti e nove i paesi, meno del 20% sente che le norme attuali possono proteggerli adeguatamente dai potenziali danni posti dall'IA.

Conclude la vicedirettore generale del BEUC: «Presto i responsabili politici dell'UE dovranno decidere come regolamentare e guidare la diffusione e l'uso dell'IA in Europa. La posta in gioco è alta: per le imprese, i consumatori e la società in generale. Questo è il momento giusto per la Commissione europea, i deputati al Parlamento europeo e gli Stati membri di ascoltare le aspettative dei consumatori. Ma in un mondo sempre più globalizzato e digitalizzato, il benessere dei consumatori europei dipende non solo dalle politiche e dai regolamenti dell'UE, ma anche dalle norme e dalla cooperazione internazionali. È quindi molto positivo che l'OCSE abbia già pubblicato nel 2019 le sue raccomandazioni e i suoi principi per una gestione responsabile dell'IA affidabile, che richiedono, tra l'altro, che tutti gli attori dell'IA rispettino lo Stato di diritto, i diritti umani e i valori democratici, come la libertà, la dignità e l'autonomia, la privacy e la protezione dei dati, la non discriminazione e l'uguaglianza, la diversità, l'equità e la giustizia sociale. ✨



Cresce e si consolida il crowdfunding di Backtowork



Il successo della
piattaforma di
equity crowdfunding
che sostiene gli
investimenti a favore
di start-up, PMI e
progetti real estate
in Italia

di Edmondo Espa

Dalla telemedicina all'intelligenza artificiale, passando per il biotech, l'IoT e la circular economy: sono oltre 40 le società che, grazie al supporto di BacktoWork, la piattaforma fintech di crowdfunding partecipata da Intesa Sanpaolo, hanno raccolto capitali per quasi 15 milioni di euro da oltre 2.000 investitori privati e professionali.

Un risultato ancora più importante se paragonato al 2019: il volume degli investimenti cresce, infatti, di oltre il 100%, rispetto ad una media dell'intero mercato di poco superiore al 50%. La corsa della società dimostra che, nello scenario di grande incertezza ma anche di grandi opportunità che si è delineato nel corso del 2020, la voglia di innovazione e di nuove opportunità di investimento in economia reale è destinata a crescere sempre più velocemente. Innovazione e tecnologia hanno accelerato enormemente la loro diffusione per rispondere alle esigenze generate dalla pandemia e si è confermata la volontà degli investitori italiani di puntare sulle nuove realtà imprenditoriali

che, grazie a modelli di business innovativi e digital-oriented, sono in grado di rispondere in maniera più efficace a necessità vecchie e nuove.

BacktoWork è la principale piattaforma di equity crowdfunding in Italia che favorisce l'investimento a favore di start-up, PMI e progetti real estate da parte di investitori privati e professionali. La mission aziendale è quella di creare un circolo virtuoso in grado di favorire, con modalità innovative, l'afflusso di finanza verso le piccole imprese al fine di velocizzare la crescita del tessuto imprenditoriale italiano. BacktoWork propone a investitori retail, professionali e istituzionali un'offerta unica di opportunità d'investimento in aziende ad alto potenziale di crescita, accuratamente selezionate.

Un aspetto interessante da tenere presente è che investendo in start-up o PMI innovative si può beneficiare di una detrazione diretta dall'IRPEF pari al 50% di quanto investito. Se ad investire è una società di capitali, a quest'ultima spetta una deduzione dal reddito IRES pari sempre al 50%. ❁

È disponibile il nuovo libro
CLOUD e MULTICLOUD



Il libro è acquistabile al prezzo di 35 euro (IVA inclusa) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444