

SIC

U


RE

Z

ZA

BUSINESS IN MOVIMENTO

TIM Impresa Semplice



Porta tutti i tuoi file e tutte le applicazioni di Office sempre con te su pc, tablet e smartphone. Con OFFICE 365.

In più hai l'assistenza tecnica sul servizio TIM inclusa.

Da **6,50€** al mese per i primi 12 mesi.



Vai sul sito
digitalstore.tim.it

SICUREZZA

Mai come oggi, le aziende si trovano a fronteggiare un vertiginoso incremento del numero di attacchi. Ad accrescere i rischi contribuiscono temi quali la scomparsa di un perimetro aziendale definito, l'estrema diversificazione delle minacce, l'accesso in mobilità a dati e applicazioni critiche, la distribuzione delle informazioni nel cloud. Nel contempo, cresce l'importanza del dato per il business aziendale, mentre i requisiti normativi a cui conformarsi per la sua conservazione diventano sempre più stringenti.

In questo complesso scenario le aziende devono prepararsi ad affrontare la gestione del rischio in modo differente rispetto al passato, rivedendo il proprio approccio strategico e predisponendo contromisure sempre più sofisticate, in grado di attingere all'analisi intelligente dei dati di sicurezza provenienti da molteplici fonti. Questa monografia di DIRECTION si pone l'obiettivo di descrivere l'attuale quadro evolutivo della business security e di evidenziare gli aspetti strategici e tecnologici idonei a contrastare il crescente livello di rischio.

SOMMARIO

Direction Reportec numero 98 2017

Direttore responsabile
Riccardo Florio

In redazione
Giuseppe Saccardi,
Gaetano Di Blasio,
Paola Saccardi

Pubblicità
Edmondo Espa

Grafica e impaginazione
Aimone Bolliger

Immagini
Dreamstime.com

Reportec

Editore
Reportec srl,
Corso Italia 50 20122 Milano

Redazione
via Marco Aurelio 8 20127 Milano
tel 0236580441
www.reportec.it
redazione@reportec.it

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

Iscrizione al tribunale di Milano
n° 722 del 21 novembre 2006

Tutti i diritti sono riservati;
Tutti i marchi sono registrati e di
proprietà delle relative società

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

Sicurezza informatica	
una questione di business per le imprese	5
GDPR tra responsabilità e best practice	6
Come essere pronti per il GDPR	7
Analisi e compliance le chiavi di volta per la cyber security	8
Mail al sicuro con Unified Data Protection e Archiving	9
Più efficace la digital transformation con la cyber security	10
Conservazione a norma e dati protetti con RDX	13
La sicurezza dei dati e delle applicazioni	14
Dati sicuri con Hyperscale Convergence	15
Videosorveglianza e sicurezza dei dati	16
Dati e business al sicuro con la Veeam Availability Suite	18
Il digital workplace accelera l'innovazione	20
<i>Vent'anni di protezione con lo sguardo al futuro</i>	<i>II</i>
<i>Uomini e macchine per una vera sicurezza agile e consolidata</i>	<i>IV</i>
Intelligenza artificiale per la sicurezza nel contesto	22
GDPR e cloud per la trasformazione digitale di Ubi Banca	22
Sicurezza integrata per proteggere i sistemi SAP	24
Individuare le vulnerabilità protegge gli end-point	26
Predictive Security per prevenire gli attacchi anziché fronteggiarli	28
Reti senza perimetro ma più sicure con l'automazione	31
La sicurezza fisica	33
La videosorveglianza interagisce con l'ambiente	34
La security che integra protezione fisica e logica	38



Sicurezza informatica una questione di business per le imprese

A maggio del 2018 tutte le imprese dovranno essere in regola con la normativa europea GDPR (General Data Protection Regulation).

Quest'obbligo non deve essere sottovalutato ed è per questo che le sanzioni previste sono molto pesanti, fino al 20% del fatturato.

Il motivo per cui va preso sul serio, però, è un altro: mettere a punto una strategia per la protezione dei dati (e, ancora prima per la loro gestione) è più che necessario.

È vitale.

La cronaca, anche recente (basti pensare a Wannacry) ha mostrato la potenza dei cybercriminali, ma è solo

l'inizio, perché questi ultimi potrebbero a loro volta utilizzare automazione e intelligenza artificiale.

Non illudiamoci che diventerà una cyber war tra macchine, anche perché il punto debole resta l'essere umano.

GDPR tra responsabilità e best practice



La norma europea General Data Protection Regulation, una scadenza imminente che richiede di riorganizzare ruoli e procedure a beneficio del business

Il GDPR è un'opportunità per le imprese che sapranno cogliere l'occasione di riorganizzare i processi interni per meglio sfruttare la potenza delle informazioni e cavalcare l'onda della digital transformation potendo contare su una struttura data driven.

La legge impone degli adeguamenti e la revisione dei processi può essere un'occasione per mettere a punto piani necessari. Ci sono però obblighi per i quali le imprese italiane non sono preparate. Lo conferma, per esempio, una ricerca di Kaspersky Lab, da cui emerge che il 20% dei responsabili aziendali non ha idea di cosa sia previsto dalla nuova normativa e non sappia cosa fare.

Tra le novità più critiche introdotte dal GDPR ci sono i ruoli da definire, come il data officer, che in molte aziende esistono già, almeno di fatto, ma che da maggio 2018 assumeranno nuove responsabilità e alcune restrizioni. Oggi esiste una distinzione tra "responsabile del trattamento" e "titolare del trattamento", che andrà a modificarsi, imponendo sanzioni per le aziende. Responsabile e titolare dovranno prendere misure di protezione più stringenti di quelle, piuttosto blande, previste oggi.

Uno dei punti più ostici riguarda le procedure di Data Breach, cioè quelle che devono attivarsi nel momento in cui si subisce una violazione

informatica. Il primo problema è che, in Italia ci sono tempi di rilevamento di un attacco che superano 200 giorni! Il secondo problema è che non solo è necessario notificare la violazione dei dati personali all'autorità di controllo competente, ma nel caso in cui la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il responsabile del trattamento (quello che oggi è definito il Titolare) deve comunicare tale violazione all'interessato.

Altra novità riguarda la valutazione d'impatto, in pratica un'analisi dei rischi, che in talune circostanze diventa obbligatoria (per esempio è richiesta nel caso di una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata sul trattamento automatizzato, compresa la profilazione).

In generale l'analisi dei rischi è utile e propedeutica all'impostazione di una strategia per l'incident response, quindi un'opportunità doverla fare, ma bisognerà imparare a farla o rivolgersi a specialisti. Un altro aspetto previsto dalla normativa è quello della sicurezza "By Default" e "By Design".

Anche qui non sono novità per gli informatici, ma quante best practise sono perseguite nella programmazione del software e nell'organizzazione dei processi? Ancora una volta opportunità da saper cogliere, ma non gratuitamente. ❁

Come essere pronti per il GDPR

Il Regolamento Europeo 2016/679 sulla protezione dei dati personali è in vigore ed entro maggio 2018 le aziende dovranno adeguare processi e tecnologie per essere "compliant". Da dove cominciare? Il miglior approccio è la "consapevolezza del rischio" e la "conoscenza delle fonti di minaccia", che impongono di comprendere i nuovi obblighi e l'impatto che il Regolamento avrà sui processi aziendali, per poi affidarsi a professionisti che guidino verso l'aderenza alla normativa. «Vista la molteplicità degli aspetti da considerare per adeguarsi al GDPR - sottolinea Paolo Marsella, CEO di Aditinet Consulting (www.aditinet.it) - servono competenze che siamo assolutamente in grado di offrire, in quanto operiamo sul mercato dal 2004, supportando le principali aziende nazionali, disegnando architetture sicure, implementando meccanismi allo stato dell'arte per la protezione e messa a norma di applicazioni e dati critici, on-premise e sul cloud».

A livello organizzativo è essenziale che il management comprenda pienamente il GDPR, per poi valutare se nominare un Data Protection Officer (DPO) per la corretta applicazione. In questo, Aditinet si affianca al cliente con un proprio consulente che ricopre il ruolo di DPO. Un successivo assessment permette di accertare il livello di rischio e individuare come

La check-list di Aditinet per non farsi cogliere impreparati dall'entrata in vigore del nuovo Regolamento Europeo

comunicare con i titolari dei dati per assicurarsi il loro assenso.

In merito ai processi e sistemi coinvolti occorre conoscere la sorgente dei dati, quali di essi sono sensibili, disporre di strumenti per dimostrare il consenso all'utilizzo, per la cancellazione e la gestione delle violazioni. Sul piano tecnologico si deve intervenire su architetture, applicazioni e dati al fine di realizzare una soluzione personalizzata. Aditinet fornisce a tal fine la consulenza professionale del DPO, unita a strumenti per l'attuazione delle misure previste, tra cui soluzioni per rispondere agli articoli:

- **28 e 30** - Gestione unificata delle Identità, delle utenze applicative, dell'accesso e visibilità dei dati strutturati (Data Base) e non strutturati (Fileshare e cloud)
- **32, 33 e 34** - Sicurezza dei dati e delle credenziali di accesso ai sistemi
- **24 e 25** - Protezione da attacchi esterni tramite Firewall

Paolo Marsella, CEO di Aditinet Consulting



perimetrali, ATP, anti-Ransomware etc.

- **24 e 25** - Protezione da Data Exfiltration (DNS, Behavioral Analysis, Data Loss Prevention)
- **33 e 35** - Gestione degli eventi (Monitoring, Log/Event Management, SIEM)
- **32 e 33** - Servizi di Change Management, Incident Management, Backup/Restore Management)
- **25, 33, 34, 35 e 35** - Servizi per la progettazione e la Privacy By-Design

«Dopo aver verificato adeguatamente quali sono i soggetti che impattano con il GDPR - osserva Marsella - occorre impiegare l'esperienza di professionisti della IT Security in grado di guidare le aziende verso la piena aderenza alla normativa. I consulenti di

Aditinet sanno affiancare i propri clienti, fornendo risorse altamente qualificate per la progettazione dei processi e l'implementazione delle soluzioni necessarie a essere assolutamente compliant al GDPR». ❁

Analisi e compliance le chiavi di volta per la cyber security

Sinergy ha sviluppato un approccio a security e compliance in linea con il business

Infrequenti casi di attacchi alla sicurezza evidenziano la necessità di ottemperare agli obblighi definiti dalle normative. Ma quello che necessita è, in primis, un framework di servizi atti a individuare le soluzioni più idonee per la specifica azienda, con un corretto bilanciamento tra investimenti e protezione dai rischi. «Il compito del nostro team di advisory consiste nell'effettuare le analisi di dettaglio che permettano di evidenziare le reali necessità di un'azienda in termini di cyber security e compliance in funzione del settore di appartenenza, della criticità dei dati da proteggere e dell'ambito di riferimento», ha osservato Marco Cecon, Senior Security Advisor di Sinergy (www.sinergy.it), system Integrator che vanta un team specializzato di Advisor in grado di finalizzare strategie pragmatiche relative alla cyber security e alla compliance.

Il problema che si nota in molti casi è che le aziende non dispongono di una puntuale definizione di ruoli e responsabilità e di processi di governo e controllo che preveda tempi, attività e fermi concordati su comparti dell'IT, con il risultato di rendere inefficaci gli investimenti fatti nella sicurezza perimetrale e il governo dei dati.

Per questo, uno studio dettagliato della situazione esistente è il primo passo che

Cecon suggerisce alle aziende. L'intervento di esperti Sinergy prevede una profonda analisi della cyber security e della compliance realizzata in modo asettico rispetto alle tecnologie. L'obiettivo è di definire un "Remediation Plan" che consiste in interventi che possono essere tecnologici (ad esempio per la protezione dai malware) oppure organizzativi e procedurali. Tutto ciò sempre con un'attenzione alla salvaguardia degli investimenti fatti. I piani di rimedio o di adeguamento fanno riferimento agli standard internazionali come la ISO27001 e la ISO22301 e a linee guida come quelle Cobit e ITIL. Oltre a ciò, i Remediation Plan pongono attenzione anche al tema fondamentale della formazione del personale in relazione ai rischi derivanti da un non corretto utilizzo degli strumenti di lavoro e della gestione dei dati di business o sensibili in termini di conformità normativa. Per le aziende che desiderano esternalizzare alcuni ambiti della gestione della sicurezza, Sinergy prevede servizi erogati dal proprio NOC di Torino per il controllo di infrastrutture e servizi IT e dai SOC di partner

di riferimento operativi a livello mondiale h24 con SLA molto stringenti. «L'impegno per la cyber security è in costante crescita all'interno di Sinergy, come risultato di un investimento continuativo e importante attuato negli ultimi anni dove alla proposta di soluzioni per la gestione di data center si è aggiunta la componente imprescindibile della sicurezza, con soluzioni e un approccio pragmatico che ha incontrato il favore dei clienti perché risponde alle sfide tecnologiche e normative dell'intero sistema IT», ha evidenziato Cecon. ❁



Marco Cecon, Senior Security Advisor di Sinergy

Mail al sicuro con Unified Data Protection e Archiving

Una tecnologia ad hoc di Arcserve garantisce la sicurezza delle mail, semplifica la ricerca e consente di adeguarsi alle normative

Arcserve (www.arcserve.com), specializzata nelle soluzioni di protezione dati e alta affidabilità ha affrontato il tema di come rendere sicure le email inserendo nelle proprie soluzioni la nuova tecnologia FastArchiver, sviluppata ad hoc per l'archiviazione della posta elettronica. In pratica, la soluzione risolve le criticità delle Pmi che, come le grandi imprese, devono proteggere gli archivi delle email al fine di renderli accessibili per audit e verifiche legali.

Disponibile come soluzione indipendente da Arcserve UDP (Unified Data Protection), Arcserve UDP Archiving conserva in modo efficiente le email archiviate on-premise o in cloud, in una posizione indipendente dal sistema di posta principale, grazie a funzionalità avanzate non presenti nei comuni servizi di posta elettronica in cloud. «Integrando la tecnologia di archiviazione delle email nel portfolio Arcserve, abbiamo risolto una delle principali criticità delle organizzazioni, non solo fornendo una straordinaria user experience, ma assicurando sinergie di protezione

dati e archiviazione della posta elettronica con una soluzione potente e semplice da usare», ha evidenziato Mike Crest, Ceo di Arcserve.

Gli aspetti considerati da Arcserve nella finalizzazione di Arcserve UDP Archiving per ridurre il rischio connesso alla conservazione sicura delle mail sono numerosi. Tra questi:

- Riduzione del rischio: permette di proteggere da interruzioni o malfunzionamenti del servizio di posta elettronica in cloud e consente l'accesso all'archivio delle email 24x7.
- Requisiti legali: abilita operazioni non sempre disponibili nei servizi di email in cloud, tra cui la ricerca su tutto il testo, tagging, evidenziazione dei risultati, salvataggio ed export della ricerca, supporto multilingue.
- Governance aziendale: consente di adeguarsi ai requisiti con la tracciabilità dei dati, reportistica, gestione degli archivi e controllo dell'accesso legato ai ruoli.

- Conservazione legale: mantiene i messaggi di posta inviati o ricevuti sotto forma di record inalterabile come richiesto per la loro conservazione legale.

- Gestione del ciclo di vita delle email: raccoglie le email inviate o ricevute tramite le piattaforme più diffuse e rimuove i record di posta al termine del ciclo di vita.

Funzioni specifiche permettono inoltre di supportare gli utenti di Microsoft Office 365, per esempio tramite la multi-tenancy per organizzazioni decentrate, postazioni remote o filiali, o l'acquisizione del Journal di Exchange per catturare le email protocollate di Exchange e memorizzarle in un sito

esterno a Office 365. Ne è anche possibile il deployment su cloud, su sistemi ibridi e on-premise per archiviare le email a basso costo. Arcserve UDP Archiving sarà disponibile in EMEA a partire dall'estate, mentre in autunno è prevista una versione integrata con appliance. ❁



Mike Crest,
Ceo di Arcserve

Più efficace la digital transformation con la cyber security

G Data ha sviluppato un processo che integra gli aspetti consulenziali, fisici, logici e gestionali per mitigare i rischi e garantire la business continuity

Le tendenze di mercato evidenziano che l'accelerazione della digital transformation interessa trasversalmente tutti i settori, dai servizi alla fabbrica, dalle aziende private alle pubbliche, dalle grandi imprese alle Pmi. Quello che però in molti casi le accomuna, osserva Paola Carnevale, Sales & Channel Manager di G Data Italia, è che si tratta di una trasformazione digitale che avviene in modo non organico, senza un preciso piano che preveda una parallela evoluzione dei processi connessi alla gestione sicura del dato e alla business continuity. I rischi che si corrono sono consistenti, dalla perdita di valore del proprio brand sino all'interruzione delle attività produttive.

Esiste indubbiamente una sensibile differenza tra grandi aziende e Pmi. Al contrario di quest'ultime le prime, infatti, sia per struttura organizzativa, sensibilità e necessità produttive, hanno adottato con maggior solerzia un approccio atto ad abilitare l'integrazione dei trend e dei paradigmi tecnologici ritenuti più adatti a sostenere la propria crescita e l'innovazione industriale.

Uno dei maggiori trend che può favorire la digital transformation a cui porre attenzione, nota Paola Carnevale, è per esempio il comparto

tecnologico dello smart working, per il quale è fresca di stampa la nuova legge regolatoria. Oramai circa il 50% delle grandi imprese utilizza questo nuovo modello di business legato a un moderno e flessibile concetto di lavoro. I numeri parlano da soli: sono quasi 250.000 gli smart worker già attivi in Italia.

Alla trasformazione del modo di lavorare si aggiunge quello di produrre, con l'Industry 4.0 che continua a diffondersi. Smart working e Industry 4.0, con i suoi risvolti connessi all'IoT, faranno sì che si incrementi sempre più la collaborazione uomo - macchina e macchina - macchina in uno scenario di connessioni virtuali in cui gli end user faranno

La sede e il campus di G Data a Bochum in Germania



sempre più ricorso alla mobilità. «È un'evoluzione apportatrice di benefici ma foriera anche di risvolti che vanno attentamente monitorati. Molte aziende non hanno ancora individuato il corretto approccio strategico per affrontare la trasformazione oramai incombente, così come non sono ancora del tutto consapevoli che l'innovazione non può essere affrontata senza aver prima definito un approccio strategico alla sicurezza informatica», mette in guardia Carnevale.

I problemi in cui sono incorse numerose aziende nel passato anche recentissimo evidenziano che più ci si espone con l'innovazione tecnologica integrando, connettendo e stratificando sistemi di provenienza diversa in un quadro non organico, più ci si espone a rischi di tipo informatico.

Per ottenere un equilibrio che possa sostenere la crescita in un quadro di sicurezza bisogna in sostanza riconsiderare profondamente tutto il comparto della cyber security e come l'azienda è esposta ai rischi, in modo da assicurare quella business continuity a cui è legata non solo la sopravvivenza operativa ma anche e ancor più la brand reputation.

Prevenire il rischio con un approccio olistico

È un dato ampiamente verificato di come lo sviluppo tecnologico sia determinante in termini di competitività, ma aver intrapreso questa strada

non garantisce da solo la cyber security. Non basta disporre di un reparto IT o persone dedicate alla security se questo non si trasforma in un approccio organico ma si limita a integrare prodotti di varia natura e origine nonché a gestire il rischio dopo che un attacco si è verificato. Quello che serve è un approccio olistico che veda in modo nativo l'integrazione tra le operation IT e quanto atto a garantirne la business continuity e la cyber security partendo da un'analisi della situazione esistente.

Paola Carnevale, Sales & Channel Manager di G Data



La gestione del rischio dopo aver subito un attacco finisce essenzialmente con il determinare la presenza di più prodotti e console non integrate che complicano la gestione e aprono la strada a nuove vulnerabilità. La soluzione consiste nell'adottare un approccio strategico preventivo

che trovi la sua genesi in una profonda analisi della realtà esistente, dell'esposizione al rischio e di cosa può essere fatto per mitigarlo a un livello accettabile.

«Il nostro approccio consiste nel fornire all'azienda e a chi al suo interno gestisce la sicurezza dell'IT, un supporto consulenziale volto in primis a capire come in quel momento è gestita e a che livello la sicurezza informatica, quali le problematiche e quali le soluzioni adottate. In un secondo tempo e una volta consolidata

la situazione e individuati gli obiettivi, forniamo le indicazioni utili a raggiungere le finalità prefissate in termini di cyber security. Nel processo consulenziale cerchiamo anche di coinvolgere il decision maker in termini di budget allocato al fine di far emergere il valore per il brand aziendale di una efficace strategia di cyber security e i rischi economici in cui si incorre nel caso di una sua assenza o scarsa efficacia a causa della limitatezza degli investimenti», ha spiegato Paola Carnevale.

Un processo, non un prodotto

Nell'intraprendere la strada della cyber security ci sono alcuni punti che G Data ritiene essere chiave per non incorrere in risultati lontani dalle aspettative. Un punto essenziale è che si deve affrontare il problema non come un semplice prodotto o somma di prodotti ma come un processo gestibile da un'unica console centralizzata.

«In G Data conciliamo il processo con il prodotto e interveniamo proponendo soluzioni che integrano tutte le componenti che determinano un processo di cyber security: dal tool anti ransomware alla gestione del dato in mobilità integrando un mobile device management, aspetto questo fondamentale per applicazioni di smart working. A questo aggiungiamo la gestione integrata delle patch tramite la console centralizzata, anche questo aspetto chiave in un processo volto a garantire la cyber security nell'epoca del ransomware», ha spiegato Carnevale.

Ci sono altri rischi che l'approccio di G Data è volto a mitigare. Tra questi,

il poter gestire da un unico strumento tutti gli aspetti connessi alla sicurezza compreso il backup che permette di uscire indenni dalla fase critica di un attacco, la navigazione sicura su internet, il determinare e controllare la policy aziendale dalla console di gestione e, non meno importante, gestire con un modulo di network monitoring quelle criticità che richiedono un intervento rapido, quali un sovraccarico di Cpu o di rete che può risultare critico in applicazioni di e-commerce.

L'approccio consulenziale e basato sul processo di G Data prevede anche il continuo supporto post installazione realizzato sia direttamente sia tramite una rete diffusa di partner e system integrator che possono gestire l'intero comparto della security e le soluzioni proposte.

Sia in fase pre che post installazione G Data organizza anche workshop in azienda volti a diffondere la cultura della cyber security. Sono workshop che permettono di trasferire agli utenti le best practice che permettono di mitigare quel rischio residuo insito nel fattore umano che può scaturire da una inconsapevole non corretta condotta del dipendente. ❁

In aumento i cyber-attacchi contro gli istituti finanziari

Le banche e gli istituti finanziari sono sempre più nel mirino degli hacker e dei criminali informatici. Il motivo è semplice: sono attratti dalla possibilità di ricavare ingenti profitti.

Quella di un elevato ritorno dell'investimento necessario per condurre un attacco con ragionevole probabilità di successo è infatti tra le motivazioni principali alla base della maggior parte di questi cyber crimini.

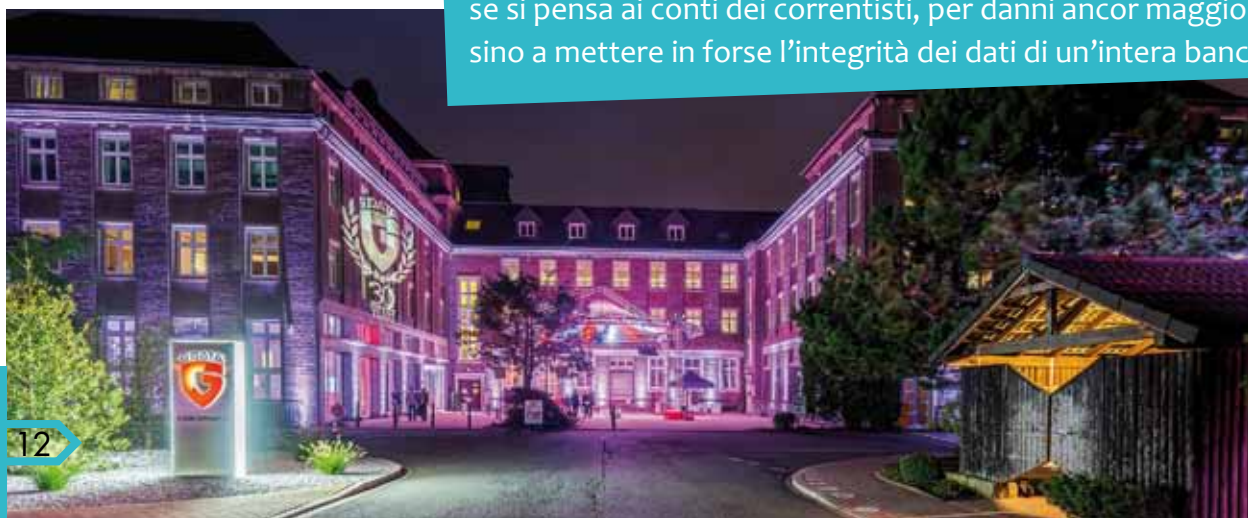
Ma non è solo questione di numero, il problema è che questi attacchi evolvono rapidamente, si fanno sempre più sofisticati e risulta complesso rilevarli in tempo utile per contrastarli.

Alcuni dati sulle dimensioni del fenomeno arrivano dal rapporto "Banking & Financial Services Cyber-Security: US Market 2015-2020", pubblicato da Homeland Security Research).

Nel suo complesso, il mercato della protezione dei servizi finanziari americani sfiorerà i 9,5 miliardi di dollari, diventando di fatto uno dei maggiori mercati extra governativi relativi alla cyber-security.

In quanto all'Italia, una ricerca su scala mondiale la vede all'ottavo posto, con un numero stimato di circa 35.000 computer compromessi all'interno delle istituzioni finanziarie. Va detto che le nazioni con il maggior numero di computer compromessi sono l'India (circa 65.000), la Germania (circa 115.000) e gli USA (oltre 140.000).

Il futuro non promette niente di buono. Gli esperti prevedono per un orizzonte non molto lontano che gli hacker saranno in grado non solo di rubare dati ma, quel che è persino peggio di modificarli, cosa che pone le basi, se si pensa ai conti dei correntisti, per danni ancor maggiori, sino a mettere in forse l'integrità dei dati di un'intera banca.



Conservazione a norma e dati protetti con RDX

Backup, disaster recovery e conservazione inalterata i punti salienti di RDX QuikStor di Tandberg Data

Salvaguardare i dati e rispondere alle normative per la conservazione di informazioni sensibili e amministrative, anche su lunghi periodi, è un problema che assilla i manager delle PMI. Una risposta al problema che coniuga classe enterprise, affidabilità, compliance e attenzione al budget è stata data da Tandberg Data (www.tandbergdata.com), con lo sviluppo di RDX, una piattaforma storage rimovibile su disco per il backup, l'archiviazione e il disaster recovery. Comprende unità inseribili in rack o ambienti di ufficio. A seconda delle necessità applicative possono alloggiare cartucce storage SSD, HDD e Worm facilmente sostituibili e spostabili fisicamente.

«Quella RDX - ha evidenziato Paolo Rossi, Channel Sales Manager della società in Italia - è una tecnologia giunta al suo decimo anno di vita e che continua a fornire funzionalità di backup e ripristino estremamente veloci ed economicamente convenienti per l'archiviazione dati a lungo termine. In pratica, combina

i benefici delle tecnologia tape e disco: la portabilità e l'affidabilità del backup basato su nastro alle velocità e semplicità dei dischi fissi e/o delle unità a stato solido».

La sicurezza nella conservazione dei dati si basa su robuste caratteristiche costruttive. Fisicamente le cartucce sono a prova d'urto e possono sostenere cadute sino da un metro di altezza, sono protette da scariche elettrostatiche e hanno una vita utile per l'archiviazione oltre i 10 anni. Gli apparati della famiglia RDX QuikStor sono inseribili nella propria rete aziendale e connessi come sistema desktop esterno o come unità server interna con connettività SATA III, USB 3.0 o USB3+.

I diversi modelli della famiglia condividono scalabilità, gestione centralizzata, crittografia e deduplica. Permettono di realizzare applicazioni di backup, archiviazione, scambio dati e disaster recovery.

Si possono archiviare fino a 4 TB per cartuccia e sino a 32 TB complessivi nella soluzione top. Le cartucce HDD

Paolo Rossi, Channel Sales Manager di Tandberg Data QuickStation a 4 unità per backup, archiviazione e disaster recovery



sono disponibili con tagli da 500 GB a 4 TB, i supporti RDX SSD con fino a 256 GB e i supporti RDX WORM per la conservazione inalterata a norma di legge in versioni da 1, 2 e 4 TB. Un accesso veloce ai dati memorizzati è assicurato tramite connessioni iSCSI Ethernet a 1 o 10 Gb.

Tutti i supporti, indipendentemente dalla capienza, sono retro-compatibili e lo saranno anche in futuro in modo da assicurare il mantenimento dell'investimento, ha evidenziato Rossi. «Alla luce dei recenti attacchi Ransomware, da Cryptolocker a Wannacry, i nostri partner si sono trovati estremamente preparati a contenere i danni del malware proprio grazie alla rimovibilità delle cartucce RDX. Molti di loro utilizzano le soluzioni RDX QuikStor installate all'interno dei server, in ambienti fisici e virtuali mentre sono aumentati coloro che le utilizzano in associazione a soluzioni NAS», ha commentato Rossi.

Sono recenti le partnership con Qnap e Synology che permettono di proteggere i dati presenti sui NAS effettuando un disaster recovery offline sui supporti RDX. *

I dati vanno gestiti, ancora prima che protetti insieme alle applicazioni che tali dati creano, elaborano, modificano per altre applicazioni. I supporti, ben lungi, dal potersi considerare semplici commodity si adattano a specifiche esigenze di business e incidono anch'essi sulle normative che dei dati pretendono la salvaguardia

La sicurezza dei dati e delle applicazioni

Dati sicuri con Hyperscale Convergence

L'architettura di NetApp assicura la disponibilità delle applicazioni e protegge i dati on-premise e in cloud

La trasformazione digitale è uno dei paradigmi che più coinvolgono le aziende. È però un paradigma che deve fare i conti con tecnologie non sempre in grado di garantire alle applicazioni business la capacità di calcolo e di storage che serve, e senza imporre costi aggiuntivi. Avere la sicurezza in ogni istante di far fronte ai livelli di servizio necessari, e garantire la sicurezza e la disponibilità dei dati, è un problema che NetApp si è proposta di risolvere con lo sviluppo di due sue nuove soluzioni: la piattaforma di calcolo e di storage iperconvergente (HCI: Hyper Convergent Infrastructure) e la nuova versione del suo sistema operativo Ontap.

NetApp HCI, disponibile nel quarto Q dell'anno, è una soluzione di classe enterprise ultra compatta per infrastrutture iperconvergenti, in pratica un data center di dimensioni scalabili. Ingloba a partire da una soluzione minima di 2 building block da 2 unità rack tutto quanto serve per



NetApp HCI a 4 nodi

le applicazioni, ne assicura la disponibilità e lo fa ottimizzando sia il Capex che l'Opex. Al suo interno comprende nodi specializzati che forniscono indipendentemente capacità di calcolo e storage, scalabili individualmente e di semplice gestione. Se serve più capacità elaborativa si aggiungono moduli di calcolo e solo quelli, lo stesso se serve esclusivamente più memoria, in modo da ottimizzare il Capex e rispondere agli SLA richiesti dalle applicazioni.

NetApp HCI utilizza storage di tipo all-flash SolidFire, una piattaforma che garantisce le prestazioni necessarie alle applicazioni, comprende servizi di replica remota dei dati, di data protection e di alta disponibilità. Ampie le possibilità d'uso della soluzione, sia per le Pmi che per le

aziende maggiori. È possibile adottarla sia a livello di sede periferica che di sede centrale dove è allocato il data center, e farlo con rapidi tempi di entrata in produzione.

«È possibile essere completamente operativi in meno di 30 minuti ed eliminare oltre il 90% dei problemi tradizionalmente legati alle esigenze prestazionali. Inoltre, un software sviluppato appositamente per ambienti VMware permette il controllo dell'intera infrastruttura mediante un'interfaccia utente intuitiva», ha evidenziato Roberto Patano, Senior Manager Systems Engineering di NetApp.

Per assicurare disponibilità e sicurezza dei dati NetApp ha rilasciato la versione 9.2 del suo sistema operativo Ontap. In particolare, ha illustrato Patano, il nuovo software migliora le performance all-flash, l'efficienza e lo spostamento dei dati nel cloud.

A quelle esistenti è stata anche aggiunta la funzionalità FabricPool, che permette di realizzare un tiering trasparente dei dati inattivi spostandoli automaticamente sul cloud, con una riduzione dei costi di storage flash on-premise anche del 40%.

Le prestazioni sono state migliorate anche tramite la deduplica inline espandibile attraverso pool di storage multipli, con un aumento dell'efficienza dello storage che, osserva NetApp, può arrivare al 30%.



Videosorveglianza e sicurezza dei dati

Western Digital fornisce gli elementi per proteggere l'ufficio o la propria casa e i dati aziendali e personali, lasciando ampia possibilità di scelta

Specialista dello storage, agnostica rispetto al tipo di supporto e tecnologia, Western Digital fornisce tecnologie e soluzioni che aiutano le persone a creare, usare e preservare i dati.

Hard disk, SSD, NAS, sistemi per data center sono a disposizione di aziende d'ogni dimensione per le proprie applicazioni e per organizzare la protezione dei dati e dell'azienda stessa.

A tal proposito va in particolare citata la nuova linea di soluzioni WD Purple, che sono state progettate per le applicazioni di videosorveglianza. Più precisamente, le unità WD Purple sono costruite per sistemi di sicurezza ad alta definizione, destinati a funzionare ininterrottamente 24 ore su 24, 7 giorni su 7, considerando anche la necessità di resistere a sbalzi di calore estremi, alle vibrazioni e alle tipiche condizioni ambientali in cui devono operare molti sistemi NVR (Network Video Recorder).

Un sistema di video sorveglianza deve essere affidabile, altrimenti è inutile. Per questo Western Digital ha ottimizzato le unità WD Purple

affinché possano supportare fino a 64 telecamere e un tasso di workload fino a 180 TB l'anno. A ciò si aggiunge l'esclusiva tecnologia AllFrame 4K di WD.

Quest'ultima permette di migliorare lo streaming ATA per ridurre la perdita di fotogrammi, ottimizzare la riproduzione, evitando immagini "pixellate", e aumentare il numero di alloggiamenti dell'hard disk supportati all'interno di un NVR.

In breve le caratteristiche base dei WD Purple sono: interfaccia SATA da 6 Gb/s; fattore forma da 3 pollici e mezzo, classe di prestazioni da 5400 RPM, capacità da 500 GB a 10 TB.

Pensando a chi possiede già un sistema di videosorveglianza DVR (Digital Video Recorder), magari da ampliare o aggiornare, Western Digital mette a disposizione un sistema di compatibilità per trovare lo storage più adatto alle caratteristiche del sistema in essere e alle eventuali nuove esigenze da soddisfare, potendo contare su un'ampia gamma di case e chipset supportati.



Soluzioni NAS WD

La protezione dei dati si basa su sistemi di backup che permettono di ripristinare i computer e le applicazioni dopo un eventuale attacco, come quelli sempre più diffusi e dannosi basati su ransomware, che compromettono proprio i dati memorizzati sui pc e server aziendali. Una soluzione di backup, per essere efficace, deve però essere costruita su componenti affidabili che consentano un funzionamento continuo, senza essere rumorose ma neanche rischiando il surriscaldamento che ne comprometterebbe il funzionamento, affinché siano operative 24x7. In particolare l'unità WD Red e WD Red Pro con il sistema NASware 3.0 è stata progettata per questi ambienti operativi, con un MTBF dichiarato (Mean Time Between Failure, cioè un tempo medio fra i guasti) che può arrivare fino a un milione di ore, in pratica non

si ferma mai.

Pensati per piccoli uffici, questi sistemi possono essere montati in case con fino a 8 alloggiamenti, per una capacità massima di 10 TB, garantendo alta compatibilità con sistemi esistenti.

La scalabilità con WD Gold

Quando si tratta di applicazioni con caratteristiche più impegnative in termini di workload, Western Digital propone la gamma WD Gold, che dispone di una tecnologia avanzata caratterizzata da affidabilità, capacità, efficienza energetica ed elevate prestazioni, arrivando a gestire carichi di lavoro caratterizzati da un ordine di grandezza superiore ai sistemi per desktop. Più precisamente, sono progettati per gestire workload fino a 550 TB l'anno, pur mantenendo il fattore forma da tre pollici e mezzo.

Come spiegano presso Western Digital, le soluzioni WD Gold sono progettate specificatamente per i server a elevata disponibilità e gli array di storage che richiedono caratteristiche tra le più robuste in abbinamento a servizi di assistenza clienti premium 24 ore su 24, 7 giorni su 7.

Elevato il livello di affidabilità, con un MTBF dichiarato fino a 2,5

milioni di ore, per una continuità senza fine.

Per una ulteriore garanzia, viene fornita l'avanzata tecnologia RAFF, che, grazie all'elettronica sofisticata controlla l'unità e corregge le vibrazioni lineari e rotazionali in tempo reale. Ne risulta un miglioramento significativo delle prestazioni in ambienti con elevate vibrazioni.

Altre garanzie derivano dalle capacità di ripristino degli errori "time limited" (TLER - Time Limited Error) per i RAID.

La tecnologia dynamic fly-height, invece, regola costantemente l'altezza della testina sia in fase di scrittura sia di lettura e, per una maggiore affidabilità, viene utilizzato un sistema con doppio attuatore che migliora l'accuratezza nel posizionamento delle tracce dati. Il secondo attuatore utilizza un movimento piezoelettrico per posizionare le testine con la massima accuratezza.

Il vantaggio dell'SSD

Finora si è parlato delle soluzioni hard drive, ottimali per tutta una serie di esigenze. Western Digital, peraltro fornisce un'importante gamma di unità a stato solido (Solid State Drive o SSD), che, invece

di supporti magnetici, per la memorizzazione dei dati usano memorie flash.

La caratteristica principali delle memorie SSD consiste nella velocità di accesso ai dati, portando un'accelerazione estremamente significativa nella lettura e scrittura rispetto ai citati Hard Disk Drive (HDD).

Oltre ai gamer, ci sono molteplici professionisti, dai musicisti ai grafici e altre figure aziendali impegnate in attività più o meno creative, che devono accedere a file di grandi dimensioni, i quali possono trarre vantaggio da un'unità SSD, usufruendo di avvisi rapidi del sistema e tempi di caricamento ridotti; lancio veloce di contenuti pesanti come video in 4K; realtà virtuale; editing o progettazione CAD/CAM.

Le SSD di Western Digital sono disponibili in due fattori di forma: 2,5"/7 mm e M.2 2280.

La rapidità di questi sistemi risulta utile anche per le applicazioni di sicurezza, per esempio, per le attività di forensic legate all'auditing relativa alle strategie di cyber security o per le indagini in caso di attacco informatico. ❁



	WD Red	WD Red Pro
Applicazioni	Sistemi NAS fino a 8 alloggiamenti	Sistemi NAS fino a 16 alloggiamenti
Garanzia limitata	3 anni	5 anni
Classe di RPM	5400	7200
Ideale per	NAS personali per ambienti domestici e per piccoli uffici	NAS per aziende di medie e grandi dimensioni
Cache	16 MB - 128 MB	64 MB - 128 MB
Massima capacità disponibile	10 TB	10 TB
Interfaccia	SATA 6 Gb/s	SATA 6 Gb/s

La gamma
Western Digital
Red

Dati e business al sicuro con la Veeam Availability Suite

La digital transformation impone a un'azienda di essere sempre disponibile. È quello che rende possibile Veeam con la sua Veeam Availability Suite

La trasformazione digitale da tempo in atto ha portato a nuovi paradigmi. Il modo di lavorare è profondamente cambiato, la forza lavoro e i clienti fruiscono sempre più di evoluti dispositivi mobili, il cloud ha accentuato lo spostamento verso i servizi, l'accesso alle applicazioni avviene indipendentemente dal luogo e dal tempo.

È uno scenario in forte evoluzione, evidenzia Albert Zammar, Regional Vice President della Southern EMEA Region di Veeam, che impone alle aziende di adottare nuove strategie e modalità organizzative che permettano di conquistare continuamente la fiducia dei propri clienti. Per ottenere e mantenere questa fiducia devono innanzitutto garantire una disponibilità e un accesso ai servizi forniti assolutamente continuo, ovunque e in ogni istante.

Quella della disponibilità continua, osserva Zammar, non è però prerogativa esclusiva delle grandi aziende. In un contesto in cui tramite Internet anche le più piccole possono proiettarsi a livello internazionale, essere sempre operativi è diventata oramai una condizione sine qua non per avere successo, ed è proprio quello che con le sue soluzioni si è prefissata di rendere possibile Veeam.

«Il nostro obiettivo consta nell'abilitare quella che viene definita la "Always On Availability", e cioè permettere alle aziende di

affrontare la digital transformation senza timore od onerosi investimenti, e far leva sulle possibilità offerte dalle nuove tecnologie senza dover avere i problemi derivanti dall'impossibilità di accedere a una applicazione quando e dove serve. Oggi abbiamo circa 245.000 clienti world wide che l'hanno adottata e tramite la quale proteggono quotidianamente un parco complessivo di svariate milioni di macchine virtuali», ha evidenziato Zammar.

Albert Zammar, Regional Vice President della Southern EMEA Region di Veeam

Proteggere il business con Veeam Availability Suite

La strategia per una Always On Enterprise di Veeam è incentrata sulla sua soluzione Veeam Availability Suite, un software giunto alla sua decima versione che permette di proteggere i dati e realizzare efficaci politiche di business continuity e disaster recovery.

La nuova versione di questo diffusissimo software ingloba numerose innovazioni tecnologiche e funzionali, quali per esempio il supporto per i server fisici e per il backup e restore su dispositivi NAS, e l'introduzione delle funzioni di Continuous Data Protection (CDP) per preservare i dati delle applicazioni business critical in caso di disastro. Sfruttando le funzioni di replica continua su cloud privato o gestito è poi possibile



garantire la disponibilità dei dati con capacità di ripristino, osserva Veeam, dell'ordine dei secondi. CDP può anche essere utilizzato con Veeam Cloud Connect per utilizzare come target primario lo storage in cloud. Un altro aspetto affrontato dalla versione 10 è relativo alle nuove tipologie di dati da gestire. Il supporto nativo per Object storage rende automatico lo spostamento dei dati basato su policy che permettono di liberare storage primario di costo elevato. Veeam prevede in tal senso il supporto per un'ampia gamma di piattaforme di Object storage su

cloud incluse Amazon S3, Amazon Glacier, Microsoft Azure Blob e tutto lo storage compatibile con S3/Swift. L'introduzione all'interno di Veeam Availability Suite v10 di una nuova Universal Storage API amplia anche l'ecosistema di partner strategici della società, aggiungendo, all'esistente supporto per i sistemi di Cisco, Dell, NetApp, Nimble, Exagrid e HPE, anche quello per le soluzioni di IBM, Lenovo e Infinidat.

In sostanza, con la versione 10 Veeam ha posto le basi per quella che evidenzia essere la prima soluzione di settore agentless, nativa per il

cloud, per la disponibilità e la data protection delle applicazioni AWS. Le nuove funzionalità consentono per esempio il backup e restore per le istanze in cloud AWS EC2, in modo da ridurre rischi nell'accesso alle applicazioni e garantire la protezione dei dati in caso di cancellazioni accidentali, attività dannose o compromissioni.

Veeam ha anche rilasciato la versione 1.5 di Veeam Backup for Microsoft Office 365 che estende ulteriormente il livello di disponibilità e di automazione per l'ambiente cloud di produttività personale di Microsoft. ❁

Cotonella di nuovo attiva in 18 ore grazie alla Business Continuity di Veeam

Cosa significa per la sicurezza del business e la continuità operativa aver allestito un efficace piano di disaster recovery, e averlo fatto con tecnologie adeguate, lo dimostra il caso di Cotonella, società del settore tessile con sede e data center a Sonico, in Valcamonica.

Cinque anni fa, su iniziativa del team IT, la società ha avviato un progetto che, con il supporto di Project Informatica, ha creato un'infrastruttura distribuita che prevedeva il backup dei dati su un secondo centro basato su software Veeam per il backup e il recovery, con RTO e RPO molto stringenti. Un progetto per una «Always On Enterprise» che, per gli obiettivi severi che si era posto, era stato considerato una sorta di assicurazione che si sperava di non dover mai riscuotere. Quattro anni più tardi, alla fine del 2016, l'investimento fatto, ha evidenziato Andrea Mariotti, IT manager di Cotonella e alla guida di un team agguerrito di 4 tecnici, è stato ripagato quando un incendio improvviso, scatenato da un banale corto circuito, ha distrutto l'intera sede e anche il data center, bloccando di fatto l'operatività aziendale.

Quello che in altre condizioni e in mancanza del robusto piano di disaster recovery allestito avrebbe costituito per l'azienda una seria ipoteca sulla sua continuità operativa e portato a consistenti perdite economiche e di mercato, si è rivelato invece, almeno per quanto concerne il business, uno scoglio superato in brevissimo tempo.

«Il piano di disaster recovery basato su software Veeam, nonché la disponibilità di un servizio cloud, ci ha permesso di tornare operativi in sole 18 ore. I primi server di backup erano già operativi e al lavoro quando l'incendio non era stato ancora del tutto domato», ha evidenziato Mariotti.



Andrea Mariotti,
IT manager di
Cotonella

Il digital workplace accelera l'innovazione

L'innovazione tecnologica sta trasformando il modo di lavorare e offre nuove opportunità d'interazione. I dipendenti ne sono consapevoli, guardano con ottimismo ai cambiamenti in atto e vorrebbero che la propria azienda traesse il massimo vantaggio dall'IT. Collaboration e mobility in un contesto sicuro sono tra i nuovi trend riconosciuti come i più rilevanti al fine di ottenere migliori livelli di produttività. Contrariamente a quanto però si riteneva, l'avvento della digital economy non ha eliminato la necessità di stampare e gestire documenti cartacei, ma ha dato la possibilità di farlo ovunque, in qualsiasi momento e da qualunque dispositivo.

Mediante le app è possibile inviare sul cloud i documenti scansionati in modo da potervi accedere anche quando ci si trova fuori sede. Con il digital workplace l'ufficio diventa sempre più intelligente e basato su smart object interconnessi tra loro, per cui da una lavagna interattiva è per esempio possibile inviare un documento in stampa oppure dividerlo in modo sicuro sui dispositivi mobili dei partecipanti a una sessione di lavoro. Gli ambienti di lavoro si trasformano anche grazie alle lavagne cognitive basate su IBM Watson in grado di rispondere a comandi, prendere appunti, annotare attività e tradurre i contenuti in diverse lingue.

Ricoh ha ridefinito il posto di lavoro con un approccio incentrato sul digital workplace. Cloud, mobility, app, IoT e sicurezza al centro dell'innovazione digitale

Davide Oriani, CEO di Ricoh Italia



paradigmi dell'IT quali per esempio cloud, mobility, app economy e Internet of Things. L'interazione tra componenti fisiche e digitali rende possibili nuovi scenari che creano valore per l'azienda e i dipendenti», ha evidenziato Davide Oriani, CEO di Ricoh Italia.

Per favorire questa evoluzione Ricoh ha ridefinito il posto di lavoro tramite una nuova offerta dedicata al digital workplace, con cui si è proposta di rispondere all'esigenza delle aziende di gestire in maniera integrata e sicura le informazioni e le comunicazioni superando i confini "fisici" degli uffici. Questo grazie anche a una serie di soluzioni "smart", tra cui dispositivi multifunzione, lavagne interattive, videoconferenza e videoproiettori che dialogano tra loro rendendo concreto l'ufficio interconnesso.

«Puntare sull'innovazione per l'efficienza del business dovrebbe diventare un obiettivo primario per le aziende. Il digital workplace di Ricoh aiuta le imprese a cambiare il proprio modo di lavorare secondo i nuovi

Nello scenario che si delinea svanisce il concetto di periferica e il dispositivo multifunzione diventa un hub intelligente su cui convergono informazioni e processi di business. È un cambiamento radicale che è confermato anche dai risultati di una ricerca commissionata da Ricoh a Coleman Parkes, secondo cui i dipendenti europei ritengono che la Digital Transformation sarà la più grande rivoluzione nel corso dei prossimi mesi. «Il digital workplace di Ricoh - osserva Oriani - rompe i canoni con i quali siamo abituati a pensare agli ambienti di lavoro rendendo le tecnologie sempre più pervasive e integrate in modo che le aziende riescano rapidamente a vincere la sfida del cambiamento».*

Proteggiamo il mondo
da 20 anni.



SAVING
THE WORLD
FOR 20 YEARS

#truecybersecurity

Vent'anni di protezione con lo sguardo al futuro

Kaspersky Lab, dal 1997 concentrata nella sicurezza di privati, aziende e pubbliche amministrazioni, s'impegna nel sociale e nello sviluppo tecnologico



Eugene Kasperky

Quando fondò la propria azienda, Evginij Kasperky (o Eugene, come la globalizzazione anglofona preferisce) si ritagliò il ruolo di capo della ricerca e tuttora che di Kaspersky Lab è il Ceo continua a seguire lo sviluppo tecnologico. Proprio alle sue intuizioni si devono anche gli sforzi in ricerca e sviluppo che hanno portato ad allargare considerevolmente il portfolio di soluzioni e servizi, per esempio nell'ambito dell'industrial security.

Una passione che si riflette in un impegno: «Crediamo che tutti, dagli utenti privati alle grandi società e ai governi, dovrebbero essere in grado di proteggere ciò che più interessa loro. Che si tratti di privacy, famiglia, finanze, clienti, il successo del proprio business o infrastrutture critiche, la nostra mission è proteggere tutto questo. Ci riusciamo offrendo la nostra competenza in materia di sicurezza, lavorando fianco a fianco

con le organizzazioni internazionali e le forze dell'ordine per combattere i cybercriminali, ed inoltre sviluppando tecnologie, soluzioni e servizi che aiutano a mettersi al riparo da ogni cyber minaccia esistente».

Nei vent'anni trascorsi dalla fondazione in Kaspersky Lab hanno fronteggiato minacce sempre più ampie e sofisticate, impegnandosi nella ricerca delle migliori soluzioni per la protezione e arrivando a maturare strategie sempre più integrate per aiutare i clienti.

Oggi Kaspersky Lab è un'azienda che opera in 200 paesi attraverso 37 sedi dislocate in 32 nazioni. Sono quasi 3mila e 700 gli specialisti altamente qualificati che lavorano per Kaspersky Lab, occupandosi delle 270mila aziende clienti e dei, complessivamente, 400 milioni di utenti.

Dallo sport al GDPR

L'impegno di Kaspersky Lab si estende anche nel "sociale", con il

supporto verso diverse iniziative in ambiti quali l'arte, scienza e sport: dalla collaborazione con il team di Formula Uno della Ferrari, al festival Starmus, senza contare ancora, il lavoro con varie organizzazioni scolastiche e le forze dell'ordine per accrescere la consapevolezza della sicurezza online e del cyber-bullismo. L'impegno e il supporto da parte di Kaspersky alle imprese si misura anche nell'approccio aperto, come per l'imminente appuntamento con la GDPR. È online un tool che consente di verificare, rispondendo a poche domande, qual è la propria posizione nei confronti della normativa. Secondo la ricerca "Dalla sopraffazione al controllo: il processo di preparazione per il GDPR del dipartimento IT per garantire la protezione adeguata dei dati", recentemente commissionata da Kaspersky Lab, il 22% dei responsabili IT non è sicuro

Salvare il mondo: Il progetto Glaciator

Oltre a sponsorizzare l'Antarctic Biennale, Kaspersky Lab ha supportato e ispirato, con la propria missione "Save the World", l'artista e ingegnere argentino Joaquín Fargas, il quale ha creato il robot Glaciator, il cui compito è mantenere il mondo salvo dai virus ormai dimenticati ma presenti nel permafrost. Questi virus potrebbero tornare a diffondersi con lo scioglimento dei ghiacciai causato dal riscaldamento globale. Il Glaciator comprime la neve camminandoci sopra e, così facendo, contribuisce a consolidare il "firn", cioè lo strato intermedio tra la neve e il ghiaccio. Questo processo accelera la formazione dei ghiacciai. Il robot, pur non essendoci a momento una connessione Internet in Antartide, a scanso di rischi è anche stato dotato di un software di sicurezza di Kaspersky Lab.

che l'organizzazione per cui lavora sarà pienamente conforme entro il 25 maggio 2018, data in cui entrerà in vigore il GDPR emanato dall'Unione Europea. Il questionario per una autovalutazione è disponibile al seguente link: <https://gdprkaspersky.com/>.

Morten Lehn, General Manager Italy di Kaspersky Lab, evidenzia che, per quanto si parli tanto del GDPR, «le imprese non stanno ancora facendo abbastanza per adeguare tutti i reparti dell'azienda alle norme di protezione e fare in modo che adempiano ai propri obblighi. Oltre a lavorare con specialisti di consulenza legale o aziendale, è importante non dimenticare coloro che trattano i dati quotidianamente».

Per questo in Kaspersky hanno approntato un sito (<https://www.kaspersky.it/gdpr>) progettato per contribuire a rendere più chiare le responsabilità delle imprese e dei singoli dipendenti attraverso un video animato, un diagramma interattivo e un white paper incentrato sull'impatto che il GDPR avrà all'interno dei reparti chiave dell'azienda. ❁

Fino a 861mila dollari il costo medio di un cyber attacco

Un'indagine di Kaspersky Lab mostra che la perdita economica per un incidente di sicurezza e i danni crescono col passare del tempo

Come tutte le norme la GDPR è vista come un onere, ma la sicurezza è un problema di business: i costi medi per un attacco diretto alle grandi enterprise, superano gli 1,4 milioni di dollari. In media il costo è di 861mila dollari, ma per una piccola e media impresa può arrivare a 86mila e 500 dollari, secondo i risultati della ricerca "Misurare l'impatto finanziario della sicurezza IT sulle imprese" basata sul Security Risks report di Kaspersky

Un dato allarmante è che i tempi in cui si rilevano gli attacchi sono lunghi e questo fa crescere i costi: le piccole e medie imprese tendono a pagare il 44% in più per riprendersi da un attacco scoperto una settimana o più dopo la violazione iniziale, rispetto agli attacchi individuati il giorno stesso.

Stimando i costi totali per il ripristino, Kaspersky Lab e la società di analisi B2B International hanno rilevato che il costo più frequente è quello degli stipendi aggiuntivi del personale, a seguire spese significative causate da opportunità di business perse, miglioramenti nella sicurezza IT, collaborazioni con specialisti esterni e assunzione di nuovi dipendenti.



Uomini e macchine per una vera sicurezza agile e consolidata

La strategia di Kaspersky Lab per la TrueCyberSecurity fa leva sulle competenze e l'esperienza dei professionisti per sfruttare al meglio gli automatismi tecnici

In vent'anni di attività nel mondo della sicurezza, in Kaspersky Lab hanno maturato una notevole esperienza, tale da comprendere che i sistemi automatici, pure i più sofisticati basati sul machine learning, non sono sufficientemente efficaci nel fermare le minacce.

Gli attacchi, non solo quelli mirati, sono sempre più compositi e difficili da rilevare. Occorre, spiegano gli esperti di Kaspersky Lab, un processo olistico costante, che non trascuri nessun tassello. Intrusion prevention, threat detection, incident response sono tutti elementi fondamentali, che devono essere uniti da una altrettanto basilare Security intelligence, in una struttura multilivello per la sicurezza, la cui gestione non è banale.

L'efficienza di tale struttura dipende da molti fattori ed è quella che in Kaspersky Lab chiamano "True Cybersecurity". Questa, secondo la loro vision, si basa su quattro elementi chiave: HuMachine Intelligence, Adaptive security; Agile security; Proven solutions.

Kaspersky Anti Targeted Attack Platform

Alcuni cybercriminali attivano minacce avanzate persistenti (APT, Advanced Persistent Threat), molto efficienti ma costose, altri usano "attacchi mirati", molto più economici e altrettanto devastanti. Entrambi questi tipi di attacchi utilizzano tecniche di base, come social engineering, furto delle credenziali e malware mascherati da software legittimo con un certificato rubato.

Kaspersky Lab ha recentemente rinnovato la propria Anti Targeted Attack Platform, che combina algoritmi di machine learning, threat intelligence a livello globale e compatibilità con le infrastrutture dei clienti per aiutare le grandi aziende a scoprire i più sofisticati e pericolosi attacchi in qualsiasi fase del loro sviluppo.

Tra le migliori: una maggiore scalabilità, sandbox clustering e maggiore visibilità con importanti aggiornamenti della GUI. Sono stati inoltre aggiunti nuovi tool, come il monitoraggio del workflow aziendale, incluso il traffico web e delle mail, quando viene integrata con la soluzione Kaspersky Security for Mail Gateway.

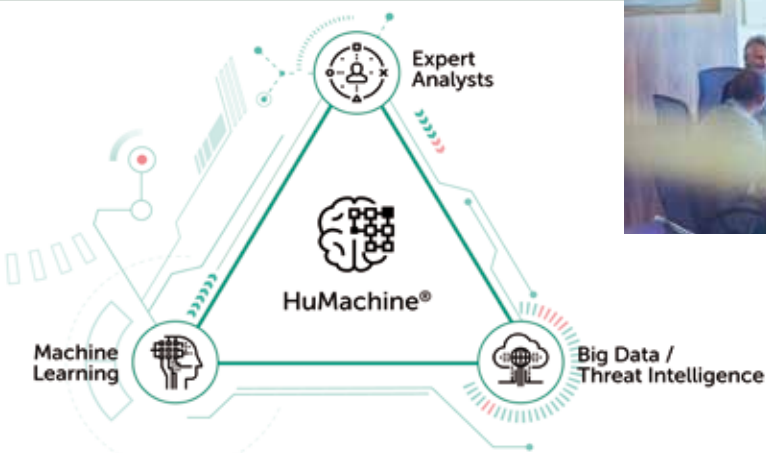
HuMachine Intelligence

In Kaspersky Lab si è osservato che non sempre le minacce vengono rilevate dagli strumenti automatici, anche quando questi sfruttano algoritmi di machine learning molto avanzati. La massima efficacia si ottiene sfruttando le conoscenze e l'esperienza dell'essere umano, realizzando, in pratica il binomio che in Kaspersky Lab chiamano l'approccio "HuMachine". L'intelligenza dei sistemi automatici viene "orientata" nella giusta direzione dagli esperti. In questo modo, la sintesi proveniente dagli algoritmi e dall'analisi dei big data viene combinata in un singolo elemento che attua la risposta adeguata alla minaccia.

Servizi di esperti

Per una protezione efficace occorre il supporto di esperti, che non sempre sono disponibili in azienda. Kaspersky fornisce servizi gestiti da personale specializzato, tra cui:

- cybersecurity awareness, per supportare le imprese nella creazione di un ambiente informatico aziendale sicuro attraverso una formazione gamificata;
- penetration Test conformi agli standard PCI DSS, Payment Card Industry Data Security Standard;
- vulnerability assessment per valutare le vulnerabilità di qualsiasi applicazione;
- analisi forense e analisi del malware, per ricostruire un'immagine dettagliata di un incidente utilizzando rapporti completi, incluse le misure di correzione dell'incidente.



Kaspersky Security per Data Center

Kaspersky Security for Data Centers funziona come una singola piattaforma integrata, facilitando la gestione e l'integrazione con diverse configurazioni di data center. L'amministrazione centralizzata consente ai team di applicare criteri di sicurezza unificati in tutto il data center. La soluzione è stata progettata per ambienti multi-hypervisor e sistemi di archiviazione diversi, fornendo sicurezza per le principali piattaforme di virtualizzazione, tra cui VMware con NSX, Citrix, Microsoft e KVM, e sicurezza per i sistemi NAS, tra cui Emc, NetApp, Dell, Ibm, Hitachi e Oracle.

Kaspersky Security per la virtualizzazione

Kaspersky Lab propone due tecnologie: la soluzione Agentless funziona a stretto contatto con le tecnologie core hypervisor (come VMware NSX), mentre la soluzione Light Agent offre ulteriori livelli di protezione per ogni macchina virtuale. L'implementazione di una soluzione Light Agent su ogni macchina virtuale assicura protezione multilivello e controlli di sicurezza ricchi di funzioni. La sicurezza per le macchine virtuali, sia con una soluzione Agentless sia con una Light Agent o con entrambe, può essere gestita da un'unica console insieme ai server degli endpoint fisici e ai dispositivi mobili.

Adaptive security

La strategia di sicurezza deve essere in grado di adattarsi alle caratteristiche di ciascuna azienda, senza rinunciare ad alcun elemento di protezione, consapevoli del fatto che non esiste più un perimetro aziendale definito nell'era dei dispositivi mobili, delle applicazioni Web, dei sistemi storage portatili, della virtualizzazione.

La sicurezza non è più solo "prevenire e bloccare" e alle imprese di ogni dimensione è necessario fornire la massima protezione attraverso un approccio adattativo e flessibile, quale quello previsto dalle soluzioni per le imprese fornite da Kaspersky Lab, in grado di scalare in base alle dimensioni, senza rinunciare alle prestazioni.

Agile security

Per "agile" security, in Kaspersky Lab intendono una sicurezza che sia facile da gestire. Un concetto meno scontato di quanto si possa pensare. Molte imprese, in fatti si trovano a fronteggiare le minacce

Kaspersky Private Security Network

Molte soluzioni standard per la sicurezza impiegano anche quattro ore per ricevere gli aggiornamenti necessari per rilevare e bloccare i software malevoli, che, dal canto loro, proliferano al ritmo di oltre 300mila al giorno. La threat intelligence tramite Kaspersky Private Security Network fornisce queste informazioni in 30-40 secondi, sottolineano gli esperti della casa, evidenziando anche il basso numero di falsi positivi l'alto livello di protezione, anche contro minacce avanzate e sconosciute.

Da segnalare che Kaspersky Security Network mette a disposizione la security intelligence di Kaspersky Lab a ogni sistema connesso a Internet.

Per quelle aziende che, avendo stringenti vincoli di privacy, Kaspersky Lab ha sviluppato Kaspersky Private Security Network, permettendo loro di sfruttare la maggior parte dei vantaggi della sicurezza assistita da cloud senza divulgare alcun dato dal perimetro aziendale controllato. Si tratta di una versione di Kaspersky Security Network personale, locale e completamente privata dell'azienda.

informatiche con risorse economiche e professionali scarse. Le problematiche che ne conseguono sono indipendenti dalle soluzioni adottate, ma queste ultime possono sopperire a talune carenze grazie alla loro semplicità e agli automatismi. Soprattutto a fare la differenza è la disponibilità di soluzioni in cloud, come quelle messe da Kaspersky Lab a disposizione dei propri partner affinché possano fornire alle imprese servizi gestiti.



Kaspersky DDoS Protection

Oggi gli attacchi DDoS sono diventati più sofisticati e mirati: i criminali svolgono ricerche sull'azienda che vogliono colpire, per scegliere gli strumenti di attacco più appropriati per raggiungere l'obiettivo. Successivamente, in tempo reale nel corso dell'attacco, i cybercriminali cambiano tattica costantemente. È quindi necessario dotarsi di una soluzione che di rilevi gli attacchi il più velocemente possibile.

Kaspersky DDoS Protection affronta tutti i tipi di tali attacchi. Sono disponibili tre opzioni di implementazione: Connect, Connect+ e Control.

La soluzione identifica l'istante di un possibile scenario di attacco e avvisa il centro operativo di sicurezza di Kaspersky Lab. Negli scenari di implementazione Connect e Connect+ la mitigazione viene avviata automaticamente con i tecnici Kaspersky che eseguono immediatamente controlli dettagliati per ottimizzare la risposta in base alla dimensione, al tipo e alla sofisticazione dell'attacco DDoS.

Con Kaspersky DDoS Protection Control sono gli addetti aziendali a decidere quando avviare la mitigazione in linea con i propri criteri di cybersecurity, con gli obiettivi aziendali e con l'ambiente dell'infrastruttura.

Il supporto è attivo 24 ore su 24, 7 giorni su 7.

Kaspersky Fraud Prevention per il digital banking

I sistemi di digital banking sono sotto assalto da parte di criminali che tentano frodi online. Kaspersky Fraud Prevention migliora il sistema di sicurezza esistente delle banche, aggiungendo un altro livello con la protezione di account digitali, i computer e i dispositivi mobili degli utenti e i sistemi delle banche, con sistemi che consentono l'analisi in tempo reale del comportamento, dei dispositivi e dell'ambiente dell'utente. Tramite l'apprendimento automatico, la soluzione rileva scenari di frode avanzati e schemi di riciclaggio di denaro.

Soluzioni messe alla prova

Kaspersky Lab partecipa continuamente a test organizzati da laboratori indipendenti non tanto o non solo per "accumulare" premi, quanto

per mettere alla prova le proprie soluzioni e garantire il miglior risultato possibile ai propri clienti. La fiducia che ci danno è ben riposta, afferma il Chief Technology Office,

Nikita Shvetsov, ricordando che su 78 confronti realizzati da società di analisi indipendenti, i prodotti Kaspersky Lab hanno ottenuto 55 primi posti e 70 piazzamenti sul podio. ✨

Kaspersky Industrial CyberSecurity

Gli attacchi ad ambienti industriali sono aumentati significativamente negli ultimi anni. Kaspersky Industrial CyberSecurity è stata sviluppata per proteggere le infrastrutture critiche, create su un determinato numero di differenti sistemi di controllo industriale.

Il portfolio di tecnologie e servizi proteggono server SCADA, pannelli HMI, workstation ingegnerizzate, PLC, connessioni di rete e persone, senza alcun impatto sulla continuità operativa e sulla coerenza del processo tecnologico. La flessibilità di Kaspersky Industrial CyberSecurity permette di configurare la propria soluzione in modo che sia strettamente legata ai requisiti specifici del sistema di controllo industriale cui fanno riferimento. In seguito all'esecuzione da parte degli esperti Kaspersky Lab di un controllo completo dell'infrastruttura, verrà selezionata la configurazione ottimale per i servizi e le tecnologie di sicurezza. La stessa Kaspersky sviluppa soluzioni specifiche, come Kaspersky Industrial CyberSecurity for Energy, un pacchetto avanzato dedicato alle aziende del settore energetico.

Kaspersky Security for Mobile

La diffusione dei dispositivi mobili e il fenomeno del BYOD hanno attirato l'attenzione degli hacker su questi sistemi e la pressione dei cyber criminali è tale per cui mensilmente si contano decine di migliaia di nuovi malware e milioni d'installazioni di codici maligni. Kaspersky Security for Mobile fornisce una protezione multilivello e una vasta gamma di funzioni MDM (Mobile Device Management) e MAM (Mobile Application Management), per ridurre significativamente il tempo richiesto per la manutenzione dei dispositivi mobili e per fornire un accesso mobile sicuro ai sistemi aziendali.

Oltre alle protezioni, le soluzioni Kaspersky Lab forniscono funzioni antifurto che possono essere controllate da remoto.

La soluzione MDM è compatibile con le principali piattaforme e consente la scansione e il controllo dei dispositivi in modalità OTA (Over the Air), migliorando in maniera significativa la protezione e la gestione dei dispositivi basati su Android, iOS e dei telefoni Windows.

Per le imprese che adottano strategie MAM, la soluzione fornisce i contenitori isolati per le applicazioni e la possibilità di cancellare in maniera selettiva la memoria del dispositivo.

Ulteriore protezione la combinazione di crittografia e protezione funzionale contro i malware.

Kaspersky Endpoint Security

La piattaforma protegge ogni tipo di endpoint, dai server e desktop fisici e virtuali ai dispositivi mobili: non a caso, le società d'analisi Gartner e Forrester hanno inserito Kaspersky Lab nel quadrante dei "leader" nella protezione degli endpoint.

Viene sfruttata l'analisi comportamentale tramite apprendimento automatico basato su dati statici e dinamici, per proteggere le imprese anche da minacce future. A questo si aggiunge la global threat intelligence, che contribuisce ad abilitare una risposta automatica in tempo reale: nel momento in cui viene rilevata una minaccia, il sistema annullerà in automatico qualsiasi modifica messa in atto dal malware.

La tecnologia Automatic Exploit Prevention è stata sviluppata per impedire ai cybercriminali di sfruttare le vulnerabilità delle applicazioni sulle macchine protette. La gestione automatizzata delle patch aggiunge un ulteriore livello di sicurezza.

La soluzione comprende tecnologie anti-ransomware, che permettono di preservare i dati ed evitare il pagamento di riscatti, proteggendo le cartelle condivise da cryptolocker avanzati.



Mission Unhackable

True Cybersecurity per aziende.

Solo l'approccio Kaspersky Lab True Cybersecurity combina la facilità d'uso e la HuMachine™ intelligence per proteggere il tuo business da qualsiasi tipo di minaccia.

Maggiori informazioni su kaspersky.it



Kaspersky®
Endpoint Security
for Business

Advanced

La cyber security

Le imprese sono sotto attacco. Wannacry ha mostrato al mondo il potenziale dei cyber criminali, delinquenti "comuni" che hanno trovato nel dark Web gli strumenti per rinnovare il business delle estorsioni.

Il ransomware, che blocca il computer e chiede un riscatto è l'attacco del momento, ma sarà presto rimpiazzato da qualcosa di ancora più potente, anche considerando che nuovi dispositivi vengono connessi alla rete e che sempre più servizi informatici sono fruiti dal cloud.

Le aziende che operano nella cyber security rispondono

accelerando lo sviluppo di soluzioni che sappiano sfruttare la security intelligence collettiva, grazie al cloud, e le nuove frontiere dell'Artificial Intelligence e del machine learning per ottenere una

protezione il più automatica possibile.

Comunque, il punto debole di

ogni infrastruttura informatica resterà l'essere umano, pertanto la formazione del personale, a partire dai receptionist fino all'amministratore delegato o viceversa, è il primo fondamentale strumento di prevenzione.



Intelligenza artificiale per la sicurezza nel contesto

Domenico Garbarino di Oracle



Nuovi servizi cloud Identity Security Operation Center di Oracle potenziano il monitoraggio del rischio col machine learning e aumentano la sicurezza

Oracle ha aumentato la sicurezza del cloud espandendo i servizi CASB (Cloud Access Security Broker), cioè una sorta di controllore che si pone tra l'utente e la risorsa in cloud che questi vuole utilizzare.

In particolare, Oracle ha potenziato queste soluzioni con nuovi servizi cloud Identity Security Operation Center (SOC), che comprendono ora tecnologie di ultima generazione, quali machine learning, intelligenza artificiale e soluzioni

context-aware (cioè sistemi che effettuano analisi di sicurezza in grado di correlare, per esempio l'utilizzo di una risorsa con la natura della stessa). «Siamo costantemente impegnati a fornire soluzioni che aiutino le imprese a gestire, adattare e rafforzare il proprio livello di sicurezza nei confronti dei rischi esterni e interni» afferma Domenico Garbarino, Sales Director Security Solutions di Oracle Italia, evidenziando come le competenze maturate in Oracle in aree come la data science

GDPR e cloud per la trasformazione digitale di Ubi Banca



La multicanalità è ormai imprescindibile per le banche, ma occorre affrontare le problematiche legate alla sicurezza dei sistemi informatici e, nel contempo, aggiornarsi per rispettare le sempre più severe regole sui dati sensibili.

Per Ubi Banca la risposta è stata scegliere soluzioni di sicurezza "business enabler", così da proteggere le informazioni dei propri clienti

alla sorgente e per avere la completa visibilità del loro ciclo di vita, garantendosi anche la conformità alle nuove normative di settore (GDPR, PSD2, NIS).

Ubi Banca è uno dei principali gruppi bancari italiani e uno dei più attivi nella trasformazione digitale dei servizi a imprese e clienti. Per tale processo sono fondamentali le soluzioni di sicurezza sia per la protezione sia

per la gestione dei dati.

A Fabio Gianotti, Chief Security Officer di Ubi abbiamo chiesto di spiegarci meglio.

Direction: Che ruolo gioca la sicurezza nel processo di trasformazione della banca?

Fabio Gianotti: Un approccio predittivo alla sicurezza IT, nella trasformazione digitale e all'adozione del

e il machine learning, portino a soluzioni all'avanguardia, scalabili e affidabili per chi passa al cloud, di Oracle o di terze parti. Tra le novità vi sono funzionalità Adaptive Access per l'implementazione di controlli di accesso dinamico alle applicazioni, il potenziamento del monitoraggio del rischio basati su machine learning e i citati servizi CASB, che supportano le soluzioni Oracle SaaS con il rilevamento automatico delle minacce.

Controllo sofisticato con Adaptive Access

Le credenziali di accesso sono una preda ambita per i cyber criminali ed è per questo che in Oracle hanno aggiunto a Oracle Identity Cloud Service le funzionalità Adaptive Access, che utilizzano soluzioni context aware per un monitoraggio degli accessi più efficace. Adaptive Access, infatti, applica un contesto di rischio dinamico per associare i controlli di accesso appropriati in base a un determinato livello di rischio.

Una gestione dinamica anche facilitata dalla gestione intuitiva delle policy e dalle integrazioni standardizzate con i componenti Oracle Identity SOC. Inoltre, Oracle CASB Cloud Service utilizza ora tecniche di machine learning, sia di tipo supervisionato sia non supervisionato, più potenti per rilevare le minacce avanzate. Per identificare con più cura anomalie, Oracle ha sviluppato il motore UBA (User Behavior Analytics) integrato, che stabilisce automaticamente particolari modelli di riferimento per ciascun utente e servizio cloud, applicativi compresi. I modelli saranno la pietra di paragone consultata costantemente dal sistema per valutare una qualsiasi deviazione. Oracle CASB Cloud Service orchestra la risposta all'incidente per mezzo di diverse opzioni compresa l'integrazione con sistemi di ticketing e gestione incidenti di terze parti, nonché le funzionalità native per la risoluzione automatica dei casi.

Il primo CASB per la sicurezza del SaaS Oracle

Oracle CASB Cloud Service è l'unica soluzione CASB sul mercato a mettere a disposizione capacità di monitoraggio della sicurezza e rilevamento delle minacce per le applicazioni SaaS (Software as a Service) di Oracle, quali come Oracle Human Capital Management Cloud, Oracle Enterprise Resource Planning Cloud e Oracle Customer Experience Cloud Suite.

Oltre alle applicazioni Oracle SaaS, Oracle CASB Cloud Service ha aggiunto anche la piattaforma Slack, che si somma alle tante applicazioni di terze parti supportate.

L'integrazione di Slack sfrutta il nuovo modello push-event favorito dalle moderne applicazioni cloud, ora disponibile in tutto il mondo con Oracle CASB Cloud Service.

Inoltre, Oracle CASB Cloud Service supporta anche il Web gateway sicuro Symantec/BlueCoat per la visibilità delle attività cloud. ❁

cloud, costituisce un asset aziendale imprescindibile per l'ecosistema di una banca in particolare con l'entrata in vigore del nuovo General Data Protection Regulation, dove i dati sensibili dei clienti sono sotto i riflettori soprattutto per le realtà del mondo finanziario.

D: In quale modo Oracle vi supporta nella vostra strategia di sicurezza, e nel processo di compliance alle normative?

F.G.:Le funzionalità di Encryption e Masking di Oracle Database Security ci consentono di mettere al sicuro il dato nella sua forma nativa, pri-

ma di essere acquisito e processato dalle applicazioni, o utilizzato per lo sviluppo, e senza gravare sulle performance del database. Non a caso la nuova normativa europea introduce l'encryption dei dati proprio a prescindere da ogni loro utilizzo. Database Security si dimostra come uno strumento fondamentale che va ad aggiungersi all'ambiente Oracle che è centrale per la nostra operatività, permettendoci di rispettare i parametri richiesti dalla GDPR.

D.: Il cloud è sempre più una realtà e anche l'EBA (European Banking Authority) sta

declinando l'uso del cloud negli Istituti Finanziari, insomma la sicurezza nel cloud è e sarà sempre un punto di attenzione soprattutto in Europa, che approccio state adottando in Ubi Banca?

F.G.:La sicurezza predittiva, per la banca, significa anche la completa visibilità dei dati durante il loro utilizzo nel cloud, un aspetto vitale perché imposto anch'esso dalla normativa in vigore. Per questo l'integrazione delle soluzioni di sicurezza ha compreso anche l'adozione, da parte di Ubi Banca, di Oracle CASB. ❁

Sicurezza integrata per proteggere i sistemi SAP

Per rispondere alle nuove sfide gli IT manager scelgono una difesa multilivello e puntano su strumenti avanzati come il machine learning. Tramite Deep Security Scanner, Trend Micro mette a disposizione una soluzione avanzata per la protezione degli ambienti SAP e delle applicazioni business critical

La minaccia più temuta dai responsabili IT per il futuro è il cyber spionaggio. Questo è quello che rivela l'ultima ricerca commissionata da Trend Micro e condotta dalla società Opinium che ha coinvolto oltre 2400 responsabili decisionali IT in Europa e Stati Uniti di cui 103 rappresentanti italiani di aziende diffuse su tutto il territorio e operanti in vari settori, in ambito pubblico e privato.

Nelle preoccupazioni dei professionisti della sicurezza italiana, dopo il cyber spionaggio indicato dal 36% degli intervistati (percentuale più alta nel mondo), vi sono gli attacchi mirati (22%), la compromissione della posta aziendale (11%) e i ransomware (7%) che sono stati la minaccia prevalente nel 2016.

Le sfide da affrontare sono sempre più impegnative e il numero di attacchi continua a crescere con 500mila

nuove minacce quotidiane, tanto che quasi l'80% degli intervistati ha affermato di aver subito un attacco di notevoli dimensioni nel 2016. Mentre smartphone, tablet, laptop e dispositivi indossabili promettono in futuro un continuo aumento del livello delle minacce, le aziende lamentano impostazioni di sicurezza di vecchia concezione (16%), sicurezza dei dispositivi non adeguata (15%), infrastrutture obsolete (28%) e mancanza di innovazione da parte dei fornitori (27%).

Puntare su misure di sicurezza avanzate e multilivello

In questo scenario emerge la progressiva affermazione di strumenti di sicurezza avanzata quali il machine learning e l'analisi del comportamento, considerati efficaci per bloccare le minacce informatiche dall'85%

dei responsabili IT italiani ma, soprattutto, la necessità di utilizzare una protezione multilivello nella lotta contro le minacce moderne che utilizzano metodi e vettori di attacco diversificati.

Trend Micro non solo tiene conto delle nuove tecnologie come il machine learning, ma propone un approccio di protezione basato su un insieme di tecniche di difesa intergenerazionali progettate appositamente e integrate nelle applicazioni critiche aziendali, che sono sia target sia vettore degli attacchi odierni.

Tra le applicazioni di questo tipo un posto di rilievo è occupato da SAP, una delle applicazioni business di livello critico più diffusa, che custodisce dati critici e sensibili che possono appartenere alle aree più disparate: dalle risorse umane all'ambito finanziario, dai clienti alla rete dei fornitori. I cyber criminali rivolgono

la loro attenzione con sempre maggiore frequenza verso i sistemi SAP proprio per il valore dei dati che contengono e, dato che le aziende accedono comunemente a questi sistemi tramite il Web, risulta più facile riuscire a sfruttare le vulnerabilità di sistemi operativi, server Web e delle altre applicazioni di business. Non a caso il numero di vulnerabilità nei sistemi SAP è aumentato del 300% nel biennio 2013-2015 ed è in continua crescita.

L'approccio difensivo tradizionale, basato sulle patch, presenta molteplici inconvenienti e richiede una gestione che non sempre è pronta a rispondere nei tempi e modi idonei. Per queste ragioni Trend Micro ha ampliato la propria soluzione Deep Security per la protezione dei server fisici, virtuali e in cloud, sviluppando Trend Micro Deep Security Scanner, un modulo specifico che permette di integrare, all'interno di SAP, un livello multiplo di protezione e di analisi automatizzata che assicura la protezione dalle violazioni e dalle interruzioni di attività.

La soluzione Trend Micro effettua una scansione approfondita di ogni tipo di contenuto caricato sulla piattaforma SAP NetWeaver (inclusi documenti, immagini e contenuti attivi integrati all'interno di documenti PDF e Office) per determinarne la vera

natura e quindi invia i risultati ai sistemi SAP tramite l'interfaccia SAP VSI (Virus Scan Interface). Sulla base di queste informazioni, gli amministratori SAP possono predisporre regole in base alle quali consentire o bloccare i diversi tipi di documento.

Deep Security per la protezione dei sistemi SAP

Deep Security Scanner protegge i sistemi SAP dalle violazioni e dalle interruzioni dell'attività, consente di semplificare le operazioni di sicurezza e garantisce la conformità alle normative attraverso un approccio multilivello che prevede le funzioni di:

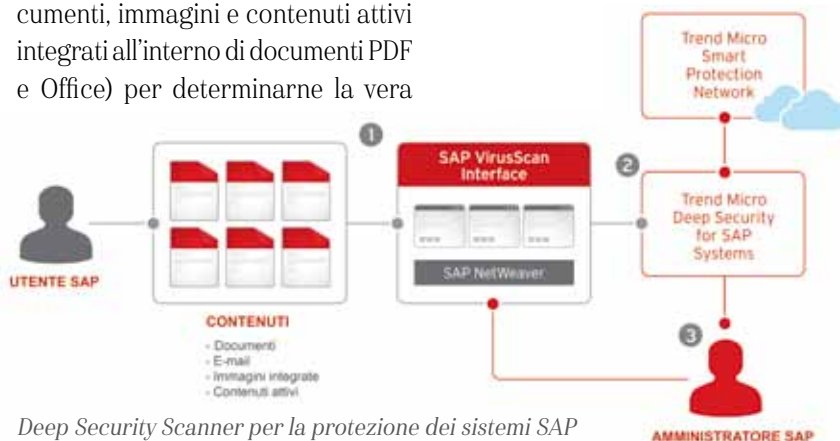
- **anti-malware con analisi della reputazione Web** sfruttando l'infrastruttura globale Trend Micro Smart Protection Network che fornisce l'analisi costante delle minacce a livello globale e predispone in tempo reale le necessarie contromisure;
- **rilevamento e prevenzione delle intrusioni** utilizzando regole di sicurezza che si aggiornano automaticamente per garantire una protezione costante dei server cloud;
- **firewall avanzato** per la creazione di un perimetro sicuro attorno a

ogni server in cloud, per analizzare il traffico, produrre report, bloccare gli attacchi e consentire solo le comunicazioni lecite;

- **monitoraggio dell'integrità** per assicurare che i file e i sistemi rispondano costantemente ai requisiti di sicurezza e affidabilità predisposti dall'azienda e richiesti dalle normative;
- **analisi dei dati legati agli eventi di sicurezza (log)** per identificare all'interno di grandi volumi di dati prodotti dai sistemi di protezione gli eventi rilevanti per la sicurezza e segnalarli a sistemi SIEM (Security Information and Event Management) per effettuare attività più approfondite di analisi e correlazione;
- **scansione e protezione dei contenuti** caricati nel database SAP e nell'archivio MIME.
- **protezione contro possibili codici nocivi (script)** che potrebbero essere incorporati o nascosti all'interno dei documenti.

Questo modulo introduce un livello di protezione aggiuntivo alle funzionalità dei sistemi standard e permette anche l'integrazione con altri moduli di Deep Security per estendere la protezione ai server SAP e all'intero data center.

La soluzione di Trend Micro protegge tutte le piattaforme SAP che supportano SAP VSI 2.0, incluse SAP NetWeaver, SAP ERP, SAP HANA e le ultime innovazioni come SAP Fiori. Le funzionalità di sicurezza fornite da Deep Security si integrano perfettamente anche con Amazon Web Services (AWS), VMware, Microsoft Azure e altri fornitori leader di tecnologia in-the-cloud e di virtualizzazione. ✨



Deep Security Scanner per la protezione dei sistemi SAP

Individuare le vulnerabilità protegge gli end-point

Con Radar e la Business Suite dedicata alla protezione degli end-point, F-Secure garantisce la cyber security

Proteggere i sistemi IT e gli end-point costituisce una delle sfide più impegnative per il responsabile IT di un'azienda. La vulnerabilità può derivare da diversi fattori, quali ad esempio software non aggiornati, sistemi mal configurati, applicazioni web non sicure o end-point non adeguatamente protetti. Gestire le potenziali vulnerabilità è quindi un passaggio obbligato per garantirsi la cyber security, la protezione dei dati e la continuità operativa. Per stare al passo con le minacce e farvi fronte, suggerisce F-Secure (www.f-secure.it), società che nel campo della sicurezza ha uno status di leader a livello mondiale, occorre eseguire scansioni regolarmente. Una volta che si sono rilevate delle

vulnerabilità, si deve però essere in grado di porre una soluzione al problema. Ma qui se ne pone un altro: da dove partire?

È a questo punto che la sua soluzione Radar costituisce un concreto aiuto. Radar è una nuova applicazione sviluppata da F-Secure per la gestione e la scansione delle vulnerabilità e che permette non solo di individuarle ma anche di risolverle. A garanzia della sua validità e corrispondenza alle normative Radar è stata certificata PCI ASV a livello europeo.

Mappatura e scansione

Il funzionamento è semplice. Attraverso degli scan node, RADAR esegue per prima cosa una mappatura di tutti gli asset presenti in un sistema. Rileva tutto ciò che risponde a un indirizzo IP: server, desktop, router, stampanti, videoregistrazione e qualsiasi altro apparato connesso alla propria rete, anche nel caso si tratti di una Wireless LAN, e in qualunque luogo esso si trovi connesso. Una volta generata una



Radar esegue la mappatura di tutti gli asset, rileva le vulnerabilità e attua policy di cyber security



Business Suite protegge gli endpoint e attua stringenti policy di sicurezza

panoramica di tutti gli asset presenti e attivi, procede ad esaminare tutte le potenziali vulnerabilità esistenti nella rete.

Le vulnerabilità possono derivare ad esempio da banali errori di configurazione, oppure da una gestione delle patch non appropriata o anche da un'implementazione sbagliata. Nel corso della scansione vengono anche identificati i punti che sono particolarmente vulnerabili e interessanti per gli hacker, che potrebbero quindi cercare di sfruttarli per penetrare le difese della rete aziendale. Inclusi in Radar vi sono inoltre strumenti di reportistica che permettono di creare dei ticket per la gestione delle problematiche riscontrate.

È quindi possibile assegnare la risoluzione di una determinata vulnerabilità a operatori incaricati, fornendo in automatico link e documenti specifici sul problema rilevato.

F-Secure Radar consiste di una piattaforma sofisticata e di un engine di web scanning che operano in abbinamento a una piattaforma basata su web di vulnerability management e reporting. A questo si aggiunge l'integrazione con funzionalità integrate di software di terze parti tramite F-Secure Radar API.

La protezione degli endpoint

Nell'odierno ambiente di business proteggere il perimetro aziendale non è più sufficiente. Il nuovo perimetro, mette in guardia F-Secure, è costituito dagli endpoint, ovunque siano, e una protezione efficace di questi ultimi non può limitarsi a una soluzione antimalware.

Quello a cui si assiste, evidenzia la società, è una vera e propria esplosione di endpoint e di applicazioni software: nuovi utenti, workstation mobili, applicazioni cloud, a cui si aggiungono nuove patch e frequenti aggiornamenti software. Il panorama delle minacce continua in sostanza a mutare e nuovi vettori di minacce come il ransomware si aggiungono alla complessità dell'enorme numero di minacce già note.

È una situazione complessa che può portare in azienda ad avere una visione frammentata della sicurezza, con tecnologie differenti che non funzionano insieme e che non permettono di disporre di una visione globale delle vulnerabilità.

Una cosa è però certa: il numero di endpoint nella rete continuerà a crescere e gli utenti non cesseranno di usare nuove applicazioni o di incorrere in vecchi errori. E gli attaccanti non smetteranno di trovare nuovi modi per violare le difese.

Business Suite: la gestione centralizzata della sicurezza

Se si vuole proteggere la propria azienda, quello che serve è una soluzione intelligente per proteggere tutti gli endpoint. Per farlo, F-Secure ha coniugato la più recente intelligenza delle minacce e l'esperienza in sicurezza informatica dei suoi esperti al fine di rilasciare continuamente migliorie per la protezione degli endpoint.

Recentemente, ha spiegato la società, ha per esempio reso disponibile una nuova versione della soluzione Business Suite per la sicurezza aziendale on-site.

Business Suite è stata progettata sia per ambienti fisici sia virtuali e per fornire una gestione centralizzata granulare della sicurezza e una protezione a più livelli contro malware e altre cyber minacce, dal gateway agli endpoint. Comprende anche funzionalità di sicurezza aggiuntive per affrontare le sfide di sicurezza delle diverse organizzazioni.

Business Suite fornisce in pratica un'approfondita ed esaustiva visibilità dello stato della sicurezza in tutta la rete aziendale, la scalabilità necessaria per far fronte alle nuove esigenze e un controllo centralizzato su ogni utente ed endpoint in modo da poter distribuire policy di cyber security adeguate.

In sostanza, diventa possibile mantenere il controllo in ogni situazione ed assicurarsi che l'azienda sia protetta contro l'enorme quantitativo in continua crescita di attacchi e di minacce online.



Predictive Security per prevenire gli attacchi anziché fronteggiarli

HPE Security propone un modello di protezione basato su sistemi avanzati di analisi, di Machine Learning e di correlazione per analizzare in tempo reale enormi volumi di dati e anticipare le minacce

La direzione verso cui deve evolvere il modello di difesa dagli attacchi è quello della Predictive Security". È questa, secondo Pierpaolo Ali, Director Southern Europe di HPE Security, la transizione necessaria per superare i sistemi tradizionali di gestione degli eventi di sicurezza (i cosiddetti SIEM) e riuscire a rispondere in modo efficace all'esplosione di dati di sicurezza e alla moltiplicazione delle fonti che li generano che mette a dura prova la capacità di analisi e risposta dei Security Operation Center (SOC) delle aziende.

Per aiutare le aziende nel processo di transizione verso un modo innovativo di approcciarsi al tema della gestione degli eventi di sicurezza HPE ha sviluppato ArcSight Data Platform, una piattaforma di protezione del dato e di security intelligence che consente di analizzare fino a un milione di eventi per secondo provenienti da più fonti, arricchire e contestualizzare i dati di sicurezza, effettuare correlazioni in tempo reale e mettere a disposizione queste informazioni ad altri strumenti avanzati di analisi e di Machine Learning. L'utilizzo di questi strumenti consente non solo di rispondere alle minacce note, ma anche di riconoscere nuovi "pattern" di attacco e fronteggiare così le minacce sconosciute.

Cambiare il paradigma di protezione

«Si tratta di cambiare il paradigma di difesa - continua Ali - per adattarlo a un nuovo scenario in cui il perimetro aziendale come lo conoscevamo in passato si è dissolto, per lasciare spazio a un nuovo perimetro definito dalle applicazioni che accedono ai dati e li spostano liberamente all'interno del Web senza vincoli geografici o di orario. Per poter anticipare e comprendere quale sarà l'attacco è necessario essere in grado di intervenire in tempo reale utilizzando strumenti automatizzati e avanzati di analisi e di Machine Learning».

Alla sicurezza delle applicazioni HPE indirizza una gamma di soluzioni specifiche, denominata Fortify, che permette di predisporre un livello di protezione non solo di tipo statico, ma anche

dinamico, capace cioè di riconoscere un possibile attacco e di adattarsi in tempo reale per fornire quella che HPE chiama una Continuous Protection.

La sicurezza non è però fatta solo di tecnologie e, un altro problema che le aziende si trovano ad affrontare, è quello della scarsità sul mercato di competenze legate al tema della sicurezza. Per affrontare questa carenza le aziende sono alla ricerca di strumenti differenti rispetto



Pierpaolo Ali, Director Southern Europe di HPE Security

ai tradizionali tool di sicurezza e stanno investendo in nuove tecnologie per aumentare la velocità, la semplicità e la capacità di analisi legate alle operazioni di sicurezza. A tal fine HPE ha sviluppato ArcSight Investigate, una soluzione di individuazione (hunt) e investigazione di nuova generazione costruita su un'avanzata piattaforma analytics che arriva a supporto degli analisti della sicurezza.

Questa soluzione sfrutta analisi effettuate in tempo reale su enormi volumi di dati per fornire ai security manager risorse di investigazione e Best Practice di altissimo livello utili a individuare in modo rapido e preciso le minacce a cui dedicare maggiore priorità.

L'importanza di proteggere il dato

Il tema della protezione del dato è sempre più centrale anche nelle agende di discussione delle grandi istituzioni come l'Unione Europea, che sta rafforzando il proprio impegno per proteggere i dati in ambito finanziario e predisporre misure per fronteggiare gli attacchi del cyber crime che si affacciano anche nelle reti internazionali di transazioni. Un caso è avvenuto recentemente nella Banca centrale del Bangladesh, penetrata da alcuni hacker che sono riusciti a ottenere l'accesso alla rete Swift sottraendo 81 milioni di dollari. La normativa comunitaria e nazionale spingono sempre più anche verso la protezione dei dati sensibili legati alle persone (dati di previdenza, numero di carta di credito, conto corrente e così via), che vengono rapidamente monetizzati dal cyber

crimine con ritorni sull'investimento che arrivano a 750% a settimana. Alla protezione dei dati HPE dedica la gamma di soluzioni di cifratura Voltage, che consente di implementare un livello di protezione che viene applicato al momento della creazione del dato e che provvede a seguirlo costantemente sia quando si trova a riposo ovvero archiviato, sia quando viene spostato. La cifratura del dato lo protegge anche nel caso della sua sottrazione e apre la strada alla possibilità, per le aziende, di non essere obbligate a dover dichiarare la compromissione, evitando possibili danni di immagine e legali.

Anche l'arrivo del regolamento GDPR va nel rafforzamento della protezione del dato introducendo il concetto di sovranità digitale e quindi liberando il vincolo della proprietà dei propri dati da un confine geografico; inoltre, sposta l'onere della prova in caso di compromissioni sul gestore del dato: non è più l'utente che deve dimostrare di aver agito bene ma il gestore di non aver agito in modo scorretto.

Il GDPR mette in evidenza anche un altro concetto che è quello della sicurezza intrinseca ovvero della cosiddetta "security by design". Si tratta di un tema da sempre centrale nell'offerta di HPE Security attraverso la gamma di soluzioni Fortify pensate per garantire la protezione da vulnerabilità nella fase di sviluppo delle applicazioni.

Sicurezza dinamica e personalizzata

La capacità di rilevamento e risposta delle aziende continua a cambiare

ed evolvere. Programmi di sicurezza efficaci richiedono una costante valutazione degli obiettivi di compliance, di sicurezza e di gestione del rischio aziendale e la continua revisione e messa a punto di persone, processi e componenti tecnologici della soluzione di sicurezza.

Un dato che emerge dalla ricerca di HPE "2017 State of Security Operations", che ha analizzato 183 SOC in 31 Paesi intervistando componenti del SOC e responsabili di business (CEO, CIO, GRC e così via), è che i tentativi di trasferire la gestione del rischio a fornitori di servizi esterni si dimostrano di solito deludenti. Le motivazioni sono che i servizi gestiti sono standardizzati e, pertanto, non riescono a tenere conto delle specificità di ogni azienda. Inoltre, si focalizzano su metriche spesso poco significative o non legate alle esigenze di business dell'azienda. Dalla ricerca emerge anche come non vi sia alcuna correlazione tra dimensione dell'azienda e maturità del SOC evidenziando che la maturità di un SOC è legata agli obiettivi di organizzazione della sicurezza e all'uso della sicurezza come elemento di differenziazione competitiva. «Non esiste una soluzione rapida, un singolo prodotto o servizio che possa fornire la protezione e la consapevolezza operativa di cui un'azienda ha bisogno - conclude Ali -. La risposta è nella Predictive Security e nella capacità di risposta dinamica, sfruttando strumenti di Machine Learning capaci di identificare e aggiornare costantemente gli scenari di intervento e le regole di correlazione all'evolversi del contesto di rischio».





Wi-Fi rapido e affidabile



Impostazione rapida e semplice



Strumenti di rete avanzati

Synology Router RT1900ac



Gestisci la tua rete dal tuo dispositivo
Android o iOS grazie a DS router

LA VOSTRA RETE, INTELLIGENTE E VELOCE

Synology Router RT1900ac è un router wireless ad alta velocità studiato per gli ambienti domestici e gli uffici. Le tecnologie wireless più recenti offrono una connettività Wi-Fi rapida e affidabile. L'esperienza software è rivoluzionaria e incredibilmente intuitiva, anche per i non esperti di tecnologia. Strumenti di rete avanzati che consentono agli utenti esperti di definire il flusso di dati nella rete.

Reti senza perimetro ma più sicure con l'automazione

Le necessità del business tradotte direttamente in azioni di sicurezza, grazie al Security Fabric di Fortinet che supporta il networking Intent-based

Un recente report di Gartner, "Emerging Technology Analysis: Intent-Based Network Design and Operation", evidenzia come la crescente complessità delle reti, assieme alla carenza di competenze critiche nei compiti di progettazione, implementazione e operatività, stia aumentando la pressione sui responsabili di infrastrutture e operazioni. Costoro devono trovare una maniera migliore di mappare in modo tempestivo, coerente e verificabile le esigenze di business rispetto al comportamento delle infrastrutture. Questa esigenza, sempre secondo Gartner, porta all'adozione di reti cosiddette "Intent-Based", per le quali la specialista della network security, Fortinet, ha sviluppato la Intent-Based Network Security caratterizzata da funzionalità avanzate quali self-provisioning, self-operating e self-correcting. In buona sostanza, aldilà delle specifiche tecnologie, la visione di Fortinet è di fornire alle reti Intent-Based una sicurezza che permetterà al Security Fabric di tradurre automaticamente le necessità di business in azioni di sicurezza di rete sincronizzate senza intervento umano.

In pratica, una serie di automatismi consente di ottimizzare la sicurezza, grazie a recenti aggiornamenti apportati al proprio Security Fabric, un "tessuto" (fabric, appunto), che

unisce le diverse componenti del sistema di sicurezza per aumentare la capacità di risposta alle minacce.

Le più recenti innovazioni apportate al Security Fabric comprendono il rilascio di FortiOS 5.6, il sistema operativo di sicurezza, assieme alla nuova soluzione Security Operations. Secondo gli esperti di Fortinet, grazie a ciò le imprese non avranno più bisogno di progettare architetture di sicurezza sempre più avanzate, semplificando le implementazioni e riducendo gli oneri operativi.

Di fatto, infrastrutture tecnologiche in gran parte autosufficienti saranno in grado di mantenere costantemente una posizione di sicurezza ottimale su tutta la superficie di attacco. Questi automatismi sono necessari, spiega Filippo Monticelli, Country Manager di Fortinet per l'Italia, perché: «Reti sempre più complesse, per problemi di scala, capacità elaborative o di automazione avanzata, non possono essere protette da prodotti specifici o dalle attuali piattaforme di sicurezza».

«È chiaro che gli approcci tradizionali alla sicurezza stanno rapidamente diventando non sostenibili» sostiene Monticelli, concludendo: «Fortinet Security Fabric offre soluzioni di sicurezza ampie, potenti e automatizzate per sostenere le sfide di oggi, mettendo al contempo le basi per una Intent-Based Network Security autonoma. Sarà fondamentale per proteggere le imprese di domani».

*Filippo Monticelli,
Country
Manager
di Fortinet
per l'Italia*



**Tu con il tuo 5x1000
puoi ridargli la vista!**



Restituisci la vista ai bambini ciechi del Sud del mondo.

*Scrivi sulla tua dichiarazione dei redditi il codice fiscale di **CBM Italia Onlus**.*

97 299 520 151

Restituisci la vista a un bambino che, senza di te, vivrebbe per sempre nel buio della cecità.

cbmitalia.org

cbm
insieme per fare di più

La sicurezza fisica

Che sia la minaccia del terrorismo islamista o la crisi e il clima d'incertezza sul futuro che psicologicamente incide sugli individui generando rabbia e frustrazione, il tema della sicurezza è al centro del dibattito pubblico. Le soluzioni per lo smart building stanno accrescendo l'automazione in questo settore, con alcune punte riguardanti non solo la protezione (come l'antincendio o l'antintrusione), ma anche la prevenzione, come nel caso della videosorveglianza. Qui si registrano notevoli sviluppi, sia sul fronte della qualità (risoluzione, luminosità, per esempio) sia, e soprattutto, su quello della gestione.



La videosorveglianza interagisce con l'ambiente

Le soluzioni di videosorveglianza intelligente di Mobotix si integrano con il business, l'ambiente e l'IoT. La società illustra come trarne beneficio

Nel mondo della sicurezza e della videosorveglianza stanno irrompendo nuovi paradigmi che mutano profondamente il modo in cui questi strumenti, ma sarebbe meglio parlare di sistemi, sempre più sofisticati possono aiutare a migliorare e a rendere sicuro il contesto in cui si lavora, ci si sposta, si comunica e si fruisce di servizi pubblici e privati.

Ma non si tratta solo di sofisticazione o di aumentare la quantità di pixel. Ora il futuro dei sistemi di videosorveglianza risiede nell'essere sempre più integrati con l'ambiente, con l'IT e con l'IoT, in modo da poter correlare eventi, fornire informazioni utili al business e alla sicurezza personale, interagire con le applicazioni e il contesto costituito dalle reti IP, dai sistemi di telefonia SIP e con il cloud.

Pioniere di questo nuovo modo di interpretare la videosorveglianza è Mobotix (www.mobotix.com/ita_IT/), azienda tedesca di recente entrata nella famiglia Konica Minolta e guidata in Italia da Alberto Vasta, un manager che nel settore ha maturato una solida esperienza.

«Fondamentalmente il mondo della videosorveglianza su IP sta cambiando profondamente. Negli ultimi dieci anni la corsa è stata verso la qualità e l'incremento dei

megapixel. Ora la tendenza si è spostata verso la disponibilità di applicazioni software evolute, ad esempio con sofisticate applicazioni per l'analisi video, e in questo Mobotix si pone all'avanguardia», ha spiegato Vasta.

Visione di sistema e integrazione con l'ambiente

La vision strategica che Mobotix ha perseguito negli ultimi anni è andata verso lo sviluppo di sistemi più che di semplici apparati, per quanto sofisticati essi siano. Un elemento chiave del suo approccio è che nelle sue soluzioni ogni telecamera costituisce un elemento indipendente di un più ampio insieme, anche di centinaia di dispositivi. È in sostanza un vero e proprio computer dotato di capacità elaborativa e di storage interno che può vivere e operare in modo del tutto autonomo anche quando dovesse rimanere scollegato da una rete a cui fosse connesso.

Come per un pc, da un sistema centrale è possibile gestirlo e modificarne i parametri o aggiornare il firmware o prelevarne i dati registrati utili per le funzioni di controllo. La disponibilità dei dati registrati è poi garantita mediante la duplicazione dei dati residenti su NAS esterni a cui le registrazioni possono essere inviate tramite l'indirizzo IP.

Un altro elemento chiave è, come evidenziato,

Alberto Vasta, Business Development Manager Italia e Malta di Mobotix



l'interazione spinta con l'ambiente. «Nella nostra concezione una telecamera non ha più il mero compito di registrare cosa avviene, fare una chiamata o lanciare allarmi. Il software residente nelle nostre soluzioni realizza quello che viene definito studio comportamentale e provvede a filtrare gli eventi che sono ritenuti interessanti per la sicurezza o per il business. Inoltre, ottimizza la quantità di informazioni generate e che devono essere memorizzate in locale o trasmesse occupando banda. Con il software è per esempio possibile analizzare il comportamento delle persone in un'area specifica, di un negozio come di un grande magazzino, in modo da individuare gli oggetti o le aree più interessanti per il pubblico», ha spiegato Vasta.

Parlare di un sistema di videosorveglianza diventa quindi pleonastico perché si tratta, nella vision Mobotix, di soluzioni molto evolute che possono essere integrate nell'IT e nell'ambiente fisico, che coniugano sicurezza e business, lanciano allarmi utilizzando lo standard SIP, filtrano e preanalizzano gli eventi e permettono di integrarli con strumenti di analisi sofisticati.



Una soluzione integrata con l'ambiente ottimizzata per la sicurezza e il business

«Un elemento chiave è l'Activity Sensor, che permette di eliminare tutte le informazioni superflue che occupano capacità di calcolo, banda e storage. Con un algoritmo proprietario siamo in grado di eludere tutti i falsi allarmi. Da poco poi abbiamo anche rilasciato un nuovo firmware chiamato MX Activity Sensor 2.0 che permette anche di stabilire il volume degli oggetti, ad esempio eliminare gli eventi dovuti al passaggio di piccoli animali. La nostra tecnologia Moonlight permette inoltre di avere una ottima visibilità notturna anche con pochissima luce, cosa che di fatto elimina la necessità di illuminatori ad infrarossi», ha spiegato Vasta.

Un IoT concreto e nei fatti

La tecnologia sviluppata da Mobotix non è qualcosa di futuribile ma una realtà già attiva in impianti equipaggiati con centinaia di telecamere inserite in contesti molto ampi e critici.

Per esempio, ha illustrato Vasta, in Liguria è attiva una installazione con 850 telecamere distribuite in dodici comuni. Il consistente beneficio conseguito è che oltre alle funzioni software sofisticate disponibili nei dispositivi non è stato necessario investire in Capex per acquistare oltre alle telecamere anche gli usuali pc, lo storage o le licenze software di applicazioni e apparati perché tutto è già disponibile a bordo. E inoltre non dipendendo da un pc esterno per le registrazioni video anche la sicurezza dell'installazione ne risulta fortemente aumentata.

Con le sue soluzioni di videocontrollo Mobotix ha precorso i tempi anche per quanto concerne l'IoT.

«E' già da un paio d'anni che siamo nei fatti nell'ambito dell'IOT. A livello mondiale abbiamo numerose installazioni pubbliche e private dove la telecamera è un anello di una catena distribuita sul territorio di una struttura di informatica, e questo perché oltre a occuparsi della videosorveglianza espleta numerose altre funzioni e interagisce con altri sottosistemi IT», ha illustrato Vasta.

Le funzioni software permettono una veloce e approfondita rianalisi degli eventi



Vicinanza al cliente e formazione nel DNA di Mobotix

L'obiettivo di Mobotix in Italia non è solo di vendere, osserva Vasta, ma anche di fare formazione e migliorare continuamente un approccio che la vede storicamente vicina al cliente finale e al canale di vendita.

Quando si parla di una soluzione come quelle Mobotix non si ha a che fare con un semplice dispositivo, evidenzia il manager, ma con un sistema complesso che deve interagire con l'ambiente circostante, con le applicazioni, con gli altri dispositivi di una infrastruttura IT, e farlo tramite reti dedicate o virtuali, fisse e mobili, con dispositivi storage locali o distribuiti e, non ultimo, con quanto inerente ai big data per l'analisi. Ciò richiede al canale e all'installatore una preparazione adeguata e di ottimo livello atta a garantire al cliente finale quella qualità che è uno dei punti fermi nella strategia Mobotix. Per questo ha in atto un programma di formazione e di collaborazione articolato su quattro giornate. A questo si aggiungono ogni anno numerosi eventi verticali per spiegare sul territorio e nei diversi settori industriali, nel pubblico e nel privato, i vantaggi del suo nuovo approccio alla videosorveglianza.

“È un approccio che mostra ai possibili clienti i benefici ottenibili con le nostre soluzioni e allo stesso tempo va incontro alle esigenze degli installatori alle prese con nuovi paradigmi, installatori che fanno riferimento ai tre distributori con cui copriamo in modo capillare l'intero territorio nazionale per essere vicini al cliente”, ha evidenziato Vasta. ✱

Blockchain si fa strada nella cyber security

Il verificarsi di attacchi alla cyber security sta accentuando l'attenzione su blockchain, una metodologia che permette di rendere del tutto sicuri e inalterabili (o in ogni caso rilevarne velocemente l'eventuale alterazione) i dati e le transazioni sensibili. Blockchain è una tecnologia da tempo conosciuta ma sino ad ora se non negletta, perlomeno relegata tra entità specializzate, generalmente del settore del finance, che sulla inalterabilità delle transazioni digitali basano il proprio business e la forza del brand. Il concetto che sta alla base della tecnologia blockchain è semplice e si rifà in un certo qual modo al detto che si possono ingannare tanti per poco tempo, pochi a lungo ma non tanti a lungo.

La soluzione è un poco come l'uovo di Colombo anche se questo richiede che sia disponibile una ampiezza di supporti di archiviazione e di connettività adeguati generalmente non alla portata della singola impresa. Era proprio il loro ammontare complessivo, costo e la inadeguatezza delle reti del passato che aveva ed in parte ha sino ad ora impedito di applicare su larga scala il concetto e la tecnologia blockchain.

Nella sua essenza la tecnologia blockchain consiste nella replicazione su un numero elevato di archivi storage dei dati sensibili organizzati in blocchi. Ciò rende praticamente impossibile apportare una modifica dei dati in uno dei nodi senza che in breve tempo gli altri nodi non se ne accorgano segnalando l'evento al sistema di gestione per gli interventi del caso.

Per le sue caratteristiche promette di essere la tecnologia del futuro per la protezione dei dati sensibili e sono già numerosi i gruppi e le associazioni al lavoro nello sviluppo di infrastrutture di sicurezza che la adottano nella loro architettura di base.

La security che integra protezione fisica e logica

Marco
Bavazzano,
Chief
Executive
Officer di
Axitea S.p.A.



Axitea propone un servizio di sicurezza convergente ideato per le Pmi che combina il meglio della sorveglianza fisica con quella logica

Il problema della sicurezza interessa in modo crescente le grandi aziende ma ancor più le Pmi, perché raramente quest'ultime dispongono di capacità tecnologiche e risorse umane che permettano di garantire in modo efficace una protezione aziendale a 360 gradi. Nonostante ripetuti interventi normativi, essere compliant non è poi sinonimo di sicurezza, come mette in guardia Marco Bavazzano, CEO di Axitea, azienda specializzata e attiva da decenni nella sicurezza fisica, nella sorveglianza e sempre più presente anche nella sicurezza informatica, soprattutto quella di tipo integrato che ne coniuga i diversi paradigmi. Gli attaccanti sono a conoscenza del fatto che le vulnerabilità delle aziende risiedono proprio nella mancanza di integrazione tra sicurezza fisica e logica e utilizzano tali vulnerabilità per portare i loro attacchi, che possono avere come obiettivo l'esfiltrazione di dati, di piani aziendali o di dati dei clienti. E per farlo utilizzano vettori di attacco integrati che sfruttano

proprio le debolezze derivanti dalla mancanza di una copertura integrata del rischio e dalla scarsa preparazione dei dipendenti. «Sulla base di una consolidata esperienza nei diversi campi della sicurezza abbiamo reso disponibile una soluzione convergente fisica e logica ideata per le PMI, a prezzi assolutamente accessibili, fruibile sotto forma di servizio, e soprattutto completamente gestita», ha spiegato Bavazzano.

Il servizio di sicurezza sia per quanto concerne eventi di cyber security attinenti al mondo IT sia per quelli fisici (video, accessi, allarmi, eccetera) viene erogato tramite la centrale SOC situata presso la sede dell'azienda a Milano, e duplicata ad Ancona. Dalla centrale operativa viene monitorato in tempo reale l'insorgere di eventuali fenomeni imputabili ai tentativi di attacco. Aspetto qualificante e unico nel panorama italiano ed europeo, evidenzia Bavazzano, è che dalla centrale si ha una gestione realmente integrata, dal malware agli allarmi che provengono dai

sistemi di antiintrusione, dalla videosorveglianza e da qualsiasi altro dispositivo di sicurezza, in modo da garantire all'azienda una protezione a tutto tondo.

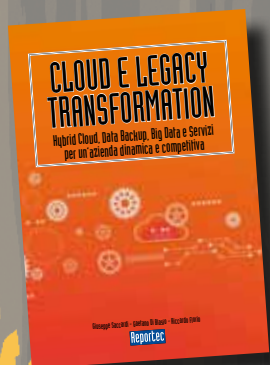
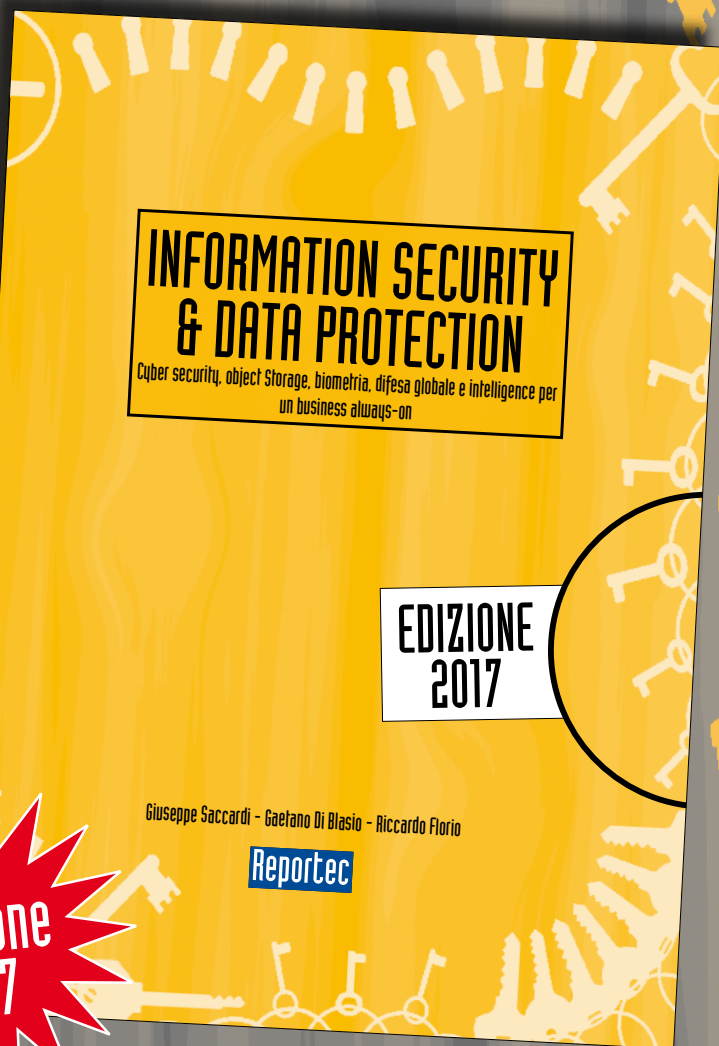
È un approccio che consente la rilevazione di eventi critici che altrimenti potrebbero essere ritenuti non rilevanti. Per esempio, se un utente accede alla rete Wi-fi interna ma risulta essere in trasferta o non ha timbrato, oppure se viene segnalata un'intrusione nella sala computer abbinata all'uso di una chiavetta Usb. Si tratta di eventi che solo una sofisticata capacità di correlazione fisico-logica è in grado di rilevare in modo da attuare immediatamente gli interventi necessari, che come servizio possono consistere sia nell'intervento di personale di sorveglianza armata Axitea che quello della forza pubblica. «Con i nostri esperti e servizi vogliamo accompagnare i nostri clienti, oltre 30mila, nel percorso verso un'azienda sicura e farlo in accordo ai nuovi paradigmi della sicurezza convergente», ha evidenziato Bavazzano.✳

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



Mission Unhackable

True Cybersecurity per aziende.

Solo l'approccio Kaspersky Lab True Cybersecurity combina la facilità d'uso e la HuMachine™ intelligence per proteggere il tuo business da qualsiasi tipo di minaccia.

Maggiori informazioni su kaspersky.it



**Kaspersky[®]
Endpoint Security
for Business**

Advanced