

Smart Security

OAD: Osservatorio Attacchi Digitali in Italia

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

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

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

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

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



INDICE

4 La Smart Security

7 Compliance al GDPR: attenti agli incompetenti e alle truffe!

10 Cloud Security

12 Ambienti di lavoro digitali protetti in base al contesto

14 SUSA Trasporti guadagna efficienza e flessibilità nell'IT grazie alla centralizzazione

15 La continuità del servizio garantita per contratto con un cloud protetto

16 Come evitare all'azienda i pericoli dovuti al DevOps

18 Un'infrastruttura impermeabile e invisibile

20 Flessibilità e adattabilità la chiave per un cloud sicuro e di successo

22 Sicurezza fisica e infrastrutture

24 Un ambiente di lavoro protetto in palmo di mano

26 Il GDPR e la protezione dei dati nei processi di stampa

29 TalkTalk si affida a Nuance per trasformare l'esperienza cliente

30 La biometria previene le frodi e semplifica l'autenticazione utente

32 Oltre la sorveglianza con la cattura e l'analisi dei dati

34 Come proteggere gli ambienti industriali e OT

35 La sicurezza intelligente

36 L'Enterprise Security di Micro Focus per prevenire anziché rimediare

38 La cyber resilienza per creare un ecosistema di fiducia

40 Aeroporti di Puglia rinnova le reti WAN con Cisco

41 L'intelligenza artificiale in aiuto della cyber security

43 La disponibilità dei dati

44 Dati al sicuro e sempre disponibili con la Hyper Availability

46 La sicurezza dei container

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

Direction Reportec • anno XV - numero 106

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

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


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

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




LA SMART SECURITY

Più intelligenza per la sicurezza, non solo informatica



I GDPR ricalca parte delle normative previste da tempo in Italia per la tutela della privacy e si concentra proprio sull'individuo e i suoi diritti per quanto riguarda il rispetto della persona. La protezione dei dati personali e ancor di più quella dei dati sensibili deve essere perseguita per legge, ma la sicurezza non può fermarsi qui. Certamente le linee guida sono un utile riferimento per imporre una maggiore attenzione nell'impostazione di un sistema di sicurezza informatica per le imprese. Ma occorrerebbe altrettanto impegno verso i singoli individui. Una buona metà, se non di più, dell'efficacia nella lotta alle minacce dipende dalla "cultura" sulla sicurezza. Oggi il tema è su tutti i giornali e telegiornali, ma i mezzi di comunicazione non hanno più la pervasività di un tempo.

In buona sostanza, ci sono ancora troppi comportamenti ingenui, per non dire stupidi, che, se corretti, ridurrebbero drasticamente le violazioni a dati e sistemi informatici. È una questione d'intelligenza che, che alcune aziende stanno



cercando di utilizzare a "dispetto" di quella dell'utente, impostando algoritmi di intelligenza artificiale per rendere la sicurezza "automatica".

Purtroppo anche i cyber criminali ricorrono al machine learning (hanno cominciato prima, in verità, automatizzando toolkit di attacco alla ricerca di vulnerabilità). La rincorsa a digitalizzare i processi industriali e commerciali porta a sviluppare applicazioni che, in buona parte finiscono negli smartphone di tutti o quasi. Se si potesse avere meno fretta, si potrebbe distribuire l'app con meno difetti, ma occorre adottare un altro punto di vista in azienda: un punto di vista a fuoco sulla sicurezza. Così si può contare sull'intelligenza, quella delle macchine e quella umana.

Nelle prossime pagine alcuni esempi di soluzioni, casi di studio, valutazioni di esperti. Si parte dal cloud, che protegge e va protetto, dalla sicurezza fisica delle informazioni (che è citata anche da GDPR, da quella delle infrastrutture e altro ancora. ❁

Compliance al GDPR: attenti agli incompetenti e alle truffe!



di Marco R. A. Bozzetti,
Presidente AIPSI

Il GDPR, General Data Protection Regulation, è il nuovo regolamento europeo sulla privacy, ed è già entrato in vigore in tutti gli stati dell'UE dal 26 maggio scorso: quindi avrebbe dovuto essere applicato ed essere operativo in ogni azienda/ente da quella data, ma ancora una non trascurabile parte degli enti e delle aziende italiane, soprattutto quelle di piccole dimensioni, sono ben lungi da un effettivo adeguamento. Anche se questo regolamento è stato approvato e rilasciato ufficialmente da ben due anni, e sono ormai 22 anni che leggi sulla privacy sono in vigore in Italia, a partire dalla 675 del 1996. La privacy e gli obblighi ad essa relativi non sono pertanto una novità, tutti dovrebbero già da tempo avere le idonee misure di protezione, ed ora semplicemente adeguarle a quanto richiesto dal GDPR, che, quale effettiva novità, prevede elevatissime sanzioni economiche:

a) una multa fino a **10 milioni di euro, o fino al 2% del volume d'affari globale** registrato nell'anno precedente nei casi di violazione degli obblighi dei titolari e dei responsabili (art. 83, Paragrafo 4)

b) una multa fino a **20 milioni di euro o fino al 4% del volume d'affari** nei casi di violazione dei principi base, dei diritti degli interessati, dei trasferimenti, degli ordini del Garante (art. 83 Paragrafi 5 e 6)

Inoltre, solo l'8 agosto scorso il Consiglio dei Ministri ha approvato il Decreto Legislativo n.101 per adeguare il quadro normativo nazionale alle disposizioni del GDPR, dopo un lungo e travagliato iter: inviato al Parlamento il 10/5/2018 con il consenso del Garante sui suoi contenuti, e pubblicato il 4/9/2018 sulla Gazzetta Ufficiale: questo decreto è in vigore dal 19/9 scorso. Il testo del D. Lgs di adeguamento, inoltre, è di assai difficile lettura, elencando tutte le correzioni rispetto alle norme del precedente codice 196/2003 in ottica GDPR: alla faccia della chiarezza e della facile comprensione della legislazione!

Nonostante tutto, le salate multe hanno risvegliato l'attenzione sulla privacy nei vertici di aziende ed enti, ed hanno riattivato l'offerta di consulenze e di strumenti informatici di supporto.

Dati i costi e gli impegni complessivi non trascurabili per una effettiva e corretta compliance agli obblighi per la privacy, in precedenza si poteva valutare più conveniente non fare nulla, o quasi, e rischiare

la piccola sanzione: ma ora? Come si comporterà l'Autorità Garante? Verranno applicate, e in che misura, le sanzioni economiche?

Nel contesto italiano, con la stragrande presenza di piccole e piccolissime imprese, a parte le ovvie eccezioni, la privacy è stata ed è considerata come uno dei tanti, troppi, obblighi burocratici costosi ed inutili, se non controproducenti, per il business e l'attività aziendale. Questo quando io azienda/ente devo trattare i dati personali dei miei interessati... Ma per me, come individuo, la protezione dei miei dati personali deve essere garantita, e bene!

Al di là di questa dicotomia, per altro riscontrabile su vari altri temi, la privacy, di fatto sempre abbastanza trascurata dalla maggior parte dei responsabili di aziende ed enti, si rivitalizza come problema, date le possibili sanzioni. La marea di articoli, di convegni, di webinar, anche se letti a campione ed in maniera abbastanza casuale e superficiale, evidenziano come adeguare la propria situazione della privacy al GDPR non sia una passeggiata e richieda comunque un impegno non trascurabile che coinvolge anche il vertice dell'organizzazione. Di conseguenza le domande tipiche che si pongono i decisori di vertice: forti sanzioni? Ma quando mai verranno a controllarmi? Ho ben altre spese cui far fronte! Sicurezza digitale? Ho già l'antivirus e il controllo degli accessi ... Il resto è troppo complicato e costoso e poi chi mai vorrà attaccarmi digitalmente? E con questo in mente, contatta persone di fiducia e si informa su quello che

fanno aziende/enti simili alla sua. Sovente senza aver ben compreso che cosa richiede il GDPR, entra in contatto con suoi, e di altri, professionisti, tipicamente commercialisti, avvocati, consulenti del lavoro, fornitori di informatica, consulenti ed altri "specialisti". Ed entra così in ginepraio di suggerimenti, proposte ed offerte dal quale, se non ha un minimo di conoscenza su privacy e sicurezza digitale, avrà difficoltà ad uscirne "vivo" col minimo dei danni.

Moltissimi dei professionisti che si propongono in tema di privacy e di adeguamento al GDPR sono seri ed affrontano correttamente ed eticamente il problema. Ma purtroppo sul mercato italiano è in forte crescita l'offerta di servizi per la privacy "chiavi in mano" a prezzi ridicoli, che non possono che offrire soluzioni e documenti generali e non contestualizzati sulla realtà del cliente. Giocoforza tali soluzioni



costituiscono una insufficiente copertura e sono soldi mal spesi, anche se pochi: la responsabilità è del legale rappresentante della azienda/ente, e non ne risponde, in prima battuta, il consulente e/o il fornitore. Per la sicurezza digitale poi, molti fornitori di informatica vendono le soluzioni che hanno, trascurando le effettive necessità del cliente ed approfittando della incompetenza sua e dei suoi collaboratori. Privacy e sicurezza digitale sono multi-disciplinari e richiedono una vasta gamma di competenze e di esperienza sul campo. Difficilmente un'azienda/Ente, soprattutto se piccola, può avere al proprio interno specifiche e aggiornate competenze di privacy e sicurezza digitale. Deve pertanto terziarizzare gran parte (o la totalità) delle decisioni e dell'operatività, e l'unico criterio di scelta è spesso il passa parola ed il costo. Ma di chi si può fidare? Come può garantirsi

sulle reali competenze dei fornitori e dei consulenti? Il problema è il medesimo per la scelta dei professionisti di riferimento, quali i commercialisti, i fiscalisti, gli avvocati e così via.

Un primo suggerimento in merito nella scelta è il verificare per la persona e/o per l'azienda, quale condizione necessaria ma non sufficiente:

- l'averne una o più certificazioni sulla privacy e sulla sicurezza digitale, in particolare le uniche con valore legale europeo: eCF - EN 162341:2016 (Per approfondimenti si veda il sito <https://www.aipsi.org/aree-tematiche/crescita-e-percorsi-professionali.html>)
- l'appartenenza ad una o più associazioni professionali esistenti in Italia per la privacy e la sicurezza digitale.

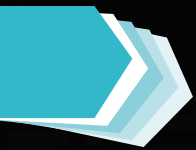
Alcune considerazioni conclusive:

- GDPR lascia alla responsabilità del titolare l'individuazione delle

idonee misure di sicurezza digitale, a seguito dell'Analisi dei rischi, ma evidenzia la necessità/opportunità di criptare i dati personali, e di individuare data breach;

- L'adeguamento al GDPR è un obbligo serio da non sottovalutare, che deve coinvolgere il personale interno dell'azienda/ente e che richiede
 - misure di tipo organizzativo, sia verso l'interno sia verso le Terze Parti coinvolte
 - misure di tipo tecnico quali l'analisi dei rischi e degli impatti, Architetture, tecniche e strumenti di sicurezza digitale, in primis la crittografia dei dati critici e sensibili, misure di sicurezza fisica per gli archivi cartacei, etc.
 - Misure di governance, con sistematico monitoraggio e controllo delle misure in atto, per rispondere al principio di accountability e di inversione dell'onere della prova, e che richiedono anche una idonea documentazione degli interventi effettuati o a piano.
 - Tutte le aziende/enti sono sempre più a rischio digitale, indipendentemente dalle loro dimensioni e dal settore merceologico di appartenenza.
 - L'idonea sicurezza digitale è necessaria non solo e non tanto per adempiere agli obblighi della privacy, ma per garantire la continuità operativa dell'organizzazione, che ormai dipende quasi interamente dal supporto informatico.
 - Privacy, GDPR e sicurezza digitale hanno dei costi non trascurabili, ma quali sono i costi della "non privacy" e della "non sicurezza digitale"? ❁





CLOUD SECURITY

Dalla sicurezza del cloud
alla sicurezza grazie al cloud



CLOUD SECURITY



Ambienti di lavoro digitali protetti in base al contesto

di
Gaetano
Di Blasio

Le regole per la security aziendale seguono gli utenti, grazie alla sicurezza contestuale di Citrix

Il Secure Digital Perimeter è il "modello" che permette a Citrix di rendere disponibili spazi di lavoro digitali, chiamati Digital Workspace, a qualsiasi tipologia di utente su qualsiasi tipo di device per accedere ad applicazioni e dati che possono essere situati ovunque, all'interno della rete aziendale, come nel cloud.

Ovviamente un modello di questo genere parte da una prerogativa, cioè che il posto di lavoro non sia più uno spazio fisico.

Ormai sempre più aziende praticano lo smart working, non solo per consentire di lavorare da casa o da una sede remota, ma anche per sfruttare le potenzialità della mobility, laddove una parte della forza lavoro è distribuita sul territorio. Inoltre il lavoro diventa sempre più "agile", con forme di organizzazione più orizzontali, che esaltano la cooperazione e il lavoro in team.

Questo significa che un information worker, oggi, potrebbe operare dall'ufficio come da altrove, usando il pc, uno smartphone o un altro dispositivo, fisso o mobile e collegandosi a una rete proprietaria, pubblica o privata, ma di terzi, come se fosse in ufficio, o quasi, rispettando i requisiti di sicurezza imposti in azienda.

In sintesi, il lavoratore può trovarsi in diverse condizioni ed è per questo che Citrix ha sviluppato il concetto di accesso contestuale: per fare in modo che le policy di sicurezza "seguano" l'utente.

È necessario cambiare l'approccio, spiega David Cenciotti, Lead Sales Engineer e Security Evangelist di Citrix, perché, rispetto alla postazione fissa in ufficio, è molto più complesso mettere in sicurezza l'accesso a dati e applicazioni distribuiti da dispositivi che cambiano continuamente, insieme alle condizioni al contorno.

Chi è in ufficio accede a dati e applicazioni da un ambito sicuro, all'interno di una rete sicura, usando un dispositivo gestito e controllato dall'IT aziendale. Quindi è possibile adottare determinate politiche di sicurezza, che garantiscono a questo tipo di utente di operare in base ai suoi privilegi di accesso e trattamento dei dati. Potrà accedere ai file che gli competono, visualizzarli, stamparli e così via.

Se quel lavoratore si sposta in aeroporto e, nell'attesa della partenza, volesse



accedere ai file sui quali stava lavorando in ufficio, il sistema dovrà valutare il nuovo contesto operativo e adattare le policy. Per esempio, poiché si sta collegando da una rete non sicura, all'utente non basterà più inserire username e password come in ufficio, ma dovrà utilizzare un ulteriore fattore di autenticazione. Inoltre, è possibile che a quell'utente collegato dall'hotspot dell'aeroporto sia permesso di visualizzare i file, ma siano impediti alcune azioni, come la stampa.

In buona sostanza, è possibile, in base al contesto, adattare le policy di sicurezza, rispondendo al "chi, cosa, quando, come e perché" si sta collegando a un determinato dato, pertanto mantenendo il controllo sui dati aziendali.

Le regole di accesso e tutte le politiche di sicurezza smettono quindi di essere statiche: non è più necessario che tutti debbano usare sempre le modalità di autenticazione, oppure che tutti debbano accedere da remoto con una VPN o, ancora, che su ogni dispositivo debba esserci il personal firewall e l'antivirus abilitato. Questi parametri cambiano a seconda del contesto, mantenendo sempre il controllo su chi, cosa, quando come e perché.

Una sicurezza che si adatta dinamicamente al contesto e che applica le regole fissate in azienda, evitando che l'utente si debba preoccupare di cambiare i parametri del

proprio dispositivo, preservando il più possibile la user experience.

Con un'intelligenza che viene pilotata centralmente dall'azienda, si ottiene la migliore esperienza possibile per operare in molteplici contesti, regolando automaticamente una sicurezza più o meno stringente per ciascun utente.

Ovviamente questo si fonda su elementi architetturali che devono capire il contesto, il che implica capacità di analisi per discriminare quale sia l'utente o il dispositivo che si collega, a cosa vuole accedere eccetera, in modo da attivare le regole del caso e applicare il profilo utente previsto per il contesto identificato.

Il perimetro digitale di Citrix

La sicurezza contestuale si basa sulla tecnologia ideata da Citrix per creare il Digital Perimeter, che "abbraccia" l'impresa e tutti i suoi dipendenti, proteggendoli e fornendo loro gli strumenti necessari per il proprio lavoro. I "building block" di questo modello (citando solo i principali), sono il controllo d'accesso, lo "strato" di application delivery control e la virtualizzazione delle sessioni, cioè l'elaborazione centralizzata delle applicazioni, indipendente da luogo, rete e dispositivo. L'utente utilizza la Workspace App, ovvero un client universale per l'accesso ad applicazioni e i dati di qualsiasi tipo, pubblicati su un app

store aziendale o nel Cloud, pubblico, privato o ibrido.

C'è, poi, uno strato di tecnologia SD-WAN (Software-Defined Wide Area Network), che serve a ottimizzare la connessione attraverso la rete geografica ed evitare ritardi in quelle applicazioni, come la videoconferenza, penalizzate dalla latenza. Per ultima, ma non meno essenziale, come accennato, la componente di analytics, che si basa su algoritmi di machine learning e analisi di big data, per l'analisi comportamentale degli utenti e per la comprensione automatica del contesto.

Questo framework, che rende sicuri i workspace virtuali, è stato adottato da imprese appartenenti ai settori più disparati, anche nella Pubblica Amministrazione. In generale, spiega Cenciotti, i nostri clienti sono aziende che hanno intrapreso un percorso di digital transformation, come le grandi enterprise, che utilizzano questo approccio per continuare ad arricchire il suddetto percorso, aumentando la sicurezza, grazie all'erogazione dei Secure Digital Workspace a un numero crescente di dipendenti.

Per esempio ci sono casi, come la scuderia di Formula 1 Red Bull (Red Bull Racing) che, grazie al modello di Citrix, permette al team impegnato in un gran premio di accedere in sicurezza a dati 3D CAD, magari a qualche continente di distanza, e di lavorare sul set up di nuovi componenti per le monoposto da corsa come se gli ingegneri di pista e quelli in sede, stessero operando dall'interno del perimetro dell'azienda.



SUSA Trasporti guadagna efficienza e flessibilità nell'IT grazie alla centralizzazione

La società, attiva nel settore della logistica, ha rinnovato la propria architettura virtualizzata scegliendo Citrix e Praim per migliorare la manutenzione e il controllo di client e periferiche

Nata nel dopoguerra, SUSA Trasporti inizia la propria attività con il trasporto di prodotti alimentari in centro Italia per poi espandersi progressivamente sul territorio. È negli anni '70 e '80 che, grazie all'attività di distribuzione di ricambi automobilistici, inizia il vero percorso di crescita. Di recente SUSA ha riscontrato la necessità di far evolvere la propria infrastruttura obsoleta sia per migliorare gli aspetti gestionali sia per sostenere l'incremento della richiesta di servizi. Necessitava, quindi, di gestire in modo centralizzato sia i client sia le periferiche a essi collegate.

SUSA ha optato per una soluzione di continuità avendo già un'infrastruttura centralizzata con le soluzioni Citrix XenApp e MetaFrame. Ciò l'ha portata ad adottare le ultime release di XenApp e XenDesktop unitamente a client molto leggeri (thin e zero) come quelli della serie Neutrino di Praim (certificati "Citrix Ready") e alla console ThinMan. In questo modo, oltre a sostenere maggiori richieste di prestazioni degli utenti e a

mantenere la stessa esperienza di utilizzo dell'architettura precedente, l'IT di SUSA può gestire centralmente anche le periferiche utilizzate dalle diverse sedi, come i terminali portatili e le pistole scanner. Anche il livello generale di sicurezza ha beneficiato dell'aggiornamento, grazie a sistemi operativi di ultima generazione, all'irrobustimento nativo delle policy di controllo e alla profilazione degli utenti, tutto gestito in modo centralizzato attraverso Citrix Universal Profile Manager.

La gestione centralizzata evoluta consente ora di controllare sia l'hardware sia il software, risparmiando tempo e risorse. «Un grosso risultato ottenuto grazie alla nuova architettura - ha spiegato Armando Tonnetti, CIO di SUSA - è che ora possiamo contare sull'uniformità del software installato e sul controllo puntuale delle licenze dei pacchetti utilizzati, come Microsoft Office».

L'esperienza utente è migliorata



in parallelo alle caratteristiche gestionali: il flusso dei dati è stato ottimizzato grazie all'evoluzione del protocollo di trasmissione verso la suite HDX. Ora gli utenti possono beneficiare di prestazioni più elevate, assicurate da XenDesktop, e utilizzare applicazioni e desktop in multiplatforma (Windows, Linux, Apple e Android).

Ma il risultato più elevato è stato ottenuto con il progetto realizzato insieme a PCS Group, grazie alle soluzioni Citrix e Praim, che ha portato alla riduzione dei tempi di ripristino: «Se prima rimettere in attività un pc richiedeva circa 3 giornate di lavoro - dice Tonnetti - oggi, grazie alla combinazione Citrix and Praim, ci vogliono solo 2 ore in caso di problemi software e 1 giorno per problemi hardware».

Con la teleassistenza, l'IT centrale di SUSA riesce a intervenire in tempo reale per configurare le postazioni o per risolvere i problemi operativi degli utenti. ❁

La continuità del servizio garantita per contratto con un cloud protetto

Radware fornisce soluzioni per proteggere le infrastrutture e assicurare le aziende dagli attacchi DDoS attraverso servizi completamente gestiti

Un numero crescente di imprese utilizza cloud pubblici o privati per attivare applicazioni e servizi. Agilità, flessibilità e riduzione dei costi sono i vantaggi di queste architetture, ma il contraltare è l'impostazione di politiche per la sicurezza diverse tra loro, che ne rende difficile la gestione.

Per aiutare i clienti ad amministrare correttamente le tematiche di sicurezza, Radware ha ideato dei servizi "fully managed" che presentano SLA (Service Level Agreement) garantiti contrattualmente con penali, come sottolinea Nicola Cavallina, Channel Manager Italy, che evidenzia le soluzioni in cloud più recenti. In particolare, Cloud DDoS protection e Cloud Waf (che include la DDoS Protection).

Queste soluzioni proteggono sia ambienti cloud privato sia cloud pubblico (come AWS e Azure) utilizzando telemetria nativa degli ambienti da proteggere.

Le tecnologie adottate rispondono alle esigenze più attuali, quali gli attacchi agli applicativi e i rischi determinati dalle pratiche DevOps. Cavallina sottolinea: «Le applicazioni stanno espandendo il proprio perimetro, si pensi ai microservizi o

alle interazioni tra le stesse applicazioni tramite API. Il mondo del fintech o quello dell'Internet delle cose, per esempio, diffondono nuovi oggetti e applicazioni espo-

nendo un numero crescente di vulnerabilità». A ciò si aggiungono le modalità frettolose con cui sono scritti molti software, sfruttando i nuovi strumenti del DevOps, ma trascurando la sicurezza. Per questo, spiega Cavallina: «Radware fornisce una protezione basata sull'analisi comportamentale, che si distingue per gli algoritmi d'intelligenza artificiale che controllano il comportamento dell'applicazione o quello dell'utente. Gli scostamenti dalla "normalità" fanno scattare l'allarme e l'indagine che porta a bloccare gli eventuali attacchi».

In maniera mirata, quindi, s'interviene senza bloccare intere transazioni. Si tratta di

Nicola Cavallina,
channel manager
Italy di
Radware



soluzioni all'avanguardia proposte in modalità OEM da altri importanti brand della security, osserva il manager, che aggiunge: «Tra i clienti di Radware figurano alcuni dei più importanti stock Exchange, vari carrier, diversi data center di aziende dell'ICT e numerose tra le principali banche mondiali». Oltre questi mercati la società d'origine israeliana propone anche soluzioni per per piccole e medie imprese. Inoltre, va riconosciuto che gli scrubbing center di Radware (cioè i centri che analizzano le applicazioni, il traffico e i dati, ripulendoli dalle minacce), sono tutti conformi al GDPR e sono dotati di certificazioni ISO avanzate di livello militare. *

Come evitare all'azienda i pericoli dovuti al DevOps

di
Gaetano
Di Blasio

Trend Micro protegge lo sviluppo delle applicazioni aziendali e la messa in esercizio delle stesse riducendo i rischi per la sicurezza nel cloud

Il DevOps sta assumendo un'importanza crescente in azienda superando i confini del sistema informatico e coinvolgendo i processi di business.

Il termine DevOps, nasce nel 2008 per descrivere l'insieme di strumenti, prassi e processi che distinguono il ciclo produttivo e operativo di un'applicazione software.

Al contrario di quanto sembra, non si tratta di una problematica puramente tecnica.

Innanzitutto, riflettiamo su come l'interazione con imprese e individui, sul lavoro come in privato, sia mediata da applicazioni. Poi consideriamo, per esempio, una banca che vuole fornire a un proprio cliente accesso all'home banking tramite smartphone con una app; oppure a un retailer che lancia un servizio di consegne a domicilio.

Si parla di business e si comprende subito la criticità dello sviluppo (development in inglese, che comprende la creazione del software e la sua manutenzione, con aggiornamenti e correzioni nel tempo) e la delicatezza delle operazioni (operations che, in maniera più o meno automatica devono garantire il flusso operativo, appunto, che permette l'erogazione del servizio: dall'attivazione del contratto alla fatturazione con tutto quello che compete alle varie funzioni aziendali).

La sicurezza dei container con Deep Security Smart Check

L'importanza del software nei processi aziendali, e l'utilizzo di soluzioni cloud altamente efficienti per il DevOps, come i cosiddetti container, pongono interrogativi sulla sicurezza delle applicazioni e dei dati aziendali, ma anche opportunità. Realizzare le applicazioni migliori, farlo con rapidità per accrescere il time to market è una prassi di successo per il DevOps, ma lo spostamento sempre crescente dei workload in cloud, l'acquisizione di container, l'integrazione automatizzata e la pipeline di comunicazione necessitano controlli di sicurezza efficaci e affidabili, per difendere i processi da una varietà di minacce e attacchi sofisticati. In altre parole, l'uso di cloud ibridi o del multcloud, spesso da parte di manager non tecnici, che attivano servizi all'insaputa del dipartimento di information technology, crea rischi alla sicurezza.



Gastone Nencini, country manager di Trend Micro

È importante avere la flessibilità per lavorare su ambienti ibridi e multicloud, per questo Trend Micro, specialista della cyber security ha realizzato Deep Security Smart Check, che rileva le criticità di sicurezza prima della messa in esercizio di un'applicazione.

La soluzione è stata progettata, come ci spiega Gastone Nencini, country manager di Trend Micro in Italia, per effettuare una continua scansione dell'immagine del container (cioè il software virtuale che contiene l'applicazione e, in genere, tutto quello che occorre per utilizzarla, dati compresi, migliorando così la protezione in runtime.

La scansione avviene prima della messa in produzione dell'applicazione, così da identificare le vulnerabilità e i malware in maniera più efficace. Infatti, in questo modo i problemi di sicurezza possono più facilmente essere risolti nel ciclo di sviluppo e non, come tipicamente accade, dopo averla rilasciata in produzione diventando un uno strumento per i cyber criminali.

API e automazione

I clienti di Trend Micro Deep Security, inoltre, possono sfruttare la nuova suite di API (Application Programming Interface) per abilitare una sicurezza automatizzata, grazie a migliori integrazioni. Le API di prodotto, spiegano gli esperti della società. Si possono impiegare per abilitare un delivery continuo, il monitoraggio dello status, l'IT service management e l'integrazione di diversi tool, come, per esempio, il recente Amazon

Elastic Container Service per Kubernetes.

Bill McGee, senior vice president e general manager of Hybrid Cloud Security di Trend Micro, afferma: «Le piattaforme container permettono alle organizzazioni di raggiungere cicli di sviluppo software più veloci, incontrando le esigenze delle aziende che non accettano rallentamenti a causa di ulteriori misure di sicurezza».

Il manager aggiunge che tutti gli ambienti di workload richiedono sicurezza, compresi i container, ma avverte: «La natura temporanea dei container può creare gap di security che i cybercriminali riescono facilmente a sfruttare. Ci aspettiamo, infatti, che gli attacchi alle applicazioni server verranno sostituiti da quelli ai cicli di costruzione software, con l'obiettivo di rilasciare i malware dall'interno».

Per questo in Trend Micro hanno realizzato Deep Security Smart Check, che supporta le richieste DevOps per costruire una sicurezza continua. Deep Security, con tecnologia XGen, inoltre, consente di estendere la security con una protezione basata su host per i container Docker. I team di DevOps possono utilizzare la soluzione di Trend Micro per sfruttarne le funzionalità di IDS/IPS, antimalware, monitoraggio dell'integrità,

controllo delle applicazioni e altro ancora in un agente su host. A ciò si può aggiungere l'automazione della sicurezza con Webhooks e con una suite completa degli API documentata, visibilità delle console e dashboard dei container distribuiti, log di eventi e notifiche per soddisfare i requisiti di conformità. *



Un'infrastruttura impermeabile e invisibile

di
Gaetano
Di Blasio

Zscaler ribalta gli approcci alla sicurezza semplificando il modello di accesso alle applicazioni grazie al cloud

Il modello per la sicurezza aziendale proposto da Zscaler "rompe" l'approccio tradizionale dell'impresa che cerca di controllare la sicurezza arroccandosi sui bastioni di un perimetro aziendale, il quale, però, si sta dissolvendo.

Finora, ci spiega Fabio Cipolat Gotet, Regional Sales Manager Italy di Zscaler, si è pensato a un sistema di sicurezza che contrastasse i cyber criminali aggiungendo strumenti di protezione per rafforzare il perimetro aziendale.

«Si cerca ancora di creare uno strato esterno di sicurezza resistente come il guscio di una noce di cocco, mentre si deve passare al modello dell'avocado, con l'esterno morbido, per consentire agli utenti di connettersi alle applicazioni, collaborare internamente e con i loro clienti e partner. Mentre le risorse preziose da proteggere devono stare all'interno del duro nocciolo».

Questo approccio è partito dieci anni fa, quando Jay Chaudhry, fondatore e attuale CEO di Zscaler creò Zscaler e la prima piattaforma di sicurezza in cloud, cogliendo la tendenza travolgente che vedeva i dipendenti uscire dall'ufficio, per lavorare sempre più in mobilità. e le applicazioni che cominciarono a lasciare il perimetro dell'azienda per andare verso il cloud. I dispositivi mobili e i primi servizi SaaS preludevano il boom della mobility.



Fabio Cipolat Gotet, Regional Sales Manager Italy di Zscaler

Da Blockbuster a Netflix

È un passaggio epocale paragonabile a quello che ha visto il fallimento di Blockbuster: un'azienda leader che noleggiava videocassette e DVD, in pratica con un modello basato "sull'hardware" posseduto a casa dal cliente. La connettività e lo streaming hanno reso obsoleto, scomodo e meno efficace il modello "on premise", così come oggi il cloud sta prendendo il sopravvento sulle infrastrutture gestite in casa.

È una questione di tempo, ma il percorso è nel cloud.

Oggi, ci racconta Cipolat: «Zscaler ha costruito nella sua piattaforma cloud lo stack di sicurezza che ancora troviamo all'interno del perimetro aziendale ed è diventata leader riconosciuta da analisti, quali Gartner e Forrester in quanto è distribuita su 100 data center a livello mondiale e gestisce ogni giorno circa 50 miliardi di transazioni (10 volte le transazioni giornaliere di Google Search), 125 milioni di minacce e 120mila update di sicurezza».



Nella piattaforma sono stati ricreati gli stessi layer di sicurezza di un modello tradizionale, ma è tutto trasparente per i clienti.

Due servizi per una sicurezza invisibile

Sono due i servizi forniti da Zscaler: Zscaler Internet Access e Zscaler Private Access.

Il primo gestisce tutti gli strumenti necessari per la sicurezza aziendale e opera, di fatto come un proxy, seppur evoluto, ma è un servizio la cui sottoscrizione è basata su un unico parametro: il numero di utenti.

Come accennato, oggi, mobilità e cloud cancellano il perimetro e la sicurezza deve essere spostata in cloud.

«Ovviamente questo può avvenire per ciascuna impresa con il proprio ritmo e attraverso il percorso più adatto - sottolinea Cipolat - grazie a una soluzione as a service, che rende la sicurezza una

commodity, eliminando appliance e sistemi, che portano oneri di gestione, complessità architetturale, aggiornamenti e difficoltà di scalabilità e performance».

I 100 data center distribuiti per il mondo, in peering diretto con più di 150 vendors, risolvono il problema della continuità del servizio e delle performance nell'accesso alle applicazioni di business, oltre a garantire scalabilità: "Zscaler significa Zenith of Scalability e vuole proprio rappresentare la massima scalabilità garantita dalla piattaforma Zscaler su tre filoni principali: il numero di dipendenti, il numero di location e il traffico che viene gestito su Internet".

Semplificare, aumentare la user experience

L'obiettivo è semplificare per Zscaler, aumentare la user experience "ognuno deve sentirsi libero di lavorare ovunque a prescindere dal numero e dalla

tipologia di devices, e questo sia per accedere alle applicazioni SaaS sia quelle private". Zscaler Private Access è la seconda soluzione per la gestione degli utenti remoti e consente il replacement della VPN per collegarsi alle applicazioni aziendali private o migrate su IaaS quali Azure o AWS. "Le imprese devono ripensare il modo in cui gli utenti accedono alle applicazioni. Per passare a un approccio moderno, in cui l'accesso è basato su utenti specifici e applicazioni specifiche, molti si sono rivolti al Software-Defined Perimeter (SDP). Questo modello consente la totale sicurezza del trust collegando esclusivamente utenti autorizzati a specifiche applicazioni interne o migrate in Cloud, senza posizionare gli utenti sulla rete, senza VPN e senza più la necessità di esporre le applicazioni che risulteranno invisibili agli utenti non autorizzati all'accesso".



Flessibilità e adattabilità la chiave per un cloud sicuro e di successo

CyberArk automatizza la sicurezza e la migrazione sul cloud Amazon di migliaia di utenti privilegiati e assicura la protezione delle credenziali e il disaster recovery

La diffusione del processo di digitalizzazione e lo spostamento progressivo delle applicazioni nel cloud pubblico o ibrido sono due aspetti chiave di quella trasformazione digitale che è riconosciuta essere l'elemento indispensabile per poter operare in un mercato globalizzato estremamente competitivo e dove le esigenze dei clienti crescono continuamente.

Se i benefici sono consistenti e il processo di trasformazione irreversibile, ciononostante non si devono trascurare, mette in guardia CyberArk, società quotata tra le prime a livello mondiale nel campo della sicurezza dell'accesso privilegiato, i problemi e i rischi connessi al dissolversi di fatto del perimetro aziendale. Cloud, digitalizzazione e mobility, solo per citare alcuni tra i principali, sono paradigmi che rendono virtuale un'azienda, ne aumentano di molto la produttività, ma allo stesso tempo fanno emergere consistenti rischi per la sicurezza di applicazioni, dati e dispositivi.

Il rischio per la sicurezza coinvolge in modo maggiore, evidenzia CyberArk, le aziende che al fine di trasformare il proprio business adottano il cloud in modo esteso, e che riconoscono come quella per la sicurezza sia una responsabilità da condividere, e non da devolvere esclusivamente al fornitore del servizio cloud. È un'esigenza che porta i responsabili della sicurezza e DevOps a richiedere strumenti automatici per diffondere in modo sicuro e rapido soluzioni per la sicurezza di account privilegiati, come nel caso della soluzione CyberArk Privileged Access Security per la protezione dei carichi di lavoro nel cloud AWS (Amazon Web Services).

Ma, aggiunge CyberArk, questo non basta. Le aziende che stanno migrando nel cloud e già usano soluzioni quali la CyberArk Privileged Access Security per proteggere il proprio ambiente on-premise, richiedono di poter disporre dei medesimi



e robusti criteri di sicurezza on-premise degli account privilegiati, nella gestione delle credenziali e dei secret, anche quando le operation avvengono in ambiente cloud.

CyberArk, la soluzione che protegge i privilegi nel cloud

Per abilitare una omogeneità nel trattamento degli utenti privilegiati e delle credenziali indipendentemente che l'utente si trovi ad operare on-premise o nel cloud, CyberArk ha sviluppato una suite di soluzioni per l'automazione delle operazioni che permettono ai responsabili della sicurezza di creare in pochi minuti, all'interno del cloud AWS di Amazon, un intero ambiente sicuro centrato sulla soluzione CyberArk Privileged Access Security. In base alle esigenze, l'ambiente di lavoro sicuro creato nel cloud tramite gli strumenti di CyberArk, può prevedere diverse funzioni e servizi. Per esempio può includere componenti e funzionalità di Digital Vault, la gestione delle sessioni e delle chiavi SSH, e un vault per il disaster recovery.



L'installazione standard della piattaforma CyberArk fa poi leva sulle best practice AWS per la sicurezza degli accessi privilegiati, compreso in questo zone AWS separate per i carichi di lavoro su cloud e digital vault primari e secondari per il disaster recovery, in modo da garantire l'indipendenza reciproca dei vault e la sicurezza dei carichi di lavoro.

Le possibilità di automazione delle operazioni nel cloud comprendono anche la funzione CyberArk AMI (Amazon Machine Images) e i template AWS CloudFormation, che permettono di automatizzare l'installazione delle soluzioni CyberArk. Per esigenze di alto livello e per operare in modo sicuro sul cloud Amazon, la piattaforma comprende anche template che permettono di creare cloud virtuali privati e sottoreti sia pubbliche sia private, security group e altro ancora.

Cloud sicuro e flessibile per migliaia di utenti

Un aspetto di base affrontato da CyberArk nell'approntare la propria soluzione per la sicurezza nel cloud è stato quello della flessibilità richiesta dalle aziende nel proprio percorso di migrazione. Il passaggio al cloud, soprattutto in grandi Enterprise o aziende distribuite su scala nazionale o internazionale, necessita della capacità di supportare un numero anche molto elevato di utenti.

In sostanza, osserva CyberArk, un punto chiave nel migrare sul cloud applicazioni e utenti privilegiati, è che si deve disporre di una

soluzione la cui configurazione sia semplicemente configurabile ma allo stesso tempo molto flessibile. Per garantirla, la piattaforma CyberArk per la sicurezza nel cloud prevede una configurazione standard che può essere installata in pochi minuti tramite gli strumenti automatici a disposizione e che di base abilita il supporto, su Amazon Web Services, potenzialmente di sino migliaia e migliaia di account privilegiati e di cloud virtuali (VPC: Virtual Private Cloud).

Architettura di sicurezza e cloud su misura

La flessibilità non si limita alla quantità ma si estende all'architettura cloud. La soluzione CyberArk può per esempio essere adattata a esigenze specifiche, ognuna con il suo carico di lavoro e impronta cloud, compreso tra queste ambienti cloud ibridi o misti.


In pratica, grandi aziende con ambienti IT complessi possono, al fine di installare le soluzioni di sicurezza CyberArk, realizzare un proprio ambiente AMI (Amazon Machine Images) invece di adottare il modello di riferimento standardizzato. La piattaforma per la sicurezza nel cloud di Cyberark è integrata anche con Amazon Inspector, in modo da rendere più semplice la individuazione e l'assegnazione delle priorità per quanto concerne i rischi degli account privilegiati. A questo si aggiunge una migliore protezione delle chiavi di accesso e un'integrazione con il servizio di sicurezza basato su token di Amazon che abilita il single-sign-on sicuro sulla console di gestione su AWS.*



SICUREZZA FISICA E INFRASTRUTTURE

Non solo i dati vanno protetti
e non tutti i dati sono digitali





Un ambiente di lavoro protetto in palmo di mano

di
Gaetano
Di Blasio

Biometria, servizi per la gestione di credenziali e privilegi d'accesso per la certezza dell'autenticazione con Fujitsu

Gli strumenti digitali rendono sempre più efficiente il lavoro degli information worker ma la tecnologia deve stare al passo con le nuove esigenze di flessibilità pretese dagli utilizzatori abituati a un uso dinamico di dispositivi mobili e applicazioni web.

Di fatto, possiamo osservare che gli utenti hanno accesso a molteplici sistemi e piattaforme varie. Per una massima efficacia e una maggiore efficienza, è importante che i dati giusti arrivino all'utente giusto, affinché possa svolgere il proprio lavoro al meglio. Ma non è solo una questione di produttività: si pone, infatti un cruciale problema di fiducia.

Fiducia, che verrebbe meno se non si avesse la certezza dell'identità di un utente con il quale si vuole comunicare, collaborare, chiudere una transazione e così via. Con Workplace Protect AD (WPP AD), Fujitsu estende la propria suite per la protezione e l'autenticazione dell'identità digitale, basata sulla tecnologia PalmSecure. Il software WPP AD abilita un sistema di accesso basato su Active Directory Windows a riconoscere i log-in con PalmSecure, attraverso qualsiasi rete.

L'autenticazione biometrica

La soluzione proposta, come accennato, espande la suite di autenticazione Fujitsu. Workplace Protect AD, infatti, sostituisce il login realizzato attraverso credenziali del provider Windows, mentre l'uso di PalmSecure con verifica biometrica sostituisce la password.

Le informazioni di autenticazione sono decifrate e passate all'Active Directory, se vengono abbinate a un template valido del palmo equindi riconosciute.

Per questo gli utenti dovranno essere registrati centralmente per ogni tipo di sensore PalmSecure che dovessero utilizzare. Infine, i modelli biometrici saranno memorizzati nell' Active Directory Service dell'impresa.

Una volta registrati, gli utenti potranno autenticarsi con uno username e con il palmo della mano in tutti i domini dell'organizzazione innalzando il sistema di sicurezza.

Il login biometrico è molto più sicuro di quello basato su una password, che è a volte facile da indovinare, quando non è scritta su un post-it attaccato allo schermo del pc o letta da un collega "curioso" mentre viene digitata.

Anche dando ingenuamente per scontato che questi comportamenti appartengono

al passato e che tutti sono più consapevoli dei rischi, ci sono cyber criminali in grado di "hackerare" anche le password più lunghe e complesse. Senza dimenticare i PIN di molti dispositivi basati su card, magari contact less, che sono tra i principali punti deboli per quanto riguarda i furti d'identità, come evidenziano i manager di Fujitsu.

Per questo Fujitsu ha progettato la tecnologia PalmSecure, che riconosce il disegno dei vasi sanguigni del palmo e non "semplicemente" un'impronta digitale. Da notare che il palmo non viene poggiato su alcuna superficie, quindi non ci sono problemi igienici.

Ma non solo: per prevenire azioni estreme degne dei thriller di Quentin Tarantino, il sistema consente l'accesso solo se rileva il sangue scorrere nelle vene.

L'affidabilità di riconoscimento, spiegano presso Fujitsu, è garantita dall'utilizzo di oltre 5 milioni di punti di riferimento che vengono mappati.

L'identità come servizio: Fujitsu IDaaS

È chiaro che questi dati devono essere gestiti con molta attenzione, altrimenti potrebbero finire in mano a malintenzionati, creando all'impresa grossi problemi, danni e perdita di denaro.

Fujitsu, che si occupa di ID management da decenni, ha ideato un servizio chiamato Fujitsu IDaaS (Identity as a Service), che è stato progettato per tenere sotto controllo e gestire in sicurezza le identità digitali degli utenti aziendali.

Il sistema è centrato sull'utente, in modo da massimizzare la sua esperienza. Del resto, le strutture, i modelli e gli ambienti d'organizzazione in un'impresa sono costantemente in evoluzione. Oggi, infatti, è usuale acquistare applicazioni web o servizi online, talvolta anche solo attivare un "trial" gratuito in cloud. Ciò determina generare username (spesso la mail aziendale) e password (magari sempre la stessa). Credenziali che vengono abbandonate se la prova non soddisfa le aspettative, ma restano sui sistemi.

Una gestione efficace

La criticità nella gestione delle identità digitali si accompagna frequentemente con oneri e costi elevati. La soluzione proposta da Fujitsu mette a disposizione delle imprese un servizio completo di identity management basato sulle identità già adottate. Le credenziali già in uso vengono salvate e mantenute nella directory dell'impresa, cui il sistema di Fujitsu si collega attraverso interfacce open standard.

In questo modo le imprese potranno utilizzare funzionalità avanzate di deployment e gestione end to end delle identità, quali: creazione, modifica e rimozione delle autorizzazioni previste per ogni utente, gestibili anche con interfacce



self-service, impostando una procedura per l'approvazione dei privilegi.

Ovviamente sta all'impresa decidere se assegnare la gestione a un help desk.

Le modalità di autenticazione previste sono diverse, da quelle più semplici alle varie possibilità di strong authentication. Molto utile è il single sign-on, che semplifica il lavoro all'utilizzatore finale e riduce gli oneri di gestione per ogni account.

La scalabilità è un'ulteriore caratteristica che differenzia il servizio e permette di aggiungere per ciascun utente, elementi distintivi, come per esempio privilegi e la loro gestione oppure il single sign on.

Il servizio può essere gestito interamente da remoto via Web e non richiede l'installazione di client.

Qualora si volesse integrare in servizio in piattaforme aziendali, come accennato sono disponibili strumenti open standard, come, per esempio, open SOA SAML (Security Assertion Markup Language), WS-Federation (Web Services Federation). *

Il GDPR e la protezione dei dati nei processi di stampa

Brother evidenzia le problematiche che le imprese devono affrontare per sostenere la conformità al regolamento dell'Unione Europea. Almeno 4 i punti critici

Concentrati sulla cyber security, molti manager e responsabili della sicurezza trascurano altri aspetti del GDPR (General Data Protection Regulation), che impongono una corretta gestione dei dati personali anche in ambito printing, assicurando che i processi di gestione della stampa e dei documenti siano conformi con la normativa.



Il GDPR, entrato in vigore nel 2016 ma lasciato in “sospeso” per dare tempo ai legislatori degli stati UE di adeguarsi, è diventato legge italiana con la pubblicazione sulla Gazzetta Ufficiale dell'8 agosto 2018. Le imprese rischiano quindi pesanti sanzioni (fino a 20 milioni di euro o il 4% del fatturato globale), in caso di violazione alla riservatezza dei dati, non solo quelli digitali.

Eppure, secondo una recente indagine di IDC, al momento in cui l'adeguamento avrebbe dovuto essere operativo, cioè lo scorso maggio, il 51% degli acquirenti di stampanti, non era consapevole che il GDPR

riguarda anche le attività di stampa. La stessa indagine ci rivela che il 40% degli acquirenti di stampanti, neanche sapeva cosa fosse il GDPR.

Un ulteriore 19% era a conoscenza del regolamento europeo, ma non delle scadenze.

Sono almeno quattro le principali criticità riguardo la sicurezza delle stampe e dei flussi documentali, come ci illustrano gli esperti di Brother che, insieme agli analisti di IDC, hanno recentemente pubblicato un white paper sull'argomento.

In particolare, gli autori evidenziano che occorre porre attenzione a:

1. uso improprio di dispositivi e documenti di stampa;
2. conservazione di dati su memorie interne a dispositivi (quali smartphone e altri device) o su memorie interne ai sistemi di stampa e/o acquisizione (come

- i buffer di memoria di stampanti, scanner, multifunzione o fax);
- 3. violazioni potenziali attraverso le porte di rete dei dispositivi;
- 4. mancata presa in consegna di documenti.

Un approccio proattivo

La protezione richiesta dal GDPR è “end to end”, quindi è condizione necessaria per la conformità avere un sistema di sicurezza che, a partire dalla rete, includa tutti gli endpoint, i quali rappresentano una porta di accesso al sistema informatico. Per questo è opportuno adottare un approccio proattivo, analizzando le potenziali vulnerabilità dell'ambiente printing e costruendo un piano avvalendosi di partner esperti e affidabili, per mitigare i rischi senza compromettere la produttività, come sottolineano in Brother.

Considerate le vulnerabilità delle infrastrutture per il printing, è opportuno che le aziende definiscano e concretizzino una sicurezza a più livelli. Ciò richiede di combinare molteplici fattori, che comprendono tanto funzioni specifiche quanto hardware e software, oltre a un ancor più importante processo educativo per gli utilizzatori.

Brother unisce funzionalità di sicurezza hardware, implementazione di strumenti software (come la stampa pull) e la formazione degli utenti sulle prassi di stampa responsabili e sicure per costruire una politica globale di protezione a misura di ogni esigenza.

Il primo passo di un approccio olistico è quello di considerare tutta l'intera flotta di periferiche. Non

è banale, perché in molte imprese si trovano numerosi dispositivi nei posti più disparati. Vanno gestiti e tenuti tutti sotto controllo indipendentemente dal modello, dalla marca, e dalla tecnologia di stampa. Per questo è consigliabile affidarsi a un partner qualificato ed esperto.

Le virtù di un ambiente printing protetto secondo Brother

Come tutti i dispositivi collegati in rete, anche quelli per il printing devono prevedere controlli che regolino l'accesso al network aziendale, gestiscano l'uso di protocolli e porte e prevengano potenziali virus e malware. Per questo è opportuno accertarsi che tutti i dispositivi usino solo protocolli di scambio dati criptati. Alcune serie di stampanti Brother sono in grado di bloccare a distanza chiunque acceda al dispositivo tramite la rete, filtrando gli indirizzi IP e sfruttando il controllo dei protocolli, che consente agli amministratori di disattivare quelli che non sono necessari, senza bloccare completamente l'accesso a tutte le funzioni, come FTP o SMTP. Occorre inoltre utilizzare standard di gestione nel controllo degli accessi in rete tramite switch conformi al protocollo 802.1X che richiedono credenziali prima dell'accesso ai servizi in rete.

La crittografia del disco rigido apporta un successivo livello di sicurezza sia durante l'utilizzo attivo del dispositivo, sia rispetto la riservatezza del precedente job di stampa.

Oltre la crittografia, è importante anche la sovrascrittura, che è necessaria sia per la manutenzione periodica del dispositivo sia in caso si debba spostare il dispositivo in un altro ufficio o lo si debba dismettere e smaltire. Con i kit di sovrascrittura è possibile eliminare tutti i dati di scansione, stampa, copia e fax memorizzati nel disco rigido.

Le macchine laser di fascia alta Brother sono tutte dotate della funzionalità di sicurezza TLS/SSL criptati con crittografia RSA e DSA, due dei possibili standard. Una alternativa è scegliere dispositivi che non necessitano di dischi fissi per l'esecuzione delle operazioni di stampa, come buona parte degli apparati Brother.

Un aspetto importante riguarda l'implementazione del processo per l'autenticazione dell'utente. Il monitoraggio di chi e cosa viene stampato è basilare per mantenere il controllo del flusso documentale e controllare i costi. Tramite schede di identificazione NFC o Pin è possibile ridurre di molto il rischio che stampe di documenti sensibili restino incustodite o abbandonate nei cassette della stampante. Grazie al pull printing, che autentica l'utente, i documenti vengono rilasciati solo al destinatario autorizzato.

Con adeguati strumenti di tracciamento, in caso di una violazione l'azienda è in grado di dimostrare che ha adottato le giuste misure per proteggere tutti i dispositivi collegati in rete.

Tipicamente è l'utente che guida il processo documentale, pertanto



le aziende devono mantenere aggiornata una mappatura dell'infrastruttura documentale esistente per ciascun utente, delle modalità di utilizzo, della produzione e scambio di documenti per garantire un'effettiva comprensione dei flussi documentali e supportare i flussi di business.

Un decalogo per le imprese

Per aiutare le aziende a proteggersi dalle vulnerabilità legate alla stampa, Brother ha realizzato, con IDC, un White Paper intitolato "Garantire la riservatezza dei dati: una crescente sfida per la gestione della stampa e dei documenti".

In particolare, gli esperti di Brother e di IDC hanno definito una lista di dieci azioni - come per esempio audit trail, accesso protetto e sicurezza dei dispositivi - che i responsabili aziendali dovrebbero considerare come parte integrante di una governance e di un business più sicuri, per la conformità alle normative sulla riservatezza dei dati.

Le linee guida per garantire per

garantire l'adempimento alla normativa riguardante la stampa e la gestione dei documenti sono disponibili sul sito Brother.it

L'implementazione di processi più efficienti volti ad adempiere alla conformità può portare anche a risparmi di costo.

Oltre la privacy: un dato perso è un dato sprecato

Brother e IDC mettono in guardia le imprese, perché, di fatto, un ambiente di stampa non protetto è sinonimo di un ambiente IT non sicuro. Al di là delle sanzioni, però, la gestione dei dati residenti su carta assume un'importanza crescente per il business. Gli analisti IDC sostengono che entro il 2025 la quantità di dati creati, acquisiti e replicati, crescerà fino a 163 zettabyte (ZB) o 163 trilioni di gigabyte (GB), dieci volte i 16,12 ZB di dati generati nel 2016.

La capacità di estrarre informazioni da questi dati può aiutare sia ad attirare sia a mantenere i clienti, ottimizzandone l'esperienza. Però occorre il massimo livello di accuratezza delle informazioni riguardanti un cliente, al fine di profilare le esigenze e fornirgli la miglior experience possibile.

L'efficacia di un ambiente di printing e document management è certamente basata sulle tematiche sopra illustrate riguardanti la sicurezza e la gestione dei flussi documentali, ma prosegue con l'implementazione di strumenti e soluzioni che consentono di sfruttare appieno le informazioni contenute nei documenti cartacei che, quindi, devono poter "rientrare" nel flusso informativo aziendale.

Per questo Brother mette a disposizione soluzioni e servizi ad hoc, come *Pagine+ Cloud*, un servizio di stampa gestita pensato per le piccole e medie imprese, oppure come

Barcode Utility, una soluzione progettata da Brother per migliorare l'acquisizione, l'indicizzazione e la sicurezza dei flussi documentali, in particolare quando si tratta di gestire grandi volumi di scansioni.

✱



TalkTalk si affida a Nuance per trasformare l'esperienza cliente

di
Paola
Saccardi

La società di telecomunicazioni introduce sia l'instradamento automatico delle chiamate basato sul linguaggio naturale sia la biometria vocale

Tal Talk è una società di telecomunicazioni che possiede 4 milioni di clienti, fornisce un prodotto Quadruple Play (servizi vocali a linea fissa, banda larga, mobile e TV) e gestisce un contact center globale con 4.500 operatori distribuiti tra Regno Unito, Filippine, India e Sud Africa.



Nel corso del tempo, TalkTalk ha raggiunto un enorme livello di complessità, con più offerte di prodotti e più sistemi di fatturazione che avevano portato a un'esperienza clienti deludente. Ciò ha spinto l'azienda a intraprendere una serie di iniziative tra cui il consolidamento dei sistemi di fatturazione in un'unica piattaforma, la razionalizzazione dei propri contact center e l'introduzione di un'unica piattaforma telefonica su tutti i siti. Il passo successivo è stato lo

sviluppo di un sistema di risposta vocale (IVR) interattivo. L'azienda si era posta l'obiettivo di semplificare l'utilizzo del canale vocale, fornendo un'esperienza semplice per i clienti e introdurre un servizio self-service facile da usare. TalkTalk voleva inoltre creare una piattaforma self-service che potesse essere estesa a sistema IVR, online, app mobile e chat dal vivo e un'esperienza self-service che ponesse il cliente completamente al centro, sicura e affidabile, e garantisse un percorso omnicanale coerente con interazioni intelligenti.

Nel 2014 ha deciso di eliminare la navigazione tra i vari livelli di opzioni all'interno del sistema IVR implementando la soluzione di instradamento automatico delle chiamate basato sul linguaggio naturale di Nuance che ha potenziato nel 2016 tramite l'autenticazione e la verifica con biometria vocale. Nuance Natural Language Call Steering (NLCS) è una soluzione che utilizza la comprensione del linguaggio naturale e avanzate strategie di dialogo.

Per implementare la soluzione Nuance Call Steering, TalkTalk ha collaborato con Nuance per dare forma a circa 400 intenti e consentire ai clienti di esprimere liberamente le proprie necessità per poi essere trasferiti all'operatore o risorsa self-service più adeguata. La soluzione NLCS ha aumentato l'utilizzo del servizio self-service del 30% e migliorato l'esperienza dei chiamanti. Inoltre i tempi di chiamata sono stati ridotti di 26 secondi e i trasferimenti tagliati del 16%.

Talk Talk necessitava inoltre di identificare e verificare la propria clientela pertanto si è affidata alla biometria vocale Nuance per aumentare il livello di automazione intelligente. L'operatore ha scelto la soluzione di autenticazione con biometria vocale attiva VocalPassword per fornire il proprio servizio TalkSafe che consente al cliente di effettuare la registrazione utilizzando un'impronta vocale unica tramite il sistema IVR per verificare l'identità del cliente.

TalkTalk ha raggiunto una percentuale di adozione di TalkSafe da parte dei clienti pari all'85%. Il tempo di autenticazione è risultato di soli 12 secondi riducendo il tempo medio di gestione da parte degli operatori di un minuto a chiamata. *

La biometria previene le frodi e semplifica l'autenticazione utente

Con Nuance maggiore sicurezza e migliore user experience, evitando problemi ed errori dei tradizionali username e password o PIN

Secundo Grand View Research, il mercato globale delle tecnologie biometriche è destinato a sfiorare i 60 miliardi di dollari entro il 2025 grazie alla crescita della domanda da parte del settore pubblico, privato e imprenditoriale. Negli ultimi anni l'integrazione delle innovative tecnologie biometriche nei dispositivi personali è stata sempre più frequente e pervasiva: si è partiti dal riconoscimento delle impronte digitali su pc e smartphone, fino ad arrivare ai più recenti sistemi di riconoscimento vocale e facciale e di scansione dell'iride, nonché all'ultima frontiera dell'autenticazione comportamentale.

La biometria vocale e gli ambiti di applicazione

Anche gli ambiti nei quali le tecnologie biometriche trovano applicazione si sono moltiplicati e Nuance Communications, pioniera nello sviluppo della tecnologia di riconoscimento vocale, è costantemente impegnata per essere all'avanguardia e rispondere alle richieste di ciascun settore.

Barclays, HSBC, Vodafone e alcune banche italiane, tra cui Widiba sono solo alcuni esempi di banche in cui l'adozione delle soluzioni biometriche di Nuance ha permesso di fornire agli utenti l'autenticazione biometrica come token per accedere ai propri conti online, oltre ad abilitare maggiore sicurezza, semplicità di utilizzo e risparmio di tempo.

Fin dal suo esordio nello sviluppo di soluzioni di intelligenza artificiale, il settore automotive è per Nuance uno dei principali mercati verticali, e, oggi, l'azienda arriva a servire praticamente tutti i brand automobilistici a livello globale, tra cui Mercedes, BMW e Ford, con un assistente automotive che permette a conducenti e passeggeri di attivare, tramite il solo utilizzo della voce, richieste di navigazione, musica, intrattenimento, informazioni e altre funzionalità dell'auto.

Un ulteriore settore di applicazione importante per Nuance è il customer service, dove l'intelligenza artificiale (AI) e la tecnologia vengono messi al servizio delle aziende. L'integrazione dell'AI e del dialogo ha, infatti, già iniziato a rivoluzionare il modo in cui le persone ricevono assistenza, rispondendo alle molteplici esigenze di semplificazione, velocità, efficacia e gradevolezza dell'interazione. La soluzione

NINA di Nuance, per esempio, fornisce un'esperienza di customer service omnicanale sotto forma di dialogo dalle caratteristiche umane, garantendo accesso rapido e semplice alle informazioni di cui clienti e operatori del servizio assistenza necessitano. In questi e in altri ambiti, Nuance gioca una partita importante grazie anche alle partnership con player internazionali che completano la sua offerta e con i quali sviluppa soluzioni specifiche.

La biometria per la smart security

Al momento la biometria è riconosciuta come tecnologia d'avanguardia in grado di aiutare le imprese ad abbattere il rischio di frodi e scongiurare accessi non autorizzati a dati sensibili e asset aziendali.

Con hacker e cybercriminali che stanno diventando sempre più abili e sofisticati la sicurezza dei dati diventa una prerogativa da tutelare.

Anche se nessuna soluzione è sicura al 100%, Infiniti Research stima che la biometria vocale possa prevenire il 90% delle frodi in un canale vocale e oltre l'80% delle frodi in un canale mobile. L'autenticazione biometrica vocale di Nuance, in particolare, sfrutta più di 100 caratteristiche del parlato proprie di ciascuna identità: sia gli attributi puramente fisici sia quelli comportamentali che includono accento, pronuncia o anche la velocità della conversazione.

Se un cybercriminale dovesse hackerare un database di voiceprint, i dati non potrebbero essere convertiti in voci utilizzabili per hackerare account e anche nel malaugurato

caso in cui venisse rubata una registrazione della voce, la tecnologia di rilevamento del playback di Nuance è in grado di testare l'audio in entrata e verificare se rappresenta il parlato dal vivo.

Eventuali impronte vocali o registrazioni sono quindi inutili per gli hacker, anche qualora il database dell'azienda venisse violato. Sebbene i nuovi metodi delle tecnologie vocali sintetiche siano in grado di creare rapidamente una voce, lo fanno a scapito della qualità. Queste voci artificiali hanno toni robotici che possono essere identificati dai sistemi di Nuance, anche se questi differenziatori non sono percepibili dall'orecchio umano.

I dati biometrici non possono essere contraffatti né duplicati e, se integrati con i dati comportamentali, aggiungono ulteriori livelli di sicurezza, impedendo, per esempio, l'utilizzo di impronte o registrazioni illecitamente sottratte, mentre, in termini di user experience, aggiungono nuovi aspetti di usabilità e di semplicità.

Ad oggi Nuance registra oltre 300 milioni di consumatori che hanno realizzato 5 miliardi di autenticazioni vocali di successo utilizzando la propria tecnologia biometrica. Questo "boom biometrico" è stato ulteriormente confermato dalla società d'analisi Forrester Research, evidenziando che le soluzioni biometriche hanno suscitato notevole attenzione da parte del consumatore sia per l'autenticazione sia per la prevenzione delle frodi e che



con l'incalzare della loro adozione accelereranno la scomparsa delle password, meno sicure e meno user-friendly.

Inoltre, da un recente studio di Forrester Consulting datato luglio 2018 volto a quantificare l'impatto economico totale e i vantaggi della soluzione Nuance Security Suite, che consente alle organizzazioni di autenticare i consumatori e prevenire le frodi tramite la tecnologia biometrica, è emerso che una banca multinazionale, che rientra nella lista Fortune 100, in tre anni ha risparmiato 24 milioni di dollari in termini di potenziali danni causati da attacchi informatici, grazie all'adozione di questa soluzione.

Oltre a migliorare la sicurezza e l'efficacia nella prevenzione delle frodi, la biometria sta migliorando il livello di soddisfazione dei clienti. Abilitando l'autenticazione vocale, facciale, comportamentale e delle impronte digitali, la tecnologia offre ai clienti metodi più rapidi e sicuri per autenticare la propria identità. I nuovi consumatori sono alla ricerca di maggiore praticità e scelta nei modi in cui comunicano con un'azienda, soprattutto per quanto riguarda i servizi finanziari, e sono ora abituati ad accedere ai loro servizi bancari senza interruzioni tramite l'attivazione vocale. ✱

Oltre la sorveglianza con la cattura e l'analisi dei dati

di
Gaetano
Di Blasio

Western Digital fornisce sistemi specializzati e per la memorizzazione di riprese video e la loro analisi, nonché l'integrazione di soluzioni avanzate

Una sorveglianza efficiente non può esaurirsi nella ripresa video e necessita di tecnologia avanzata in grado di supportare le esigenze di sistemi integrati.

Per questo in Western Digital sottolineano che "sorveglianza non significa vedere, ma vedere oltre".

Pensiamo a una telecamera di sicurezza che serve per monitorare l'ingresso di un'azienda, come un supermercato aperto 24 ore su 24 o un altro esercizio commerciale (una farmacia?) o pubblico (una stazione?). In ogni caso deve essere garantito il funzionamento e l'affidabilità, altrimenti le immagini saranno inutili. Non è banale, perché i dati delle riprese devono essere memorizzati, la loro qualità preservata.

Occorre archiviare e analizzare dati usando la tecnologia più adatta, stando al passo con i tempi, per esempio utilizzando videocamere 4K.

Ma il punto più delicato è lo strato infrastrutturale della soluzione, perché se

la capacità di memorizzazione è scarsa, se le condizioni climatiche danneggiano il sistema, se i video presentano difetti che non permettono di decifrare le immagini, la sorveglianza è inutile.

WD fornisce sistemi e soluzioni per catturare, archiviare e analizzare tutti i dati relativi a un sistema di sorveglianza di ultima generazione.

Le unità WD Purple

Le unità WD Purple sono state progettate e costruite per sistemi di sicurezza ad alta definizione, destinati a funzionare ininterrottamente per 24 ore, 7 giorni su 7.



Lo storage di video sorveglianza WD Purple, disponibile con capacità da 1 a 12 Terabyte fornisce l'esclusiva tecnologia AllFrame, che consente di migliorare le riprese video, riducendo gli errori, le immagini "pixellate" e le interruzioni dei video che possono verificarsi nei sistemi di videoregistrazione. Inoltre, migliora lo streaming ATA per ridurre la perdita di fotogrammi, ottimizzare la riproduzione video generale e aumentare il numero di alloggiamenti dell'hard disk supportati all'interno di un NVR.

Le unità WD Purple, evidenziano presso la casa madre, hanno un tasso di workload ottimizzato fino a 180 Terabyte per anno (circa il triplo rispetto alle unità desktop), ma che può arrivare fino a 360 Terabyte per anno.

Supportano poi, sistemi per una registrazione video continua h24, con un massimo di 64 telecamere collegate.

Le soluzioni si adattano a diverse tipologie d'utilizzo in ambito videosorveglianza, da quella domestica a quella ad alta risoluzione, per esterni, che resiste ad alte temperature e prevede una registrazione continua.

Le unità sono state progettate per durare nel tempo (presentando un mean time between failure, cioè il tempo medio fra due guasti, fino a 1,5 milioni di ore, disponendo già di tecnologie di prossima generazione e permettendo di espandere il sistema di sicurezza.

Ricordiamo, inoltre la disponibilità di unità con 8 alloggiamenti e di componenti anti ossidazione,



adatti per sistemi di grandi dimensioni e per ambienti con condizioni difficili. Già alla quarta generazione, si trova la tecnologia Helioseal collaudata sul campo, che fornisce la capacità per la registrazione in 4K. Si tratta di una tecnologia consolidata, come dimostrano le oltre 27 milioni di unità vendute, secondo i dati forniti dal costruttore. Caratteristica importante è anche l'ampia compatibilità, che rende più semplice integrare soluzioni, anche grazie a una maggiore possibilità di implementare componenti aggiuntive per arricchire il sistema di videosorveglianza. Da questo punto di vista, va segnalata anche la disponibilità di numerosi case supportati, che consente di trovare la configurazione giusta per le proprie soluzioni. Apprezzabile sotto diversi punti di vista, la tecnologia Intellisek di

Western Digital, grazie alla quale le unità WD Purple sono in grado di calcolare le migliori velocità di ricerca e di mantenere basso, così, il consumo energetico, quindi anche, a seguire, il rumore e le vibrazioni. La garanzia, limitata, è inclusa per tre anni.

La scheda microSD WD Purple

Un'accurata analisi delle ultime tre generazioni di prodotti industriali dedicati alla sorveglianza, ha portato alla realizzazione della scheda microSD WD Purple, che, come evidenziano in Western Digital, si distingue per l'elevata resistenza e una capacità

fino a 256 Gigabyte. Rappresenta uno storage on camera a lunga durata. Tra le caratteristiche interessanti, figura il supporto della funzionalità per il monitoraggio dell'integrità. Questa è disponibile anche in modalità utilizzabile per la gestione preventiva. I tecnici di Western Digital evidenziano le elevate prestazioni e l'alta affidabilità, opportuna per il workflow continuo durante la registrazione video ad alte prestazioni, richiesto da un numero sempre più crescente di applicazioni per la sorveglianza 24x7.

Altri ambiti di applicazione comprendono il supporto di memoria per applicazioni in ambito edge computing, a favorire lo sviluppo dell'Internet delle cose.

Da segnalare la robustezza, con il supporto di temperature da meno 25 gradi centigradi a più 85°. ❄

Come proteggere gli ambienti industriali e OT

di
Giuseppe
Saccardi

Cyber Shield è una soluzione di RAD e fornita da CIE Telematica che protegge la sede centrale, le sedi periferiche e le comunicazioni di un ambiente industriale

L'informatizzazione degli ambienti produttivi si trova ad affrontare la sfida di come proteggere gli impianti critici distribuiti e interconnessi tramite reti dati e IP.

Un problema, osserva Luigi Meregalli, general manager di CIE Telematica, che è stato affrontato da RAD, società di cui CIE Telematica è rappresentante in Italia ed opera come system integrator nel campo delle reti industriali, smart city, di accesso e per la sicurezza industriale.

RAD, che ha in atto da anni un accordo strategico con Check Point, ha affrontato il problema della sicurezza di impianti industriali alla radice, sviluppando Cyber Shield, una soluzione che abbina tecnologie RAD e Check Point ideata per la protezione di siti industriali e impianti remoti, e, in particolare, di tipo SCADA.

La soluzione è costituita da tre elementi chiave per la security industriale. Il primo è il dispositivo SecFlow di RAD disponibile nelle versioni SecFlow-1/SecFlow-2, il quale espleta la funzione di switch e di router sicuri in ambienti SCADA presso le sedi remote.

Il secondo è Check Point



Luigi Meregalli, general manager di CIE Telematica

Security Gateway, un dispositivo con funzione di gateway per la sicurezza di sistemi di controllo di impianti industriali. È specificatamente adatto per la protezione da vettori di attacco cibernetico diretti sia verso il piano di gestione sia SCADA. Opera a livello centrale e si posiziona tra la rete SCADA e la rete multiservizio usata per la connessione degli impianti e delle sedi remote.

Il terzo elemento è RADview Management and Domain Orchestration, un sistema di gestione che offre un'elevata visibilità della rete, dei suoi elementi, degli eventi e che abilita funzioni di orchestrazione. Si

posiziona a livello centrale ed è protetto da cyber attacchi dal Checkpoint Security Gateway. Due le incarnazione della soluzione: Cyber Shield for management traffic (NERC CIP Intermediate System); Cyber Shield for SCADA traffic. In particolare, le funzioni:

- permette di aggiornare le reti OT (Operational Technology) con sistemi che assicurano un accesso sicuro agli impianti da locale o da remoto, opera come firewall "SCADA aware", mette a disposizione funzioni per la prevenzione delle intrusioni, previene attacchi di tipo man-in-the-middle, cripta le comunicazioni, controlla la connessione di dispositivi, provvede al log degli eventi e rileva le anomalie comportamentali.
- Si adatta alle diverse tipologie di architetture di reti OT e di connettività di dispositivi ICS/SCADA, sia seriale sia TCP.

"Cyber Shield è la soluzione più economicamente vantaggiosa e completa sul mercato, è ideale per la sicurezza operativa delle Public Utility, nei trasporti e nell'ambito governativo, dove abilita un'elevata sicurezza senza dover ricorrere a soluzioni multi-box complicate da integrare, gestire e mantenere", ha evidenziato Meregalli. ✱



LA SICUREZZA INTELLIGENTE

Sistemi automatici e strumenti avanzati

L'Enterprise Security di Micro Focus per prevenire anziché rimediare

Micro Focus Security propone un approccio alla sicurezza basato su tecnologie di analytics e machine learning per garantire la protezione di utenti, applicazioni e dati

La rivoluzione digitale sta cambiando il modo di fare business. Oggi, la più grande catena di distribuzione non possiede negozi, la prima azienda di trasporti con conducente non ha un parco auto, la principale organizzazione di hospitality non è proprietaria di alcun albergo e il più importante creatore di contenuti non dispone neppure di un giornalista. Questo rinnovamento dei modelli di business offre certamente nuove opportunità, ma porta con sé anche nuove sfide che richiedono un ripensamento nell'approccio alla sicurezza.

Protagonisti nell'Enterprise Security

Nel 2017 il merge tra HPE Security e Micro Focus ha dato vita alla settima azienda di software al mondo, con un fatturato di oltre 4 miliardi di dollari.

All'interno delle sette business unit di Micro Focus, la Security contribuisce per circa il 25% al fatturato complessivo dell'azienda e riveste un ruolo centrale nella sua strategia complessiva.

«Le soluzioni di Micro Focus forniscono una risposta efficace ai problemi che affliggono i responsabili della sicurezza aziendale - sottolinea Pierpaolo Ali, Director Southern Europe di Micro Focus Security - come l'aumento esponenziale delle minacce, il sovraccarico di dati, le nuove normative sempre più stringenti come il GDPR e la crescente complessità di gestione delle infrastrutture. Per affrontare queste sfide è necessario abbandonare vecchie logiche di difesa di un perimetro aziendale che non esiste più, puntando invece ad anticipare le mosse del cyber crimine. Per farlo è necessario agire su più dimensioni: quella dei dati, delle applicazioni e degli utenti».

Per rispondere a queste esigenze Micro Focus ha predisposto una gamma di soluzioni per l'Enterprise Security organizzate in famiglie di prodotti che possono essere utilizzati in modalità standalone, ma che forniscono i migliori risultati quando operano in modo integrato, utilizzabili sia on-premise sia all'interno di ambienti IT ibridi.



Pierpaolo Ali, Director
Southern Europe di Micro
Focus Security

L'insieme di queste soluzioni compone un modello di protezione integrata, predittiva e dato-centrica all'interno del quale si inseriscono strumenti di Data Analytics (tra cui spicca il "motore" Vertica, portato in dote da HPE Software) e di Machine learning, che consentono di individuare le nuove modalità di attacco e rispondere in modo predittivo a minacce sempre più sofisticate.

ArcSight e Voltage per una sicurezza "smart"

Con le soluzioni ArcSight Micro Focus realizza una sicurezza preventiva, basata su tecnologie di Security intelligence in grado di interpretare i segnali e le tracce che ogni tentativo di attacco porta con sé e predisporre contromisure adeguate prima che vengano arrecati danni.

La piattaforma ArcSight riceve grandi volumi di dati di sicurezza generati da differenti tecnologie di protezione, da sistemi operativi, da applicazioni e altre fonti. Analizza in tempo reale questi dati utilizzando tecnologie di data analytics e machine learning alla ricerca di possibili segni di compromissione, attacco o altre attività dannose, per inviare avvisi agli amministratori e avviare processi automatizzati di risposta.

Al tema della data security Micro Focus indirizza la famiglia Voltage SecureData, che mette

a disposizione strumenti per la cifratura e la Tokenization, per la gestione delle chiavi di cifratura e la sicurezza della messaggistica basati su tecnologie innovative e brevettate.

Applicazioni sempre protette con Fortify

Le applicazioni rappresentano il vettore privilegiato per gli attacchi di nuovo tipo.

Alla protezione applicativa si indirizza la famiglia Fortify, che raggruppa una serie di strumenti pensati per favorire uno sviluppo sicuro, che elimini alla fonte le possibili vulnerabilità in base al principio che è più efficace e conveniente proteggere le applicazioni mentre sono in fase di sviluppo, che farlo dopo che sono state rilasciate.

Le soluzioni Fortify integrano la sicurezza all'interno del ciclo di sviluppo del software fornendo l'analisi statica del codice, il test dinamico della sicurezza applicativa, la predisposizione di tecnologie di Runtime Application Self-Protection (RASP) che auto-proteggono l'applicazione dall'interno.

«La sicurezza va integrata by design all'interno delle applicazioni - puntualizza Ali -, che devono essere costantemente testate e aggiornate durante il loro intero ciclo di vita. Le soluzioni Fortify permettono di accelerare questo ciclo aumentando il time-to-value».

Governance di identità e accesso con NetIQ

Attraverso le soluzioni NetIQ Micro Focus abilita una governance degli accessi intelligente, ma semplice, combinando i requisiti di autenticazione con la gestione del rischio e rafforzando il principio di fornire all'utente il livello di privilegi minimo necessario per lo svolgimento dei suoi compiti.

«Per prevenire minacce interne e attacchi mirati è importante porre attenzione specifica alla gestione degli utenti con privilegi - spiega Ali -, perché l'accesso ad account privilegiati può potenzialmente esporre l'organizzazione a un rischio molto elevato. È importante acquisire la consapevolezza che alcuni addetti ai lavori abuseranno dei loro privilegi e che attaccanti creativi ben finanziati possono riuscire a ottenere credenziali interne privilegiate».

Anche al centro delle soluzioni NetIQ vi sono innovative tecnologie di analytics, che rappresentano la componente abilitante per la realizzazione di un modello di sicurezza basato sull'identità che Micro Focus chiama Identity-Powered Security. ✱



La cyber resilienza per creare un ecosistema di fiducia

Cisco fornisce la tecnologia e propone una strategia per rendere resiliente un'impresa imparando ad affrontare l'eventualità di un attacco informatico

Cisco è impegnata nel costruire soluzioni fidate che integrino la sicurezza digitale attraverso piattaforme multiple, ma, prima di affidarci a tecnologie intelligenti, capaci di rilevare i problemi e risolverli autonomamente, grazie all'uso dell'intelligenza artificiale, occorre modificare l'approccio alla security. Il cloud, la mobilità, l'Internet of Everything (IoE), i social media, insieme alle recenti strategie commerciali digitali, hanno aiutato molte imprese a trasformare il loro business, ma hanno anche contribuito ad aumentare la superficie di attacco. La sicurezza perimetrale è insufficiente, essendo del resto impossibile delineare un perimetro ben definito.

Le aziende sanno che subiranno attacchi e devono, quindi, adottare un approccio resiliente: la classica foglia che si piega ma non si spezza.

Per questo si deve passare da una strategia reattiva a una proattiva e affrontare i rischi informatici con fiducia.

Lo scenario attuale vede le imprese raccogliere e analizzare numeri crescenti di dati, per ricavare informazioni le quali alimentano il business, l'innovazione e la collaborazione, anche grazie a tecnologie, come IoE, cloud computing, mobile computing e altre che accelerano il ritmo del cambiamento, diventando indispensabili.

Intanto le minacce aumentano in «questo contesto di iper-collegamento», come osserva Chuck Robbins, Ceo di Cisco che afferma: «Mentre pensiamo a questo nuovo mondo e ai sistemi intrecciati che si stanno creando, è necessario un nuovo livello di fiducia, al di là di qualsiasi cosa nella nostra storia. Dobbiamo

fidarci dei sistemi che gestiscono ed elaborano i dati, delle persone e dei partner che accedono ai dati e delle tecnologie e dei processi fondamentali che proteggono i dati».

La resilienza informatica è la capacità di prepararsi e adattarsi alle mutevoli condizioni di minaccia, resistendo e recuperandosi rapidamente dagli attacchi che limitano la disponibilità delle infrastrutture.

I concetti di resilienza informatica afferiscono in gran parte alla gestione dei rischi: identificazione degli eventi che potrebbero accadere, valutazione della loro probabilità di accadere e del loro impatto, fino alla decisione sulle azioni da intraprendere.

Rischi e costi

In azienda si è abituati a bilanciare rischi e costi. Gli enormi vantaggi competitivi della digitalizzazione vanno confrontati con l'esposizione ai rischi e ai costi della sicurezza informatica. A tal riguardo, secondo una ricerca promossa da Cisco, il costo medio consolidato, nel 2015, di una violazione alla sicurezza è stato di 3,8 milioni di dollari, con un aumento del 23% dal 2013. Il trend si è mantenuto in salita, ma il problema è che, per le aziende che non possono fare affidamento sulla disponibilità della loro infrastruttura informativa a seguito di un attacco informatico, i costi continueranno ad aumentare nei giorni, nelle settimane e nei mesi successivi alla violazione.

Il panorama delle minacce non rassicura e gli attacchi si fanno sempre più sofisticati:

Solo nella prima metà del 2015, Gemalto ha scoperto che il 41% dei quasi 246 milioni di record infranti in tutto il mondo sono il risultato di attacchi altamente sofisticati e taluni sono sponsorizzati dagli stati.

Non dovrebbe sorprendere che il 65% degli intervistati a un recente studio di Cisco, "Security Risk and Trustworthiness Study", ha rivelato che le organizzazioni si trovano ad affrontare un livello significativo di rischio per la sicurezza.

L'inevitabilità degli attacchi che si annunciano sempre più efficaci deve spingere le organizzazioni verso la resilienza informatica.

Le misure di resilienza informatica possono aiutarli a resistere, reagire e riprendersi da violazioni alla sicurezza potenzialmente catastrofici.

Vantaggi di un'architettura cyber resiliente

La risposta agli incidenti è ancora più efficace con un'architettura resiliente, per questo le organizzazioni stanno esplorando la possibilità di passare da una semplice focalizzazione sui controlli di sicurezza informatica, che proteggono computer, reti, programmi e dati, a architetture di resilienza informatica, che automaticamente sono in grado di proteggere le infrastrutture e ripristinare rapidamente e, a tendere, in tempo reale, la piena operatività. ❁

Ecco 6 domande che dovrebbero porsi i consiglieri d'amministrazione

Le strategie in un'azienda devono godere del supporto da parte degli amministratori, ancor di più su temi vitali come la sicurezza informatica.

Ecco i quesiti che i membri del board dovrebbero affrontare:

- 1 Abbiamo effettuato una valutazione approfondita della nostra infrastruttura IT?
- 2 Qual è l'attuale livello di rischio informatico e il potenziale impatto aziendale dei rischi informatici sulla nostra azienda?
- 3 La nostra strategia di cyber resilienza è focalizzata sui nostri obiettivi di business, proteggendo i nostri asset e ricavi più critici e garantendo la continuità aziendale?
- 4 In che modo il nostro programma di cyber security applica gli standard e le best practice del settore e come si confronta con quelli dei colleghi del settore?
- 5 Come misuriamo l'efficacia del nostro programma di cyber security?
- 6 La nostra funzione di cyber resilienza è organizzata, formata, equipaggiata, dotata di personale a sufficienza e finanziata in modo appropriato?

Aeroporti di Puglia rinnova le reti WAN con Cisco

di
Paola
Saccardi

Per offrire un miglior servizio a clienti dell'aeroporto e al personale interno, sono state realizzate connessioni WAN più affidabili e sicure

Le connessioni WAN sono sempre più un aspetto cruciale e centrale negli aeroporti sia per offrire un'esperienza positiva ai clienti, come navigare sul web o effettuare il check-in, sia per lo stesso personale che lavora all'interno. Senza la giusta infrastruttura e servizi infrastrutturali, gli aeroporti faticano a trovare l'affidabilità di cui hanno bisogno e il personale IT è costretto a dedicare il proprio tempo alla manutenzione invece di risolvere altri problemi.

Un esempio lo testimonia Luigi Campese, IT Manager di Aeroporti Di Puglia Spa, che spiega: «Per molto tempo all'aeroporto, la nostra infrastruttura di rete WAN è stata inaffidabile e non veramente sicura. Semplicemente non potevamo contare sulla nostra rete per rimanere in piedi quando ne avevamo più bisogno. La nostra configurazione era costituita da router e switch di base, invece che da una legittima infrastruttura IT. Ciò di cui avevamo bisogno era una solida base e il nostro personale meritava di meglio. In qualità di IT Manager, era mio compito sistemarlo».



Una rinnovata focalizzazione

Le difficoltà riscontrate da Aeroporti di Puglia hanno portato a mettere in atto un cambiamento per ricostruire correttamente le fondamenta.

«Avevamo anche bisogno di dare priorità alla sicurezza. I dati che passano attraverso le nostre reti sono troppo importanti. Non avevamo nemmeno i firewall sulle connessioni WAN. Per i nostri switch e router, abbiamo scelto il leader del settore Cisco. Ci siamo anche rivolti a Cisco Prime e Cisco ISE per gestire in modo più efficace e monitorare in tempo reale la nostra rete. Dal punto di vista della sicurezza, sapevamo di voler utilizzare anche un prodotto Cisco poiché riteniamo importante avere coesione all'interno delle nostre operazioni IT. Ecco perché abbiamo scelto la soluzione

che consideriamo leader del settore: Cisco FirePOWER» ha spiegato Campese.

Con l'aiuto di Cisco la società ha potuto implementare le nuove soluzioni e soddisfare gli standard stabiliti anche negli aeroporti gemelli. «Grazie a Cisco e al loro partner Security Architect, siamo stati in grado di sostituire la nostra infrastruttura esistente in due mesi. Il processo è stato più rapido di quanto avremmo potuto immaginare» ha commentato Campese. L'aggiornamento ha riguardato un paio di firewall FirePOWER ai margini di ogni aeroporto pugliese. Grazie alla semplicità del sistema, l'intera operazione è ora gestita come un'unica connessione attraverso Cisco Prime e Cisco ISE integrato nella directory. Per i team questo si traduce in meno amministrazione e più automazione. È stata anche messa in atto una gestione automatica di diverse connessioni WAN (con diverse tecnologie e provider) e connessioni internet che assicurano una logica di connessione di rete sicura senza interruzioni. Conclude il manager: «In pratica, la nostra trasformazione fa sì che non sia richiesta quasi nessuna interazione umana se i sistemi si guastano. Il nostro sistema consente di trovare e risolvere il problema senza alcuna interruzione del servizio».



L'intelligenza artificiale in aiuto della cyber security

di
Paola
Saccardi

Non è sulla massa degli attacchi che va posta l'attenzione, ma sullo 0,1% che produce i danni più gravi. F-Secure utilizza tecnologie di threat intelligence, sample analysis e decision-making per proteggere le aziende

Lo dice Gartner: il 99,9% degli attacchi produce danni limitati. Resta però quello 0,1% di minacce, che in termini percentuali può apparire un dato quasi insignificante, ma rappresenta la quota non trascurabile di un totale assoluto quantificabile in milioni.



Le minacce che si possono definire "commodity" sono ancora oggi quelle largamente più diffuse, ma la disponibilità di soluzioni efficaci contro questi pericoli ne ha ampiamente attutito l'impatto. Tuttavia è dal cybercrime che le aziende si devono proteggere. Le tradizionali tecnologie di difesa del perimetro, come i firewall e la protezione degli endpoint, sono efficaci nel bloccare le minacce più comuni e standardizzate.

Gli avversari più esperti, tuttavia, non possono essere contrastati in questo modo.

Combattere le minacce con "intelligenza"

Le tecnologie di intelligenza artificiale e machine learning rappresentano oggi la sola soluzione scalabile che possa essere applicata, ma la risposta più efficace è data dall'unione fra le tecniche di ultima generazione e il lavoro degli esperti di cybersecurity. L'intelligenza artificiale fornisce senza dubbio maggiori possibilità di automatizzare la rilevazione di potenziali minacce, grazie alla capacità di analizzare enormi volumi di dati e usare gli algoritmi di machine learning per trovare, interpretare e analizzare le relazioni e le tendenze più significative nel contesto della sicurezza preventiva.

Per questo motivo, F-Secure ha dedicato gli ultimi anni allo sviluppo e al perfezionamento di servizi gestiti di rilevazione e risposta. Questi servizi non

forniscono solo competenze ed esperienza delle persone, ma sono costruiti su tecnologie di threat intelligence, sample analysis e decision-making. L'offerta è disponibile in differenti livelli e soluzioni, per adattarsi alle caratteristiche di ogni organizzazione, che si tratti di una realtà di grandi dimensioni o di una Pmi. Dal proprio centro di Rapid Detection & Response Service (RDS), gli esperti di F-Secure tengono sotto monitoraggio 24x7 gli ambienti dei clienti e, quando viene rilevata un'anomalia, si procede rapidamente all'analisi. Qualora si capisca che si tratta di una reale minaccia, parte una segnalazione di allarme al cliente nell'arco di 30 minuti dal momento della rilevazione. La cyber security secondo F-Secure è un processo continuo di miglioramento costante, che si evolve e si adatta con la stessa rapidità degli attacchi. Non funziona come una bacchetta magica, ma richiede una combinazione di competenza professionale e tecnologia in costante miglioramento per prevedere, prevenire e rilevare. Per Gartner, nel 2020 il 60% dei budget di IT Security sarà destinato a soluzioni Rapid Detection & Response, mentre oggi, a livello mondiale siamo sotto il 30% e in Italia, verosimilmente, sotto il 10%. C'è ancora molto da fare. *



LA DISPONIBILITÀ DEI DATI

Servizi e soluzioni per non perdere informazioni

Dati al sicuro e sempre disponibili con la Hyper Availability

Hyper-Availability Platform di Veeam è una soluzione di Intelligent Data Management che permette di sviluppare e fornire in modo sicuro servizi digitali innovativi

La sicurezza permea qualsiasi aspetto del funzionamento delle aziende, si tratti di beni materiali o immateriali, di processi amministrativi, produttivi, di relazioni con clienti o di business.

Garantire sicurezza e disponibilità, stante il progredire della virtualizzazione, della migrazione al cloud e di dissolvimento del perimetro fisico aziendale, richiede però un cambiamento profondo nell'approccio e nella propria postura per quanto concerne la sicurezza.

In particolare, osserva Veeam, società specializzata nella hyper availability di infrastrutture IT e dati, l'esigenza di modificare in profondità l'approccio adottato sino ad ora nella gestione delle informazioni, passando ad uno proattivo basato sull'intelligenza artificiale e analytics, è conseguenza dell'evoluzione del mondo

produttivo e delle modalità da parte delle aziende e privati di fruire dell'IT, sempre più basate su ambienti multcloud.

Sia che si parli di reti di sensori IoT inerenti infrastrutture di tipo sanitario, dei trasporti, di grid per l'erogazione di energia sia di servizi della PA, si tratta di realtà che devono poter essere orchestrate e garantite sia per quanto concerne la loro disponibilità assoluta che per quanto riguarda i tempi di latenza e velocità alle richieste di dati inoltrate.

«La Hyper-Availability è la nuova frontiera nel trattamento del dato e nella sua fruizione per il business. La Hyper-Availability Platform di Veeam, già utilizzata da numerose grandi aziende ed operatori mondiali



Albert Zammar, Vice President
Southern EMEA Region di Veeam

e italiani è una soluzione completa di Intelligent Data Management che permette di sviluppare e fornire rapidamente e in modo sicuro servizi digitali innovativi», ha osservato Albert Zammar, Vice President Southern EMEA Region di Veeam.

Alleanze e strategie vincenti

La strategia di prodotto, volta ad assicurare l'always-on del business nel quadro della hyper availability, è solo uno degli aspetti che hanno visto le sue soluzioni adottate dalle principali industrie italiane e mondiali. L'altro aspetto è la forte politica di alleanze con aziende primarie dell'IT al fine di proporre congiuntamente soluzioni chiavi in mano ad elevata affidabilità.

Sotto il profilo finanziario l'azienda è reduce dal quarantesimo trimestre consecutivo in crescita a due cifre degli ordini, una crescita che per quanto concerne il settore Enterprise è stato del 24% anno su anno. Crescita derivata anche dal numero di clienti. Nel secondo trimestre 2018, Veeam ha acquisito oltre 13.000 nuovi clienti, raggiungendo una base complessiva di oltre 307.000.

«Il nostro focus sull'hyper-availability è costante e i clienti stanno rispondendo positivamente. Continuiamo a conquistare quote di mercato sia su aziende tradizionali che su nuovi protagonisti del settore, che provano a raggiungerci e ad essere profittevoli, un benchmark che Veeam ha raggiunto e mantenuto per oltre un decennio», ha affermato Peter McKay,

Co-CEO e President di Veeam.

L'altro pilastro della strategia di go-to-market di Veeam sono le alleanze, con partnership con società di primo piano nell'IT come HPE, Lenovo, Nutanix e Microsoft. In particolare, per Microsoft ha sviluppato una soluzione che estende a Microsoft Office 365 il concetto di Hyper Availability.

Veeam Backup per la disponibilità su Microsoft Office 365

Per la disponibilità e sicurezza del dato su cloud, Veeam ha di recente rilasciato la versione 2 di Veeam Backup for Microsoft Office 365. Ha aggiunto alle funzionalità già disponibili la protezione per Microsoft OneDrive for Business, SharePoint Online e le installazioni on-premise di SharePoint, oltre ad Exchange Online e Exchange on-premises.

In pratica, ha commentato l'azienda, la nuova versione permette di proteggere i dati all'interno dell'infrastruttura Office 365, migliorare la replica automatica dei dati che Microsoft fornisce nei suoi data center e, non ultimo, la combinazione delle soluzioni Veeam con quelle Microsoft permette alle aziende di avere un controllo esaustivo sui loro dati e garantirne la disponibilità per gli utenti su Exchange Online, SharePoint Online e OneDrive for Business.

«Grazie alla nuova release, Veeam estende il proprio impegno a lungo termine per fornire ulteriori funzionalità di controllo e backup per i dati Microsoft Office 365. Nessuna azienda che usa Office

365 dovrebbe rinunciare a Veeam Backup for Microsoft Office 365 v2. Con Veeam, l'azienda mantiene pieno controllo e i dati sono sempre disponibili e protetti», ha dichiarato Danny Allan, Vice President of Product Strategy di Veeam.

Certificazione IMQ garantita da Veeam

Tra gli enti che hanno adottato le soluzioni Veeam è da annoverare IMQ, che ha scelto Veeam Availability Suite come piattaforma di replica e protezione dei dati in ambiente VMWare vSphere all'interno di una più ampia strategia di back-up e disaster recovery.

Tre i principali benefici derivati dall'adozione della piattaforma Veeam: il ripristino veloce dei dati nel caso di perdita o corruzione di un file; l'uso di tecnologie che evitano la perdita di dati effettuando copie dei dati in modo regolare; backup immediatamente utilizzabili.

IMQ si è affidata a Veeam, ha evidenziato la società, anche perché le è stato così possibile risultare conforme alle normative vigenti in termini di conservazione dei dati, che prevedono che siano accessibili fino a 10 anni oltre la fine del ciclo di vita del prodotto.

«Oggi i dati e le informazioni sono il vero patrimonio di ogni azienda ed è essenziale impostare una corretta strategia per garantirne disponibilità e sicurezza. Siamo lieti di aver saputo rispondere alle esigenze e ai requisiti di IMQ, fornendo un vantaggio competitivo ad una importante istituzione italiana», ha commentato Albert Zammar.



La sicurezza dei container

Con la virtualizzazione crescono le criticità nello sviluppo delle applicazioni

di
Gaetano
Di Blasio

Le tematiche di DevOps agitano i sogni dei responsabili della sicurezza. In particolare si devono proteggere le applicazioni realizzate dai reparti operativi e di sviluppo, che vengono distribuite nei container. Una sicurezza che deve restare attiva durante tutto il ciclo di vita del container. Questo non basta, perché la sicurezza deve essere integrata nella cosiddetta pipeline del DevOps.

È un prerequisito per una sicurezza by design, cioè una applicazione progettata intrinsecamente sicura.

Purtroppo, la digital transformation, che pure ha contribuito al boom delle applicazioni, impone troppo spesso ritmi frenetici di sviluppo, revisione e aggiornamento.

Le prassi di DevOps dovrebbero considerare la sicurezza al centro del progetto, solo così, infatti, si riduce il rischio di rilasciare un'App che presenta una vulnerabilità.

Se i microservizi possono fornire una qualche garanzia, è comunque preferibile verificare fonti e risultati, mentre con le API, si hanno maggiori garanzie.

Ci sono, infatti, rischi dovuti a pacchetti software non verificati.

Altri problemi potrebbero



arrivare dal mettere in esercizio container con configurazioni non sicure o con valori predefiniti.

Gli amministratori devono considerare tali problematiche, equipaggiando il proprio reparto di sviluppo e operation, affinché possa soddisfare le esigenze interne, senza trascurare la sicurezza.

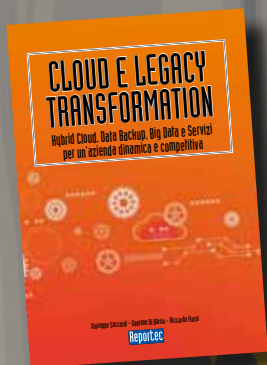
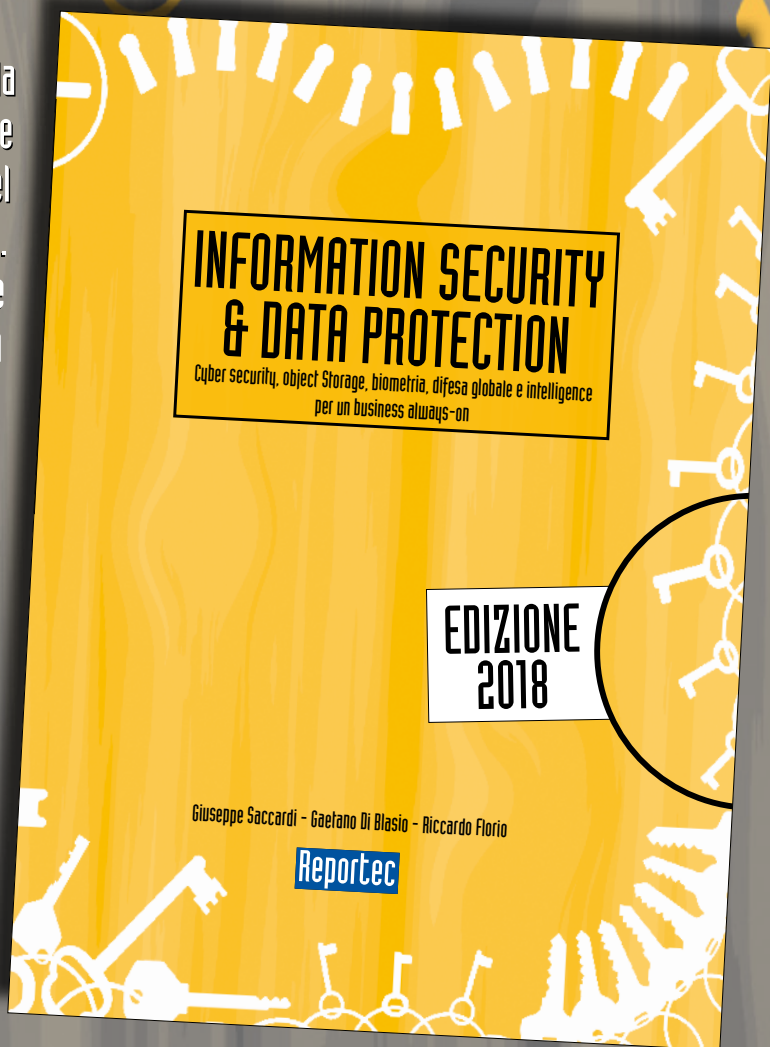
Le imprese devono predisporre programmi di incident response aggiornati e capaci di raccogliere informazioni sul sistema informativo dei container e sulla piattaforma di orchestrazione. In questo modo, sarà possibile introdurre, con

le opportune pianificazioni, una modalità di sostituzione completa del programma per la risposta agli incidenti.

Nella fase d'implementazione, occorre fare attenzione a che le immagini presenti nei vari repository siano prive di vulnerabilità, quindi va tenuto costantemente aggiornato l'inventario dei registri e dei repository. Il che significa avviare l'analisi delle vulnerabilità tutte le volte che si aggiunge una nuova immagine. Resta però utile controllare sistematicamente tutte le immagini e pianificare scansioni automatizzate periodiche. *

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 30 euro (IVA inclusa) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444



FUJITSU

Una
combinazione
perfetta

FUJITSU Server PRIMERGY
e Windows Server 2016



Windows Server: Power your business

Iperconvergenza, qualità e affidabilità:
i Server PRIMERGY e Windows Server 2016
sono la perfetta combinazione per vincere
le sfide del futuro. Cosa stai aspettando?

Info:

www.fujitsu.com/windowserver2016

Numero verde: 800 466 820

customerinfo.point@ts.fujitsu.com

blog.it.fujitsu.com

© Copyright 2018 Fujitsu Technology Solutions

Fujitsu, il logo Fujitsu e i marchi Fujitsu sono marchi di fabbrica o marchi registrati di Fujitsu Limited in Giappone e in altri paesi. Altri nomi di società, prodotti e servizi possono essere marchi di fabbrica o marchi registrati dei rispettivi proprietari e il loro uso da parte di terzi per scopi propri può violare i diritti di detti proprietari. I dati tecnici sono soggetti a modifica e la consegna è soggetta a disponibilità. Si esclude qualsiasi responsabilità sulla completezza, l'attualità o la correttezza di dati e illustrazioni. Le denominazioni possono essere marchi e / o diritti d'autore del rispettivo produttore, e il loro utilizzo da parte di terzi per scopi propri può violare i diritti di detto proprietario.

shaping tomorrow with you