

DIRECTION

Reportec

LA DIGITAL ECONOMY AL SUPPORTO DEL BUSINESS



Eroi per la Sicurezza

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 sicurezza tallone d'Achille per le imprese

- | | | |
|---|--|--|
| 6 Nuovi modelli rendono le reti virtuali più veloci e sicure | 16 Come proteggere gli accessi privilegiati con la biometria | 28 Videosorveglianza senza angoli bui per le soluzioni smart |
| 8 AI e machine learning sempre più al servizio della sicurezza | 18 L'Intelligenza artificiale motore della nuova Security intelligence | 31 Con il cloud servono reti più sicure, vicine e flessibili |
| 10 OrisLine, service provider di odontoiatria, si protegge con Webroot | 20 La sicurezza deve seguire l'utente ovunque esso sia | 32 La varietà delle difese nella cyber security è un imperativo strategico |
| 11 Ecosistema e vicinanza alle aziende migliorano la security | 22 La protezione degli endpoint e come garantirla | 34 La cyber security inizia con la disponibilità di dati e applicazioni |
| 12 Il tessuto che rende la sicurezza informatica un fattore di business | 24 L'AI è la nuova frontiera della cyber security | 36 Crescono gli enti della PA locale attaccati da ransomware |
| 14 I servizi SaaS semplificano ed automatizzano la sicurezza multicloud | 25 Crittografia e accesso Zero Trust proteggono la rete e i dati | 38 Ansaldo Energia protegge il suo ecosistema |
| | 26 Cloud Azure e Web sicuri con la gestione completa del servizio | |

Direction Reportec • anno XVII • numero 111 - gennaio 2020

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

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

Editore: Reportec Srl, 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 sicurezza tallone d'Achille per le imprese

di
Gaetano
Di Blasio

La pressione del cybercrime si allarga a ogni tipologia d'azienda: occorre una strategia per gestire i rischi

In copertina l'imponente Ercole Farnese, scultura ellenistica in marmo databile al III secolo dopo Cristo, custodita nel Museo Archeologico Nazionale di Napoli, simboleggia le fatiche degli odierni eroi: i responsabili della sicurezza aziendale e, in particolare, gli addetti alla cyber security.

Le analisi sulle minacce e gli attacchi alle infrastrutture e ai dati aziendali sono sconcertanti. Le superfici di attacco crescono, con la diffusione di sistemi e soluzioni IoT, che consentono di sfruttare le tecnologie "smart", le quali non sembrano abbastanza "furbe", perché realizzate senza concepire la sicurezza sin dalle fasi preliminari dei progetti. La security by design, che viene citata anche nel GDPR, appare ancora una chimera.





In questa monografia, vari esperti del settore illustreranno lo stato dell'arte di tante soluzioni e strategie per uscire da questa morsa.

Una delle frontiere che sembra promettente si trova nell'ambito dell'Artificial Intelligence. Anche la collaborazione tra "buoni" consente di ridurre l'esposizione agli attacchi. È importante, al riguardo la condivisione degli incidenti, ancorché obbligatoria per legge.

In effetti, su questo fronte le aziende italiane sembrano ancora indietro.

Secondo un recente sondaggio della nostra redazione (cui hanno partecipato 70 persone, e che ci teniamo a precisare avere una validità puramente qualitativa, non basandosi su base rigorosamente statistiche) si evidenzia che l'attenzione per la conformità alle normative e al GDPR in particolare è presa con molta attenzione, considerando la legge uno strumento utile.

Lo scorso anno già si pensava potesse essere un vantaggio per il 62% dei rispondenti. Oggi sono convinti dell'utilità l'82% dei manager coinvolti, si potrebbe considerare un plebiscito.

Per questo abbiamo voluto approfondire un po' di più, cercando i consensi su tre fronti: la paura delle sanzioni, la convinzione che generi consapevolezza sul tema sicurezza e, infine, la capacità di aiutare le imprese a costruire un sistema adeguato agli asset informatici e ai dati trattati, per raggiungere la conformità alla legge.

Quello delle sanzioni è stato l'aspetto più dibattuto al momento in cui era necessario recepire il regolamento. La multa in caso di violazione può arrivare, infatti, sino al 20% del fatturato. Però solo il 14,1% dei rispondenti la teme.

In alcuni casi si tratta di aziende che non ritengono di correre grossi rischi, magari perché non trattano dati sensibili o trattano solo pochi dati relativi alla relazione con la clientela, spesso gestita direttamente.

Un 17,65% ritiene che il GDPR sia utile a focalizzare l'attenzione

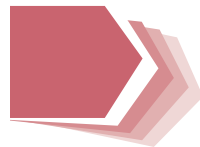
dell'azienda sulla sicurezza, mentre un ben più ampio gruppo pari al 67,65%, confida che il GDPR spinga a realizzare un sistema per la sicurezza più efficace.

Non possiamo, come spiegato, ritenere questi dati rigorosi, ma alcuni manager con cui abbiamo parlato sono convinti che sia uno

scenario corretto.

Del resto è evidente che solo il raggiungimento della "compliance" costringa a ragionare sulla sicurezza.

Ma la compliance non garantisce la protezione, mentre per troppe aziende questa rappresenta il traguardo finale.



di
Giuseppe
Saccardi

Nuovi modelli rendono le reti virtuali più veloci e sicure

La migrazione delle applicazioni in periferia della rete, cloud e mobility richiedono un nuovo modello di rete in grado di garantire una miglior sicurezza

La virtualizzazione della rete e la distribuzione della capacità di calcolo in periferia o la sua fruizione presso service provider richiede nuovi modelli e una maggior integrazione di rete e sicurezza.

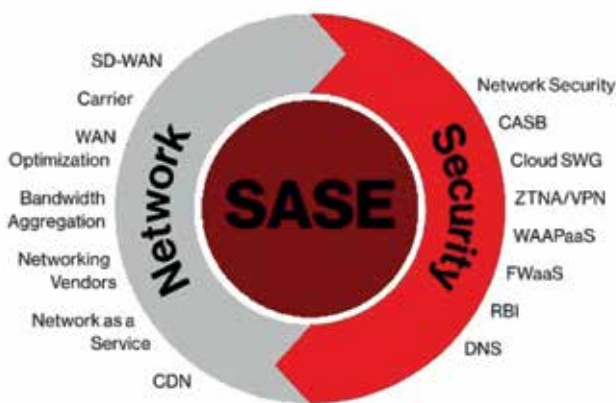
Di crescente interesse è il modello di networking definito da Gartner come "Secure Access Service Edge" riassunto nell'acronimo SASE.

Il modello prende atto della distribuzione della capacità di calcolo o di preelaborazione di dati prima di inviarli in rete (per esempio per applicazioni IoT) e quindi che l'affidarsi al data center come elemento centrale dell'IT aziendale perde sempre più di significato man mano che le applicazioni si spostano verso il cloud e gli utenti accedono alle reti da

La spesa prevista dai partecipanti al nostro sondaggio rende evidente che non si investe abbastanza. Prima del GDPR rilevammo una spesa per l'IT molto bassa: meno del 10%, che si può considerare il minimo indispensabile per la manutenzione e c'erano anche casi che si possono considerare

"limite", con cifre di spese sotto l'%. Se sommiamo le risposte di tutti quelli sotto il 10%, troviamo che il 73,53% delle aziende sono sotto la "linea di galleggiamento" per quanto riguarda la manutenzione della sicurezza, sulla cui efficacia non abbiamo ancora indagato. Le soluzioni non mancano, come

potrete approfondire nelle prossime pagine e, anche se la sicurezza totale non esiste, l'importante è organizzarsi per essere pronti a rispondere agli attacchi, piegandosi, ma non spezzandosi. Gli eroi come Ercole non mancano e non siamo tutti condannati come Achille. ❁



Il modello Secure Access Service Edge prevede una forte e sinergica integrazione tra applicazioni di sicurezza e rete di edge

ovunque e tramite un'ampia varietà di dispositivi. Alla base del modello c'è la constatazione che l'interesse dei provider e degli utenti è di migrare le attività di calcolo e l'erogazione dei servizi ai margini della rete nei POP ivi installati, in modo che siano vicini agli utenti, cosa che permette di ridurre la latenza tra applicazioni ed endpoint. SASE, in sostanza, è una piattaforma con caratteristiche che abilitano:

- Integrazione di funzioni di rete e di sicurezza all'interno di un servizio di rete cloud ibrida o multicloud.
 - Erogazione di un servizio olistico e scalabile.
 - Realizzazione di una piattaforma distribuita basata su cloud.
 - La connessione sicura delle periferie della rete siano esse WAN, cloud, mobile o dispositivi IoT
- Ci si aspetta che SASE abbia impatti significativi sul modo nelle aziende di organizzare ed erogare l'IT. Con i servizi spostati a livello di Edge ci sarà meno bisogno di fornire una connettività di rete

occupata da traffico diretto dalla periferia al data center e viceversa. I servizi risiederanno direttamente nell'edge della rete e gli utenti non avranno bisogno di sapere dove si trova un'applicazione, che potrà risiedere ovunque in Internet. Parallelamente alla diffusione di SASE si assisterà prevedibilmente per l'accesso remoto al calare di interesse per le più tradizionali reti private virtuali (VPN), che hanno storicamente rappresentato un'estensione della rete fisica per i dipendenti quando lontani dalla scrivania o per quelle terze parti con la necessità di accedere alla rete e ai servizi dell'azienda cliente. Il calare di interesse è poi enfatizzato dalla costante diffusione del cloud e delle applicazioni che vi risiedono, che fa venir meno l'esigenza in senso stretto di ricorrere a una VPN. Va poi considerato che le VPN sono costose, richiedono investimenti infrastrutturali e per il personale, che deve disporre di competenze specifiche. Capex e Opex che invece il ricorso al cloud permette di contenere o di distribuire nel tempo. ❁

AI e machine learning sempre più al servizio della sicurezza

Elaborate reti neurali sfruttano enormi moli di dati per una sicurezza predittiva che anticipa le minacce e le elimina.

Il come sfruttarle lo spiega Achab

cyber criminali si fanno sempre più agguerriti, ma ora le aziende hanno a loro disposizione per contrastarli i potenti strumenti dell'intelligenza artificiale (AI) e del machine learning, in grado di elaborare una quantità pressoché illimitata di dati inerenti programmi dannosi.

Il vantaggio di tecniche di contrasto basate su AI e machine learning è che questi, tramite potenti meccanismi, permettono di sfruttare un'elaborata rete neurale per individuare in tempo reale gli attacchi, individuare nuovi virus e mettere al sicuro l'IT anche da minacce zero-day o da varianti particolari di malware.

Un esempio di azienda operante nella security che ha intrapreso questa innovativa strada nello sviluppo di soluzioni di security è Webroot. La società analizza ogni giorno mezzo miliardo di oggetti, ognuno dei quali può contenere fino a 10 milioni di caratteristiche. Questa mole di informazioni viene elaborata da complesse reti neurali per produrre mille modelli matematici al giorno, modelli che consentono al software Webroot di rilevare se un determinato attacco, comportamento o programma è malevolo o meno.

«Oggi le principali soluzioni di security lavorano in maniera reattiva e quindi insufficiente. Serve perciò un modello completamente diverso. L'idea è che siano i computer a prevedere da soli gli attacchi informatici, ovvero dotando le macchine di una forma di intelligenza in modo che siano in grado di distinguere autonomamente ciò che è un virus da ciò che non lo è e poter intervenire di conseguenza in maniera indipendente», ha spiegato Claudio Panerai, CTO e Tech Evangelist di Achab (achab.it), che distribuisce le soluzioni Webroot in Italia dal 2014.

Il connubio AI, machine learning e cloud

Operativamente, Webroot è una soluzione di sicurezza informatica, sia business che consumer, che ha l'obiettivo di garantire la protezione in tempo reale di dispositivi endpoint e mobili contro tutti i tipi di malware, garantendo



Andrea Veca, CEO di Achab

la riservatezza e l'integrità dei dati aziendali.

La soluzione implementa un modello distribuito grazie al quale l'intelligence ricavata dagli endpoint di tutto il mondo protegge istantaneamente tutti gli altri endpoint collegati a Webroot Intelligence Network. Per farlo utilizza anche la potenza del cloud, grazie al quale le è possibile bloccare minacce informatiche note o sconosciute utilizzando le informazioni in tempo reale del machine learning e l'analisi comportamentale.

Per identificare e fermare le minacce, si avvale anche della grande rete mondiale di rilevamento malware "Webroot Intelligence Network". Il tutto è gestibile tramite una console web-based che abilita una gestione da remoto e un supporto clienti integrato ideato per PMI e MSP.

«Molti fornitori di servizi IT hanno le idee confuse su quale sia la reale differenza tra intelligenza artificiale e machine learning e molto spesso non conoscono gli incredibili benefici che possono apportare in termini di protezione e sicurezza dei sistemi informatici. Webroot è un antivirus di nuova generazione, che riteniamo rappresenti un'ottima opportunità di crescita per gli MSP, considerate sia le caratteristiche peculiari della soluzione» ha osservato Andrea Veca, CEO di Achab.

I dati sugli attacchi e l'esigenza di AI e machine learning

L'esigenza di approcci innovativi e proattivi basati sull'AI emerge anche dai dati di una ricerca



Claudio Panerai, CTO e Tech Evangelist di Achab

realizzata da Webroot che ha analizzato l'evoluzione del panorama della cybersecurity. Sulla base dei trend osservati durante la prima metà del 2019, è emerso che 1 link su 50 è malevolo, quasi un terzo dei siti di phishing utilizza il protocollo HTTPS e gli exploit di Windows 7 sono cresciuti più del 70%.

Il report evidenzia peraltro l'importanza di un'adeguata educazione informatica degli utenti dal momento che i messaggi di phishing sono sempre più personalizzati.

Tra gli aspetti più significativi e preoccupanti, ma che non possono essere ignorati, si trova che:

- Gli hacker si servono di domini considerati attendibili e del protocollo HTTPS per ingannare gli utenti e quasi un quarto dei link dannosi sono ospitati su domini sicuri.
- Gli attacchi phishing hanno avuto un forte incremento nel 2019. La crescita degli URL malevoli, nel periodo da gennaio a luglio 2019 è stata pari al 400%. Tra i settori maggiormente attaccati le aziende di

servizi web, istituti finanziari, social media e retail.

- Gli attacchi sono personalizzati grazie ai dati personali raccolti a seguito di una violazione. Le password violate vengono utilizzate sia per il controllo dell'account che per altre azioni tra cui l'invio di email a scopo di ricatto. Va osservato che il phishing non sempre mira ad acquisire username e password, ma punta a violare anche le domande segrete e le relative risposte.
- Windows 7 a rischio con infezioni aumentate di oltre il 70%, conseguenza questa anche del mancato aggiornamento del software o del non aver apportato le patch necessarie.

La validità di un approccio basato su AI e machine learning è confermato da report indipendenti. Per le sue soluzioni Webroot è stata riconosciuta come "Trail Blazer" all'interno dell'Endpoint Security Market Quadrant 2019 di The Radicati Group. Il report valuta i principali fornitori per la sicurezza endpoint sulla base delle funzionalità offerte e della visione strategica. Secondo Radicati, il "Trail Blazer" dispone di una tecnologia innovativa in grado di imporsi sul mercato. Il report evidenzia quali punti di forza della soluzione Webroot Business Endpoint Protection, la facilità di gestione, la rapida installazione, le prestazioni fornite da un sistema non invasivo, la capacità di lavorare con qualsiasi browser e la possibilità di coesistere in un ambiente in cui sono state installate altre piattaforme per la sicurezza degli endpoint.

OrisLine, service provider di odontoiatria, si protegge con Webroot

La soluzione di sicurezza adottata ha permesso al provider di ridurre i ticket di sicurezza dell'80%, gli attacchi ransomware del 90% e le infezioni del 95%

OrisLine è un provider di servizi gestiti con sede a Milano specializzato nel settore odontoiatrico.

L'azienda è presente in oltre 70 paesi dove gestisce migliaia di clienti. La sua infrastruttura di endpoint è basata su procedure che richiedono una soluzione di sicurezza efficiente e facile da utilizzare.

«Operare nel settore odontoiatrico comporta numerosi problemi in termini di privacy, dati personali dei pazienti, dati clinici e così via. Molti nostri clienti sono ospedali e cliniche e se i sistemi non sono disponibili per motivi di sicurezza, i problemi potrebbero essere enormi», ha spiegato Diego Pasqua, responsabile IT di OrisLine.

A causa della natura altamente sensibile delle informazioni ospitate, come dati di cliniche, centri chirurgici, ospedali e pratiche private, il problema principale per OrisLine è sempre stato il ransomware perché periodi di inattività dei sistemi o violazione dei dati personali dei clienti non sono tollerabili.

Per contrastare le minacce, nel passato l'azienda proponeva ai

clienti diverse soluzioni di sicurezza ma nessuna realmente idonea per difficoltà di installazione o scarsità di opzioni.

«In passato ho utilizzato diverse soluzioni di sicurezza. Ma, alla fine, ho provato a cercare una soluzione facile da distribuire, con tempi di installazione ridotti e gestione centralizzata, che offrisse controllo dell'IT, sicurezza e monitoraggio in un unico pannello» ha evidenziato Pasqua.

Per controllare i costi e preservare i margini di profitto, la soluzione di sicurezza doveva disporre inoltre di un unico pannello di gestione e di ampie opportunità di integrazione con le soluzioni esistenti.

Al termine di un'approfondita analisi delle soluzioni esistenti OrisLine si è indirizzata sulla soluzione Webroot Business Endpoint Protection fornita da Achab. L'implementazione è stata rapida e i risultati immediati. Particolarmente importante è stata l'API Unity di Webroot. Fondamentale per



Diego Pasqua, responsabile IT di OrisLine

la gestione della sicurezza informatica, l'API è utile in tutte le attività quali acquisire nuovi clienti, controllare lo stato di un agente, eseguire procedure o modificare un criterio.

Consistenti i benefici per l'operatività quotidiana derivanti dalla riduzione dei ticket di sicurezza dell'80%, dei ransomware del 90% e delle infezioni del 95%. Non ultimo, le scansioni sono più veloci, con una durata che da una media di 45 minuti è scesa a un paio, ed è stato anche possibile assegnare un tecnico ad altre attività. «I risultati ottenuti da OrisLine con la soluzione Webroot da noi fornita sono straordinari e dimostrano che la nostra proposta semplice e innovativa rappresenta per gli MSP un vero valore aggiunto» ha commentato Andrea Veca, CEO di Achab. ❁

Ecosistema e vicinanza alle aziende migliorano la security

Per promuovere un nuovo ecosistema di partnership e ampliare la presenza sulle imprese, ESET apre la sede in Italia

ESET (eset.com/it/), attore globale nella cyber security che a livello mondiale protegge oltre 110 milioni di utenti, ha aperto la propria sede italiana con l'obiettivo di accelerare le strategie di go-to-market rivolte alle organizzazioni nazionali.

La società, che ha l'headquarter a Bratislava in Slovacchia, ha sviluppato dal 1991 una rete di distribuzione globale che si estende in 200 paesi e regioni. Nel 2001 ha dato il via a una collaborazione esclusiva con il partner italiano Future Time e dopo diciotto anni di crescita nel settore consumer è ora impegnata nel rispondere alle sfide che devono affrontare le imprese di qualunque dimensione.

Country Manager della filiale italiana è stato nominato Fabio Buccigrossi, con il compito di avviare lo sviluppo di un nuovo modello di partnership. In particolare, per espandere la rete dei rivenditori specializzati e potenziare la sua proposta nel mercato small/medium business, nello scorso novembre ha siglato un accordo con Allnet.Italia, un distributore a valore specializzato in soluzioni

innovative nell'informatica e nelle telecomunicazioni.

«ESET da sempre fornisce soluzioni apprezzate per la loro capacità di proteggere gli utenti dalle minacce informatiche, con il minor impatto sull'infrastruttura IT», ha evidenziato Buccigrossi. «La maggiore distribuzione sul territorio, la vicinanza ai clienti e il coinvolgimento proattivo di partner altamente qualificati, aumenteranno il nostro supporto alle aziende, coprendo tutte le regioni. Avvieremo poi collaborazioni mirate, avvalendoci di rivenditori qualificati e Managed Service Provider



Fabio Buccigrossi, Country Manager di ESET per l'Italia

specializzati nel settore, al fine di supportare al meglio le esigenze delle imprese di medie e grandi dimensioni».

In particolare, per permettere alle aziende di mantenere la continuità del business, sviluppa tecnologie di cyber security a più livelli basate sul motore di scansione, sull'apprendimento automatico e sugli elementi di protezione del cloud.

Facendo leva sui dati di intelligence raccolti, le soluzioni permettono di respingere attacchi mirati, proteggere dal phishing, bloccare le botnet e rilevare le minacce più persistenti.

Il portfolio comprende anche soluzioni di crittografia e l'autenticazione a più fattori, elementi cruciali per aderire alla normativa GDPR e consentire alle aziende di migliorare la sicurezza dei dati nel rispetto della facilità d'uso.

«Nel 2018 siamo stati riconosciuti unico Challenger nel Magic Quadrant di Gartner per la protezione degli endpoint e la nostra azienda continua ad aumentare gli investimenti in R&D, incrementati oggi del 66% rispetto agli ultimi 4 anni, che ci assicurano un portfolio completo e all'avanguardia per la cyber security» ha evidenziato Buccigrossi. ✪

Il tessuto che rende la sicurezza informatica un fattore di business

Soluzioni integrate sfruttano l'automazione per acquisire visibilità e controllo, raggiungendo ogni elemento da proteggere

Quando abbiamo chiesto a Giorgio D'Armento, Distribution Led Business Manager di Fortinet quale fosse la visione di Fortinet sulla security, ha esordito spiegando: «In Fortinet riteniamo innanzitutto che la sicurezza debba essere un fattore abilitante per l'ottimizzazione del business e della competitività aziendale. Poiché il tema sicurezza si declina in molteplici aspetti, è bene precisare che in Fortinet si parte da un presupposto: per essere considerata tale, essa deve offrire una copertura totale. Il che significa avere visibilità e controllo della situazione nel suo complesso.»

Visibilità, controllo e integrazione

Ciò detto, la visione di Fortinet si concretizza nel Fortinet Security Fabric.

«'Fabric' significa tessuto e, proprio come trama e ordito danno origine a qualcosa di concreto, le nostre soluzioni, grazie alla loro capacità d'integrazione e automazione supportata dalla visibilità, assicurano la protezione e la possibilità di rispondere agli eventi con rapidità ed efficacia», continua D'Armento.

Alla base ci sono le soluzioni che il Fortinet Security Fabric integra in un'unica visione, comprendendone anche alcune di partner tecnologici che consentono di estendere l'automazione.

«Quello che ci distingue - specifica D'Armento - è la capacità di sviluppare internamente la nostra tecnologia, con un numero di brevetti che è almeno tre volte quello dei nostri concorrenti».

Il manager, al riguardo, evidenzia la spinta verso il cloud che, secondo uno studio dell'Osservatorio Cloud Transformation promosso dalla School of Management del Politecnico di Milano, negli ultimi due anni è in continua crescita con cifre intorno al 20%. «Le imprese italiane stanno investendo nel cloud, perché li trovano strumenti per ottimizzare e competere. Quanto più è alta la strategicità del servizio fruito con questa modalità, tanto più si può abbassare il TCO dell'infrastruttura». In altri termini, pensando al public cloud e ai servizi SaaS, si può "demandare l'affidabilità di uno SLA" sfruttando un costo moderatamente più conveniente e senza impegnare risorse. Fermo restando, però, la capacità delle linee dati.

A tal proposito, Fortinet sta investendo sull'edge della rete. Come dimostra, tra gli altri,



Giorgio D'Armento,
Distribution Led Business
Manager di Fortinet

un accordo con Microsoft per la SD-WAN (Software Defined Wide Area Network), che consente di assegnare delle priorità alle applicazioni in modo da renderle più dinamiche, veloci e produttive, sfruttando le diverse tecnologie di connettività - dall'ADSL al MPLS, LTE e così via.

Più precisamente, Fortinet ha stretto una partnership con Microsoft per inserire Secure SD-WAN nell'offerta Virtual WAN di Microsoft Azure per le sedi branches che maggiormente risentono della necessaria capacità delle linee.

Con l'integrazione del Fortinet Secure SD-WAN, le imprese possono ottimizzare la connettività aziendale - filiali comprese - garantire sicurezza e protezione, conservare i requisiti di ottimizzazione, risparmio e flessibilità per i quali si sceglie il cloud.

«Tutto ciò ci riporta al fattore critico di successo che è la connettività delle aziende», conclude D'Armento, evidenziando che l'integrazione del Secure SD-WAN nella soluzione FortiGate (alla quale viene demandata la sicurezza di Fortinet) è completamente gratuita. Questo significa che anche tutta la parte di networking, con la sicurezza ad essa relativa, può essere fornita in un'unica soluzione integrata».

Questo porta un vantaggio importante per l'impresa, poiché i partner di Fortinet possono fornire un servizio completo, assumendosi tutta la responsabilità nella gestione delle operazioni IT e OT, essendo queste ultime comprese.

Per l'azienda c'è un ulteriore vantaggio, ci spiega D'Armento: «Avere un partner e un vendor di

riferimento come Fortinet consente di semplificare la gestione, grazie a una console omogenea attraverso la quale è immediatamente reperibile lo storico di ogni evento sull'infrastruttura. Al contrario, se un'azienda dispone di uno o più sistemi eterogenei, occorre moltiplicare per ciascuno di essi il numero di analisi, con ritardi che, oltre a favorire chi attacca, non sono ammessi anche secondo il GDPR».

Evidenzia ancora il manager come il partner ottimizzi gli sforzi di formazione, con un beneficio a cascata sul cliente. Lo stesso si può dire per gli SLA (Service Level Agreement): «Grazie all'architettura di Fortinet Security Fabric, si ottiene un incremento della velocità e affidabilità della rete, con un conseguente miglioramento dei livelli di servizio».

La facilità d'integrazione con il Fortinet Fabric Ready Program

"La community", cioè l'insieme dei partner che hanno aderito al Fortinet Fabric Ready Program, favorisce l'integrazione anche per quanto riguarda le Operations e consente di estendere i benefici del Fortinet Security Fabric, anche a tutela di investimenti pregressi e soprattutto per l'aggiunta di soluzioni nuove. In pratica i partner tecnologici collaborano e interagiscono con le soluzioni Fortinet, mentre i partner di canale possono sfruttare la collaborazione per fornire le migliori practice e soluzioni.

Non solo, questa collaborazione predispone le basi per una più ampia integrazione, che può sfociare finanche nell'acquisizione del

partner tecnologico, come è recentemente accaduto con enSilo e in precedenza con ZoneFox.

Endpoint Protection e Response (EDR)

Proprio con l'acquisizione di enSilo, Fortinet ha aggiunto un tassello importante nel Fabric, che costituisce un ulteriore beneficio di business per le aziende che dispongono di dispositivi endpoint.

enSilo, spiega D'Armento, offre una tecnologia EDR (endpoint detection e response) in grado di monitorare continuamente tutti i dispositivi connessi alla rete per identificare immediatamente la presenza di minacce avanzate e continuare a tracciarne l'azione, per attivare le possibili reazioni.

In particolare, la tecnologia EDR enSilo è in grado di individuare gli attacchi "senza file", che sfruttano le capacità native del mezzo che stanno attaccando, per esempio instaurandosi sulla sua memoria. Per bloccare i tentativi di intrusione si può ricorrere a diversi strumenti: Machine Learning, analisi manuale del codice e a un anti-ransomware basato sulla analisi comportamentale). Queste capacità si integrano con quelle di monitoraggio appena descritte, cisi da contenere gli incidenti sul singolo endpoint e poi controllando quanto accaduto, poter ripristinare il sistema allo status precedente l'attacco. Inoltre, il malware potrà essere riconosciuto in tutta l'infrastruttura, grazie all'integrazione con il FortiSIEM di Fortinet, ovvero la console per la gestione degli eventi di sicurezza e il FortiNAC per il Network Access Control.



I servizi SaaS semplificano ed automatizzano la sicurezza multicloud

Il servizio Cloud One di Trend Micro automatizza e semplifica la cloud security delle applicazioni, di container e devops in ambienti ibridi e multicloud

Il progressivo rivolgersi al cloud per tutta una serie di esigenze aziendali che spaziano dalla Business Continuity al Data Recovery, dalle e-mail all'ERP, dai DevOps allo sviluppo di Container applicativi, sta complicando enormemente il problema di come garantire la sicurezza di un insieme così variegato di applicazioni con esigenze, normative ed enti di riferimento per la protezione dei dati e la loro riservatezza anche molto dissimili.

Emblematico è quanto inerente i processi DevOps o di containerizzazione delle applicazioni, processi che permettono da un lato di accelerarne lo sviluppo e il loro passaggio in produzione, ma che dall'altro stanno imponendo un'accelerazione di passo per quanto riguarda la capacità di adeguare altrettanto velocemente l'architettura di sicurezza e la protezione contro modalità e vettori di attacco che si rivelano sempre più sofisticati.

«Il fattore velocità non è però l'unico con cui i manager aziendali e i responsabili della security si devono fronteggiare. Un problema parimenti importante e correlato al precedente è costituito dal come diminuire la complessità derivante dal dover gestire in modo integrato e semplice la sicurezza in complessi ambienti cloud e ancor più multi cloud. E' una sfida a cui abbiamo risposto con lo sviluppo del servizio Cloud One», evidenzia Salvatore Marcis, Technical Director per l'Italia di Trend Micro (trendmicro.com), società annoverata tra i principali attori mondiali per la cyber security.

Cloud One è una soluzione ideata per aiutare le aziende a soddisfare le priorità del cloud maggiormente strategiche e per farlo integra un'ampia gamma di funzioni di sicurezza in una singola piattaforma. A livello operativo consente di migrare le applicazioni esistenti nel cloud, erogare nuove applicazioni cloud-native e portare ad un alto livello l'operatività nel cloud.



Salvatore Marcis, Technical Director di Trend Micro Italy

Sicurezza semplificata e automatica

Cloud One è un servizio di sicurezza che è stato sviluppato da Trend Micro

per permettere di approcciare in modo olistico e chiaro quanto concerne la sicurezza di un complesso progetto cloud e di definirne le caratteristiche operative.

Si compone di un insieme di servizi che supportano le principali piattaforme cloud esistenti incluse Amazon Web Services (AWS), Microsoft Azure e Google Cloud. Le diverse piattaforme possono essere integrate direttamente nei processi DevOps e relative "tool-chain", e cioè l'elenco di passi che un team di sviluppo può seguire, dalla progettazione alla sua manutenzione, nel processo di rilascio di un nuovo software.

Numerose le esigenze a cui Trend Micro si è posta l'obiettivo di rispondere con lo sviluppo del servizio Cloud One. Tra queste:

- **La migrazione al cloud e al multi cloud:** il servizio Cloud One permette di automatizzare il processo di security e di protezione di ambienti cloud privati e pubblici. La protezione si estende sino a comprendere il livello di rete in modo da semplificare e rendere sicuro il processo di migrazione verso il cloud o di sua espansione in ambiti ancor più complessi.
- **Rilasci DevOps:** Cloud One abilita una protezione automatica per le applicazioni che può essere inserita direttamente nella pipeline CI/CD (Continuous Integration/Continuous Delivery), per assicurarne la protezione, identificare e risolvere più velocemente i problemi di sicurezza che dovessero insorgere e migliorarne le tempistiche connesse al loro rilascio da parte dei team DevOps.

- **Containerizzazione:** Nello sviluppo e nel ricorso a processi di containerizzazione, Cloud One permette di disporre di una sicurezza in cloud di tipo nativo e integrata con la pipeline CI/CD. La sicurezza nativa è ottimizzata al fine di abilitare la protezione e

la scalabilità tra ambienti cloud diversificati. In particolare, permette ai team DevOps di prevenire che immagini che sono state identificate come potenzialmente rischiose per la sicurezza vengano passate in produzione. Il servizio permette altresì di individuare vulnerabilità, malware e dati sensibili quali chiavi e password all'interno delle immagini del container e risolvere le vulnerabilità prima che queste possano essere sfruttate da attaccanti in fase di esecuzione.

- **Serverless:** abilita la protezione di applicazioni serverless il cui sviluppo si basa su una combinazione di servizi di terze parti tipicamente ospitati in cloud. La protezione opera proattivamente nei confronti di possibili exploit che potrebbero danneggiare i sistemi, i dati e il business ad essi correlato. Il servizio è stato sviluppato in modo da avere un impatto minimo sulle prestazioni e sul codice della applicazione.

- **Data center:** il servizio, una volta integrato con l'ambiente fisico e virtuale, abilita l'elevata

Cloud One semplifica la sicurezza di applicazioni, container e devops in ambienti multi cloud



efficienza operativa richiesta per supportare il funzionamento continuo e sicuro di un modern data center. Tra i compiti svolti da Cloud One è compreso, tramite un numero limitato di agenti, la rilevazione automatica e la distribuzione delle applicazioni di sicurezza. Il servizio permette anche di consolidare gli strumenti per la sicurezza in modo da rilevare, proteggere e rispondere alle vulnerabilità, al malware e alle modifiche non autorizzate del sistema più efficientemente.

«Cloud One sarà disponibile nel corso del Q1 2020 con tre servizi pienamente integrati: workload security, network security e application security. Le altre componenti saranno disponibili come soluzioni singole e verranno integrate con Cloud One entro la fine del 2020. Per fruirne, sfruttando le caratteristiche di AWS Marketplace come SaaS Contract API e le offerte dei partner, le aziende possono stipulare un contratto direttamente con Trend Micro o attraverso un partner» ha evidenziato Marcis. ❁

Come proteggere gli accessi privilegiati con la biometria

Zero Trust, biometria e provisioning just-in-time si combinano in Alero di CyberArk per permettere ai fornitori di servizi di accedere solo alle applicazioni abilitate

La proiezione di un'azienda verso l'esterno, il dissolversi dei confini di sicurezza tradizionali, la mobilità, il cloud e il multi-cloud sono paradigmi che allo stesso tempo offrono la possibilità di sviluppo aziendale e criticità per chi deve garantire che il tutto debba svolgersi in modo controllato e sicuro.

I benefici derivanti dall'esternalizzare della gestione di un IT sempre più complesso sono di certo molti, soprattutto perché diventa possibile concentrarsi sul proprio core business, ma questo ha come implicazione che le organizzazioni aziendali per gestire sistemi anche critici si debbano affidare a fornitori a loro remoti in base a specifici contratti.

Il dissolversi del perimetro aziendale richiede però che i fornitori remoti di un servizio di gestione dispongano di un accesso ai sistemi di cui necessitano per svolgere il compito loro assegnato e contrattualizzato, sistemi ai quali deve essere permesso di accedere solo quando ne hanno un effettivo bisogno.

Per mitigare i rischi le organizzazioni tengono in genere traccia di chi accede a sistemi aziendali ricorrendo ad un primo livello di autenticazione in cui gli utenti in qualche modo sono tenuti a dimostrare di essere realmente chi o cosa affermano di essere.

Solo al termine della fase di identificazione e autenticazione del fornitore remoto del servizio il processo di abilitare o disabilitare l'accesso ha inizio.

Il problema, osserva però Andrew Silberman, senior product marketing manager di CyberArk (cyberark.com/it/), risiede nel fatto che l'affidarsi a processi manuali per eseguire abilitazione o disabilitazione dell'accesso nei confronti dei fornitori remoti del servizio contrattualizzato è lungi dall'essere infallibile e introduce molti potenziali problemi.

Questo perché quello siglato con fornitori remoti è un contratto limitato nel tempo e gli stessi non sono in genere parte di Active Directory o servizi di directory equivalenti.

Non ultimo, hanno la necessità di accedere non all'intero panorama dei sistemi

IT ma solo ad un loro sottoinsieme e in base al tipo di contratto, alle operazioni da effettuare o alle sessioni richieste al fine di espletare il compito loro assegnato.

I team IT, osserva Silberman, hanno quindi bisogno di un modo per garantire automaticamente che questi dispositivi siano sicuri anche quando ai sistemi critici accedono da remoto.

I benefici di un approccio Zero Trust e a più fattori

La risposta alle esigenze evidenziate la si trova in quello riferito come "Zero Trust", e cioè un modello di sicurezza basato su un rigido processo di verifica delle identità che prevede che solo gli utenti e i dispositivi autenticati e autorizzati possano accedere a dati e applicazioni.

Zero Trust, in sostanza, focalizza le politiche di sicurezza e i controlli di accesso sull'identità dell'utente e del dispositivo anziché sulla posizione dell'utente o del dispositivo. Ne deriva una forte influenza su quello che costituisce un modello ideale di autenticazione.

Il verificare un'identità attraverso l'autenticazione è un processo che può tuttavia assumere molte forme. Esempi classici sono il digitare una combinazione di nome utente e password o metodi più attuali quali i sistemi di riconoscimento biometrico o l'utilizzo di un dispositivo trusted e noto.

Ad alto livello, l'autenticazione in genere assume tuttavia tre possibili forme e si esprime in:

- Qualcosa che sai (e.g. una parola segreta o una combinazione di

nome utente e password).

- Qualcosa che hai (e.g. lo smartphone personale o un badge con il nome).
- Qualcosa che sei (e.g. l'impronta digitale o la scansione della retina).

Un approccio generalmente raccomandato, evidenzia Silberman, soprattutto quando si tratta di accedere a risorse critiche, è istituire un ulteriore livello di sicurezza con autenticazione a più fattori, che richiede agli utenti di utilizzare contemporaneamente più di un metodo per dimostrare la propria identità.

Ciò può includere qualcosa che conoscono, come la risposta a una domanda su qualcosa che hanno, ad esempio a un messaggio di testo inviato al telefono cellulare.

Zero Trust e Biometria per una sicurezza ad alto livello

Il problema è che "Qualcosa che sai" e "Qualcosa che hai" sono entrambi metodi che presentano punti ciechi. Il primo espone al fatto che i cyber criminali hanno una esperienza trentennale di

cracking di password, il secondo che "Quello che hai" può essere rubato o intercettato.

La criticità insita nei primi due approcci enfatizza la valenza del terzo perché un'impronta digitale costituisce un modello unico. L'uso di una retina o delle impronte digitali può perciò bloccare le vie di attacco e migliorare notevolmente la sicurezza. Inoltre, una autenticazione biometrica non può essere rubata, persa o decifrata.

In sostanza, combinando l'autenticazione biometrica con una soluzione di back-end avanzata si dà alle organizzazioni aziendali la possibilità di concedere ai fornitori remoti di servizi esclusivamente l'accesso a quello che loro necessita e di effettuare automaticamente il processo di provisioning e di deprovisioning.

«Questo, è ciò che fa CyberArk Alero, una nuova soluzione di CyberArk fruibile in modalità SaaS. Alero combina l'accesso Zero Trust, l'autenticazione biometrica e il provisioning just-in-time in modo da garantire che i fornitori remoti possano accedere esclusivamente e in modo sicuro ai sistemi loro necessari. È una soluzione che non richiede la realizzazione di VPN, l'installazione di agenti o password e permette di creare un'esperienza senza soluzione di continuità e sicura per amministratori IT, team operativi e utenti di fornitori remoti», ha evidenziato Silberman. ❁



Sicurezza a più fattori con riconoscimento facciale

L'Intelligenza artificiale motore della nuova Security intelligence

Micro Focus, attraverso tecnologie innovative come Intersect, inserisce nelle sue soluzioni di sicurezza la potenza dell'Intelligenza artificiale e del Machine learning

L'Intelligenza Artificiale (AI) ripercorre le fasi dell'intelligenza umana che, a livello più elementare, segue una progressione in tre fasi: acquisizione delle informazioni (input), elaborazione (processing) e azione (output).

L'apprendimento nell'Intelligenza artificiale

Per ognuna di queste tre fasi esiste un corrispettivo nell'AI. Analogamente al cervello umano le macchine possono creare rappresentazioni della conoscenza (per esempio database di grafici), effettuare previsioni ottimizzate per conseguire un obiettivo e apprendere.

Le modalità di apprendimento possono avvenire tramite:

- esempio: è ciò che viene definito Machine learning con supervisione, in cui il computer ha a disposizione un set di dati con "etichette" che fungono da risposte e impara a distinguere tra diverse etichette;
- osservazione: è il Machine learning senza supervisione in cui il computer impara in modo autonomo a distinguere gruppi e schemi quando i set di dati non dispongono di etichette;
- algoritmo: è ciò che accade quando un programmatore istruisce un computer esattamente su cosa fare, passo dopo passo, attraverso un programma software.

Applicare l'Intelligenza artificiale al rilevamento delle minacce limitandosi a forme di Machine learning con supervisione, non protegge efficacemente dalle minacce interne e da quelle che non sono riconducibili a casistiche note.

Una protezione efficace richiede una combinazione di tutti i metodi di apprendimento che una macchina può utilizzare.

La Security analytics estesa di Micro Focus

L'approccio di Analytics più comune oggi nella sicurezza riguarda modelli predittivi, che combinano dati storici e comportamento in tempo reale per

rispondere alla domanda "Cosa succede dopo?".

L'analisi predittiva è, tuttavia, solo un tassello di un puzzle molto più esteso. L'approccio analitico ideale dovrebbe combinare sensori intelligenti e fonti di dati distribuiti con molteplici forme di analisi avanzata: comportamentale, delle minacce, forense, dei rischi, delle anomalie e altro ancora.

Questo approccio permette di fare molto più che prevedere o identificare una minaccia, fornendo non solo un rilevamento avanzato, ma anche informazioni su come rispondere in modo più efficace.

Questi presupposti guidano la strategia e l'offerta tecnologica di Micro Focus, che ha integrato sofisticate tecnologie di Analytics, Machine learning e Intelligenza artificiale all'interno delle sue soluzioni di Security, Risk e Governance, realizzando un efficace modello di Security intelligence.

Tecnologie come Interset, IDOL e Vertica permettono di ampliare la portata di uno dei panieri più innovativi e completi nel settore della security, organizzato nelle soluzioni ArcSight (SIEM), Fortify (sicurezza applicativa), Voltage Security (cifatura dei dati), NetIQ (identity and Access Management).

Il modello di Security analytics di Micro Focus consente non solo di prevedere "Cosa succede dopo?", ma anche di rispondere ad altre domande chiave, come: "Quante e quali minacce ci sono?" e "Qual è la migliore reazione possibile?"

La potenza del Machine learning di Interset

Interset è un software per l'analisi di sicurezza di tipo predittivo che coniuga funzionalità di analisi del comportamento di utenti e entità con tecnologie di Machine learning per fornire analisi rapide e accurate di rilevamento delle minacce. Si basa sull'attribuzione di indici di rischio individuali, definiti in base all'analisi del comportamento di un utente rispetto al suo modello esperienziale o a quello di utenti con un profilo analogo.

Interset vanta tre caratteristiche uniche rispetto ad altre soluzioni di Security analytics.

La prima è l'estensione del suo motore di Analytics, che copre più superfici di minaccia e prevede molteplici "use case" pronti all'uso, per rispondere ad attacchi noti, di tipo sconosciuto ed emergenti, a minacce interne, ad attacchi mirati e a frodi, visualizzando ogni fase dell'attacco. Queste caratteristiche eliminano la necessità di ricorrere a costosi interventi di consulenza o a complesse attività di personalizzazione del prodotto, rendendo Interset una soluzione particolarmente economica sul lungo termine.

Il secondo aspetto caratteristico è il modo di elaborazione. Interset utilizza una libreria (in costante espansione) di oltre 350 modelli testati di Machine learning e Analytics, in grado di considerare sia gli eventi sia le entità, creando un modo rapido e accurato per rilevare, correlare e quantificare i comportamenti a più alto rischio.

Infine, la sua architettura altamente scalabile, capace di combinare il proprio motore di analisi avanzata con tecnologie open source per la gestione dei Big Data, include Kafka, Spark, Phoenix, Hadoop, HBase, Elasticsearch, ZooKeeper, d3 e Kibana.

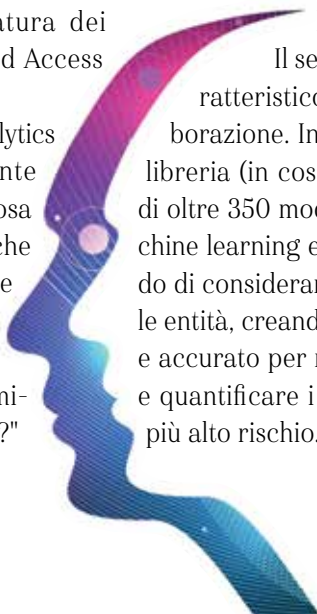
Interset e ArcSight: una combinazione vincente

L'integrazione di Interset all'interno dell'ecosistema di soluzioni Micro Focus estende le caratteristiche del motore di correlazione ArcSight ESM.

ArcSight ESM è un motore di correlazione in grado di analizzare grandi quantità di dati e rilevare, in tempo reale, minacce riconducibili a casistiche note. Consente, per esempio, di individuare molto rapidamente un malware che si è inserito nella rete, identificare dove si è propagato e attivare strumenti di risposta e messa in quarantena.

Interset utilizza tecniche di Machine learning non supervisionato per apprendere qual è la condizione da considerare normale all'interno della rete enterprise, analizzando i processi attivi su ogni singola workstation. Dopo aver definito la condizione normale, diventa possibile mettere in evidenza ogni situazione che se ne discosta, focalizzando l'attenzione dei team di sicurezza sulle anomalie che possono nascondere minacce.

La combinazione tra le due soluzioni rafforza, dunque, la capacità di individuare anomalie e permettere di rispondere a minacce di ogni tipo.



La sicurezza deve seguire l'utente ovunque esso sia

di
Gaetano
Di Blasio

Zscaler rende invisibili i dati e l'infrastruttura dell'azienda semplificando e ottimizzando le operazioni

Oltre dieci anni fa, un numero crescente di dipendenti, non solo quelli appartenenti alla classica "field force" ha cominciato a operare in mobilità. Zscaler è nata grazie alla visione del suo fondatore, Jay Chaudhry, che notò il fenomeno e comprese quanto impellente sarebbe diventata la necessità di collegarsi al dato di business ovunque si fosse. Di conseguenza, intuì come le applicazioni sarebbero uscite dal perimetro aziendale storico per andare verso Internet e il cloud.

La sicurezza così come era stata concepita fino allora avrebbe dovuto cambiare logica: «Come previsto da Chaudhry - ci spiega Fabio Cipolat, Regional Sales Manager, Italy di Zscaler - la rete intesa come confine dell'impresa sta sparendo insieme al concetto di un punto centrale in cui concentrare tutti i dati da gestire, conservare, elaborare e così via».

Basandosi su un approccio "Cloud First" Zscaler mette a disposizione 150 data center (al momento-n.d.r.), attraverso i quali fornire l'essenza di ciò che occorre ai lavoratori delle aziende: accedere alle applicazioni di business da qualsiasi rete, attraverso qualsiasi dispositivo e con le migliori prestazioni, mantenendo la sicurezza.

Distribuiti a livello globale, i suddetti data center gestiscono ogni giorno oltre 80 miliardi di transazioni, 100 milioni di malware, 120mila update di sicurezza. Sono però numeri in costante crescita, non a caso, Zscaler deriva da Zenith of Scalability, a dimostrare la possibilità di dare accesso senza limiti al Cloud agli utenti.

Per ottenere l'obiettivo di fornire un accesso ai dati di business sicuro, veloce e stabile, evidenzia il manager italiano, non occorre sapere dove sono questi dati, che possono risiedere on premise oppure in cloud, tanto quanto in applicazioni as a service quanto in infrastrutture IaaS (Infrastructure as a Service), presso fornitori terzi, come Amazon AWS, Microsoft Azure e tanti altri.

Rispetto al tradizionale approccio alla sicurezza basato su appliance, che vanno gestite con onerose operazioni di aggiornamento e dimensionamento hardware e software per garantire la scalabilità del traffico, predisponendo un sistema per il disaster recovery, e così via, Zscaler ha portato tutto in cloud, as a service, con la solidità rappresentata dai 150 data centers mondiali.



Fabio Cipolat, Regional Sales Manager Italy di Zscaler

L'accesso è garantito dalla disponibilità di Internet, che possiamo considerare una commodity, spiega Cipolat, che aggiunge: «Le applicazioni e gli utenti erano entrambi all'interno dell'azienda. Oggi le applicazioni sono in cloud e gli utenti lavorano sempre più da remoto. Sul fronte della sicurezza non possiamo guardare al vecchio perimetro, ma dobbiamo portare la sicurezza sempre con noi basandola su regole di business».

Oltre il perimetro rompendo gli schemi da Netflix a Sky

È un cambiamento epocale, ma è il futuro: «Non si può rimanere ancorati a un modello ormai superato, come fece Blockbuster, i cui vertici rifiutarono di comprare Netflix, in difficoltà agli inizi, per chiudersi nel loro castello fino al fallimento. Noi siamo passati al modello Netflix, afferma il manager per evidenziare il nuovo paradigma.

«Così come oggi posso fruire di una piattaforma streaming attraverso la quale raggiungo i contenuti che preferisco, senza dovermi preoccupare dell'infrastruttura, ma dovendo semplicemente avere un accesso a Internet, analogamente posso raggiungere le applicazioni che mi servono e con la qualità che m'interessa grazie a una connessione a Internet e alla scalabilità e sicurezza fornita da Zscaler».

Mantenendo la metafora delle piattaforme di contenuti a pagamento, il manager adotta il modello di Sky per spiegare che ogni

azienda ha esigenze di sicurezza dettate dal proprio livello di maturità.

«Su Sky posso attivare il pacchetto TV, che immaginiamo sia "la security di base", poi posso scegliere il pacchetto Cinema, che aggiunge una protezione, come potrebbe essere il Next Generation Firewall as a service. Cresce la famiglia e desidero il pacchetto bambini, così aggiungo la Sandbox. La scalabilità è un fattore chiave, ogni azienda ha un percorso di trasformazione diverso, proprio come noi a casa che cambiamo abitudini nell'uso quotidiano della tecnologia. Ciò che ieri era complesso e costoso da mantenere, come l'hardware, oggi è un pensiero in meno grazie al cloud.

Semplicità e risparmio

A tal proposito, Zscaler è leader nel traffico outbound, cioè traffico verso Internet e SaaS, grazie alla soluzione Zscaler Internet Access, sottolinea Cipolat, citando società di analisi come Gartner che posizionano l'azienda nel verticale Secure Web Gateway. Il manager aggiunge anche che, presso molte grandi imprese internazionali, Zscaler raccoglie la soddisfazione dei clienti in quanto la soluzione consente un incremento pari all'80% delle prestazioni e una riduzione di 35 volte del malware che entra nell'azienda, nonché un incremento del 60% relativamente alla riduzione dei costi.

Questi dati sono il frutto della semplificazione che non richiede connessioni VPN, reti MPLS, o, in altre parole, il dover passare

attraverso l'infrastruttura aziendale, con il rischio di non poter lavorare in mobilità perché c'è un problema nel data center.

Con Zscaler basta una connessione a Internet. Grazie a Zapp, un agente che può essere installato su qualsiasi dispositivo mobile, si accede alle risorse aziendali che sono sempre raggiungibili in cloud, attraverso i 150 data center mondiali. Zapp riconosce l'autenticazione degli utenti e abilita i livelli di sicurezza dell'utente per garantire performance e sicurezza ovunque si voglia lavorare.

Traffico invisibile e Zero Trust

Con la soluzione Zscaler Private Access, Zscaler è pioniere nell'approccio Zero Trust Network Access, cioè la possibilità di accedere alle applicazioni private, ovunque esse siano, dal data center privato alle piattaforme IaaS, senza bisogno di una VPN e tramite un accesso "direct to internet".

Rispetto alla tradizionale VPN, in essere da ormai 30 anni, come accennato, si riduce la latenza per l'accesso, si garantisce la sicurezza rendendo invisibile il mondo applicativo cliente, si incrementa la user experience garantendo velocità nei processi di business.

Zero Trust Network Access si traduce nella soluzione Zscaler Private Access e porta benefici importanti anche in scenari quali: accesso di fornitori esterni a risorse aziendali, merger e acquisizioni societarie, replacement VPN, semplificazione architetturale e riduzione dei costi interni. ❁

La protezione degli end-point e come garantirla

La soluzione di Endpoint Detection and Response di F-Secure migliora la protezione di utenti e dispositivi con algoritmi di analisi avanzata e il machine learning

Le nuove modalità di lavoro basate su una crescente mobilità, sull'home working o sul co-housing, il ricorso al cloud e al multi cloud hanno accresciuto gli aspetti a cui si deve porre attenzione al fine di garantire la sicurezza di dati e applicazioni. Tra questi, per esempio, utenti, dispositivi, applicazioni, avvisi, vulnerabilità, patch e non solo.

È un compito oneroso per l'IT, soprattutto nelle aziende più piccole che non hanno la possibilità di tenere sotto controllo le reti IT nell'arco delle 24 ore. Il risultato è che dati riferiti al 2018 evidenziano che circa il 58% delle PMI ha subito una violazione, non poche delle quali hanno portato alla chiusura dell'azienda.

La domanda che ci si pone è: cosa può fare un manager IT che disponga di risorse limitate?

La risposta può consistere nel ricorso alla tecnologia EDR (acronimo di Endpoint Detection and Response). In essenza, si tratta di soluzioni studiate per incrementare la protezione degli endpoint facendo ricorso a funzionalità di rilevamento e risposta altamente efficaci.

Come funziona una soluzione EDR e con quali benefici

Una volta in funzione una soluzione EDR raccoglie un numero enorme di eventi comportamentali relativi ai dati (come esecuzioni di processi, connessioni di rete e operazioni sui file) dalle workstation e dai server dell'organizzazione attraverso sensori endpoint non invasivi.

Questi dati sono estremamente utili per il rilevamento degli attacchi ma, se sono troppi, sono impossibili da gestire per gli analisti.

Utilizzando strumenti di analisi avanzata e con il supporto del machine learning, l'EDR è invece in grado di analizzare questi dati e intercettare gli indicatori di attacco cui corrispondono minacce sia note che nuove. Esempi di cosa una soluzione EDR può fare sono:

- Identificare processi insoliti avviati dalle workstation aziendali.



Carmen Palumbo,
Country Sales Manager
F-Secure Italia



risolverli» osserva Carmen-Palumbo, Country Sales Manager di F-Secure Italia, società specializzata nella sicurezza degli end-point.

La soluzione EDR di F-Secure e come funziona

Come evidenziato, il funzionamento della soluzione

EDR di F-Secure si basa su sensori invisibili agli utenti installati nei computer Windows, Mac e nei server in modo da monitorare il comportamento degli stessi utenti. Gli eventi/dati raccolti vengono inviati a un database in cloud per l'analisi in tempo reale. Il software in cloud esamina i dati raccolti e distingue gli eventi sospetti dalle normali attività degli utenti. Questo avviene con l'analisi comportamentale, reputazionale e dei big data, in associazione al machine learning.

A questo punto sulla dashboard di gestione viene visualizzato un elenco filtrato di avvisi e informazioni sugli attacchi. Gli avvisi sono contestualizzati e tengono conto dell'importanza degli host coinvolti, del panorama delle minacce e dei livelli di rischio attuali.

Due le strade che a questo punto si presentano per rispondere a un attacco:

- a) Esaminare il problema e rispondere mediante il team IT aziendale, utilizzando le azioni di risposta automatizzate e le indicazioni fornite dalla soluzione.
- b) Inoltrare il problema agli esperti di F-Secure in materia di risposta agli incidenti ricorrendo alla funzionalità integrata

"Segnalare a F-Secure". Gli esperti eseguiranno un'indagine approfondita sulla minaccia e consiglieranno le misure appropriate per correggerla.

I benefici dell'EDR per manager e azienda

L'EDR è un approccio alla sicurezza che ne migliora la postura e permette di disporre e fornire risposte precise e rapide sul suo stato generale.

Sempre più spesso ai manager IT viene chiesto di segnalarne lo stato ai vertici aziendali e di farlo con il supporto dei dati provenienti dalle piattaforme di gestione delle vulnerabilità e di protezione degli endpoint. Compreso in questo quali tipi di attacchi sono stati riscontrati nei sistemi, se i dipendenti stanno seguendo le linee guida per la sicurezza IT, eccetera.

Nel caso di problemi complessi è possibile, come osservato, anche ricorrere al supporto di esperti.

«Con la funzionalità 'Segnalare a F-Secure', i rilevamenti di minacce più gravi o complesse possono essere inoltrati direttamente agli esperti del nostro centro specializzato nella risposta agli incidenti, le stesse persone che gestiscono quotidianamente la cyber security dei clienti Enterprise - evidenzia Palumbo -. Ma non solo. L'EDR aiuta anche a rispettare il GDPR e a dimostrare alle autorità di avere adottato le misure basilari per proteggere l'ambiente IT. E qualora un attacco riuscisse a penetrare le difese, di raccogliere informazioni per segnalarlo alle autorità entro la scadenza delle 72 ore». ❁

- Individuare i dipendenti che utilizzano applicazioni sconosciute o dannose.
- Isolare dalla rete i computer e i server compromessi per evitare che un cyber attacco si diffonda.
- Rilevare nuovi tipi di malware nell'ambiente, anche senza firme esistenti.
- Rilevare attacchi malware fileless distribuiti da siti web che contengono codice malevolo, documenti PDF caricati sui browser o macro incorporate in file di MS Office.

In sostanza, invece di segnalare una miriade di falsi positivi in cui è difficile districarsi, l'EDR è in grado di evidenziare solo i risultati rilevanti. Una volta identificate le minacce, l'EDR supporta poi nell'eseguire ulteriori indagini e rispondere con azioni automatizzate e raccomandazioni.

Questo è un aspetto chiave soprattutto per le PMI che non dispongano delle risorse e delle competenze necessarie per gestire autonomamente i cyber incidenti di un certo rilievo.

«Con una soluzione EDR come F-Secure Rapid Detection & Response, non solo si può scoprire se ci sono problemi sulla rete IT, ma ottenere anche un aiuto concreto per

L'AI è la nuova frontiera della cyber security

di
Giuseppe
Saccardi

Il "Project Blackfin" sfrutta l'intelligenza distribuita basata su agenti autonomi che collaborano tra loro per garantire un elevatissimo livello di sicurezza

Cosa riserverà il futuro per la sicurezza non è facile prevederlo, ma di sicuro si farà sempre più ricorso all'Intelligenza Artificiale (AI). L'AI si prospetta uno strumento avanzato per assicurare la sicurezza non solo dell'IT aziendale ma anche di ambienti distribuiti quali quelli costituiti da dispositivi IoT, la cui protezione si rivela sempre più critica proprio a causa della loro crescente intelligenza.

"Quando un dispositivo è intelligente significa che è vulnerabile", è il semplice assioma di Mikko Hypponen, Chief Research Officer di F-Secure, esperto di sicurezza e docente a Stanford, Oxford e Cambridge. Per fronteggiare una situazione che per quanto concerne la sicurezza potrebbe sfuggire di mano, F-Secure ha avviato un progetto per sviluppare meccanismi di intelligenza artificiale decentralizzati.

L'iniziativa, denominata "Project Blackfin", mira a sfruttare le tecniche di intelligenza collettiva, come la swarm intelligence (o intelligenza dello sciame), per creare agenti di AI autonomi e adattativi che collaborano tra loro per raggiungere obiettivi comuni.

Invece di ricevere istruzioni da un unico modello di AI centralizzato, gli agenti sarebbero però sufficientemente intelligenti e autonomi da comunicare e lavorare congiuntamente per perseguire obiettivi comuni.

Sicurezza basata su agenti distribuiti e cooperanti

L'idea di fondo è che gli agenti imparino a proteggere i sistemi in base a ciò che osservano ma facendo leva sulla visibilità in profondità resa disponibile da una vasta rete di informazioni senza che venga però richiesto loro di condividere set di dati completi.

Questo non solo aiuterebbe ad aumentare le prestazioni degli asset IT di un'organizzazione ma eviterebbe anche la condivisione, tramite il cloud o la telemetria del dispositivo, di informazioni riservate o sensibili.

«È un progetto che richiederà diversi anni prima di realizzare appieno il suo potenziale, ma i meccanismi di intelligenza su dispositivo sviluppati



Mikko Hypponen, Chief Research Officer di F-Secure

dal Project Blackfin sono già stati integrati nelle soluzioni di rilevamento delle violazioni di F-Secure» ha evidenziato Hypponen.

Le potenziali applicazioni della ricerca Project Blackfin vanno però oltre le soluzioni di sicurezza aziendale e persino oltre il settore della sicurezza informatica e potrebbero portare a ripensare il ruolo che l'AI può svolgere nella vita quotidiana.

"Guardando oltre il rilevamento di violazioni e attacchi, possiamo immaginare queste flotte di agenti di intelligenza artificiale che monitorano lo stato generale, l'efficienza e l'utilità delle reti di computer, o persino di sistemi come reti elettriche o auto a guida autonoma. Soprattutto, penso che questa ricerca possa aiutarci a vedere l'AI come qualcosa di più di una semplice minaccia per il nostro lavoro e la nostra sussistenza", ha commentato Hypponen. ❁

Crittografia e accesso Zero Trust proteggono la rete e i dati

Le applicazioni migrano nel multicloud, ma servono reti più sicure. Un aiuto per una maggior sicurezza lo forniscono la crittografia e l'accesso Zero Trust

Sino a pochi anni fa le applicazioni aziendali sono state localizzate all'interno della rete aziendale costituita dall'insieme della rete geografica e delle reti locali con i loro router, accessi Wifi, e così via. La proprietà e la localizzazione fisica ha permesso di conseguenza di esercitare sulle stesse un forte controllo e applicare criteri di sicurezza robusti ai diversi livelli e distribuirla sugli apparati. Ora la situazione, con la diffusione del cloud e la mobility è profondamente cambiata. Qualsiasi sia il tipo di rete disponibile o in via di adozione sorge forte il problema di come proteggere la rete e i dati che vi transitano. Una risposta la si trova nella crittografia.

Dati rilevati dall'analisi di Google della crittografia HTTPS sul web, indicano che ad ottobre 2019 il traffico criptato globale su Web negli USA è risultato pari all'80% di quello

complessivo. Poco meno è risultato essere quello di Germania e Francia. La tendenza è comunque in forte crescita ed è prevedibile che nel giro di due-tre anni in rete viaggi solo traffico criptato, viste anche le normative sulla Privacy emesse dai vari paesi sempre più stringenti e l'impennata degli interessi delle aziende per la security.

Un approccio adottato, e adottabile, per mitigare i rischi è quello della creazione di reti virtuali che permettono di attuare un accesso sicuro alle applicazioni ma in modo isolato dalla rete.

Questo modo di garantire la sicurezza è riferito come Zero Trust Network (ZTNA: Zero Trust Network Access), inteso anche come una sorta di perimetro definito a software. L'obiettivo è di porre rimedio al

fatto che una volta in rete, gli utenti, inclusi tra questi quelli malintenzionati, sono liberi di spostarsi lateralmente e di accedere o esfiltrare dati.

In pratica, permette agli utenti di accedere alle applicazioni senza accedere all'intera rete, ma solo a una sua porzione. Viene in sostanza creato all'interno di questa un segmento sicuro tra l'utente previamente autenticato e una specifica applicazione che utilizzi Internet. È però l'approccio concettuale che cambia profondamente rispetto al modo di definire le reti e come proteggerle. Con il modello ZTNA non si lavora sull'intera superficie della rete ma si identifica una superficie da proteggere che comprende dati, risorse, applicazioni e servizi critici, una porzione molto ridotta rispetto alla superficie complessiva e quindi molto più facile da proteggere. Una volta stabilita la superficie da proteggere e i suoi elementi diventa parimenti possibile identificare in dettaglio i flussi di traffico che vi incidono e applicare una policy atta a garantire un accesso sicuro.

Un vantaggio di questo approccio è poi che sia le applicazioni sia gli indirizzi IP non vengono mai esposti a Internet e sono invisibili agli utenti non privilegiati o non autorizzati.*

Il modello ZTNA isola insieme di dati, applicazioni ed endpoint dal resto della rete per evitare attacchi ed esfiltrazione di dati



Cloud Azure e Web sicuri con la gestione completa del servizio

I servizi di sicurezza gestita di Radware proteggono le applicazioni nel cloud Azure e bloccano gli attacchi BOTnet che ne inibiscono il funzionamento

Per la propria digital transformation le aziende fanno sempre più ricorso all'esternalizzazione dei servizi IT. In questo processo di trasformazione l'esigenza primaria è quella di servizi completamente gestiti, soprattutto per quanto concerne la componente sicurezza, incluso in questo le Web Application Firewall (WAF) e cioè quelle applicazioni che filtrano, monitorano e, se previsto dalle policy, bloccano il traffico HTTP da e verso un'applicazione Web. Il crescente interesse per applicazioni WAF deriva dal fatto rilevante che ispezionando il traffico HTTP è possibile prevenire gli attacchi dovuti a falle nella sicurezza delle applicazioni Web.

L'interesse nel passaggio a servizi in cloud e ancor più nel multi cloud non è però dovuto solamente al desiderio di ottimizzare Capex e Opex ma anche dalla pressione esercitata sui team dediti alla security a causa della velocità con cui si sviluppano nuove applicazioni o si modificano quelle esistenti. Sono tutti eventi che richiedono un assessment continuo e frequente delle policy per la sicurezza e un livello di conoscenza molto elevato che è sempre meno disponibile nell'ambito aziendale, soprattutto nelle PMI.

Nello scenario che ne deriva, l'esternalizzazione non si traduce quindi unicamente nel fruire di un servizio di security erogato da un provider, ma anche nella richiesta di quei servizi professionali necessari per configurare e gestire le policy inerenti le applicazioni WAF.

Il servizio Cloud WAF per la sicurezza su Azure

Una risposta alle esigenze connesse alla gestione e alla manutenzione di soluzioni di sicurezza è quella data da Radware (radware.com), che sviluppa e tramite i suoi distributori di canale propone soluzioni che sono completamente gestite da esperti Radware. In particolare, il "Cloud WAF Service" è un servizio h24 completamente gestito da un team di "Emergency Response" di cui fanno parte esperti che si fanno carico di configurare e aggiornare le policy



Nicola Cavallina,
Channel & Alliance Manager
per l'Italia di Radware

di sicurezza e allo stesso tempo monitorare, individuare, allertare e mitigare in tempo reale gli attacchi apportati a un'azienda.

Come tipologia è un servizio di "Security as a Service (SaaS)" di classe Enterprise volto a proteggere le applicazioni nel Cloud Azure di Microsoft, un ambiente cloud in cui opera in modo nativo.

Operativamente, il servizio fa ricorso a tecnologie di nuova generazione per creare e distribuire le firme aggiornate automaticamente che proteggono e bloccano i vari tipi di attacchi, compresi quello molto pericolosi di tipo zero-day.

«Azure Cloud WAF fa ricorso a tecnologie di machine learning per rilevare e bloccare automaticamente i diversi tipi di attacco che possono essere portati su Web. Inoltre, man mano che le applicazioni mutano, provvede ad aggiornare automaticamente le policy in modo da permetterne rapidamente il passaggio in produzione» evidenzia Nicola Cavallina, Channel&Alliance Manager per l'Italia di Radware.

Il servizio, che tramite Azure e Azure Networks opera con una bassissima latenza, fornisce in sostanza una approfondita ed esaustiva sicurezza su Azure, accompagnata dal monitoraggio in real-time e dalla fornitura di dati statistici, oltre che alert e un reporting dettagliato degli attacchi bloccati.

Applicazioni sempre disponibili con il servizio di BOT management

Tramite computer infettati con virus possono essere avviati seri attacchi a siti web, noti come Distributed Denial of Service (DDoS). Vengono portati simulando e subissandoli di richieste lecite che ne rallentano anche di molto i tempi di risposta. L'insieme collettivo dei dispositivi in rete coinvolti è riferito come Botnet, acronimo dove BOT è l'abbreviazione di roBOT, riferendosi alla possibilità che ha una macchina intelligente di agire autonomamente.

«Non tutto il traffico Bot è malevolo - osserva Cavallina -, ma lo è circa il 26%, in pratica un quarto del traffico Internet. E in 4 casi su 5 il fornitore dei servizi non è in grado di distinguere il traffico malevolo da quello legittimo».

Una protezione da questo tipo di attacco è fornita da Radware BOT Manager, una soluzione che persegue quattro obiettivi fondamentali nella protezione delle applicazioni e dei siti Web: la protezione da

attacchi provenienti dai diversi canali esistenti; blocco proattivo e automatizzato degli attacchi tramite modelli di analisi e apprendimento in profondità del loro comportamento;

l'allestimento di un ampio database delle impronte di Bot mediante attività di intelligence realizzate con i dati raccolti da migliaia di sorgenti; opzioni di installazione delle difese di tipo non intrusivo attuate mediante API che non hanno impatto sullo stack di tecnologie già installate.

«BOT Manager è stato progettato - evidenzia Roberto Branz, Division Director Security & Cloud di Arrow ECS (arrow.com/ecs/it/), società che distribuisce e supporta le soluzioni Radware - anche per operare congiuntamente con l'intero portfolio di soluzioni Radware per la sicurezza, e in primis i servizi Cloud, tramite la sua integrazione con Cloud WAF. A questa interoperabilità si aggiunge quella con le soluzioni per mitigare gli attacchi tramite la condivisione e la sincronizzazione delle attività di intelligence».

Per le aziende che non dispongono di personale specializzato o che sono orientate ad esternalizzare il servizio di security è disponibile anche il servizio gestito di Cloud Security, un servizio di classe Enterprise che mira a proteggere da attacchi multi vettore ed a ottimizzare le prestazioni delle applicazioni.

Alla soluzione si affianca anche quella di Bot Analyzer, un servizio di valutazione gratuita per ambienti business che possono essere soggetti ad attacchi Bot e per quegli utilizzatori che desiderano disporre di una miglior comprensione dell'impatto che Bot di tipo malevolo possono avere sulla loro organizzazione. ❁



Roberto Branz, Division Director Security & Cloud di Arrow ECS

Videosorveglianza senza angoli bui per le soluzioni smart

La sicurezza fisica diventa sempre più "smart" grazie alle tecnologie digitali e alla crescita dell'Artificial Intelligence

La videosorveglianza sta crescendo in tutto il mondo, compresa l'Italia. Ci sono paesi, come la Cina, che ne fanno un uso anche eccessivo, riprendendo i pedoni che attraversano con il rosso e "additandoli virtualmente", proiettando il loro volto su tutti gli schermi digitali nelle vicinanze. Altri, come il Nostro, in cui l'installazione di telecamere è regolamentata, anche dalla legge sulla Privacy e successive modifiche, comprese quelle relative al GDPR (General Data Protection Regulation).

«Lo sviluppo di applicazioni automatizzate, fino a quelle che utilizzano algoritmi di artificial intelligence contribuiranno alla crescita di questo settore», ci evidenzia Davide Villa, Director, Business Development EMEA di Western Digital. L'ambito di utilizzo va ben oltre la video camera piazzata davanti una banca, l'ingresso di un supermercato, il varco al gate in aeroporto e così via. Sta crescendo l'uso in sistemi integrati.

Uno degli esempi più importanti, in un paese come l'Italia, ricco di musei è l'analisi in tempo reale del comportamento dei visitatori in un'esposizione di opere d'arte. Grazie all'artificial intelligence e all'analisi in tempo reale delle espressioni del viso e di altri segnali corporei, il sistema riesce ad anticipare azioni vandaliche, segnalando il rischio e permettendo ai custodi di attivarsi, magari aumentando i vigilanti in una sala.

Molto diffuse sono, inoltre le soluzioni in ambito industriale e, più in generale, manifatturiero.

È evidente che la qualità delle riprese video deve essere adeguata all'utilizzo previsto: le espressioni facciali, nel caso su descritto, non possono generare continui allarmi, altrimenti la soluzione è inutile. Analogamente, in contesti industriali occorre considerare le condizioni al contorno, tipicamente critiche in un impianto chimico o meccanico che sia.

Al di là delle videocamere, è necessario poter garantire l'operatività della soluzione che comprende i sistemi storage e di analisi posti all'edge o periferia. Laddove esiste un'esigenza di trasmissione in real time dei dati analizzati o del video, bisogna contare su tecnologia all'altezza. Non basta una telecamera 4K per avere una



visione senza angoli bui, occorre studiare e installare una soluzione, analogamente, ogni dettaglio e caratteristica deve essere valutata per ottenere il risultato cercato.

Western Digital fornisce sistemi e soluzioni per catturare, archiviare e analizzare tutti i dati relativi a un sistema di videosorveglianza di ultima generazione. Dalle soluzioni endpoint, ottimizzate per riprese 24/7 ad alta resistenza e lunga durata, progettate per operare in condizioni estreme con temperature da -25 a +85 gradi Celsius, alle soluzioni SSD e HDD progettati specificatamente per registrazione continua all'interno dei Network Video Recorders (NVRs), capaci di memorizzare diversi giorni, anche in alta risoluzione.

La gamma di soluzioni cloud, inoltre, fornisce prestazioni e ampia capacità per elaborazione dati.

La scheda microSD WD Purple di Western Digital è invece il frutto di tre generazioni di prodotti industriali dedicati specificamente al settore della sorveglianza tra cui gli storici Hard Disk Purple, evidenzia Villa, che specifica: «Con la sua elevata resistenza e una capacità fino a 256 GB, questa scheda offre uno storage on-camera a lunga durata, con possibilità di provvedere un sistema per la gestione preventiva dello storage, grazie alla funzionalità di monitoraggio che controlla l'integrità della scheda».

L'utilizzo di schede microSD WD Purple all'interno delle telecamere permette di garantire la registrazione del filmato anche nel caso



di perdita della connessione con il registratore. Le caratteristiche distintive di queste schede sono le elevate prestazioni e il numero di cicli di scrittura supportati, caratteristiche necessarie per registrare video ad alta definizione 24/7, come richiesto da un numero crescente di applicazioni di sorveglianza.

Un altro vantaggio è la manutenzione preventiva dello smart storage, grazie, al monitoraggio dell'integrità della scheda. Le telecamere compatibili sono in grado di inviare notifiche quando è il momento di fare la manutenzione della scheda microSD WD Purple, riducendo i costi della manutenzione e la possibilità di down-time. ❁



È disponibile il nuovo libro
SMART & DIGITAL TRANSFORMATION

SMART & DIGITAL TRANSFORMATION

Aziende, ambienti produttivi e città sono sempre più Smart, ma si deve garantire flessibilità, always-on, sicurezza e accesso al multicloud

Giuseppe Saccardi

Reportec

Il libro è acquistabile al prezzo di 30 euro (IVA inclusa) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444



Con il cloud servono reti più sicure, vicine e flessibili

di
Giuseppe
Saccardi

La migrazione delle applicazioni nel cloud richiede più sicurezza e flessibilità e apre spazi a provider che rispondono meglio alle esigenze degli utenti

Che sia l'ultimo del decennio o il primo degli anni Venti, il 2020 è comunque foriero di trasformazioni profonde che interesseranno sia le infrastrutture IT aziendali sia le organizzazioni dei processi.

Di certo, i temi maggiormente dibattuti degli ultimi anni sono stati la diffusione del cloud, una mobility basata su reti sempre più veloci e capillari, per non parlare della oramai prossima e politicamente dibattuta 5G, e le problematiche di sicurezza, ma meglio sarebbe dire di insicurezza, che tutto questo si è portato addietro.

Sino a pochi anni fa e in buona parte anche oggi le applicazioni aziendali sono state localizzate all'interno della rete aziendale costituita dall'insieme, perlomeno per aziende medio-grandi, della rete geografica e i suoi nodi e delle reti locali delle varie sedi con i loro router, Wifi, e così via. La proprietà e la localizzazione fisica ha permesso di conseguenza di esercitare sulle stesse un forte controllo e applicare criteri

di sicurezza robusti ai diversi livelli.

L'approccio descritto di una rete fisica che coincide con quella virtuale si va, per effetto del cloud, dissolvendo e mentre la rete virtuale vista dall'azienda rimane sostanzialmente invariata, viene sempre più a mancare la corrispondenza con quella fisica. In pratica, volendo sintetizzare, si sa cosa fa ma non si sa dove sia.

Se quello della progressiva migrazione delle applicazioni e dei servizi infrastrutturali verso il cloud è un processo oramai ben avviato, le aziende e gli utenti che vi ricorrono si aspettano di poterlo fare in tutta sicurezza, in modo "trusted" e senza doversi preoccupare di questioni legate a controlli legacy o alla corrispondenza alle normative per quanto concerne la riservatezza dei dati.

Questo esercita una forte pressione sui service provider, che d'altro canto traggono il loro profitto e si affermano come brand proprio garantendo

flessibilità, economicità, trasparenza e sicurezza.

Il contraltare della perdita di corrispondenza tra rete fisica e virtuale risiede quindi nel fatto che le aziende hanno l'opportunità di fruire dei servizi di ridondanza e business continuity tipici delle grandi reti di operatore o provider e di poter spostare le applicazioni in sedi meno costose e più efficienti dal punto di vista aziendale. Se le applicazioni possono trovarsi ovunque, le aziende hanno in sostanza la possibilità di decidere se modificarne o meno la posizione in qualsiasi momento senza influire sul servizio offerto all'utente finale.

Tale flessibilità presenta un ulteriore vantaggio: creare una maggiore concorrenza sul mercato. Le imprese non sono più legate a un unico fornitore di servizi cloud e gli operatori più piccoli o locali, più adatti a soddisfare le esigenze di un'azienda con prezzi più competitivi, hanno quindi la possibilità di entrare in gioco. ✱

La varietà delle difese nella cyber security è un imperativo strategico

Con il mercato IT in una fase di profonda trasformazione, fusioni e acquisizioni e di migrazione al cloud, la prudenza si impone. I suggerimenti di Stormshield.

Ci troviamo in una fase di profonda trasformazione dell'IT, del come viene fruito ed organizzato. Il passaggio al cloud o l'esternalizzazione delle infrastrutture IT a fornitori di servizi apre di certo nuove e concrete possibilità di affari e di ottimizzazione di Capex, Opex e per quanto concerne i risultati finanziari, ma può rivelarsi problematico nel momento in cui intervengano eventi non previsti, come improvvise situazioni di monopolio a fronte di consolidamenti o fusioni che limitano la libertà degli utenti e riducono le opportunità di scelta a disposizione. In situazioni di forza come queste non è raro il caso in cui singole aziende o - a seguito della concentrazione di aziende che offrono un dato servizio in una particolare area geografica - addirittura governi si arroghino il diritto di imporre proprie regole e prassi.

Pur tuttavia, come in natura, anche nella sicurezza IT ciò che riduce la vulnerabilità di una specie è la varietà dei tipi che la compongono.

Differenziare le soluzioni adottate e i marchi selezionati nell'ambito della cyber security ricopre quindi un ruolo fondamentale perché rappresenta l'unica garanzia di libertà e sicurezza delle aziende e degli utenti.

Ma come procedere? Un *modus operandi* lo suggerisce Matthieu Bonenfant, CMO di Stormshield (<http://www.stormshield.com>), società specializzata nella cyber security.



Matthieu Bonenfant, CMO
di Stormshield

Garantirsi una protezione efficace e adeguata

«La standardizzazione, per non dire 'livellamento' delle soluzioni per la sicurezza IT incrementa concretamente il rischio di compromissione dei sistemi e di conseguenza di intere organizzazioni» evidenzia Bonenfant.

Il dato di fatto è che se tutti gli utenti dovessero avvalersi della stessa soluzione, un hacker cercherà di norma il modo migliore per bypassarla massimizzando l'efficacia delle proprie malefatte, certo di colpire numerosi obiettivi vulnerabili con il minimo dello sforzo e del costo da sostenere.

A fronte della crescente complessità e diversità degli attacchi, l'unico modo per assicurarsi un livello di protezione ottimale non è la standardizzazione delle soluzioni, che pur in certi casi ha aspetti condivisibili, ma il ricorso e l'approntamento di un sistema di tutela articolato su più livelli.

Per esempio, il traffico e-mail va protetto da minacce come spam, phishing o spear phishing, l'uso di Internet e del cloud può essere salvaguardato attraverso processi di filtraggio URL, sandboxing, CASB (Cloud Access Security Broker), la rete può essere protetta con firewall o soluzioni UTM (United Threat Management) e i singoli computer e server possono essere dotati di software antivirus e/o altri strumenti EDR (Endpoint Detection and Response) come ultima linea di difesa contro il malware.

In pratica, si tratta di rendere il più difficile possibile il compito di un attaccante diversificando le difese e costringendolo a investire molto, allo scopo di dissuaderlo.

L'elenco non è certo esaustivo, ma rappresenta quello che può essere definita la colonna portante di una efficace difesa, ovvero l'impiego delle tecnologie più diverse, naturalmente a patto che questa protezione multistrato dia luogo ad un insieme correlato e non trascuri alcun aspetto della sicurezza.

Il volto di una protezione moderna

Ma non è solo questione di tecnologie o di come queste sono stratificate se poi fanno riferimento ad un unico brand, che può aver



applicato criteri omogenei nei diversi apparati che ha sviluppato e soluzioni che fornisce.

Oltre al mix di tecnologie, una seconda colonna portante di una protezione che sia realmente moderna, osserva Bonenfant, risiede nella diversificazione dei marchi selezionati.

In questo modo infatti si evita di restare totalmente alla mercé dei cybercriminali qualora un produttore svanisca o i suoi meccanismi di protezione dovessero fallire.

Si tratta peraltro di un principio che è anche alla base del concetto di una doppia barriera tecnologica, che consta nell'impiego in cascata di due soluzioni di produttori diversi per realizzare la medesima funzione di sicurezza. Se il primo sistema non riconosce la minaccia, probabilmente il secondo ha maggior successo e probabilità di riuscirci.

Integrare la varietà

Naturalmente ricorrere a più soluzioni di cyber security e orchestrarle ha un suo prezzo e comporta una maggiore complessità rispetto all'adozione di una singola e monolitica soluzione.

Tuttavia, questi aspetti vanno posti e pesati in relazione ai rischi

cyber a cui potrebbe essere esposta l'azienda e alle risorse che questa dovrebbe mettere in campo per limitare l'impatto di un grave attacco.

Pur adottando soluzioni diverse al fine di migliorare la postura complessiva in termini di cyber security, i sistemi più eterogenei possono essere coordinati e gestiti simultaneamente tramite interfacce di programmazione (API), che consentono di sviluppare canali di comunicazione per lo scambio di dati o comandi.

Sul mercato è infatti disponibile un numero crescente di soluzioni per l'automatizzazione e l'orchestrazione delle attività in grado di interagire con le tecnologie di sicurezza. Una cosa è indiscutibile: concetti quali "ecosistema" e "interoperabilità" non sono mai stati tanto rilevanti nell'ambito della cyber security come oggi.

«In un mercato esposto in maniera continuamente crescente alle minacce informatiche, appare quindi sensato adottare diverse soluzioni. Un aspetto strategico che, se ignorato, rischia di minare le possibilità dei CISO di fornire una protezione adeguata per i propri sistemi informativi», mette in guardia Bonenfant. ❁

La cyber security inizia con la disponibilità di dati e applicazioni

La cyber security è questione di strategia, prevenzione e pianificazione. Il Cloud Data Management su Azure e AWS di Veeam permette di migliorarla

La cyber security è un argomento che non fa dormire sonni tranquilli ai manager aziendali. Se anche le difese di aziende del settore Finance vengono infrante significa che tutte le aziende sono a rischio.

Il punto critico è che poiché tutti i dati che gestisce un'azienda, compresi i backup e i dati archiviati, possono essere un obiettivo per i criminali informatici, quello che si evidenzia essere necessaria è una solida strategia di Cloud Data Management affinché le aziende possano garantire che non siano proprio i back-up a costituire la porta d'ingresso di un attacco.

Tuttavia, mentre è possibile esternalizzare la gestione dei dati, non è possibile esternalizzare completamente la responsabilità relativa ai dati. La risposta a questo problema è che i reparti IT adottino la gestione dei dati nel cloud e allo

stesso tempo garantiscano che questi dati siano sottoposti a una gestione che ne abiliti backup, recupero e protezione.

«Quello di cui le organizzazioni necessitano è di poter contare su un approccio efficace per la protezione in-house e in ambienti multi-cloud dei dati e il loro ripristino per rispondere e reagire velocemente e responsabilmente a qualsiasi tipo di attacco che ne abbia causato l'alterazione o la perdita. E' inoltre fondamentale disporre di funzionalità che permettano di documentare il rispetto dei livelli di servizio, l'efficacia dei piani di Disaster Recovery e di migrazione attraverso test automatizzati anche a dimostrazione delle conformità della gestione rispetto alle normative vigenti» osserva Albert Zammar, vice president EMEA di Veeam Software (veeam.com).



*Albert Zammar,
vice president EMEA di
Veeam Software*

Dati al sicuro con il Cloud Data Management

La gestione dei dati nel cloud o "Cloud Data Management" è una componente chiave del portfolio Veeam e tramite essa, quale parte integrante della soluzione di "Intelligent Data Management", i dati possono essere sempre disponibili a livello di intera azienda, essere gestiti centralmente, controllati e posizionati dove possono costituire e fornire il massimo del valore. Rappresenta quindi una grande opportunità che deve essere accettata ai livelli più alti dell'organizzazione ed essere condivisa e implementata in tutta l'azienda.

Il Cloud Data Management deve però essere in grado di operare e garantire la movimentazione dei dati in un contesto che è sempre più multi-cloud e in primis in ambienti Microsoft Azure e Amazon Web Services (AWS).

«È quello che abbiamo reso possibile con il recente rilascio di Veeam Backup for Amazon Web Services e di Veeam Backup for Microsoft Office 365» ha evidenziato Zammar.

Backup e Recovery in Amazon Web Services

Veeam Backup for Amazon Web Services (AWS) è una soluzione per la protezione dei dati su AWS, integrata con Veeam Backup & Replication, che consente agli utenti Veeam di gestire i propri dati, siano essi in cloud, virtuali o fisici, all'interno della stessa piattaforma. Permette ai responsabili IT di intervenire direttamente per proteggere i dati critici e consentire

la business continuity in caso di interruzione, calamità o attacchi informatici.

Le principali esigenze a cui la soluzione risponde sono:

- **Backup nativo per AWS e ripristino:** è stata progettata per garantire i carichi di lavoro originati nel cloud. Supporta le snapshot native e i backup Veeam e ottimizza i costi connessi alla conservazione a lungo termine dei dati in Amazon Simple Storage Service.
- **Mobilità ibrida:** evita il cloud lock-in, ripristina o migra i diversi carichi di lavoro on-premise direttamente ad AWS e ripristina file o dati da AWS a qualsiasi altro ambiente supportato da Veeam (es. VMware V-Sphere, Microsoft Hyper-V, Nutanix AHV).
- **Costi di gestione ottimizzati:** supporta nel gestire, eseguire il backup e recuperare i carichi di lavoro da un'unica interfaccia.
- **Portabilità licenze cloud-ready:** permette di movimentare i carichi di lavoro in ambienti cloud con una licenza Veeam che segue in modo flessibile il carico di lavoro.

«La protezione dei dati è fondamentale sia per la business continuity sia per rispettare le normative e mantenere la reputazione del marchio. Il cloud in tutto questo è di notevole aiuto ma i responsabili IT devono comunque intervenire direttamente per proteggere i dati critici e consentire la business continuity in caso di interruzione, calamità o attacco informatico» ha commentato Zammar.

Backup nel cloud Microsoft Azure

Per il Cloud Azure, Veeam ha di recente annunciato una nuova versione di 'Veeam Backup for Microsoft Office 365 v4' (disponibile attraverso il Marketplace Azure) e la preview della soluzione di protezione dati nativa per il cloud 'Veeam Backup for Microsoft Azure' per i carichi di lavoro su Microsoft Azure. Le due soluzioni rafforzano la strategia cloud dell'azienda volta a fornire agli utenti Microsoft funzionalità aggiuntive per la protezione dei dati, scalabilità e un migliore controllo dei dati nel cloud. L'esigenza della soluzione Veeam deriva dal fatto che con Office 365, Microsoft è responsabile dell'operatività dell'infrastruttura Office 365, ma il backup e la gestione dei dati restano di competenza dei clienti.

In particolare, Veeam Backup for Microsoft Office 365 v4 fornisce un'integrazione diretta con Microsoft Azure Blob Storage, e permette alle aziende che desiderano tenere i loro dati Office 365 in Azure una soluzione scalabile e sicura. Disponibile con la soluzione anche uno strumento integrato che permettere agli utilizzatori un maggiore controllo sui costi del cloud e sui risparmi ottenuti.

Il controllo in ambiente Azure è migliorato anche tramite l'integrazione con Veeam Backup & Replication, integrazione che consente alle aziende di assumere il controllo dei propri dati nel cloud proteggendo e gestendo i backup di Azure insieme ai dati fisici, virtuali e cloud. ❁

Crescono gli enti della PA locale attaccati da ransomware

Il 2019 ha visto crescere gli attacchi ransomware ai Comuni e il rischio per i dati biometrici. I suggerimenti per proteggersi degli esperti di Kaspersky

Il ransomware è un problema con cui sempre più organizzazioni aziendali si trovano a dover fare i conti, e di sovente i conti sono molto onerosi. Nel corso del 2019 si è però assistito, ha osservato Kaspersky (kaspersky.it), società specializzata nelle soluzioni di Cybersecurity on-premise e nel cloud, allo sviluppo di una nuova e pericolosa tendenza, ovvero quella di prendere di mira le organizzazioni municipali.

I ricercatori Kaspersky hanno rilevato che, sebbene questi obiettivi non siano in grado di pagare una somma di denaro molto alta per il riscatto, risultano però i più propensi ad accettare le richieste dei criminali informatici.

Questo perché il blocco di un qualsiasi servizio comunale, influirebbe direttamente sul benessere dei cittadini e si tradurrebbe non solo in perdite finanziarie, ma anche in altre conseguenze socialmente significative ed impattanti, con conseguenze sia amministrative che penali per i manager pubblici responsabili. Ma essere sotto ricatto evidenzia anche una situazione compromessa per quanto concerne la sicurezza.

«Nel momento in cui un Comune subisce un attacco, l'intera infrastruttura viene compromessa ed è necessario richiedere un'indagine sugli incidenti e un audit approfondito. Ciò comporta inevitabilmente costi aggiuntivi che si vanno a sommare a quelli richiesti per il riscatto. Per evitare questi attacchi, però, il migliore approccio consiste nell'investire in misure proattive: soluzioni di sicurezza e di backup collaudate e regolari controlli di sicurezza», suggerisce Morten Lehn, General Manager Italy di Kaspersky

Adottare un comportamento e soluzioni adeguate

Un ruolo primario nel proteggersi dal ransomware lo ricoprono sia le persone che le soluzioni tecniche adottate.

Per esempio, uno strumento per il miglioramento della postura dei dipendenti nei confronti degli attacchi è quello offerto dalla soluzione Interactive



Morten Lehn, General Manager Italy di Kaspersky

Protection Simulation Games, che Kaspersky ha sviluppato proprio per aiutare nell'educare i dipendenti al "cyber igiene". Lo strumento fornisce uno scenario rivolto alla PA locale e si concentra sulle minacce che più la riguardano.

Sul piano tecnico invece la società di security evidenzia l'importanza di installare gli aggiornamenti di sicurezza appena disponibili, proteggere l'accesso da remoto alle reti aziendali e disporre di copie recenti di backup conservate sia su un dispositivo fisico che nel cloud storage.

Un ulteriore modo per proteggersi è poi quello di far ricorso a una soluzione come Kaspersky Endpoint Security for Business, che ha sviluppato specificatamente per proteggere i dati aziendali dai ransomware e basata sul rilevamento dei comportamenti, il controllo delle anomalie e su funzionalità di prevenzione che rilevano minacce note e sconosciute e prevengono attività dannose.

Mettere al sicuro i dati biometrici

Come se non bastasse la crescita del ransomware, mette in guardia Kaspersky, a crescere sono anche gli attacchi a quello che si considera uno dei modi più sicuri per garantire una sicurezza di alto livello: la protezione biometrica.

I dati biometrici fanno sempre più parte della vita quotidiana e sempre più frequentemente vengono utilizzati come metodo di autenticazione in alternativa ai metodi tradizionali come quelli basati su login e password.

L'autenticazione basata sulla biometria viene utilizzata per accedere a uffici governativi e commerciali, sistemi di automazione industriale, laptop aziendali e personali e smartphone.

Così come molte altre tecnologie in rapida evoluzione, anche i sistemi di autenticazione biometrica hanno tuttavia evidenziato aspetti negativi legati in particolare proprio a questioni di sicurezza.

Nel terzo trimestre del 2019, evidenzia in proposito il report di Kaspersky ICS CERT *"Threats for biometric data processing and storage systems"*, il 37% dei computer, server e workstation utilizzati per raccogliere, elaborare e memorizzare dati biometrici (come impronte digitali, geometria della mano, viso, voce e iride) e su cui sono installati prodotti di security Kaspersky, ha subito almeno un tentativo di infezione da malware.

Non sorprendentemente la principale fonte delle minacce è risultata essere internet, che è stata fonte di attacco bloccati sul 14,4% di tutti i sistemi di elaborazione dei dati biometrici.

Dopo internet, sono i supporti rimovibili (8%) la principale fonte delle minacce per i sistemi che elaborano dati biometrici, che risultano tra i più utilizzati per distribuire worm. Dopo aver infettato un computer, i worm scaricano comunemente spyware, Trojan di accesso remoto e ransomware. «Sebbene riteniamo che i nostri clienti siano cauti, dobbiamo sottolineare che l'infezione causata dal malware che abbiamo rilevato



Proteggere dai rischi l'identità digitale e i dati biometrici

e prevenuto potrebbe aver influito negativamente sull'integrità e la riservatezza dei sistemi di elaborazione biometrica. Questo vale in particolare per i database che contengono dati biometrici e che non sono dotati di alcun sistema di protezione», ha commentato Lehn. Ma cosa fare per proteggersi? Quello che gli esperti di Kaspersky consigliano è di ridurre al minimo l'esposizione a Internet dei sistemi biometrici. È preferibile per esempio che questi sistemi facciano parte di un'infrastruttura 'air-gapped', e cioè completamente isolata da altri sistemi informatici. Anche in questo caso il ruolo del personale e delle tecnologie è estremamente importante. Oltre ad assicurarsi che siano stati attivati tutti i controlli necessari per la sicurezza informatica e prevedere regolari controlli atti ad identificare possibili vulnerabilità, va anche previsto l'inserimento di un team dedicato di esperti di sicurezza altamente qualificati che deve essere regolarmente aggiornato su strategie e tattiche di threat intelligence. ❁

ANSALDO ENERGIA PROTEGGE IL SUO ECOSISTEMA

di
Giuseppe
Saccardi

Nel suo percorso di trasformazione digitale la multinazionale ha scelto Kaspersky per mettere in sicurezza impianti, macchine e filiera industriale



Luca Manuelli, Chief Digital Officer di Ansaldo Energia

Ansaldo Energia con oltre 4.000 dipendenti, di cui 2.500 in Italia, è uno dei principali player internazionali nel settore della generazione di energia.

Sul fronte della sicurezza IT ha come partner Kaspersky sin dal 2013. Tramite il partner protegge gli endpoint con tecnologie come la componente reattiva Kaspersky EDR (Endpoint Detection and Response), oggi applicata a oltre 5.000 nodi. In prospettiva, però, il problema della protezione di dati e apparati sta diventando molto più ampio e strategico, in primis per la convergenza tra i mondi IT e OT abilitata anche dalle tecnologie IoT.

«Negli ultimi anni ci sono stati alcuni importanti punti di discontinuità nella storia di Ansaldo Energia - racconta Luca Manuelli, Chief Digital Officer di Ansaldo Energia -. Ma il fattore di cambiamento più significativo è il percorso di digital transformation iniziato qualche anno fa. Un percorso che per noi significa, tra l'altro, l'adozione di macchine smart, la connessione degli impianti

produttivi e l'introduzione, nel prossimo futuro, di processi innovativi come la manutenzione predittiva. Sono passi importanti che ci aiutano a guadagnare efficienza e competitività ma allo stesso tempo aprono numerosi fronti in tema di cyber security».

La sfida della cyber security

Di fronte alla sfida complessa rappresentata dalla convergenza di IT e OT, Ansaldo Energia ha fatto una scelta strategica: non puntare su una singola soluzione o una tecnologia, ma bensì identificare un modello di partnership con cui percorrere la strada della trasformazione digitale.

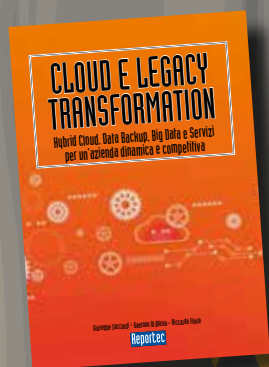
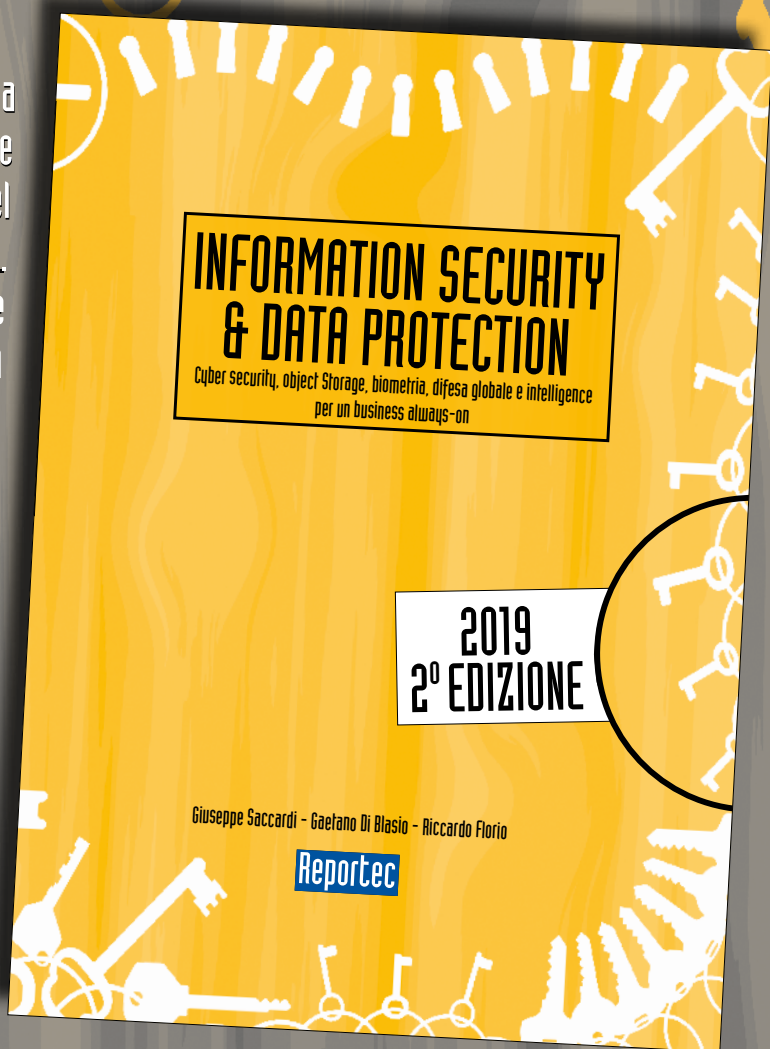
«Abbiamo adottato un modello collaborativo e abbiamo scelto Kaspersky come uno dei partner strategici» spiega Manuelli -, perché in grado di permetterci di affrontare una sfida così difficile. Stiamo implementando il collegamento delle nuove macchine di produzione smart che ci permetteranno di raccogliere in un unico data

lake tutti i dati utili al monitoraggio e controllo delle attività finalizzati anche alla manutenzione, in modo da ridurre al minimo i rischi di fermo. Oggi il nostro centro di monitoraggio controlla in tempo reale le macchine di oltre 70 clienti in tutto il mondo».

La copertura funzionale, oggi implementata su oltre 5.000 endpoint tradizionali, sarà estesa all'ambito industriale con antivirus e soluzioni di rete, per esempio sonde che monitorano in modo non intrusivo le attività così da individuare comportamenti anomali. «Il punto di forza della partnership con Kaspersky - prosegue Manuelli - è la capacità che abbiamo insieme di progettare apparati e impianti intrinsecamente sicuri. Con l'avvento delle tecnologie smart la cyber security, sta diventando un elemento strategico per tutto l'ecosistema del nostro mercato, tanto da essere ormai inserita come requisito nei bandi di appalti». ❁

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

PRODUTTIVITÀ, EFFICIENZA E RISPARMIO SUI COSTI: LE AZIENDE CHIEDONO, LA STAMPA GESTITA RISPONDE.

Sempre più aziende nel mondo stanno adottando soluzioni di MPS (Managed Print Services)

PERCHÉ NASCONO I SERVIZI MPS?

Per monitorare e gestire tutte le risorse di printing in azienda (le pagine stampate, i materiali di consumo, la reportistica) seguendo un modello in cui tutti i processi risultano ottimizzati sulle esigenze produttive.



COSA SIGNIFICA PER UN'AZIENDA RICORRERE A SOLUZIONI MPS?

Garantirsi il raggiungimento di determinati obiettivi, fondamentali per il successo nel business!

OBIETTIVI PIÙ IMPORTANTI DA RAGGIUNGERE

In termini di parco stampa e gestione documentale, le PMI italiane si prefiggono:



**RIDUZIONE
DEI COSTI**
Hardware e
consumabili



**AUMENTO DELLA
SICUREZZA**
Di documenti
e stampanti



**MIGLIORE
QUALITÀ E
AFFIDABILITÀ
DEI SERVIZI**



FATTORI CHIAVE DI SUCCESSO NEL PERSEGUIMENTO DEGLI OBIETTIVI

Sono 5 i fattori di soddisfazione che determinano il successo dei servizi di stampa gestita:

RIDUZIONE:

- del carico di lavoro sullo staff IT
- dell'impatto ambientale

MIGLIORAMENTO:

- dei flussi di lavoro
- dei costi predittivi
- del reporting/analytics

LA SOLUZIONE?

BROTHER PAGINE+

È un servizio flessibile ideato da Brother per le PMI: una soluzione di **stampa completa** che **semplifica la gestione** del parco stampa e **abbatte i costi**.



COSTO COPIA CERTO E COMPETITIVO

- Report dettagliato di stampa
- Tool web incluso per monitoraggio completo



GARANZIA PREMIUM E CONSEGNA AUTOMATICA DEI TONER ORIGINALI

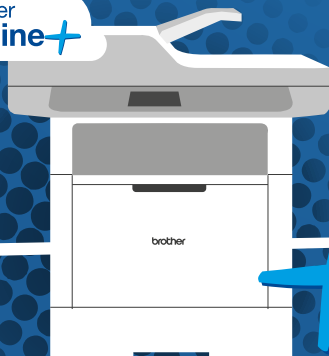
- Parco tecnologico di ultima generazione
- Funzionamento e ripristino garantiti per tutta la durata del contratto
- Consegna automatica dei toner nella sede del cliente



CONSULENZA STRATEGICA

- Per identificare i costi e le criticità dei processi di stampa
- Soluzione personalizzata sulle esigenze reali del cliente

Brother
Pagine+



brother
at your side

Scopri di più: www.brother.it