

DIRECTION Reportec

LA DIGITAL ECONOMY AL SUPPORTO DEL BUSINESS

SECURITY WANTED

La sfida per proteggere
dati e asset aziendali

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 cyber security e il GDPR un anno dopo | 16 SCADA e Industry 4.0 a rischio per protocolli IoT che non sono sicuri | 22 La sicurezza intelligente e multidimensionale di Micro Focus |
| 7 Visibilità, automazione e controllo per abilitare il business | 18 Enel: la cyber security abilita la digitalizzazione | 24 Proteggere rete aziendale e siti Web da attacchi Bot |
| 10 L'IT Security cambia pelle | 20 La nuova frontiera della sicurezza è nei servizi gestiti | 26 Applicazioni e utenti privilegiati al sicuro in SAP e nel cloud |
| 13 Oltre la compliance: proteggere un dato e tutta l'azienda | | 29 Il Cloud Data Management riduce i rischi e ottimizza i costi |

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

Stampa:
Media Print Srl, via Brenta 7,
37057, S.Giovanni Lupatoto (VR)
Editore: Reportec Srl, via Marco Aurelio 8,
20127 Milano

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

**Direction Reportec
anno XVI - numero 109**

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 cyber security e il GDPR un anno dopo

di
Gaetano
Di Blasio
e
Giuseppe
Saccardi

La riservatezza dei dati assurge a diritto civile e le aziende non possono permettersi di essere associate a un abuso di questo diritto. Previste severe sanzioni





Sembra ieri, ma è già trascorso un anno da quando il GDPR (General Data Protection Regulation) è diventato legge italiana con il Decreto Legislativo 101/2018, varato a settembre, leggermente in ritardo rispetto a quanto previsto dalla Commissione Europea, ma in linea rispetto ai tanti Paesi dell'UE. In Italia, come rivela l'inchiesta realizzata dalla redazione di Partners, la nuova legge è stata vista come un'opportunità, ma, nella pratica, in pochi hanno sfruttato l'occasione per aumentare la sicurezza, limitandosi a cercare la conformità. Quest'ultima, per la verità, era in parte già raggiunta, considerando che la nostra legislatura aveva già ispirato alcuni dei principi inseriti nel GDPR.

La novità più importante riguarda la proprietà dei dati (in Italia già affrontata), che appartiene all'individuo. Oltre a questo principio, vengono introdotte per la prima volta delle sanzioni anche molto pesanti.

L'impatto di queste caratteristiche ha reso il data privacy un argomento fortemente sentito in tutto il mondo, al pari, e detto senza enfattizzazioni, dei diritti fondamentali dell'uomo.

In pratica, tutte le aziende che trattano dati devono rispettare il GDPR, un significativo passo avanti e un successo per tutto il settore IT perché la tecnologia non può esprimere il suo pieno potenziale finché i consumatori non saranno assolutamente sicuri del trattamento dei propri dati.

Uno strumento di chiarezza

Una delle caratteristiche più virtuose del GDPR è la sua chiarezza: si sa a chi serve; si conosce la sua corretta applicazione; si conoscono le sanzioni a cui si va incontro in caso d'inadempienza. Dato di fatto è che oggi come oggi le persone reputano la riservatezza dei dati come uno dei diritti umani fondamentali, alla stregua della libertà di parola.

La ragione risiede nel fatto che ha reso tutti più consapevoli, sia a livello individuale sia organizzativo. Una delle ragioni per cui il GDPR ha fatto scalpore anche al di fuori dei settori della privacy dei dati e del diritto aziendale, è la pesante politica di sanzioni per il mancato rispetto della legge.

La Commissione Europea ha l'autorità di multare le aziende fino a 20 milioni di euro, oppure il 4% del proprio fatturato globale, in caso venga dimostrata anche solo una violazione a un punto del regolamento.

Le autorità addette alla regolamentazione della riservatezza dei dati hanno applicato queste sanzioni e la Commissione Europea dichiara che sono state notificate ben 91 sanzioni nei primi otto mesi dall'entrata in vigore del GDPR.

La più famosa di queste sanzioni è stata emessa dalla Commissione

Nazionale francese per la protezione dei dati, che ha multato Google per 50 milioni di euro nel gennaio 2019, mentre le autorità tedesche hanno eseguito oltre 40 sanzioni per violazioni al GDPR.

Senza contare i danni all'immagine. Altre conseguenze tangibili che possono essere ricondotte all'entrata in vigore del GDPR sono il calo nell'utilizzo dei cookie da parte dei siti web e una crescente diffidenza nei confronti delle attività marketing.

Il Reuters Institute for the Study of Journalism riporta in proposito un



calo del 22% nell'utilizzo dei cookie tre mesi dopo l'introduzione del GDPR.

Allo stesso tempo gli editori, le agenzie pubblicitarie e le aziende che operano nel settore IT stanno modificando i propri accordi commerciali per evitare di essere implicati in caso di violazioni dei dati in loro possesso.

Un aspetto interessante da tenere sotto controllo è quello di capire

se le discussioni che i CIO stanno facendo sul GDPR potranno avere ripercussioni a livello globale, in particolare in paesi come la Cina e gli Stati Uniti.

Il punto è se la Commissione Europea continuerà a mostrare i muscoli e il modo in cui le organizzazioni utilizzano i dati personali, sempre più la linfa vitale delle imprese.

I dati raccolti oggi possono, per esempio, avere diversi vantaggi:

- essere conservati pensando al domani.

- essere utilizzati per offrire una migliore user experience.
- servire per sviluppare nuovi prodotti che rispondano alle reali esigenze del mercato.
- essere usati per premiare la fedeltà dei propri clienti.

Con l'aumento della consapevolezza degli utenti, la tolleranza

verso le aziende che raccolgono e utilizzano i dati senza rispettare le regole, sarà minima.

Le organizzazioni che non sono in grado di affrontare in modo corretto la privacy dei dati e farla diventare parte della propria cultura aziendale, possono andare incontro a una crisi e dover pagare le sanzioni che verranno applicate dalle autorità di regolamentazione.



Visibilità, automazione e controllo per abilitare il business

L'architettura di HPE Aruba per catturare i dati in sicurezza, direttamente dove sono prodotti

Il complesso scenario della cyber security va calato nel contesto della digital transformation funzionalmente alle strategie aziendali per l'utilizzo dei dati. Per questo l'acquisizione di Aruba Networks, oltre quattro anni fa, è stata uno degli investimenti più importanti per HPE, in quanto centrale nella definizione della strategia di HPE, che si è focalizzata sull'Hybrid IT, (quindi il "core" rappresentato da, server, storage e servizi professionali, per abilitare la digital transformation sul fronte della gestione dei dati dal punto di vista computazionale e di archiviazione) e sulle tecnologie di edge.

Quest'ultima talvolta è la "periferia delle aziende", laddove nascono i dati che alimentano i processi di business: il livello di approvvigionamento di un materiale in fabbrica, la temperatura di un paziente in ospedale e via dicendo.

«È qui che si cala verticalmente il ruolo di HPE Aruba nella strategia aziendale, quale tecnologia innovativa, largamente riconosciuta nel mondo dell'accesso», afferma Fabio Tognon, che di HPE Aruba è Country Manager.

Tecnologia recente che il lungimirante fondatore, Keerti Melkote, ha impostato con logica open per accogliere e integrare facilmente tutte le novità tecnologiche del futuro.

L'approccio cloud ibrido nativo, ben coordinato con la strategia di tutta HPE, ne esalta le potenzialità nel "catturare" i dati, nel modo più sicuro, là dove vengono generati. Si tratta di dati di utenti, sempre più in mobilità, o relativi a dispositivi di varia natura, riferiti sia al mondo dell'IoT sia a quello dell'industrial IoT.

HPE Aruba non a caso è chiamata internamente la divisione dell'edge, il cui ruolo è centrale in quanto direttamente collegato al raggiungimento di obiettivi di business.

È evidente, rimarca il country manager, che il dato raccolto deve essere veritiero, integro, sicuro e garantito sia se si tratta di informazioni per le vendite in ambito retail sia che il dato regoli un parametro industriale in un'applicazione di manutenzione preventiva.

Per questo HPE Aruba ha realizzato un'architettura di sicurezza che risponde alle odierne sfide legate alla robustezza e flessibilità della rete nonché alla sua gestione e alla capacità di risposta alle minacce.



*Fabio Tognon, Country
Manager HPE Aruba*



Visibilità, automazione e controllo

La rete e l'accesso alla stessa devono avere tre caratteristiche fondamentali per HPE Aruba: visibilità completa di tutto ciò che sta sulla rete, il che è possibile solo realizzando partnership e avendo un sistema aperto. In futuro, infatti, i dispositivi collegati sulla rete, come su accennato, apparterranno a differenti tipologie, come lampade, condizionatori, irrigatori, tornelli d'ingresso in azienda, se pensiamo alla domotica e al building, ma anche sistemi medicali e tanti altri che, per collegarsi tipicamente tramite WiFi, dovranno poter dialogare con la rete.

Attraverso il software di HPE Aruba, a ogni "entità" che si attesta sulla rete, sia utenti sia dispositivi, viene fornito un profilo. Ciò permette anche di gestire tali entità in gruppi omogenei, per esempio, i quali avranno un comportamento coerente.

Un secondo punto fondamentale è quello dell'automazione, che è necessaria per gestire la complessità e, soprattutto la sostenibilità di

tutto quanto accade sulla rete.

«Molti nostri clienti dispongono di professionalità e strumenti per osservare il comportamento della rete e attivare un'azione d'intervento, che sempre meno può essere gestita da un individuo, a favore di sistemi automatici», sottolinea Tognon

Occorre, però, uno strumento di controllo che consenta di verificare il corretto funzionamento e l'adesione alle politiche definite per le diverse entità connesse in rete. Attraverso la soluzione ClearPass, HPE Aruba fornisce uno strumento di prevenzione e controllo, in grado di agire, per esempio bloccando un traffico sospetto, isolando un dispositivo o segnalando un comportamento anomalo. ClearPass, in sintesi, applica le azioni previste dalle policy definite e concordate con tutto l'ecosistema che attiene alla rete.

L'ecosistema di sicurezza e il controllo con ClearPass

Secondo la visione di HPE Aruba, la sicurezza deve coinvolgere più attori di un ecosistema, perché

non esiste un factotum che possa gestire da solo sistemi tanto complessi ed eterogenei. Per questo ClearPass è una soluzione multi vendor aperta.

Non è pensabile che si possa utilizzare solo tecnologia HPE Aruba, ribadisce Tognon, che spiega: «L'azione di controllo, difatti, è il risultato della collaborazione tra più aziende della security, ciascuna con le proprie specializzazioni verticali. In sostanza ClearPass è il "giudice" che prende la decisione finale su quale azione attivare per risolvere l'eventuale problema, il quale potrebbe essere rilevato da un sistema per la sicurezza perimetrale oppure da un comportamento anomalo di un applicativo». Questo a prescindere dalla tecnologia di rete utilizzata dall'utente finale. ClearPass, infatti, introduce il controllo attraverso le policy che è possibile definire per qualsiasi entità, sfruttando la capacità di dialogare con tutti i sistemi di rete. Ciò anche a garanzia degli investimenti pregressi sostenuti e nel solco della logica open sposata da tutta HPE.

Oltre che in base a policy predefinite il controllo si può gestire attraverso algoritmi UEBA (User Entity Behaviour Analytics), che sfruttano il machine learning, osservano costantemente il comportamento delle entità, assegnano dei punteggi di rischio e proprio basandosi su quest'ultimo consentono a ClearPass di attivare un'azione. Per esempio se una lampada mostra un consumo di banda molto più alto del solito, si può approfondire ed eventualmente intervenire. La logica del controllo, in questo modo, permette di applicare la sicurezza, senza bloccare indiscriminatamente la rete o l'accesso a un servizio, riducendo i disagi per gli utenti.

Con l'approccio di HPE Aruba si evitano i muri e si abilita l'innovazione, permettendo al responsabile della sicurezza di avere sogni tranquilli.

Questo è realmente possibile, afferma Tognon, nel momento in cui si comprende come la sicurezza,

grazie a un'architettura che abilita i processi aziendali, coinvolge tutta l'azienda.

HPE PointNext Services e il futuro consumption driven

Trasversalmente c'è la divisione HPE PointNext, che accompagna i clienti verso la trasformazione, anche organizzativa, che l'uso dei dati nei processi di business comporta, con anche tutte tematiche legate ai big data.

Tra i servizi HPE Pointnext, importante è il servizio GreenLake, che fornisce tali tecnologie in modalità a consumo, secondo la roadmap che il CEO di HPE, Antonio Neri, ha disegnato affinché l'azienda sia totalmente "consumption driven" entro il 2022.

Una modalità di fruizione già disponibile, ovviamente, in ambito hybrid IT e, oggi in parte ma del tutto a fine anno, anche per le tecnologie di networking HPE Aruba, quando HPE espanderà il suo offering GreenLake con "HPE



GreenLake for Aruba".

La tematica del network as a service viene ulteriormente rafforzata grazie alla flessibilità relativa alla gestione dei dispositivi di rete, che può essere on premise o in cloud. Questo è possibile, come accennato, grazie all'architettura di HPE Aruba che Melkote ha previsto nativamente in cloud, con Aruba Central, che fornisce massima flessibilità e scalabilità.

«Secondo le nostre simulazioni - evidenzia Tognon - i team aziendali riescono a gestire solo un 10% degli incidenti sulla rete. Crescendo i dispositivi connessi la situazione esploderà, rendendo impensabile che le aziende possano sostenere i costi di una gestione preventiva della rete e degli incidenti che su essa avvengono».



L'IT Security cambia pelle

di
Giancarlo
Lanzetti

La sicurezza si avvia a diventare sempre più un enabler dell'innovazione: non serve più solo per ridurre i rischi ma per creare anche nuovo valore aziendale

Dopo avere ascoltato gli esperti che si sono succeduti sul palco in occasione della IDC Security Conference 2019 sembra che si debba parlare di una nuova IT Security più che di una pura evoluzione della stessa osservando il futuro immediato di questa disciplina.

Sostiene Giancarlo Vercellino, Associate Research Director di IDC Italia: «Nel corso dell'evento abbiamo cercato di argomentare una traiettoria evolutiva della sicurezza IT: all'inizio il perimetro di sicurezza era la rete, poi è diventato il dato, forse domani sarà l'individuo. La tutela della persona potrebbe diventare il fine ultimo della sicurezza, migliorando la postura di sicurezza nei comportamenti individuali e tutelando quegli asset intangibili che ciascun individuo usa con leggerezza e senza particolare attenzione, come la sua identità digitale. Inoltre oltre che sulla tecnologia sarà necessario investire in processi e formazione, in modo tale che ciascun individuo comprenda che la battaglia per la sicurezza IT si vince o si perde in base ai suoi comportamenti di ogni giorno».

Dal lato dell'offerta sono da aspettarsi delle modificazioni: «Nell'immediato, aggiunge il manager di IDC, possiamo attenderci un ridisegno sempre più ampio e profondo delle tradizionali categorie applicative attraverso un impiego estensivo del machine learning.

A livello globale è prevedibile un riassetto del mercato con un consolidamento nel numero degli operatori in un orizzonte di qualche anno».

A proposito di mercato il software per la sicurezza IT, segmentato nelle aree della Web Security, del Security & Vulnerability Management, della Network Security, dell'Identity & Access Management e dell'Endpoint Security, rappresenta in Italia un valore complessivo di circa 380 milioni di euro nel 2018 con un CAGR 2018-2021 di circa 7 punti percentuali.

Tra i nuovi fenomeni in ascesa viene additato il Doxware, di cui in verità si parla già da un paio



di anni. Si tratta di una nuova forma di estorsione dove il criminale minaccia di rivelare informazioni riservate nel caso in cui non riceva in cambio una somma di denaro.

In definitiva secondo IDC la Security si avvia a diventare sempre più un enabler dell'innovazione: non serve più solo per ridurre i rischi ma per creare anche nuovo valore aziendale, grazie a nuovi modelli di business come l'Edge computing. Questo significa che la sicurezza sta cambiando pelle, diventa più estesa e integrante con altre funzioni o domini aziendali, IT e non IT, con la

conseguenza, ad esempio, che il Ciso dovrà occuparsi anche di cose al di fuori del suo raggio di azione.

Lo Zero Trust di Oracle

Come noto negli ultimi anni, con i processi di adozione del cloud, il perimetro aziendale da proteggere non è più delimitato soltanto dalla infrastruttura "on premise". Di conseguenza un fornitore di soluzioni di sicurezza non può più proporre ai propri clienti forme di difesa tradizionali: si deve fare un salto di qualità, in particolare integrando il controllo e la gestione dell'identità, la protezione del cloud, le applicazioni.

Negli ambienti ibridi, o cloud-only, servono modelli nuovi e dinamici che sappiano contrastare efficacemente minacce sempre più complesse e strutturate.

«Per rispondere a queste istanze, Oracle - come ci spiega

Marella Folgori, Country Sales Leader, Security & Manageability Oracle Italia - ha elaborato un proprio modello di sicurezza multi livello, definito Zero Trust. Tale approccio indirizza la difesa delle identità, delle applicazioni web e degli ambienti multicloud proprio per mitigare le minacce riducendo costi e complessità. La chiave è l'utilizzo strutturato di nuovi strumenti che consentono l'analisi

del comportamento e delle attività anomale degli utenti, l'introduzione di algoritmi di machine learning che automatizzano le attività di analisi, il controllo capillare delle modalità di accesso alle applicazioni tramite meccanismi quali Single Sign On e l'autenticazione multi-fattore; a questo si affianca la capacità che questo tipo di soluzioni offre di avere sempre in tempo reale una visione della propria situazione in termini di security e di compliance, per capire sempre dove e come migliorare».

Per ridurre costi e complessità, precisa ancora Folgori, soprattutto in caso di ambienti cloud, è necessario orientarsi verso opzioni di sicurezza cloud native, che consentono un'implementazione rapida e semplice e una fruizione anche da parte di personale con competenze di sicurezza meno elevate. Per evitare oneri operativi eccessivi, infine, è buona pratica adottare strumenti di analisi degli accessi, delle identità integrati tra loro e automatizzati.

Tale strategia verrà intensificata perché il cloud avrà un ruolo sempre maggiore in questo percorso di continuo miglioramento delle capacità di sicurezza. «Tutti i cloud provider, conclude, stanno lavorando per aumentare continuamente il livello di sicurezza dei loro ambienti; ma solo sviluppando soluzioni native in cloud si potrà realmente rispondere in modo adeguato alle nuove minacce, beneficiando, per le proprie analisi, delle possibilità computazionali e di scalabilità che solo il cloud può garantire».





I binari paralleli di Akamai

Nel settore della cybersecurity l'elemento sostanziale, dal quale dipende la funzionalità e il successo dell'intero sistema di sicurezza, sostiene Nicola Ferioli, Head of Engineering di Akamai Italia, è quello dell'interazione con l'utente: è fondamentale che sistema di difesa e utente viaggino su due binari paralleli. Il primo non deve mai impattare sul secondo; non è pensabile che i sistemi di difesa rallentino l'utente oppure ne impediscano l'accesso erroneamente. Se questo avviene, significa che la difesa non agisce in maniera corretta.

Grazie anche al contributo dell'intelligenza artificiale, le minacce si stanno evolvendo di continuo e in modo molto rapido. Le reti bot, nella loro continua evoluzione, utilizzano tecniche sempre più sofisticate per lanciare gli attacchi

e dal punto di vista della difesa è fondamentale passare ad utilizzare tecniche di intelligenza artificiale che tramite il machine learning analizzino quali sono i trend e le evoluzioni dei vettori di attacco, per poterle poi affiancare all'intelligence operata da personale umano. In poche parole, mentre in passato i meccanismi di difesa erano relativamente semplici, si poteva contare il numero di pacchetti in arrivo o mettere delle semplici soglie di accesso, ad oggi un'analisi profonda degli attacchi si basa necessariamente su tecniche di intelligenza artificiale. Senza questa, ancora una volta, viene meno l'efficacia.

Abbiamo chiesto a Ferioli cosa il recente accordo firmato da Akamai con Microsoft sta insegnando? La sua risposta: «Akamai lavora con Microsoft per quel che

riguarda l'integrazione della sua CDN con i Media Services e il Blob Storage di Microsoft Azure. La collaborazione, dice, facilita le aziende del settore media a rendere più conveniente la combinazione tra il processing del video sul cloud Azure con la delivery sull'Edge, sia nelle fasi di preparazione che di riproduzione dei contenuti. Akamai ora connette direttamente l'Edge ad Azure tramite una connessione Azure ExpressRoute ad alta velocità. Questo sta portando un notevole incremento di efficienza nella memorizzazione e nella delivery dei contenuti tra Azure e la CDN di Akamai e allo stesso tempo i clienti avranno a disposizione strutture con costi ridotti e più facilmente preventivabili. I nostri clienti stanno ampliando le proprie librerie e distribuendo una maggior quantità di contenuti a un pubblico più esteso, con livelli di qualità più elevati rispetto al passato. Molti di loro chiedono assistenza su come semplificare la gestione e la delivery dei video, rendere scalabili i propri servizi e spostare le funzioni dei propri workflow sul cloud. Unendo le forze di Microsoft Azure, Azure Media Services e Azure Storage con l'ampia portata dell'Akamai Edge, stiamo riuscendo a creare un ambiente in grado di contenere i costi, ottimizzando, al tempo stesso, le performance e la scalabilità per i fornitori di contenuti. Lavorando a stretto contatto, Azure e Akamai potranno offrire una piattaforma in grado di aiutare i clienti ad aumentare la loro reach e a soddisfare meglio le esigenze dei consumatori». ❁

Oltre la compliance: proteggere un dato e tutta l'azienda

Check Point Software Technologies illustra le problematiche di una limitata visione sulla sicurezza. Gli errori del cloud e l'auditing con un clic

Il ridotto budget che le imprese italiane dedicano alla sicurezza informatica, nell'ultimo anno, è stato principalmente dedicato alla conformità con le norme e, in primis per il GDPR (General Data Protection Regulation), il che non sarebbe negativo, se non fosse che buona parte delle imprese non ha «compreso bene il GDPR», sostiene David Gubiani, Regional Director Security Engineering Southern Europe di Check Point Software Technologies, che precisa: «per molti si è trattato di rispondere alle "domande" poste all'ufficio legale, invece di mettere in piedi una vera strategia per la cyber security e spendendo solo in consulenza strategica, ma senza acquistare soluzioni di prevenzione e protezione. Per una vera strategia ci vogliono tempo, strumenti e le persone giuste. Occorre però distinguere il comportamento delle piccole e medie imprese da quello delle medio grandi».

L'esperto di Check Point continua, evidenziando che presso le Pmi, ci si affida talvolta a qualche piccolo system integrator, non sempre dotato di una conoscenza approfondita sulla sicurezza nel suo complesso. Quindi si tende a coprire le falle con le soluzioni "minime", come sono definite dal GDPR. Questo perché manca una cultura della sicurezza e una conoscenza delle minacce reali. In pratica ci si "limita" a tutelarsi dal rischio delle sanzioni, ma non s'impone una strategia, avendo comunque pochi fondi da investire, a differenza delle grandi aziende.

Il problema cloud

Il cloud è sempre più presente, anche nelle grandi aziende, ma la facilità con cui viene utilizzato rende difficile assegnare la responsabilità della sua gestione: molto spesso i progetti cloud partono in autonomia. È capitato che il dipartimento Risorse Umane di una grossa organizzazione abbia contattato un'azienda esterna per attivare dei portali cloud, senza coinvolgere la filiera di controllo preposta, in altre parole il dipartimento



David Gubiani, Regional Director Security Engineering Southern Europe di Check Point Software Technologies

IT. I suddetti portali erano rivolti all'esterno, ma permettevano l'accesso.

Non si tratta di un caso isolato: «Gli analisti di Gartner - cita Gubiani - affermano che l'80/90% dei problemi relativi alla sicurezza nel cloud sono dovuti a errori di configurazione».

«Questo anche perché è tutto apparentemente molto semplice ed è facile creare funzioni molto rapidamente e altrettanto farlo con automatismi (si pensi alle funzioni Lambda di Amazon Web Service)», continua l'esperto.

Così anche le aziende medio piccole si ritrovano con centinaia di funzioni sulle quali, in pratica, non ha controllo. Le aziende spesso rincorrono questi progetti senza pensarli subito in ottica di cyber security, per poi correre a tappare i buchi, evidenzia il manager italiano, il quale segnala anche quanto spesso i dati più sensibili siano proprio in cloud, che non sempre viene protetto adeguatamente con un forte rischio, come nel caso su citato, di esporre dati personali e sensibili.

Sono prassi consolidate che nascono dalla scarsa cultura e dalla mancanza di fondi. Nella Pubblica Amministrazione è anche peggio a causa della lentezza dei processi decisionali, rimarca ancora Gubiani.

Una protezione, una gestione e l'auditing on demand

Data la situazione finora illustrata, è comprensibile perché l'esperto di Check Point Software

Tecnologies sottolinea che, prima ancora di preoccuparsi della cyber security, occorre concentrarsi dell'infrastruttura: «Siamo sicuri delle logiche di accesso, networking, controllo, cloud? Perché senza le cognizioni basilari si lascia la porta aperta a qualsiasi malintenzionato».

Nel tempo, continua l'esperto, si sono avvicinate diverse formule per affrontare le minacce cyber, dalla soluzione unica al best o breed, che comporta grossi investimenti e richiede grandi capacità di management, che non tutti possono permettersi.

«La nostra visione - spiega il Regional Director Security Engineering Southern Europe, - è quella di proteggere tutto il perimetro, che parte dal singolo dato per abbracciare tutta la rete e i dispositivi. Tutto, però, deve essere gestibile attraverso un'unica soluzione di management. Aldilà dell'essere rapidi nell'affrontare qualsiasi tipo di attacco e, prima ancora, di prevenirli».

Prevenire invece che curare dunque, semplificando la gestione grazie a un software che è sempre lo stesso per ogni strumento e grazie a «ottime soluzioni posizionate nei vari punti di controllo, abbinate a politiche e capacità di monitoraggio, focalizzando il know how delle persone».

Il sistema unico, in pratica, permette a ciascun operatore di essere autonomo e ottimizza gli sforzi di formazione. Inoltre, si ottiene una visibilità più "alta", indipendentemente dall'ambito in cui sta lavorando, che sia: cloud, endpoint,



network, gateway e così via. Una visibilità completa frutto del monitoraggio continuo, afferma Gubiani, che consente in qualsiasi momento di approfondire ogni evento di sicurezza nel dettaglio. Addirittura, questa visibilità permette di, con un solo clic, di ottenere immediatamente lo stato della compliance, potendo stampare un documento pronto per essere direttamente consegnato a un eventuale auditor.

Il software unico che unifica il management si abbina a una serie di soluzioni, sempre in evoluzione risolvono alcuni temi importanti.

Cloud Guard Dome9

Il primo di questi temi è il citato cloud: la soluzione SaaS di Cloud



Guard Dome9 fornisce efficienza operativa per un più rapido time-to-protection. Va bene per il cloud, anche per quelle funzioni che si attivano per pochi secondi, perché si ha traccia e possibilità di risalire a tutto quanto accaduto.

In aggiunta a questo, evidenzia Gubiani: «c'è tutta la componente cloud che permette di gestire allo stesso modo tutti i tipi di cloud, privati, ibridi, pubblici, e tutti i servizi PaaS, IaaS e SaaS.»

Maestro

Maestro risponde all'esigenza di fronteggiare minacce che evolvono rapidamente e richiedono improvvisi picchi di capacità computazionale. Di fatto consiste in un maestro "d'orchestra", che può

aggiungere "musicisti" e "strumenti" a piacere. In termini tecnici è un hyperscale di sicurezza, che, spiega Gubiani: «permette di collegare fino a 52 gateway in maniera lineare, con la stessa velocità con cui si collega uno switch. In pratica il tutto si autoconfigura in 6 minuti. Quindi Maestro permette di aggiungere apparati senza dover sostituire vecchi dispositivi ma sommandoli a questi».

Check Point Infinity Total Protection

Dall'architettura Infinity, nasce un'offerta innovativa, con un modello di servizio che, agli abbonati, consente di attivare rapidamente la soluzione di sicurezza che occorre, in una modalità tipo a

consumo.

Le soluzioni disponibili includono: *Real-time Threat Prevention*: protezione contro le Advanced Persistent Threat (APT) e i malware zero-day, che utilizza la tecnologia sandboxing in tempo reale; protezione anti-ransomware e tecnologie anti-bot, basate su un sistema di threat intelligence in tempo reale integrato e cloud-based e sulla tecnologia machine learning per l'identificazione di nuove minacce.

Advanced Network Security: firewall per la prevenzione delle intrusioni e il controllo delle applicazioni, in reti di qualsiasi dimensione.

Cloud Security: sicurezza avanzata di prevenzione delle minacce in ambienti SDN e nei sistemi cloud pubblici, privati e ibridi.

Mobile Security: prevenzione dei malware sui dispositivi mobile iOS e Android, identificazione delle reti corrotte, container sicuri, protezione dei dati e crittografia dei documenti.

Data Protection: anti-ransomware per ransomware noti e sconosciuti, protezione dei dati e crittografia dei documenti, sicurezza del browser, suite di Endpoint Protection integrata e sicurezza forense.

Integrated Security & Threat Management: un ambiente di gestione della sicurezza unificato che supporta la gestione multi-dispositivo, multi-dominio e multi-admin, con visibilità completa delle minacce che supporta la raccolta, la correlazione e l'analisi degli attacchi e gli strumenti di reporting per conformità e audit. ❄

SCADA e Industry 4.0 a rischio per protocolli IoT che non sono sicuri

I laboratori Trend Micro hanno individuato difetti di progettazione utilizzabili per sottrarre dati o compiere attacchi. Quello che serve sono soluzioni IPS che prevengano le intrusioni

Due tra i principali protocolli IoT sono a rischio attacco a causa di vulnerabilità significative nella progettazione e questo rende i dispositivi esposti. Il vulnus lo ha individuato e segnalato Trend Micro, azienda globale nello sviluppo di soluzioni di cybersecurity, all'interno della sua ricerca "The Fragility of Industrial IoT's Data Backbone".

In particolare, le criticità si evidenziano per quanto concerne la sicurezza in ambito OT (Operational Technology) a seguito della individuazione di difetti e vulnerabilità all'interno di Message Queuing Telemetry Transport (MQTT) e Constrained Application Protocol (CoAP), due protocolli machine-to-machine (M2M) molto utilizzati. I punti deboli possono essere sfruttati a fini di spionaggio industriale, attacchi mirati o di tipo denial-of-service.

Le cifre in gioco sono da vero allarme. In un periodo di soli 4 mesi, i ricercatori Trend Micro hanno scoperto che oltre 200 milioni di messaggi MQTT e più di 19 milioni di messaggi CoAP erano stati trafugati a causa di server esposti. Gli attaccanti possono localizzare questi dati utilizzando semplici parole di ricerca e trasformarli in informazioni su asset, personale o tecnologie che possono essere utilizzate per attacchi mirati.

Il problema, ha commentato Gastone Nencini, Country Manager di Trend Micro Italia, è che i protocolli citati non sono stati progettati pensando alla security, ma sono utilizzati in un numero sempre maggiore di ambienti critici e questo rappresenta un grande rischio.

Le criticità che ne derivano vanno seriamente considerate ma possono anche essere l'occasione per un approccio olistico alla sicurezza degli ambienti OT che blocchi gli attacchi volti a controllare da remoto gli endpoint IoT, compiere attacchi denial-of-service e, sfruttando funzionalità specifiche dei protocolli, muoversi lateralmente nella rete aziendale.

Peraltro, la ricerca ha evidenziato anche diverse vulnerabilità, rese pubbliche dalla Zero Day Initiative (ZDI): CVE-2017-7653, CVE-2018-11615 e CVE-2018-17614.

Ma cosa fare in proposito? Quello che suggerisce Trend Micro sono quattro punti:

- Implementare le corrette policy per rimuovere i servizi M2M che non sono necessari
- Effettuare controlli periodici utilizzando servizi di scansione internet-wide, per assicurarsi che i dati sensibili non vengano trafugati attraverso servizi IoT pubblici
- Implementare un workflow per la gestione delle vulnerabilità, per proteggere la supply chain
- Mantenersi al passo degli standard industriali, perché la tecnologia è in continua evoluzione

Non ultimo, osserva Nencini, utilizzare strumenti adeguati di Intrusion Prevention System (IPS) come quelli che fanno parte della famiglia Trend Micro TippingPoint,

Proteggere dati e applicazioni in tempo reale con TippingPoint

La soluzione di security sviluppata da Trend Micro ha la sua genesi nella considerazione che oggi la salvaguardia degli asset e dei dati di rete dalle minacce richiede una visibilità dettagliata in tutti i suoi livelli e risorse, nonché un approccio dinamico che utilizzi la consapevolezza e l'automazione necessaria per adattarsi a nuove minacce, vulnerabilità e cambiamenti quotidiani della rete.

Tali minacce anche molto diverse, osserva Nencini, richiedono un approccio integrato alla sicurezza, una integrazione che trova la sua risposta in TippingPoint Threat Protection System (TPS), una

sofisticata piattaforma di sicurezza della rete che permette di disporre di una protezione ad alta precisione dalle minacce contro le vulnerabilità note e non divulgate. Nel complesso, TPS fornisce una copertura per tutti i diversi vettori di minacce, da quelle avanzate al malware e al phishing

Operativamente TPS utilizza una combinazione di tecnologie, tra cui il controllo approfondito dei pacchetti, la reputazione delle minacce/degli URL e l'analisi avanzata dei malware su base flow-by-flow per rilevare e impedire gli attacchi sulla rete.

Nel suo complesso, la combinazione di tecnologie consente di assumere un approccio proattivo relativamente alla sicurezza che fornisce una consapevolezza contestuale molto approfondita e un'analisi dettagliata del traffico di rete.

È una tale consapevolezza, osserva Nencini, che combinata con le informazioni sulle minacce provenienti da Digital Vaccine Labs (DV-Labs) fornisce la visibilità e l'agilità



Gastone Nencini, Country Manager di Trend Micro Italia

necessarie per tenere il passo con le moderne reti aziendali e dei data center caratterizzate da dinamismo ed evoluzione continua. Numerose le funzionalità che prevede. Tra queste il controllo SSL on-box per contrastare attacchi crittografati, prestazioni scalabili, modello di licenza flessibile, machine learning in tempo reale, Enterprise Vulnerability Remediation per risolvere le vulnerabilità integrando le soluzioni di terze parti con il portfolio TippingPoint, l'analisi delle minacce con protezione estesa tramite l'integrazione con Deep Discovery Analyzer, la prevenzione integrata con le soluzioni di rilevamento delle minacce Trend Micro Deep Discovery e il controllo del traffico asimmetrico. A questo aggiunge il supporto di un'ampia varietà di tipi di traffico e di protocolli, con il controllo del payload simultaneo IPv6/v4 e il supporto per le relative varianti di tunneling (4in6, 6in4 e 6in6). Inoltre, supporta il controllo del traffico IPv6/v4 con VLAN e tag MPLS, traffico IPv4 mobile, GRE e GTP (tunneling GPRS) e jumbo frame. Non ultimo, osserva Nencini, abilita la gestione centralizzata mediante TippingPoint Security Management System (SMS), un'interfaccia utente grafica di gestione unificata di criteri ed elementi che fornisce un meccanismo singolo per monitorare le informazioni operative, modificare i criteri di sicurezza della rete, configurare gli elementi e distribuire i criteri di sicurezza della rete in tutta l'infrastruttura sia essa fisica o virtuale. ❁

Enel: la cyber security abilita la digitalizzazione

di
Giancarlo
Lanzetti

Il Gruppo Enel ha inserito la digitalizzazione nel proprio piano strategico nel 2016 e ad oggi può dirsi Total Cloud, ma si aprono anche nuove sfide per la sicurezza

Il Gruppo Enel ha inserito la digitalizzazione nel proprio piano strategico nel 2016 e, negli anni, ha confermato la centralità di tale scelta. La trasformazione digitale è anche e soprattutto un elemento fondamentale per conseguire gli obiettivi relativi alle altre dimensioni della strategia (Efficienza operativa, Crescita industriale, Semplificazione del Gruppo e Gestione attiva del portafoglio). Oggi il Gruppo Enel è Total Cloud.

«Il cloud - sostiene Yuri Rassega, Head of Cyber Security (CISO) di Enel Group - è un abilitatore strategico fondamentale che ci consente benefici nel time to market, rispondendo in modo elastico alle esigenze di capacità di calcolo e di storage. Cloud significa usufruire di servizi di calcolo gestiti in maniera industrializzata da aziende per le quali tali servizi sono il core business. La digitalizzazione apre a nuove opportunità, ma lancia anche diverse sfide nel campo della sicurezza. Gli attacchi cyber stanno crescendo esponenzialmente, sia numericamente che come

livello di sofisticazione. La capacità di far fronte agli attacchi è particolarmente importante nel settore elettrico, dove la continuità del servizio ha un'importanza fondamentale. Non a caso la cyber security è, nella strategia di Enel, uno degli abilitatori per la digitalizzazione; diamo molta attenzione alla sicurezza dei nostri asset nei diversi paesi del mondo in cui siamo presenti».

Da settembre 2016 è stata costituita in Enel una specifica unità di Cyber Security a diretto riporto del Chief Information Officer (CIO) con un responsabile che ricopre il ruolo di Chief Information Security Officer (CISO) del Gruppo.

Enel fonda la gestione della cyber security su due principi base: cyber security by design, che significa porre attenzione agli aspetti di sicurezza fin dalle primissime fasi di scelta, disegno e realizzazione di una soluzione e risk-based-approach, che vuol dire mettere le considerazioni sul rischio alla base di tutte le decisioni strategiche. Il cloud non fa eccezione: per questo viene prestata la massima attenzione



Yuri Rassega, Head of Cyber Security di Enel Group

alla scelta, progettazione e implementazione dei servizi in cloud più adeguati per i rischi e le esigenze di sicurezza del gruppo. Un'accurata selezione dei cloud provider, che tenga conto anche della rispondenza ai criteri di cyber security e un attento disegno dei servizi, che comprenda anche la progettazione e l'implementazione delle più adeguate misure di sicurezza, significa ottenere miglioramenti nella resilienza e affidabilità delle infrastrutture e una maggiore sicurezza per applicazioni, sistemi e dati.

«Il cloud - prosegue ancora il manager di Enel - è un esempio importante, ma non certo l'unico, di interdipendenza tra aziende per servizi, sistemi o componenti, che evidenzia la necessità di cooperare sui temi cyber con le realtà e le organizzazioni esterne. La cyber security di Enel è attiva in collaborazioni con organizzazioni private, istituzioni, accademie e università al fine di condividere le migliori pratiche, i modelli operativi, sviluppare i potenziali canali per la condivisione delle informazioni, nonché contribuire alla definizione di nuovi standard, regolamenti e direttive. Le collaborazioni esterne della cyber security sono mirate anche ad esercitare una sensibile pressione verso produttori e vendor per un immediato allineamento dei loro servizi, prodotti o componenti ai più elevati standard di sicurezza, in una visione a tutto tondo del concetto di cyber security by design. Tale visione si attua anche attraverso collaborazioni con startup o partnership tecnologiche per sviluppo congiunto di soluzioni che

rispettino i più aggiornati standard di sicurezza e rispondano a tutti i requisiti del Gruppo».

I nuovi impegni del CISO

Abbiamo chiesto a Rassega di raccontare come cambia in dette ottiche il ruolo del CISO.

«In un'azienda digitalizzata come Enel, diventa sempre più rilevante il ruolo di questa figura per l'indirizzamento strategico delle iniziative di prevenzione e protezione. Il CISO ha il compito di definire, con il supporto delle diverse linee di business, la strategia di cyber security, indirizzare e monitorare le iniziative, nonché coordinare le relative attività di investimento per l'intero Gruppo. La progressiva adozione del cloud non cambia sostanzialmente questi impegni. Il CISO non ha più bisogno di dedicare la sua attenzione alle problematiche di sicurezza connesse alla gestione di un data center ma diventa sempre più rilevante il suo ruolo di indirizzamento nella fase di individuazione di servizi, sistemi, componenti. È un'evoluzione del rapporto tra CISO e le altre funzioni aziendali in un'ottica di sempre più stretta integrazione e sinergia. Il Chief Information Security Officer è membro del Technological e Transformation

Committee, a cui sono affidate tutte le decisioni tecnologiche del Gruppo, per valutarne fin dall'inizio la rispondenza ai requisiti di sicurezza. Diventa particolarmente importante la cooperazione con il Procurement, che deve ingaggiare il CISO fin dalle prime fasi di qualificazione dei fornitori, per valutarne anche gli aspetti di sicurezza, di esplicitazione delle specifiche tecniche, per inserire anche i requisiti di sicurezza e infine, nella definizione dei documenti contrattuali, perché siano completi di tutte le clausole per la salvaguardia di riservatezza, integrità e disponibilità, nel rispetto dei vincoli normativi e dei requisiti aziendali».

Analogamente, conclude il nostro interlocutore, è fondamentale la relazione con le Business line per valutare e gestire opportunamente gli aspetti di rischio cyber. Non ultimo il CISO è sempre attivo con le Unità responsabili del disegno, sviluppo e gestione di soluzioni, che devono mettere in pratica il principio di cyber security by design. E deve essere anche un CISO che si proietta verso l'esterno, consapevole che la cyber security di Enel dipende anche da un approccio collaborativo con partner, fornitori, competitors, enti normativi e regolatori. ❁



La nuova frontiera della sicurezza è nei servizi gestiti

Uomo e macchina assieme in servizi gestiti, evidenza F-Secure, garantiscono la sicurezza informatica e una rapida risposta agli attacchi entro 30 minuti

La digitalizzazione sta cambiando le aziende trasformandole sempre più in software company. In quanto tali, queste dovrebbero proteggere al meglio i propri asset e le risorse digitali.

Il panorama delle minacce a cui un ambiente IT o produttivo è sottoposto è profondamente mutato e serve affrontarle con nuove tecnologie e investimenti.

Ma non sempre il budget lo consente, osserva F-Secure, da tre decenni pioniera nella cyber security e le cui soluzioni difendono decine di migliaia di aziende tramite tecnologie che combinano il machine learning con l'esperienza degli esperti dei suoi laboratori. Il problema non è però solo di budget, ma anche di competenze. Le previsioni parlano di 3.5 milioni di posizioni nella sicurezza IT che resteranno vacanti entro il 2021. Nel frattempo, oltre il 67% delle Enterprise avrà subito una violazione di dati (Fonte: 2018 Thales Data Threat Report). Ancor più allarmante, è che molti di questi attacchi si basano su tattiche di attacco impossibili da rilevare con soluzioni standard anti-malware o di protezione degli endpoint.

In sostanza, il problema da risolvere riguarda le risorse: non semplicemente i soldi, bensì il tempo e l'esperienza accumulata. Ed è qui che interviene in aiuto il paradigma dei servizi gestiti come quello sviluppato da F-Secure. Tramite sensori sofisticati su endpoint e reti di un'azienda, una soluzione basata su un servizio abilita rapidamente una profonda visibilità in un ambiente IT anche molto ampio e dai confine estesi al mobile e al multi-cloud. Quello che ne risulta è una soluzione che può rilevare le violazioni analizzando il comportamento, e non i meri segnali di un'attività malevola.

È quello che ha fatto F-Secure con lo sviluppo di servizi di sicurezza gestiti che hanno l'obiettivo di consentire anche azioni di risposta rapide, supportate dall'automazione o dalle decisioni umane, o da un loro sinergico connubio.



Antonio Pusceddu, Country Sales Manager per l'Italia di F-Secure

Vincente il connubio uomo - macchina

Una cosa è evidente: nessun esperto è in grado di rilevare da solo le minacce avanzate, perché non danno chiari segnali che qualcosa non va. Gli allarmi del software di endpoint non li rilevano e, per esempio, la protezione della posta elettronica non cattura le e-mail di phishing sul gateway che le inoltra all'utente.

L'unico modo per rilevare attacchi come questi, osserva F-Secure, è mediante una combinazione uomo e macchina tramite sensori che raccolgono dati rilevanti, l'intelligenza artificiale che processa questi dati e la competenza di esperti che analizzano rilevazioni sospette di violazioni.

Questo è il messaggio di allarme che F-Secure lancia e che sta alla base della sua vision di servizio e di connubio uomo-macchina, e come il modo più efficace e rapido per contrastare le minacce tramite un nuovo servizio di rilevazione delle intrusioni e di risposta agli incidenti che permette di scoprire e bloccare al loro insorgere e in tempi utili le minacce presenti sulla rete aziendale.

Segnalazione di una minaccia entro 30 minuti

Il fattore "tempo" è un punto chiave nella sicurezza. In media le violazioni di dati possono durare settimane o mesi prima di essere rilevate. La capacità nel riuscire a rilevare e rispondere velocemente alle intrusioni è quindi fondamentale, ma purtroppo non semplice da attuare.

È a questo vulnus temporale che pone rimedio il servizio gestito come quello sviluppato da F-Secure, che combina il meglio dell'uomo con l'intelligenza delle macchine, con la promessa di informare le aziende in soli 30 minuti dalla rilevazione di una minaccia.

Le aziende che si stanno rendendo conto che da sole fanno fatica a rilevare intrusioni e a rispondere agli incidenti hanno con F-Secure, osserva la società, la possibilità di affidarsi a un team di esperti di sicurezza, costruire un'infrastruttura di monitoraggio e ottenere validi dati per un'efficace intelligence delle minacce.



Il servizio gestito di Rapid Detection&Response

«Per scenari del tipo analizzati, in F-Secure abbiamo sviluppato F-Secure Rapid Detection & Response Service (RDS), un servizio gestito di rilevamento e risposta ai cyber attacchi mirati» osserva Antonio Pusceddu, Country Sales Manager per l'Italia.

RDS include sensori leggeri per il rilevamento delle intrusioni per endpoint, reti e server esca distribuiti nell'intera infrastruttura IT. I sensori monitorano le attività degli attaccanti e trasmettono le

informazioni al cloud di F-Secure in tempo reale.

Il servizio basato su cloud ricerca eventuali anomalie nei dati utilizzando una combinazione di tecnologie avanzate, come l'analisi del comportamento in tempo reale, l'analisi dei Big Data e l'analisi della reputazione.

La ricerca delle anomalie procede in due direzioni: comportamenti malevoli noti e sconosciuti. Questo perché l'adozione di tipologie di analisi differenti garantisce il rilevamento degli attaccanti, anche se usano tattiche di evasione progettate per eludere metodi di rilevamento specifici.

Una volta rilevate, le anomalie vengono segnalate al team di esperti del Rapid Detection & Response Center di F-Secure, che ricercano minacce h24 per verificarle e filtrare i falsi positivi.

Il processo di alert è molto rapido. Quando è confermato che un'anomalia

è una minaccia effettiva, il cliente riceve un avviso entro 30 minuti. Ma non è tutto. Gli esperti di F-Secure propongono contestualmente i passaggi necessari per contrastare e correggere la minaccia. E non ultimo, vengono fornite informazioni dettagliate sull'attacco utilizzabili come prova in procedimenti forensi.

Nei casi più difficili o laddove le risorse IT del cliente non siano disponibili, è poi sempre possibile contare sull'assistenza del servizio di risposta agli incidenti on-site di F-Secure. ❁

La sicurezza intelligente e multidimensionale di Micro Focus

Proteggersi preventivamente dalle minacce, eliminare le vulnerabilità applicative, cifrare i dati in ogni situazione e gestire in modo sicuro identità digitale e accesso. Il tutto sorretto da tecnologie di machine learning e analytics

Attaverso un'offerta integrata Micro Focus mette a disposizione tutti gli strumenti necessari per un'efficace protezione e governance delle tre dimensioni di rischio: dati, utenti e applicazioni. A ognuno di questi temi Micro Focus dedica una famiglia di soluzioni modulari che compongono una soluzione di Security, Risk & Governance avanzata, intelligente, integrata e aperta.

Tutte le soluzioni Micro Focus sono sorrette da tecnologie avanzate di machine learning e analytics (inclusa la piattaforma di analytics Vertica) che permettono di correlare in tempo reale miliardi di dati, analizzando anomalie di comportamento, rilevando minacce note e di nuovo tipo e fornendo una protezione preventiva.

«Micro Focus prosegue nel percorso di rafforzamento delle sue soluzioni di sicurezza - ha osservato Pierpaolo Ali, Director Southern Europe di Micro Focus Security - attraverso un consistente piano di investimenti in Ricerca e Sviluppo, per mantenere le sue tecnologie sempre all'apice dell'innovazione e in grado di rispondere alle reali esigenze degli utenti. Negli ultimi 12 mesi Micro Focus ha emesso 10 nuove release delle sue piattaforme e molte altre novità sono in arrivo».



Pierpaolo Ali, Director Southern Europe di Micro Focus Security

Protezione intelligente e preventiva dalle minacce

Per proteggere le reti aziendali da ogni possibile attacco Micro Focus mette a disposizione la famiglia di soluzioni e tecnologie di security intelligence ArcSight, che Gartner da 13 anni di seguito inserisce tra i leader all'interno del Magic Quadrant per le soluzioni di Security Information and Event Management.

Le soluzioni ArcSight effettuano un monitoraggio continuo sull'intera infrastruttura aziendale correlando log, ruoli dell'utente e flussi di rete in modo da individuare possibili minacce prima che possano avere impatto sul business aziendale e predisporre contromisure efficaci in tempi rapidi.

Grazie a un'impostazione modulare, ArcSight può essere inserito facilmente all'interno dell'infrastruttura aziendale e operare con soluzioni di sicurezza di

altri fornitori.

I tasselli fondamentali della soluzione sono ArcSight ADP e ArcSight ESM. ArcSight Data Platform (ADP) mette a disposizione oltre 400 connettori pronti all'uso e un tool per la creazione di connettori personalizzati, consentendo di raccogliere dati praticamente da ogni tipo di fonte esistente. ArcSight Enterprise Security Manager (ESM) è una soluzione SIEM che effettua la raccolta, l'analisi e la correlazione delle informazioni di sicurezza per identificare minacce ad alta priorità all'interno dell'intero ambiente aziendale.

Gestione sicura dell'accesso e dell'identità

La componente umana è uno degli anelli più deboli nella catena di protezione, soprattutto in un contesto in cui scompare il perimetro aziendale e le risorse aziendali sono accessibili sempre, da ogni luogo e con ogni tipo di dispositivo. Le soluzioni Micro Focus NetIQ si indirizzano alle esigenze delle aziende di media e grande dimensione mettendo a disposizione tecnologie per identity and access management, security management e data center management.

Queste soluzioni permettono di garantire la coerenza e la sincronizzazione delle identità, di predisporre modelli di accesso flessibili e sicuri, di effettuare correlazioni dinamiche per individuare possibili anomalie di accesso o di utilizzo dei propri privilegi.

NetIQ interviene dove altre soluzioni si fermano: per esempio, fornendo funzioni di gestione specifiche

per gli account privilegiati la cui compromissione può avere ripercussioni critiche per l'azienda.

Garantire la sicurezza dei dati

Attraverso le soluzioni Voltage SecureData Enterprise, Micro Focus permette di cifrare i dati aziendali offrendo un livello di protezione che nessun'altra soluzione è in grado di garantire.

Questa suite di tecnologie di crittografia protegge i dati nel corso del loro intero ciclo di vita, dal momento in cui sono creati in tutte le fasi successive ovvero quando sono a riposo (archiviati), in uso (dalle applicazioni) e anche mentre si spostano da un'applicazione a un'altra e attraverso il perimetro esteso dell'azienda (sulla rete o il Web); anche le policy di sicurezza si spostano insieme ai dati.

Grazie a tecnologie brevettate uniche, le soluzioni Voltage SecureData permettono di mantenere cifrati i dati senza alterarne il formato originale. In questo modo ogni set di dati memorizzato in un database può essere utilizzato dagli operatori per attività di analisi e correlazioni restando cifrato perché un indirizzo e-mail, un nome, un numero di contratto mantengono la loro struttura senza, tuttavia, avere alcuna relazione con i corrispettivi dati reali. Solo gli utenti con specifiche autorizzazioni mantengono la possibilità di visualizzare i dati in chiaro mentre il resto degli utenti continuerà a usarli vedendone solo una rappresentazione che mantiene la struttura formale.

Anche in caso di sottrazione del

database, il cyber criminale si troverà con un elenco di dati privo di qualsiasi corrispondenza con il mondo reale e, di conseguenza, inutilizzabile. Questo approccio permette di gestire la protezione a livello di singolo record del database, senza che sia necessario cifrare o decifrare all'occorrenza l'intero database.

Applicazioni sicure

Tutti gli analisti concordano nell'individuare le applicazioni come fonte preferenziale per le vulnerabilità sfruttabili dai cyber crimine. Le vulnerabilità del software costituiscono il nuovo punto di ingresso per le attività illecite perché sono semplici da sfruttare e perché le soluzioni di sicurezza network-based sono inefficaci contro questo tipo di minaccia.

Le soluzioni Micro Focus Fortify proteggono le applicazioni durante il loro intero ciclo di vita a cominciare dalla fase di sviluppo.

La gamma Fortify comprende, infatti, una serie di strumenti pensati per favorire uno sviluppo sicuro che elimini alla fonte le possibili vulnerabilità e per predisporre ambienti di test di tipo statico, dinamico e in tempo reale adatti a verificare le caratteristiche di sicurezza del codice. I test possono essere effettuati anche sulle applicazioni commerciali rendendo davvero completa la gamma di intervento.

Con la soluzione Fortify on Demand (FoD) queste funzionalità sono disponibili anche in modalità "as a service", permettendo di controllare il livello di sicurezza del software in modo rapido e granulare. ❁

Proteggere rete aziendale e siti Web da attacchi Bot

I servizi per la gestione e la valutazione gratuita del traffico Bot di Radware e di NPO Net permettono di identificare e bloccare gli attacchi ai siti web e alle applicazioni

Nel processo di trasformazione digitale le applicazioni sono cruciali per il successo del business e devono di conseguenza essere sempre accessibili da parte dei clienti.

Il negare questo accesso è però quello che invece si prefiggono i malintenzionati che utilizzano attacchi di tipo Botnet, ovvero una rete controllata da un hacker composta da dispositivi di proprietari ignari infettati da malware specializzato, detti Bot. Tramite i computer infettati possono essere avviati attacchi a siti web, noti come Distributed Denial of Service (DDoS), subissandoli di richieste che ne rallentano di molto i tempi di risposta, molto spesso confondendosi alle richieste lecite o simulandole.

L'importanza del contrastare efficacemente attacchi DDoS e Botnet sta nella analisi comportamentale basata su AI, Machine Learning, e Big Data, evidenzia Nicola Cavallina, Channel Manager and Alliance Manager Italy, Greece, Malta di Radware (www.radware.com), società di livello mondiale specializzata nelle soluzioni per la security di reti e applicazioni, il cui portfolio Soluzioni è stato inserito ed integrato anche nell'offerta della società americana CISCO.

I dati di una recente ricerca Forrester hanno ad esempio rivelato che il traffico su Internet è per il 52% costituito da Bot e solo per il 48% dovuto ad agenti umani. Non tutto il traffico Bot è malevolo, 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 identificare il traffico malevolo da quello legittimo.

Tra i tipi di attacchi Bot più comuni, evidenzia Antonio Lancellotti, Business Development Manager di NPO net (www.nponet.it), società che aiuta Aziende e Service Provider nel rendere più efficaci le infrastrutture digitali con soluzioni progettate e implementate su misura e che ha in Radware il partner tecnologico per la security, vi sono ad esempio quelli riferiti come Web Scraping (utilizzato per estrarre dati da un sito



*Antonio Lancellotti,
Business Development
Manager di NPO Net*



*Nicola Cavallina,
Channel & Alliance Manager
Italy, Greece, Malta di
Radware*

web), Denial of Inventory (utilizzato per bloccare la disponibilità di beni, presenti a magazzino, senza completarne l'acquisto), per arrivare all'Account Takeover (che permette all'attaccante di ottenere beni o servizi utilizzando l'account di un ignaro cliente).

Il rischio connesso a tali attacchi è enfatizzato dallo sviluppo stesso della tecnologia e dal fatto che possono fare leva sulla diffusione di siti web, di App mobile e di API

Ma cosa serve per rispondere efficacemente a questo aumento continuo delle minacce?

«Quello che serve - osserva Cavallina - è una soluzione che permetta di individuare e bloccare i diversi tipi di attacchi, provenienti dai diversi canali disponibili per un malintenzionato, ma che allo stesso tempo riduca al minimo i falsi positivi».

Radware BOT Manager

La risposta alle esigenze sopra evidenziate Radware l'ha data sviluppando Radware BOT Manager, una soluzione che permette di perseguire quattro obiettivi fondamentali nella protezione delle applicazioni aziendali e dei propri siti Web:

- Protezione da tutti gli attacchi provenienti dai diversi canali esistenti.
- Blocco proattivo e automatizzato degli attacchi tramite modelli di analisi e apprendimento in profondità e di tipo "semi supervised" del loro comportamento.
- 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 installate.

L'approccio "semi supervised" adottato da Radware ha il vantaggio di combinare il meglio delle caratteristiche delle tecnologie di machine learning supervisionate con quelle non supervisionate, e permette di ottenere una elevata precisione per quanto riguarda il rischio di incorrere in falsi positivi o negativi.

«Un aspetto fondamentale nella soluzione Bot Manager di Radware - osserva Lancellotti - è la facilità e l'ampiezza delle possibilità che si offrono a livello di sua installazione, e che comprendono il Reverse Proxing, l'Out-of-Path e il Cloud Service».

BOT Manager è stato progettato anche per integrarsi con l'intero portfolio di soluzioni Radware per la sicurezza quali:

- I servizi Cloud: Integrazione con Cloud WAF (Web Application Firewall).
- Le soluzioni per mitigare gli attacchi: tramite la condivisione e la sincronizzazione delle attività di intelligence.
- ADC (Application Delivery Controller): Integrazione con WAF

Di particolare utilità pratica è l'integrazione con Cloud WAF, realizzata tramite dashboard e widget che evidenziano graficamente il traffico Bot in corso, i diversi tipi di Bot e la geo mappa dei Bot stessi.

«Per le aziende che non dispongono di personale altamente

specializzato o che vogliono esternalizzare il servizio è disponibile anche il servizio completamente gestito e di classe enterprise di Cloud Security, che protegge da attacchi multi vettore ed ottimizza le prestazioni delle applicazioni», evidenzia Lancellotti

Il posizionamento tecnologico di Radware nella protezione da Bot si è di recente rafforzato con l'acquisizione di Shieldsquare, azienda specializzata e quotata tra le prime tre aziende a livello mondiale nella gestione dei Bot e nella protezione delle API.

Integrate nel portfolio Radware, le soluzioni di Shieldsquare permettono di rivelare un attacco, realizzare ricerche sulle minacce, disporre di analisi e rapporti e identificare la roadmap per migliorare l'approccio al mercato.

Valutazione gratuita di traffic Bot con Bot Analyzer

Al rilascio della soluzione Radware Bot Manager, l'azienda ha fatto seguire quello del servizio Bot Analyzer, un servizio di valutazione gratuita per ambienti business che possono essere soggetti ad attacchi Bot e per gli utilizzatori che desiderano disporre di una miglior comprensione dell'impatto che Bot di tipo malevolo possono avere sulla loro organizzazione.

Lo strumento, ha spiegato Lancellotti, aiuta in particolare nel dimostrare l'esigenza di disporre di una evoluta soluzione di Bot Manager che faccia leva su processi di analisi in grado di mettere a disposizione analisi dettagliate entro le 48 ore.



Applicazioni e utenti privilegiati al sicuro in SAP e nel cloud

CyberArk ha realizzato soluzioni e un marketplace che mettono al sicuro applicazioni SAP, utenti privilegiati e dati in ambienti Enterprise, cloud e multi-cloud

Proteggere applicazioni quali ERP, CRM o complessi ambienti SAP, e gli utenti privilegiati che ne fruiscono, è un aspetto chiave per il business.

Un recentissimo sondaggio di CyberArk (www.cyberark.com/it), al top tra le aziende mondiali attive nella sicurezza per l'accesso privilegiato, evidenzia tuttavia che quasi il 70% delle aziende non ne prioritizza la protezione e le gestisce allo stesso modo di dati, applicazioni e servizi a più basso valore. E questo nonostante un downtime anche minimo possa creare problemi significativi all'impresa.

Il dato, osserva CyberArk, evidenzia come vi sia un notevole disallineamento tra il focus della strategia di sicurezza e il valore di business di ciò che è più importante per l'impresa.

Il sondaggio ha riscontrato inoltre che il 74% delle organizzazioni indica di aver migrato le applicazioni business critical al cloud o che lo farà entro due anni. Un approccio che prioritizza il rischio per la protezione di questi asset è necessario affinché questa transizione avvenga con successo.

«I CISO dovrebbero adottare un approccio prioritizzato basato sul rischio che applica le protezioni più rigorose, salvaguardando in particolare gli accessi privilegiati e garantendo che, indipendentemente dagli attacchi perpetrati, continuino a operare», ha osservato Claudio Squinzi, Country Sales Manager in CyberArk.



*Claudio Squinzi,
Country Sales Manager in
CyberArk.*

Mettere al sicuro gli utenti privilegiati in SAP e multi-cloud

Oggi giorno le organizzazioni fanno affidamento su sistemi informativi dalla struttura complessa che

ha fatto propri paradigmi come il cloud, la mobility, l'AI, l'always-on e i servizi forniti da operatori qualificati.

In tutto questo SAP ricopre un ruolo essenziale. La diffusione di SAP attrae però l'interesse di hacker e di chi può essere interessato a impossessarsi di dati aziendali critici. Proteggere le applicazioni critiche e chi vi accede diventa quindi prioritario.

Il rischio in cui si può incorrere è enfatizzato dal fatto che in molti casi i criteri di autenticazione forte posti in essere per proteggere le informazioni sensibili sono condivisi tra più dipendenti di un ufficio e le password ampiamente conosciute.

Seppur SAP disponga di misure di sicurezza ideate per indirizzare tali vulnerabilità, il dover garantire un accesso sicuro a utenti privilegiati può costituire una complessità operativa addizionale che spesso porta a mancare gli obiettivi mandatori di sicurezza e di compliance.

L'approccio CyberArk per un SAP sicuro

Le soluzioni sviluppate da CyberArk complementano le caratteristiche di SAP in termini di sicurezza, incluso la rilevazione dei rischi e quanto concerne il controllo GRC (Governance, Risk, Compliance), in modo da rafforzare la postura complessiva di un'organizzazione per la sicurezza.

Ampio il loro campo di azione. CyberArk supporta sia i classici sistemi SAP ERP, così come un'ampia gamma di prodotti e



tecnologie SAP, comprese tra queste SAP CRM, SRM, SCM, SAP NetWeaver Java, SAP HANA e Sybase ASE.

Innanzitutto rende possibile gestire e proteggere le credenziali SAP mediante l'integrazione degli account nel repository centralizzato crittografato di CyberArk.

Si ha, inoltre, la possibilità di automatizzare la rotazione delle password e abilitare il controllo della sicurezza dell'accesso privilegiato a più livelli attraverso lo stack SAP, dal livello dell'applicazione ai database, al sistema operativo, le macchine virtuali e i server.

La gestione centralizzata si estende anche ai database più

comunemente usati in SAP quali Oracle, SAP HANA, Sybase, SQL Server e DB2.

E' anche possibile isolare le sessioni degli utenti privilegiati e rafforzare il controllo degli accessi al fine di proteggere i sistemi SAP da utenti e dispositivi non autorizzati.

Protezione delle sessioni privilegiate estesa al cloud

Se proteggere adeguatamente ambienti SAP è il primo passo da compiere, non è però sufficiente se si sfrutta la flessibilità del cloud ibrido.

Un punto critico, ad esempio, è costituito dal fatto che i Cloud Administrator e gli utenti business



privilegiati dispongono di sovente di diritti elevati nell'accesso a dati sensibili e alle applicazioni web, ma ciononostante le loro attività non sempre ricadono sotto la gestione del team IT dedito alla sicurezza.

Per estendere la protezione degli account privilegiati, le applicazioni e i dati a cui questi hanno accesso, ad ambienti esterni al perimetro aziendale fisico come nel caso del cloud ibrido, CyberArk ha sviluppato una specifica applicazione, CyberArk Privileged Session Manager for Cloud.

Il punto chiave dell'approccio adottato, ha illustrato David Higgins, EMEA Technical Director di CyberArk, è che mediante una user experience trasparente l'applicazione estende la protezione per le sessioni di accesso privilegiate e il monitoraggio delle attività oltre che il loro controllo, alle più comuni applicazioni web, nel cloud e sui social media, come ad esempio AWS, Azure o Salesforce. Parte integrante del portfolio CyberArk, Privileged Session Manager for Cloud fa inoltre leva sulle numerose le possibilità offerte dalla soluzione al fine di migliorare la sicurezza in ambienti cloud ibridi per la protezione degli utenti privilegiati. Tra queste:

- Supporto delle piattaforme cloud e web compreso Amazon (AWS), Red Hat OpenShift, Salesforce.com e social media quali Twitter, LinkedIn, Facebook e Instagram.
- Accesso trasparente e veloce con connessione sicura verso le piattaforme cloud e web.



David Higgins, EMEA Technical Director di CyberArk

- Isolamento delle sessioni degli utenti privilegiati e degli amministratori cloud.
- Monitoraggio delle sessioni degli utenti privilegiati in cloud e su web.
- Valutazione dei rischi inerenti le sessioni privilegiate.

«Al fine di supportare le strategie di difesa in profondità dei nostri clienti è vitale bilanciare un facile accesso alle piattaforme cloud e alle applicazioni web con un controllo degli accessi basato su policy, workflow di sicurezza, e una strategia consistente che abbracci sia ambienti on-premise che cloud, e questo è quello che è possibile fare con CyberArk Privileged Session Manager for Cloud», ha evidenziato Higgins.

Sicurezza "à la carte" nel CyberArk Marketplace

Per facilitare la fruizione delle soluzioni di sicurezza, CyberArk ha espanso anche il suo Marketplace

con funzionalità volte a supportare i contributi basati su community e la loro integrazione "trusted". Alla data ha totalizzato oltre 13.000 download distribuiti tra le 25 categorie di soluzioni presenti nel portfolio.

Alla base vi è un ecosistema di alleanze, la CyberArk C3 Alliance, partner strategici, clienti e comunità che possono contribuirvi aggiungendovi le proprie integrazioni realizzate a partire dalla soluzione CyberArk Privileged Access Security.

Due gli obiettivi del marketplace. Da una parte quello di rappresentare un punto di riferimento e di collaborazione per le aziende. Dall'altro quello di offrire uno spazio dove è possibile identificare soluzioni che migliorino la sicurezza degli accessi privilegiati più adatte alla propria realtà aziendale ed applicativa.

Di particolare valenza è l'attenzione posta all'integrazione della sicurezza inerente nuove e paradigmatiche tecnologie, architetture e processi alla base della trasformazione digitale.

Tra queste, quanto per esempio inerente la sicurezza nel cloud anche nelle sue varianti ibride e multi-cloud, i container, DevOps e l'automazione ulteriore dei processi robotizzati.

Le integrazioni di sicurezza sviluppate con e dai partner possono essere scaricate dal marketplace praticamente con pochi click, e dare ad una organizzazione la velocità e l'agilità atta a migliorare ed innalzare ulteriormente la sicurezza e ridurre i rischi. ❁

Il Cloud Data

Management riduce i rischi e ottimizza i costi

di
Giuseppe
Saccardi

Oltre il 70% delle aziende non garantisce un accesso ininterrotto ai dati e rischia forti perdite economiche. La soluzione, evidenzia Veeam, è il Cloud Data Management

Gli ultimi due lustri si sono caratterizzati per una vera e propria esplosione dei dati, al punto che si prevede che entro il 2025 si aggiungeranno oltre 175 Zettabyte di dati all'anno, una crescita di quasi due terzi rispetto al 2018. È evidente, nota Veeam, società di caratura mondiale specializzata nelle soluzioni per la always-on enterprise, la necessità che le aziende hanno di gestire e proteggere le informazioni, indipendentemente da dove queste risiedano.

La considerazione è confermata da una sua recente ricerca in cui il 73% delle organizzazioni ammette di non essere in grado di garantire agli utenti un accesso ininterrotto a dati e applicazioni.

Una scarsa gestione dei dati può costare ad una Enterprise fino a 20 milioni di dollari l'anno, dato che evidenzia l'impatto devastante che le interruzioni possono avere su fatturato, produttività e fiducia da parte dei clienti. Su scala più ridotta la cosa vale naturalmente anche per medie e piccole aziende.

Lo studio evidenzia anche che le aziende stanno fortunatamente agendo per combattere questo problema: il 72% prevede di adottare strategie di Cloud Data Management, spesso sfruttando le possibilità offerte dal cloud ibrido, per avere successo e ottenere un maggior valore dai propri dati.

In uno scenario critico, per accelerare il proprio successo, le aziende stanno poi adottando tecnologie quali il cloud, cloud ibrido, Big Data, Intelligenza Artificiale (AI) e Internet of Things (IoT).

Quasi la metà degli intervistati ammette che la protezione dei dati è indispensabile per poter sfruttare gli investimenti in queste tecnologie.

È allarmante tuttavia notare, osserva Veeam, di come solo il 37% delle aziende nutra molta fiducia nelle attuali soluzioni di backup e come la maggioranza (73%) degli intervistati confessi di non essere in grado di soddisfare le richieste degli utenti.



*Albert Zammar, Vice President
Southern EMEA Region di Veeam
Software*

Business più sicuro e smart con il Cloud Data Management

Il Veeam Cloud Data Management Report 2019 rivela che le organizzazioni hanno iniziato il loro percorso verso un business più intelligente sfruttando tecnologie come il Cloud Data Management e l'Intelligenza Artificiale in modo da disporre di una vista in tempo reale di tutto il business, agendo di conseguenza sulla base dei dati a disposizione. Quattro gli aspetti comuni alle aziende che hanno intrapreso questo percorso:

- **Cloud:** il Cloud Data Management è una componente essenziale per la gestione intelligente dei dati. Tre quarti delle aziende intervistate utilizzano piattaforme SaaS (Software-as-a-Service). Molte utilizzano il cloud per le attività di backup e ripristino, il 51% opera in modalità Backup-as-a-Service (BaaS) e il 44% utilizza servizi DRaaS (Disaster Recovery-as-a-Service).
- **Competenze:** Le aziende devono migliorare le competenze, per far sì che i loro dipendenti possano attingere informazioni dai dati a disposizione e utilizzare le nuove tecnologie man mano che vengono implementate: 9 aziende su 10 considerano le competenze digitali dei dipendenti vitali per il loro successo.
- **Cultura:** È necessario creare una cultura che si adatti e recepisca senza ostacoli le nuove tecnologie. Far sì che le persone evolvano insieme con l'azienda è essenziale.

• **Fiducia:** Le aziende devono creare fiducia nei confronti della propria capacità di implementare un business digitale, business che ha nei dati le sue solide fondamenta.

«Ciò che emerge con grande chiarezza è la necessità di agire da subito, partendo con solide fondamenta digitali e facendo in modo che i dati siano protetti e sempre disponibili. Una volta superato questo primo passo, le aziende possono implementare con fiducia nuove iniziative digitali, creando valore di business e vantaggio competitivo e sfruttando tutto il potenziale del Cloud Data Management come quello messo a disposizione da Veeam» ha osservato Albert Zammar, Vice President Southern EMEA Region di Veeam Software.

Dati al sicuro in Euro Service

La conferma che le aziende vedono nel Cloud Data Management un modo rapido per migliorare la postura per quanto concerne la sicurezza dei propri dati è offerta da realizzazioni come quelle sviluppate da Veeam per Euro Service, realtà attiva nei servizi per la gestione del credito, che ha scelto Veeam Availability Suite per assicurare la data availability, migliorare l'efficienza operativa e aumentare la produttività dei suoi dipendenti.

Euro Service è un gruppo che offre servizi per la gestione del credito nei mercati delle telecomunicazioni, finanziario ed assicurativo. Annovera circa 800 operatori

distribuiti nelle 5 sedi operative italiane, cui si aggiungono i dipendenti della filiale in Romania. Gestisce oltre 120.000 pratiche all'anno ed affianca i suoi clienti ponendosi come partner per la mediazione e la riconciliazione di debitori e creditori.

La sua infrastruttura IT consta di un data center a Roma e di un sito remoto a Milano per un totale di circa 20 TB processati da 35 virtual machine in ambiente VMware. E' in un tale contesto che Euro Service ha scelto Veeam per le sue caratteristiche di protezione dei dati, business continuity e recupero dei dati.

«Veeam ci ha dato un approccio innovativo alla gestione dei dati, che ci permette di garantire la disponibilità dei dati e la continuità del business, senza aumentare i carichi di lavoro del team IT. Possiamo ora gestire in modo intelligente i nostri dati anche per migliorare la customer experience, mantenere l'efficienza operativa e aumentare la produttività dei nostri dipendenti», ha commentato Fabio Rubino, IT Manager di Euro Service.

Le funzionalità di backup e replica dei dati scalabili che Veeam ha messo a disposizione, hanno l'obiettivo di garantire la disponibilità dei dati di Euro Service. La tecnologia di data loss avoidance e di verified recoverability, inoltre, assicura il backup automatico e garantisce al team IT che file, applicazioni e virtual server possano essere ripristinati in modo affidabile in caso di interruzioni.

«Euro Service opera in un mercato altamente competitivo, in cui la



disponibilità e la protezione dei dati sono essenziali per il successo delle aziende. Veeam assicura ai propri clienti la capacità di gestire i dati in modo intelligente, affidandosi a questi per prendere decisioni strategiche che rispondano a specifiche esigenze di business per una piena eccellenza operativa», ha commentato Albert Zammar.

Utenti ATM a destinazione ogni giorno

Un altro esempio di come la sicurezza dei dati sia essenziale è offerta da quanto realizzato da ATM, l'azienda dei trasporti milanese. L'adozione e la diffusione degli ambienti virtualizzati nei Data Center di ATM ha reso necessaria la ricerca di una soluzione in grado di garantire la continua disponibilità dei dati.

In questa prospettiva l'utilizzo di Veeam Availability Suite va visto, osserva l'azienda, come la continuità con le primissime adozioni delle soluzioni Veeam, una tecnologia che in ATM riconoscono pionieristica.

«Abbiamo provato altri strumenti ma nessuno ci ha soddisfatto come Veeam Availability Suite», ha commentato Paolo Tunesi, Responsabile Gestione ed Evoluzione Sistemi. «È una piattaforma che non richiede l'installazione di agenti, veloce e facile da gestire che ci ha permesso di puntare sui processi di back-up e restore dei dati come componente fondamentale della disponibilità dei nostri sistemi».

Nelle aziende sempre più data-centriche, la disponibilità è un fattore che si dà per scontato. L'affidabilità con cui i dati di ATM

vengono ripristinati in caso di problemi è un aspetto del tutto trasparente all'operatività.

Concreti i risultati ottenuti. Avere i dati sempre disponibili permette ad ATM la massima operatività e servizi online come il pagamento tramite carte contactless. Un sistema efficiente che fidelizza i cittadini e contribuisce alla sostenibilità. ATM gestisce anche i parcheggi per conto del Comune di Milano. La soluzione adottata tutela i servizi in caso di downtime e consente di evitare ingenti perdite economiche per le casse pubbliche.

Non ultimo, i risparmi generati contribuiscono a progetti di sostenibilità ambientale perché al centro del piano strategico ci sono trasporti ecologici e servizi sempre più affidabili grazie anche alla disponibilità dei dati. ❁

Fujitsu consiglia Windows 10 Pro.

Affidabile,
potente
e leggero

FUJITSU Notebook
LIFEBOOK U938

FUJITSU

shaping tomorrow with you



Sottile e ultra-mobile.
Il notebook Fujitsu LIFEBOOK U938 è per i
professionisti che desiderano il meglio, ovunque.

Windows 10 Pro | Intel® Core™ i7-8650U | 20 GB RAM

Info: www.fujitsu.com/it/ultrabook | Numero verde: 800 466 820
customerinfo.point@ts.fujitsu.com | blog.it.fujitsu.com

© Copyright 2019 Fujitsu Technology Solutions GmbH

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

 Windows 10

Windows 10 Pro è sinonimo di business.