

SPECIALE CLOUD SECURITY

Il numero di applicazioni in cloud utilizzate dai privati sta crescendo rapidamente e presto travolgerà le imprese. Il fenomeno dello shadow IT è già un problema per molte imprese, ma la soluzione sarà semplicemente un progressivo passaggio al cloud ed è molto probabile che l'offerta di applicazioni "pret a porter" finirà con il cancellare il concetto di applicazione "on premise".

Una risposta che, pur non potendo risolvere tutte le esigenze di sicurezza, può soddisfare alcune urgenze aziendali è rappresentata dai servizi Cloud Access Security Brocker (CASB).

pag.10

CYBER ATTACK

CON SOLI 20 DOLLARI È POSSIBILE BUCARE UNA RETE AZIENDALE

Con soli 20 dollari è possibile bucare una rete aziendale. I ricercatori di Kaspersky Lab hanno esaminato i tool hardware e software disponibili online che consentono di intercettare password segrete.

pag.06-07

CYBER ATTACK

IL FUTURO DELLA SICUREZZA IT È NEL MACHINE LEARNING

Il futuro della sicurezza IT è nel machine learning. Per l'88% dei manager IT con le tecniche di sicurezza avanzata è meno necessario il giudizio umano. Lo evidenzia una ricerca Trend Micro sulla Cyber Security

pag.09

IN QUESTO NUMERO:

OPINIONE

pag.03

- Il costo e il futuro della sicurezza informatica

pag.04-05

- Il rilancio di AIPSI

CYBER ATTACK

pag.06-07

- Con soli 20 dollari è possibile bucare una rete aziendale

pag.09

- Il futuro della sicurezza IT è nel machine learning

SPECIALE

pag.10-11

- L'emergenza della sicurezza sul cloud

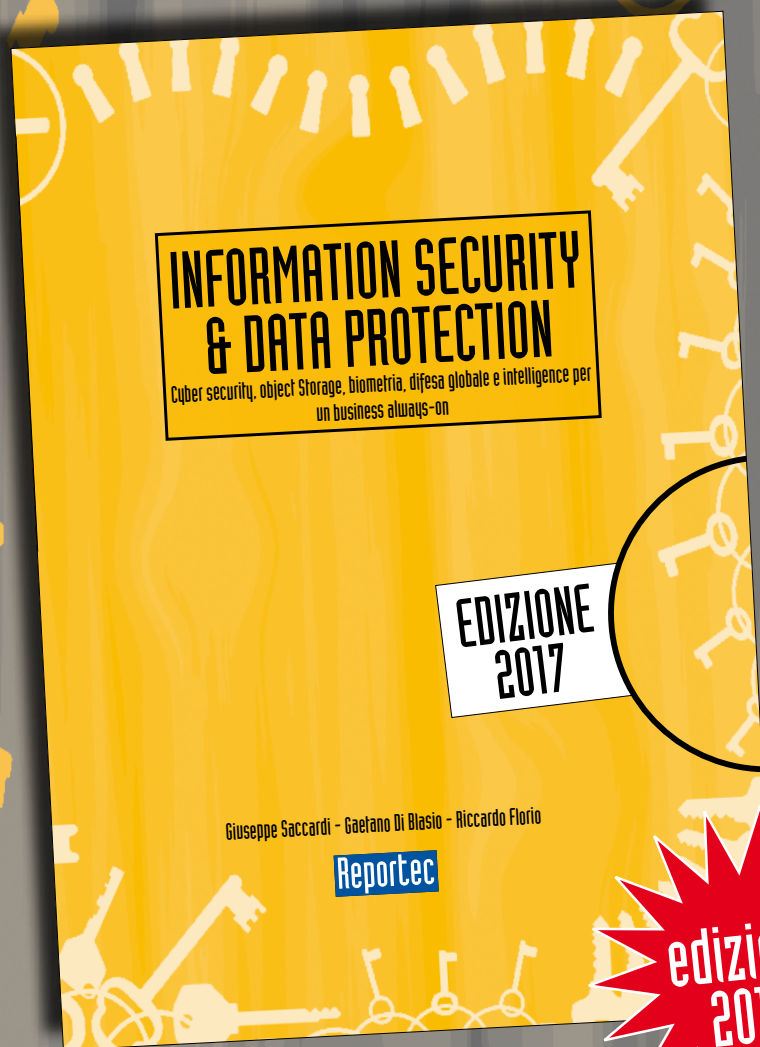
pag.12-13

- I servizi CASB di Oracle sfruttano l'intelligenza artificiale

pag.14-15

- Ripensare la sicurezza nel cloud ibrido

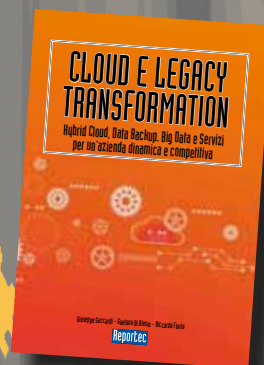
È disponibile il nuovo libro **SICUREZZA E PROTEZIONE DEI DATI**



In oltre 200 pagine il punto sulla situazione della cybersecurity e sulle dinamiche aziendali nella protezione del dato e della continuità del business. Una tematica sempre più vitale per le imprese, le quali devono mettere in conto che saranno attaccate. Ormai esistono sistemi automatici e pressioni da parte dei cybercriminali, tali per cui nessuno può sentirsi al sicuro: chi non è ancora stato attaccato lo sarà e, se non subirà danni gravi, sarà solo perché chi l'ha assalito cercava qualcos'altro.



È disponibili anche
CLOUD E LEGACY TRANSFORMATION



Il libro è acquistabile al prezzo di 48 euro (più IVA 22%) richiedendolo a
info@reportec.it - tel 02 36580441 - fax 02 36580444

IL COSTO E IL FUTURO DELLA SICUREZZA INFORMATICA

Sappiamo benissimo che, per quanto blindata, la nostra porta di casa non può impedire ai ladri di entrare, ma sappiamo di potergli rendere difficile la cosa. Lo stesso vale per la sicurezza informatica, ma, invece di investire in una porta il più possibile robusta, gli amministratori delegati hanno sempre pensato che la cyber security fosse un problema tecnico già "pagato" con gli stanziamenti per l'IT. Poi le cose sono cambiate e gli attacchi ransomware hanno il merito di aver dato una scossa. Però, se oggi si è compreso quanto importante sia la formazione sulla sicurezza, ancora gli investimenti per la protezione dei dati e dell'azienda sono insufficienti.

Il problema è anche che si stanno continuamente aprendo nuovi fronti di attacco a causa dell'inevitabile successo del cloud e della Digital Transformation.

In questo numero di Security&Business poniamo alcune questioni legate alla crescente adozione di IaaS, PaaS e soprattutto SaaS, che devono essere supportate da soluzioni per la sicurezza, anche in virtù dei prossimi cambiamenti normativi. L'accento è sulla crescita dell'offerta Cloud Access Security Broker, la cui adozione non può essere vista come una panacea, ma certamente come uno strumento fondamentale.

In Cyber Attack sono affrontati alcuni temi che cominciano a interessare anche a livello di consiglio d'amministrazione. Stiamo parlando dei costi della mancata sicurezza. Un report realizzato da Kaspersky Lab evidenzia un dato allarmante: i tempi in cui si rilevano gli attacchi sono lunghi (va anche ricordato che il GDPR prevede la comunicazione immediata di un avvenuto incidente) e i tempi lunghi fanno crescere i costi.

Sempre Kaspersky Lab mostra come con 20 dollari e minime capacità di programmazione si possa rubare facilmente password.

Invece da una ricerca commissionata da Trend Micro si apprende che l'88% dei manager IT (italiani) la soluzione della sicurezza arriverà dall'automazione, in particolare dai sistemi avanzati basati sul machine learning. Però potrebbero aver ragione il 7% dei manager per i quali artificial intelligence e machine learning esiste solo nella finzione cinematografica.

IL RILANCIO DI AIPSI

di Marco R. A. Bozzetti, Presidente AIPSI

Con l'elezione del nuovo Consiglio Direttivo (CD) con Marco Bozzetti Presidente, nel gennaio 2016 prende vita il piano di rilancio dell'Associazione, che nei tempi d'oro pre-crisi economica, quindi prima del 2008, contava più di 200 associati ed effettuava numerose iniziative, compreso un convegno "nazionale" a Roma, spesso con autorevoli invitati delle aziende, delle Pubbliche Amministrazioni e del vertice della ISSA statunitense, di cui AIPSI è il Capitolo Italiano. Il rilancio delineato da Bozzetti, già in progressiva attuazione e confermato anche dalla recente Assemblea dei Soci del 12/7 scorso, si basa da un lato sull'obiettivo strategico primario di AIPSI, che è la crescita professionale dei Soci, dall'altro sull'obiettivo operativo primario per il triennio 2016-18, che è aumentare significativamente il numero degli associati così da aumentare la visibilità e conoscenza di AIPSI in Italia, e di aumentare la cassa e il finanziamento delle varie iniziative. Dato che buona parte della quota di iscrizione ad AIPSI va a iSSA, le quote di iscrizione non bastano a mettere in positivo il conto economico di AIPSI e sono necessari i guadagni dalle sponsorizzazioni. Si rammenta che AIPSI è una associazione di persone, e non possono quindi "isciversi" Enti e aziende: queste ultime possono solo sponsorizzare specifiche iniziative dell'associazione, tipicamente workshop, convegni e indagini come l'Osservatorio Attacchi Informatici in Italia (OAD).

Per raggiungere gli obiettivi sopra elencati occorre attivare e gestire efficacemente un insieme

coordinato di iniziative che includono alla data:

- la realizzazione del nuovo sito web;
- sfruttare al meglio i servizi e le iniziative ISSA, in particolare i webinar internazionali, ISSA Journal, ISSA European Chapter Leaders, e i piani di carriera;
- realizzare concreti servizi per Soci attuali e potenziali: indagini, workshop, webinar, formazione professionale (anche e-learning), supporti alle certificazioni;
- Presidiare e supportare soci attuali e potenziali sul territorio con la creazione di sedi territoriali (oltre alle sedi di Lecce e Ancona-Macerata, si stanno aprendo quelle di Verona-Venezia e Torino).

Grazie all'essenziale contributo del Consigliere Chirivì è stato realizzato su base totalmente volontaristica il nuovo sitoWeb (<http://www.aipsi.org/>), che fornisce l'accessibilità separata a informazioni e documenti per i generici visitatori, per i visitatori che si registrano, per i soci. Il nuovo sito non è solo un basilare "biglietto da visita" di AIPSI, ma lo strumento primario attraverso cui essa eroga servizi ai propri Soci e tende a realizzare tra di loro una reale "comunità professionale". A fianco del sito, ancora in fase di messa a punto, AIPSI sta rivitalizzando la sua presenza sui social network, in particolare su LinkedIn, dove da tempo ha creato un Gruppo AIPSI. Per quanto riguarda eventi e indagini, AIPSI ha patrocinato e sponsorizzato il Rapporto OAD 2016 e 2017 sugli attacchi agli applicativi (entrambi scaricabili dal sito www.aipsi.org).

Cyber Security Career Lifecycle®



I cinque stati previsti da CSCL nella carriera di un professionista (Fonte: ISSA)

Numerose le partecipazioni di AIPSI a vari convegni, sia sui temi di OAD sia su altri temi, e in particolare la partecipazione a SMAU Roadshow in diverse città. Il 5/7/017 ha avuto luogo a Milano l'evento AIPSI sponsorizzato da Qintesi Spa sul tema degli attacchi agli applicativi: "Come prevenire e contrastare attacchi digitali alle applicazioni SAP". Si spera che questo sia il primo di una lunga serie di workshop "fisici" a livello territoriale sia di webinar. Il primo webinar con Reportec, Media Partner di AIPSI, è previsto a settembre 2017. In collaborazione con Reportec e con Malabo (l'azienda del Presidente e realizzatrice di OAD), AIPSI sta organizzando l'iniziativa OAD 2017 che, sulla base di un unico questionario produrrà:

- il "tradizionale" Rapporto annuale per il 2017, sponsorizzato dagli Sponsor Silver
- tre Rapporti verticali di approfondimento su 3 temi caldi scelti dagli Sponsor Gold, che parteciperanno anche ai tre webinar previsti poco dopo la pubblicazione dei Rapporti verticali.

Un tema centrale per la crescita professionale dei

Soci è la "formazione continua" e la loro certificazione secondo le nuove norme italiane ed europee. ISSA ha definito un approccio metodologico per il piano di carriera di un professionista di sicurezza digitale, chiamato CSCL, Cyber Security Career Lifecycle, che prevede l'evoluzione da "pre-professionista" (per esempio uno studente) fino a "leader" (si veda fig. 1). Questo approccio sistematico converge fortemente con quello definito da AICA sulla base dello standard europeo eCF, (UNI 11506 - EN 16234 1:2016) ora unico riferimento con validità legale in Europa e in Italia per le certificazioni delle competenze ICT. Oltre a questo, eCF ha alcune caratteristiche peculiari, rispetto alle più tradizionali e diffuse certificazioni: si basa sulla provata esperienza maturata sul campo dal professionista e lo qualifica considerando l'intera sua biografia professionale e le competenze ed esperienze effettivamente maturate nella sua vita professionale (e non solo per aver seguito un corso e superato un esame). In tale ambito AIPSI sta studiando e preparando corsi modulari di e-learning e webinar di approfondimento.

CON SOLI 20 DOLLARI È POSSIBILE BUCARE UNA RETE AZIENDALE

I ricercatori di Kaspersky Lab hanno esaminato i tool hardware e software disponibili online che consentono di intercettare password segrete

di Giuseppe Saccardi

Un'analisi realizzata dagli esperti di Kaspersky Lab mostra che, con 20 dollari e poche ore di lavoro, chiunque abbia conoscenze di programmazione anche di base è in grado di creare uno strumento di hacking con cui penetrare una rete. Per dimostrarlo, è stato fatto un esperimento utilizzando un dispositivo USB "fatto in casa" basato su Raspberry Pi, configurato in modo specifico ma senza che contenesse nessun software dannoso. Con il dispositivo sono stati in grado di sottrarre i dati di autenticazione degli utenti di una rete aziendale ad una velocità di 50 password decodificate ogni ora. La ricerca è partita da un fatto reale perché gli esperti di Kaspersky Lab hanno scoperto il caso di un dipendente di una società di pulizie che aveva usato una chiavetta USB per infettare con un malware la workstation di un'organizzazione. Gli esperti di Kaspersky Lab hanno iniziato la loro indagine per comprendere quali altri mezzi potessero essere utilizzati per compromettere una rete e soprattutto quali consentissero di farlo senza utilizzare un malware.

Il cavallo di Troia

I ricercatori hanno utilizzato un microcomputer Raspberry-Pi configurato come un adattatore Ethernet al quale sono state apportate alcune modifiche di configurazione del sistema operativo in esecuzione. Dopodiché, hanno installato alcuni tool facilmente reperibili per il packet sniffing, la raccolta e l'elaborazione dei dati. Infine, i ricercatori hanno creato un server per raccogliere i dati intercettati. Quando il dispositivo è stato connesso alla macchina presa di mira ha cominciato a caricare automaticamente nel server le informazioni relative alle credenziali rubate.

Il motivo per cui questo è stato possibile è che il sistema operativo presente sul computer attaccato ha identificato il dispositivo Raspberry-Pi connesso come una scheda LAN cablata e ha automaticamente assegnato una priorità superiore a quella di altre connessioni di rete disponibili e, soprattutto, ha consentito l'accesso allo scambio di dati all'interno del network.

La rete sperimentale simulava il segmento di una vera e propria rete aziendale. Di conseguenza, i ricercatori sono stati in grado di raccogliere i dati di



autenticazione inviati dal pc attaccato e dalle sue applicazioni e di autenticare i server di dominio e remoti. Inoltre, i ricercatori sono stati anche in grado di raccogliere questi dati da altri computer presenti nel segmento del network.

Linux più sicuro

Considerato che le specifiche dell'attacco consentono di inviare in tempo reale i dati intercettati in rete, più il dispositivo rimane connesso al pc e più saranno i dati che verranno raccolti e trasferiti ad un server remoto. Dopo solo mezz'ora dall'inizio dell'esperimento i ricercatori sono stati in grado di identificare quasi 30 password trasferite attraverso la rete attaccata.

Nel peggiore dei casi, potrebbero essere intercettati anche i dati di autenticazione dell'amministratore di dominio e si potrebbe avere accesso al suo account mentre il dispositivo è collegato a uno dei pc all'interno del dominio.

La superficie di attacco potenziale per questo metodo di intercettazione dei dati è estesa: l'esperimento è stato riprodotto con successo su computer locked e unlocked con sistemi operativi Windows e Mac. I ricercatori non sono stati in grado, però, di riprodurre l'attacco su dispositivi basati su Linux.

«Dopo aver eseguito questo esperimento ci sono due cose importanti che ci preoccupano maggiormente: in primo luogo il fatto che non sia stato necessario sviluppare un software, ma è bastato utilizzare strumenti facilmente reperibili in Internet. In secondo luogo ci preoccupa la facilità con cui siamo stati in grado di preparare il proof of concept del nostro dispositivo di hacking. Ciò significa che potenzialmente chiunque abbia familiarità con Internet e abbia una capacità di programmazione

di base, può riprodurre questo esperimento», ha dichiarato Morten Lehn, General Manager Italy di Kaspersky Lab.

Sebbene l'attacco consenta d'intercettare solo gli hash delle password (stringhe ottenute elaborando le password con una funzione di offuscamento non invertibile), quest'ultimi potrebbero essere utilizzati per identificare le password in chiaro in quanto gli algoritmi delle funzioni per l'hashing sono noti, oppure potrebbero essere utilizzati in attacchi pass-the-hash.

Come proteggersi

Al fine di proteggere i pc o le reti da attacchi perpetrati con l'aiuto di dispositivi fai da te, gli esperti di Kaspersky Lab consigliano agli amministratori di sistema di:

- utilizzare esclusivamente il protocollo Kerberos per l'autenticazione dei domain user;
- limitare ai soli utenti di dominio con privilegi l'accesso ai sistemi legacy, in particolare agli amministratori di dominio;
- modificare regolarmente le password dei domain user e imporre nelle policy questa pratica;
- proteggere i computer con una soluzione di sicurezza regolarmente aggiornata.
- impedire la connessione di dispositivi USB non autorizzati;
- attivare, se si è proprietari della risorsa Web, l'HSTS che impedisce la commutazione da HTTPS a protocollo HTTP e la manipolazione delle credenziali di un cookie rubato;
- se possibile, disattivare la modalità di listening e attivare l'impostazione di isolamento Client (AP) nei router Wi-Fi e negli switch;
- attivare l'impostazione DHCP Snooping.

FINO A 861MILA DOLLARI IL COSTO MEDIO DI UN CYBER ATTACCO

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

di Gaetano Di Blasio

I costi medi per un attacco diretto alle grandi enterprise superano gli 1,4 milioni di dollari. In media il costo è di 861mila dollari, ma per una piccola e media impresa può arrivare a 86mila e 500 dollari. Sono alcuni dei risultati della ricerca "Misurare l'impatto finanziario della sicurezza IT sulle imprese" basata sul Security Risks report di Kaspersky Lab. Un dato allarmante è che i tempi in cui si rilevano gli attacchi sono lunghi. I tempi lunghi fanno crescere i costi: le piccole e medie imprese tendono a pagare il 44% in più per riprendersi da un attacco scoperto una settimana o più dopo la violazione iniziale, rispetto agli attacchi individuati il giorno stesso. Le grandi imprese, nelle stesse circostanze, pagano il 27% in più. Kaspersky Lab ha anche confrontato il budget di sicurezza di un'azienda con le perdite subite a causa di gravi incidenti. Complessivamente, le imprese si aspettano che i budget per la sicurezza informatica crescano almeno del 14% nei prossimi tre anni, a causa dell'aumento della complessità delle infrastrutture IT. La spesa è molto variabile: mediamente per una piccola impresa è attualmente il 18% del proprio budget IT, mentre una grande dedica il 21% del budget IT alla sicurezza, ma la forchetta è ampia, perché per la sicurezza vengono allocati anche solo mille dollari da una Pmi e oltre

Morten Lehn, General Manager Italy di Kaspersky Lab



un milione di dollari per una grande azienda. A far lievitare i costi contribuiscono varie voci, compresi i costi degli straordinari dei dipendenti. Per la stima, dei costi totali per il ripristino, Kaspersky Lab e la società di analisi B2B International hanno chiesto alle imprese di suddividere le perdite causate dagli incidenti di sicurezza più gravi in diverse categorie. È emerso che, nonostante il costo più frequente sia quello degli stipendi aggiuntivi del personale, le imprese hanno riportato spese significative causate da opportunità di business perse, miglioramenti nella sicurezza IT, collaborazioni con specialisti esterni e assunzione di nuovi dipendenti.

Il 19% della perdita totale per le grandi imprese è destinato in collaborazione con esperti esterni (mediamente 85mila dollari) e in formazione dei dipendenti (79mila dollari in media).

Morten Lehn, General Manager Italy di Kaspersky Lab ha commentato: «In base alla nostra indagine mondiale, mediamente il budget per la sicurezza IT "vale" solo il 2,5% dei cyber-attacchi. Considerate le migliaia di minacce che colpiscono quotidianamente il mondo delle imprese, una cyber-sicurezza efficiente ripaga sicuramente».

IL FUTURO DELLA SICUREZZA IT È NEL MACHINE LEARNING

Per l'88% dei manager IT con le tecniche di sicurezza avanzata è meno necessario il giudizio umano. Lo evidenzia una ricerca di Trend Micro sulla Cyber Security

di Giuseppe Saccardi

Secondo una ricerca pubblicata da Trend Micro, per la quale sono stati intervistati oltre 2mila e 400 responsabili decisionali IT in Europa e Stati Uniti, le tecniche di sicurezza avanzate renderanno sempre meno necessario fare affidamento sul giudizio umano, per distinguere quelle sottili differenze tra minacce e anomalie. In particolare, questa considerazione vede d'accordo l'88% dei responsabili IT italiani. Il 59% del campione italiano prevede poi che questo cambiamento avverrà nei prossimi 5 anni. Lo studio rivela altresì che i responsabili IT italiani sono attratti da strumenti di sicurezza avanzata come il machine learning e l'analisi del comportamento. L'85% di questi ritiene che questi strumenti siano efficaci per bloccare le minacce informatiche e più di tre quarti (77%) dichiara di utilizzarli già, mentre l'88% inizierà a farlo nei prossimi 12-18 mesi.

Nonostante la maggior parte degli intervistati auspichi tecniche di sicurezza avanzate, permane anche un po' di scetticismo e confusione. Prendendo in considerazione il machine learning, evidenzia lo studio, il 19% del campione italiano lo considera una trovata di marketing, mentre il 7% ritiene che esista solo nella finzione cinematografica.

Una parte dei responsabili IT, inoltre, non riesce a

quantificare l'efficacia del machine learning e delle analisi comportamentali nella prevenzione degli attacchi. Lo studio Trend Micro mette in risalto anche la mancanza di consapevolezza riguardo i falsi positivi, ovvero il momento in cui un sistema di sicurezza crede di aver rilevato una minaccia e si prepara ad agire ma non esiste alcuna minaccia. Queste azioni richiedono un impiego massiccio di risorse che possono danneggiare il funzionamento delle organizzazioni rendendo inutilizzabili programmi e sistemi operativi.

Il 40% degli intervistati a livello globale non tiene in considerazione questa criticità e il problema sembra essere prevalente in Europa con percentuali alte in Norvegia (78%), Svezia (64%), Austria (60%) e Svizzera (59%). L'Italia si distingue in positivo, infatti solo il 41% degli intervistati non aveva mai preso in considerazione la criticità dei falsi positivi.

Le aziende fronteggiano oggi 500mila nuove minacce quotidiane e il 2016 ha visto una crescita del 752% negli attacchi ransomware. Per questo, mentre le nuove tecnologie come il machine learning sono importanti, Trend Micro propone anche un insieme di tecniche di difesa intergenerazionali progettate appositamente e integrate nelle applicazioni più importanti per le aziende.

L'EMERGENZA DELLA SICUREZZA SUL CLOUD

Cresce l'offerta dei servizi Cloud Access Security Broker, mentre l'arrivo del GDPR impone una condivisione del rischio

di Gaetano Di Blasio

Il numero di applicazioni in cloud utilizzate dai privati sta crescendo rapidamente e presto travolgerà le imprese. Il fenomeno dello shadow IT è già un problema per molte imprese, ma la soluzione sarà semplicemente un progressivo passaggio al cloud ed è molto probabile che l'offerta di applicazioni "pret a porter" finirà con il cancellare il concetto di applicazione "on premise". Sta già avvenendo: basta pensare a Office 365 e considerare quante piccole imprese utilizzino questo software di Microsoft per gestire l'intera impresa.

Un passo analogo per le grandi imprese non sarà scontato, ma molto probabile, anche se graduale.

Peraltro, soluzioni come quelle legate ai Big Data sono un altro esempio dello spostamento degli applicativi nella nuvola e la progressiva affermazione della Digital Transformation non potrà che confermare queste tendenze. Unico, ma determinante ostacolo è la carenza di banda necessaria in ancora troppe zone del nostro Paese.

Si pone, in ogni caso una questione emergente: la sicurezza degli ambienti cloud,



oltre che quelli di rete.

Una risposta che, pur non potendo risolvere tutte le esigenze di sicurezza, può soddisfare alcune urgenze aziendali è rappresentata dai servizi Cloud Access Security Broker (CASB).

I CASB sono "intermediari", come suggerisce il nome, che vanno a inserirsi fra l'utente di un servizio cloud e il fornitore dello stesso. Il loro compito è organizzare le security policy aziendali con i criteri di sicurezza del fornitore di servizi. Ci sono servizi Casb che fungono praticamente da advisor e soluzioni più approfondite. Ciascuno dovrà valutare in base alle proprie esigenze.

Considerazioni accurate andranno fatte in funzione delle regole europee dettate dalla GDPR (General Data Protection Regulation) che entreranno in vigore nel maggio 2018 e, che tra l'altro, comportano una condivisione di responsabilità tra il titolare del trattamento dei dati e il titolare dei dati stessi. Per le imprese che operano in outsourcing e per gli outsourcer stessi si tratta di cambiamenti importanti che si sommano all'evoluzione verso il cloud.

I SERVIZI CASB DI ORACLE SFRUTTANO L'INTELLIGENZA ARTIFICIALE

Rilasciati nuovi servizi per la sicurezza del cloud di Identity Security Operation Center che sfruttano il machine learning, l'intelligenza artificiale e soluzioni context-aware

di Gaetano Di Blasio

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

In particolare, Oracle ha potenziato queste soluzioni con nuovi servizi cloud Identity Security Operation Center (SOC), che comprendono ora tecnologie di ultima generazione, quali machine learning, intelligenza artificiale e soluzioni context-aware (cioè sistemi che effettuano analisi di sicurezza in grado di correlare, per esempio, l'utilizzo di una risorsa con la natura della stessa).

«Siamo costantemente impegnati a fornire soluzioni che aiutino le imprese a gestire, adattare e rafforzare il proprio livello di sicurezza nei confronti dei rischi esterni e interni» afferma Domenico Garbarino, Sales Director Security Solutions di Oracle Italia, evidenziando come le competenze maturate in Oracle in aree come la data science e il machine learning, permettano di realizzare soluzioni all'avanguardia,

scalabili e affidabili per chi intende passare al cloud, di Oracle come di terze parti.

Tra le novità vi sono funzionalità Adaptive Access per l'implementazione di controlli di accesso dinamico alle applicazioni, il potenziamento delle capacità di monitoraggio del rischio basati su machine learning e i suddetti servizi CASB, che supportano le soluzioni Oracle SaaS con il rilevamento automatico delle minacce.

Adaptive Access per il controllo d'accesso

Le credenziali di accesso, sia quelle degli utenti finali sia quelle privilegiate, sono una preda ambita

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



Domenico Garbarino, Sales Director Security Solutions di Oracle Italia

anche dalla gestione intuitiva delle policy e dalla integrazioni standardizzate con i componenti Oracle Identity SOC.

Oltre a questo, Oracle CASB Cloud Service utilizza ora tecniche di machine learning sia di tipo supervisionato sia non supervisionato, più potenti per il rilevamento delle minacce avanzate.

Per rilevare più accuratamente anomalie, Oracle ha sviluppato l'engine UBA (User Behavior Analytics) integrato, che stabilisce automaticamente dei particolari modelli di riferimento per ciascun utente e servizio cloud, applicativi compresi. Tali modelli saranno la pietra di paragone consultata costantemente dal sistema per valutare una qualsiasi deviazione. Oracle CASB Cloud Service orchestra la risposta all'incidente per mezzo di diverse opzioni compresa l'integrazione con sistemi di ticketing e gestione incidenti di terze parti, nonché le funzionalità native per la risoluzione automatica dei casi.

Il CASB per la sicurezza del SaaS Oracle

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

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

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

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

UBI Banca

«Le funzionalità di Encryption e Masking di Oracle Database Security ci consentono di mettere al sicuro il dato nella sua forma nativa, prima di essere acquisito e processato dalle applicazioni, o utilizzato per lo sviluppo, e senza gravare sulle performance del database». *Fabio Gianotti, Responsabile della Direzione IT Security & Business Continuity UBI.*

Levi Strauss & Company

«Abbiamo sottoscritto i servizi Oracle CASB Cloud Service perché ci aiutassero a ottenere una maggiore visibilità e una migliore protezione dei nostri investimenti IaaS». *Steve Zalewski, Chief Security Architect di Levi Strauss & Company*

Ooyala, una sussidiaria di Telstra

«Con Oracle CASB Cloud Service possiamo vedere cosa facciano i diversi attori dei processi, potendo monitorare il loro comportamento sul cloud e rilevare automaticamente cambiamenti nelle configurazioni. Questo ci fornisce una visibilità consistente, dettagliata e chiara delle attività eseguite dagli utenti e dalle applicazioni» *Bill Billings, Chief Information Security Officer di Ooyala,*

RIPENSARE LA SICUREZZA NEL CLOUD IBRIDO



Gli ambienti ibridi richiedono modelli di sicurezza centrati sui dati, una visione unificata degli eventi di sicurezza e un controllo accurato a livello applicativo. HPE fornisce una risposta efficace a queste esigenze.

di Riccardo Florio

Nel cloud ibrido le infrastrutture pubbliche e private restano separate, ma sono connesse tramite opportune tecnologie che abilitano lo spostamento di dati e applicazioni da un ambiente all'altro. Questo modello è certamente promotore di innovazione, ma può creare nuove sfide di sicurezza poiché la sua protezione può dimostrarsi più complessa.

La differenza nel contrastare le minacce da una prospettiva cloud è l'aumento di accessibilità che interessa i dati e la sfida per gli IT security è adattare i processi di sicurezza standard e i controlli per farli funzionare bene anche in un ambiente ibrido.

Proteggere le applicazioni nel ciclo di vita

In un ambiente cloud, in cui l'enfasi è su modelli DevOps improntati alla massima agilità e caratterizzati da aggiornamenti molto frequenti del codice, la sicurezza è spesso sottostimata o trascurata. Per esempio, la piattaforma cloud e le istanze di elaborazione possono essere configurate in modo molto sicuro ma, spesso, il punto debole restano le applicazioni.

Una ricerca interna di HPE ha mostrato che,

attualmente, l'84% delle breccie sono indirizzate alle applicazioni, evidenziando come il focus del cyber crimine sia mutato rispetto al passato quando, a essere presi di mira, erano le vulnerabilità a livello infrastrutturale, di sistema operativo e di prodotti commerciali. Tutti i software, sia sviluppati in casa sia acquisiti commercialmente, presentano vulnerabilità e, senza un approccio indirizzato al Software Development Life Cycle, è probabile che applicazioni vulnerabili siano rilasciate in produzione con poca attenzione verso le possibili conseguenze. Il processo di integrare la sicurezza all'interno del ciclo di sviluppo del software è noto come Software Security Assurance (SSA) e si concretizza attraverso tre approcci complementari: l'analisi statica del codice, il test dinamico della sicurezza delle applicazioni e la predisposizione di tecnologie di Runtime Application Self-Protection (RASP).

Attraverso la gamma di soluzioni Fortify, HPE fornisce tutti i tasselli necessari per rispondere a ciascuna di queste esigenze e predisporre un modello SSA. Le soluzioni Fortify per il test statico della sicurezza delle applicazioni effettuano, in modo automatizzato, la scansione di codice sorgente, identificando possibili vulnerabilità, mentre gli strumenti per il test dinamico simulano le tecniche di attacco reali analizzando come le applicazioni e i servizi si comportano in risposta a esse. Soluzioni quali Fortify Application Defender implementano tecnologie RASP che autoprotteggono l'applicazione dall'interno.



Una sicurezza data centrica

Oltre a rendere sicure le applicazioni è necessario rendere sicuri i dati che queste utilizzano. L'uso di tecnologie di cifratura rappresenta un elemento chiave all'interno di un ambiente cloud e si manifesta in diverse modalità correlate al differente stato dei dati nel loro ciclo di vita.

I dati possono essere a riposo ovvero memorizzati in un formato persistente all'interno del cloud sotto forma di file all'interno di sistemi storage oppure di record all'interno di un database e la loro protezione va garantita anche in caso di breccia delle difese esterne. I dati possono essere in movimento tra due punti o due reti e, in tal caso, proteggerli significa evitare che possano essere intercettati. A tal fine è tipico l'uso di soluzioni di cifratura punto a punto che prevedono a creare canali di comunicazione cifrati all'interno dei quali, però, i dati si spostano senza essere cifrati. Infine, ci si deve preoccupare anche di proteggere i dati in uso da un'applicazione che possono essere intercettati perché sono in chiaro.

Le soluzioni tradizionali di cifratura manifestano lacune in ognuno di questi passaggi perché, anche se l'informazione è cifrata in alcuni momenti o condizioni, non è estesa attraverso l'intero ciclo di vita del dato. HPE supera questo ostacolo sfruttando un approccio di sicurezza "data centrico" basato sull'utilizzo di tecnologie specifiche e brevettate di cifratura come FPE (Format Preserving Encryption). Le soluzioni HPE

di Data Security prevedono la cifratura dei singoli "pezzi" di dati memorizzati anziché dello storage o del canale di trasporto. In tal modo, il dato rimane in forma cifrata attraverso il suo intero ciclo di vita e viene decifrato solo quando serve.

Un'altra efficace tecnologia di sicurezza nelle soluzioni di HPE è la "tokenization" utilizzata per proteggere i dati sensibili che si muovono nel cloud. Questo approccio prevede a sostituire i dati sensibili (per esempio il numero di carta di credito) con un token che mantiene formato, comportamento e significato equivalente del dato, ma che viene privato delle informazioni di tipo sensibile. Le soluzioni HPE estendono ulteriormente questa tecnologia utilizzando la Secure Stateless Tokenization (SST), che prevede l'introduzione di token casuali che non richiedono alcun database o sincronizzazione dei dati.

Un SIEM per monitorare gli ambienti ibridi

Il cloud pone anche nuove sfide di controllo e compliance. Con la transizione al cloud ibrido, per avere una vista unificata della sicurezza, è necessario avere la visibilità delle informazioni di sicurezza generate in un ambiente cloud e correlarle in tempo reale con gli allarmi provenienti dai tradizionali data center.

A questa sfida HPE risponde con ArcSight, una soluzione SIEM capace di raccogliere dati di sicurezza da molteplici fonti distribuite, filtrarli, consolidarli, correlarli in tempo reale e aggiungere metadati per organizzarli in contesti di sicurezza omogenei.

Nelle grandi aziende i dati ricevuti da una piattaforma SIEM possono arrivare a miliardi di eventi al giorno. La piattaforma Fortify utilizza una serie di tecniche avanzate di analytics per ridurre alla fonte il volume di informazioni e fornire solo le informazioni di sicurezza rilevanti.

SICUREZZA COSTANTE, INTELLIGENTE

E PUOI AVERLA SUBITO.

Le tue aree di vulnerabilità aumentano. I contenuti si moltiplicano.

I cybercriminali sono sempre più scaltri.

Fortinet offre una singola infrastruttura di sicurezza intelligente che protegge la tua rete dalle minacce attuali e future.

Visita www.fortinet.it per maggiori informazioni.

FORTINET®

Sicurezza senza compromessi