APRILE | 2013

ICT4E.GUIDE

BRIDGING THE GAP BETWEEN TECHNOLOGY & BUSINESS

SICUREZZA NEL CLOUD, I BENEFICI E LE SFIDE

I servizi di sicurezza IT gestiti e fruiti via Cloud risultano di forte interesse per gli utenti aziendali, e soprattutto per le piccole e medie imprese, grazie alla maggior agilità di attivazione e le opportunità di riduzione del TCO (Total Cost of Ownership).
Tuttavia, prima di scegliere, è consigliabile valutare in maniera approfondita alcuni fattori chiave, come l'efficienza dell'infrastruttura Cloud-based e la capacità di personalizzazione dei controlli. Questa **eGuide di ICT4Executive** fornisce qualche utile indicazione in merito.

- La crescita nell'adozione dei servizi di sicurezza in-the-Cloud
- I benefici di gestire la sicurezza nel Cloud
- Le sfide da affrontare nel percorso verso il Cloud
- Best practice per gestire i dati in sicurezza nel Cloud
- Le domande da fare al service provider

SPONSORED BY

F-Secure

.1. L'ADOZIONE DEI SERVIZI DI SICUREZZA IN-THE-CLOUD

L'onda del Cloud Computing sta investendo molte delle attività aziendali, compresa anche la security.
Lo testimonia anche uno studio della società di analisi Gartner in base al quale le soluzioni di sicurezza in ambito Cloud registreranno una crescita importante fra il 2011 e il 2016.
Vediamone alcune particolarmente significative.

SECURE E-MAIL GATEWAY

La fornitura di funzionalità di *Secure E-mail Gateway* in modalità Cloud passerà dal 40 al 55%.
I controlli di sicurezza sulla messaggistica (identificazione di spam e malware) sono in effetti indicati per un utilizzo as-a-service, perché possono tollerare la latenza ed essere ampiamente amministrati attraverso un'interfaccia Web. Usandoli, gli utenti beneficiano anche della conoscenza acquisita dal service provider nell'analisi del traffico proveniente dal tutti i propri clienti.

SECURE WEB GATEWAY

Un'altra categoria in crescita (dal 13 al 25%) sono i servizi di *Secure Web Gateway* (SWG). Per SWG si intendono le soluzioni in grado di rafforzare le policy aziendali preservando, durante la navigazione in Internet, i PC degli utenti dalle infezioni che tali macchine possono contrarre in seguito al "contatto" con malware e software pericoloso.
Alla capacità di individuare il codice malevolo si aggiungono le funzionalità di filtraggio degli indirizzi Web (URL filtering), dei contenuti dei siti, e di controllo delle applicazioni Web-based più diffuse, come quelle di messaggistica istantanea (ad esempio Skype). Sotto forma di servizi, i gateway SWG sono spesso caratterizzati da infrastrutture ibride, e proteggono gli addetti dell'organizzazione che navigano sul Web, bloccando l'accesso agli URL sospetti o dannosi, identificando e bloccando l'esecuzione di malware, controllando le applicazioni.
L'erogazione delle funzionalità SWG as-a-service abilita una miglior protezione degli addetti in mobilità, gestendo via proxy tutti gli accessi Internet attraverso i servizi di filtraggio Cloud-based. L'adozione progressiva di servizi SWG nella nuvola sarà guidata dalla sempre maggiore focalizzazione delle imprese sulla sicurezza degli endpoint mobili.

REMOTE VULNERABILITY ASSESSMENT

È crescita poi anche per i controlli di *Remote Vulnerability Assessment* (RVA), usati per identificare i punti deboli dell'infrastruttura, valutare i rischi, i problemi prioritari e le procedure per eliminarli o prevenirli.
Di solito il VA si abbina anche a test di pene-

trazione, per saggiare dall'esterno il livello di vulnerabilità della rete (porte logiche aperte non utilizzate), dei sistemi e delle applicazioni aziendali (bug software utilizzabili come punti di accesso) ad eventuali attacchi informatici.
I servizi di VA erogati da service provider e fornitori di prodotti in quest'area, sono stimati in espansione (dal 21 al 35%), soprattutto grazie alla domanda di servizi di scansione per requisiti specifici e all'applicazione delle best practice previste dai piani di gestione delle vulnerabilità.

SECURITY INFORMATION AND EVENT MANAGEMENT

Un'altra area è quella SIEM (*Security Information and Event Management*).
Si tratta di soluzioni di intelligence che facilitano l'analisi degli eventi di sicurezza, correlando fra loro le informazioni (alert, stati, ecc.) generate dall'attività dei vari dispositivi e applicazioni, e i dati registrati nei log di sistema. Le funzionalità SIEM possono essere ospitate dall'utente presso il fornitore di servizi gestiti, oppure erogate dallo stesso provider attraverso la propria tecnologia.
Quando completamente Cloud-based, le tecnologie SIEM sono più adatte a chi deve eseguire specifici controlli di conformità, come quella allo standard PCI-DSS (Payment Card Industry Data Security Standard), che definisce le misure di protezione dei processi di pagamento con carta di credito. Requisiti come la memorizzazione locale di dati o i vincoli di banda potranno limitare lo sviluppo delle SIEM, tuttavia la loro adozione as-a-service, passerà dal 3% del 2011 al 12% nel 2016.

DDOS

Ci sono poi gli attacchi informatici DdoS (*Distributed Denial of Service*), miranti di solito a interrompere l'operatività di server aziendali di grosso calibro (server bancari, server di fornitori di servizi online, ecc.).
L'obiettivo è far cadere i servizi del server, inondandolo con un'enorme quantità di traffico proveniente dalle richieste di molteplici PC e macchine distribuiti in rete e precedentemente infettati dall'hacker. Oggi i DdoS continuano a svilupparsi in frequenza e complessità, e contro di essi la difesa attuata dalle infrastrutture on-premise si rivela difficoltosa e inefficace, mentre risultano di maggior successo azioni di filtraggio operate direttamente dagli ISP. In quest'area, l'adozione dei servizi Cloud-based crescerà dal 40 al 65%.

IDENTITY AS-A-SERVICE

L'elenco continua con i controlli di *Identity as-a-service*. Questi sistemi sono framework per i processi di business che facilitano la gestione automatica delle identità elettroniche dei vari utenti e dei relativi privilegi di accesso, concedendo l'ingresso nei sistemi in conformità alle policy aziendali stabilite.
L'adozione dei servizi IAM (*Identity and Access Management*) passerà, da meno del 5, al 30%, via via che tali tecnologie matureranno abbastanza da permettere una gestione fuori dalle sedi aziendali.

PROTEZIONE DEI SITI WEB

La protezione dei siti Web è un altro ambito di diffusione. Qui i sistemi di difesa Cloud-based

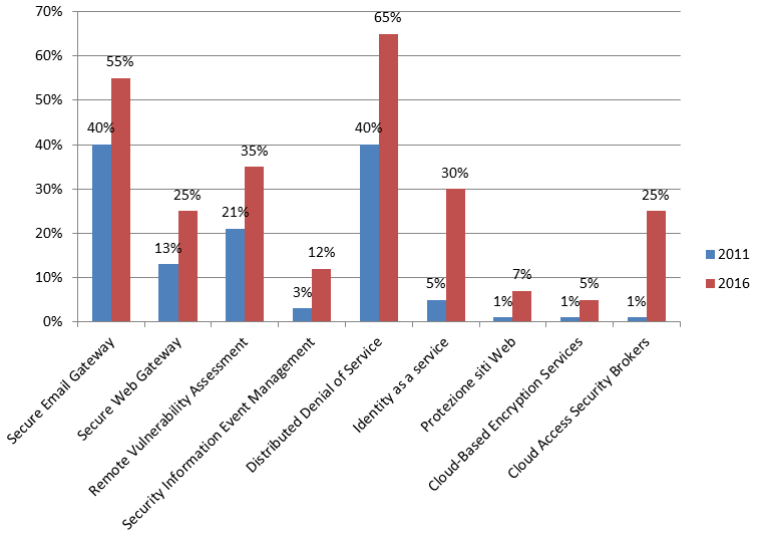
passeranno dall'1 al 7%, spinti dalle esigenze dei siti Web pubblici, dove le specifiche PCI richiedono l'uso di Web Application Firewall (WAF) per proteggere i server che accettano pagamenti con carte di credito.
In applicazioni come queste, i normali firewall aziendali non sono infatti sufficienti, mentre i WAF forniscono un più alto livello di security controllando il traffico Web indirizzato alle applicazioni da proteggere, e bloccando azioni non consentite. Non disponendo di budget per acquisire e gestire WAF di proprietà, molte piccole organizzazioni tenderanno a scegliere i relativi servizi Cloud.

SERVIZI DI ENCRYPTION

Ancora, il modello as-a-service è destinato a svilupparsi anche nella gestione delle operazioni di cifratura dei dati. L'adozione dei servizi di encryption Cloud-based passerà dall'1 al 5%, soprattutto a causa della complessità che molte organizzazioni incontrano nell'implementare on-premise la gestione delle chiavi.

CLOUD ACCESS SECURITY BROKER

Infine, esiste anche il dominio dei CASB (*Cloud Access Security Broker*), ossia i punti infrastrutturali di applicazione delle policy di sicurezza, posti fra gli utenti e i Cloud service provider, in cui solitamente si eseguono controlli di auditing, verifiche delle identità, monitoraggio dei dati sensibili, operazioni di cifratura o interventi di protezione dal malware.
I CASB possono essere ubicati on-premise, sotto forma di appliance, o forniti come servizi Cloud. Di questi ultimi si prevede una crescita dell'adozione, da meno dell'1 al 25%.
Da questa rapida rassegna, si può quindi vedere come molte attività che hanno a che fare con la sicurezza in azienda saranno sempre più erogate in ambito Cloud.



Percentuale di delivery dei servizi di sicurezza in modalità Cloud: il raffronto fra il 2011 e le previsioni 2016 (Fonte: Gartner Group)

.2. SICUREZZA NEL CLOUD, I BENEFICI DI GESTIONE

Nelle aziende, per riuscire a mantenere e, se possibile, rafforzare la sicurezza IT, occorre saper affrontare nuove sfide tecnologiche, legate ai cambiamenti nelle modalità con cui i servizi informatici sono distribuiti e utilizzati.
Oggi, ad esempio, l'utilizzo crescente di tecnologie e risorse informatiche Cloud-based, non gestite direttamente dall'organizzazione, crea un divario fra l'infrastruttura nella nuvola e le funzionalità di controllo della security installate on-premise, nella sede aziendale: tuttavia, specie nelle realtà imprenditoriali di minori dimensioni, migrare verso servizi sicurezza Cloud-based permette di ottenere vantaggi, soprattutto in quattro aree chiave.

1. EFFICIENZA

Acquisendo i servizi di IT security in modalità Cloud, l'impresa utente non deve stanziare un budget per l'acquisto di attrezzature, e può tagliare i costi per il dispiegamento e la manutenzione delle tecnologie necessarie.
Nei casi in cui i controlli possono essere forniti come un mix di funzionalità on-premise e di security as-a-service, diventa anche possibile estendere i controlli di sicurezza esistenti verso nuove aree, senza incorrere in significativi incrementi dei costi.
Nelle soluzioni Cloud-based fornite dai fornitori di IT security, lato utente, i vantaggi di efficienza si misurano anche nel fatto che la configurazione dei parametri e delle funzionalità chiave non richiede l'uso di una console dedicata o di tunnel VPN (Virtual Private Network), ma si può eseguire direttamente via Web, su connessione cifrata, attraverso un portale e in maniera centralizzata: in questo modo si può mantenere un controllo e un update unificato per tutti i sistemi e dispositivi, compresi quelli mobile (tablet, smartphone), sia in termini di protezione antivirus, sia a livello dei periodici aggiornamenti finalizzati a sanare le vulnerabilità più pericolose, indicando via via gli update più critici da effettuare.
Ciò permette di amministrare la security, e configurare e utilizzare i vari strumenti, ovunque e in qualsiasi momento, tramite dispositivi diversi.
Non occorre ordinare e acquistare pacchetti di upgrade, perché l'aggiornamento dell'applicazione avviene in automatico su tutti gli endpoint, in modo da rendere disponibile sempre l'ultima tecnologia. In caso di necessità di supporto tecnico per la risoluzione di problemi, in genere l'assistenza può essere fornita direttamente online, senza richiedere l'uscita di un tecnico.
La registrazione al portale avviene mediante la semplice creazione di un account, che consente poi di accedere ai servizi di security fornen-

do come credenziali nome utente e password. Possedendo un account di amministratore, dal portale è in genere possibile assegnare nuovi profili di sicurezza, riavviare il firewall o la scansione in tempo reale, modificare gruppi o, ancora, rimuovere computer o dispositivi pericolosi o infetti.
Per quanto concerne le capacità di reporting, queste soluzioni, oltre a fornire rapporti di protezione e informazioni dettagliate su tutte le macchine e a consentire varie operazioni di test, permettono anche di configurare ciascun endpoint per inviare periodicamente un aggiornamento completo sul proprio stato di funzionamento.
La configurazione di diversi profili di protezione fornisce un controllo di quali impostazioni di protezione rendere modificabili dagli utenti sui propri computer.
Un'altra funzionalità possibile è la localizzazione e il blocco di un dispositivo mobile, ad esempio un telefono, o anche la cancellazione dei dati al suo interno da remoto, in caso di furto del dispositivo.

2. EFFICACIA

Se ben amministrati, i controlli di sicurezza Cloud-based consentono di fornire risposte più rapide alle nuove minacce o vulnerabilità scoperte.
Le funzionalità di difesa, e i miglioramenti delle stesse, non dipendono dalle azioni dell'utente, ma vengono erogate dal service provider.
Inoltre quest'ultimo, monitorando l'efficacia dei propri servizi sull'intera base clienti, ha l'opportunità di ricevere feedback continui, che gli consentono di incrementare ulteriormente la qualità dei servizi.

3. FLESSIBILITÀ

Come si è detto, rispetto al passato, oggi ci sono molte novità in merito a come e dove l'IT viene utilizzata a supporto delle attività di lavoro. Si pensi solo a fenomeni come la "consumerizzazione" dell'informatica o alla mobility, e al modo in cui hanno ridotto il rigido controllo dei responsabili dei sistemi informativi sul tipo di hardware, dispositivi, sistemi operativi, software e servizi usati dagli utenti per svolgere i loro compiti. Oggi, per il reparto IT non dover dipendere dallo sviluppo di tecnologia on-premise significa ridurre la complessità, i costi di modifica dei controlli di sicurezza, e velocizzarne il deployment.
Nei moderni contesti IT, più fluidi e dinamici, dove occorre amministrare sistemi tradizionali e dispositivi "mobile", passare a servizi Cloud-based permette di modificare le funzionalità di security più facilmente. In prospettiva, uno dei modi più efficaci per rendere sicuro l'utilizzo dei servizi IT via Cloud a livello enterprise sarà fornire controlli di security direttamente dalla nuvola.

4. CONTROLLO DEI COSTI

Dal punto di vista della capacità di governance sui costi legati alle attività di IT security, il modello Cloud offre di certo benefici non trascurabili.
Specialmente per le piccole e medie aziende, e per tutte quelle organizzazioni in cui questa voce di spesa sta andando fuori controllo, o lo

è già. Spesso infatti le imprese non possiedono una chiara comprensione dei costi reali che stanno sostenendo per la gestione della sicurezza IT on-premise.
Migrando verso il modello as-a-service questo controllo si può riprendere, perché si passa da un paradigma fondato sui costi Capex (Capital Expenditure), quindi sugli investimenti, a uno che pone in primo piano i costi Opex (Operational Expenditure), cioè le spese operative. Chi opta per la sicurezza gestita nel Cloud si impegna solo a pagare un canone commisurato all'effettivo consumo del servizio, e non deve più preoccuparsi di tutte le altre voci di spesa: in primis, l'acquisto dell'hardware (server, security appliance, ecc.) e del software (firewall, IPS, antivirus, ecc.), con la relativa gestione delle licenze e degli aggiornamenti. L'azienda non è costretta, periodicamente, a rinegoziare i contratti di assistenza tecnica con terze parti, né a pagare costosi interventi di manutenzione effettuati da personale esterno; non ha nemmeno la necessità di assumere addetti specializzati nella gestione e controllo dell'infrastruttura di sicurezza on-premise.

	Licensed products:	Security as a Service:
Finance	• CAPEX • Ownership	• OPEX • Subscription
Flexibility	• High risk • Only growth	• Low risk • Grow or reduce
Solution	• Long term strategy • Situational snapshot	• Continuous strategy • Evolves, or exit
Relationship	• Fulfillment • Solution focused	• Service partner • Service focused

Le principali differenze fra i modelli on-premise e SaaS (fonte: F-Secure)

-3- LE SFIDE NEL PERCORSO VERSO IL CLOUD

Accanto ai benefici, occorre però anche considerare tutti i possibili fattori in grado di compromettere la qualità di erogazione dei servizi di sicurezza via Cloud. In particolare, è bene assicurarsi che tali servizi soddisfino i requisiti in alcune aree specifiche.

DISPONIBILITÀ DEL SERVIZIO

I controlli di sicurezza forniti as-a-service dipendono dalla connettività di una rete esterna, e i problemi sulle sue prestazioni possono influenzare negativamente la disponibilità dei servizi di security. Quando sono richieste alta disponibilità e bassa latenza per i controlli, deve esistere un supporto sufficiente per assicurare la capacità e continuità di servizio, e ciò può far crescere i costi di connettività e infrastruttura per i service provider e gli utenti. Inoltre, nei casi in cui la disponibilità dei controlli di sicurezza dev'essere più elevata della disponibilità garantita per la connettività Internet, devono essere previsti controlli di sicurezza installati anche on-premise.

SCALABILITÀ

Nel tempo i requisiti di business possono cambiare e, di conseguenza, i servizi di security Cloud-based devono essere in grado di adeguarsi a tali fluttuazioni nell'intensità di utilizzo, sia espandendo, sia riducendo la capacità. Oltre a dover soddisfare questi requisiti, il service provider deve anche essere in grado di contabilizzare i consumi, attraverso un'operatività che permetta di verificare i sistemi di billing e gli SLA (Service Level Agreement) concordati con gli utenti.

PERSONALIZZAZIONE

È questo un importante aspetto da considerare, perché in molte situazioni i controlli di sicurezza si devono adattare a ruoli e casi d'uso differenti, richiedendo una raffinata "customizzazione" per soddisfare i requisiti delle policy. Laddove si renda necessario personalizzare i controlli, i servizi Cloud-based potrebbero non fornire sufficiente granularità di configurazione per conformarsi ai requisiti, dando luogo a incrementi di costi associati alla customizzazione dei servizi. In generale, si può dire che controlli di sicurezza strettamente abbinati a requisiti specifici di business sono meno probabilmente forniti con efficacia o efficienza via Cloud.

INTEGRAZIONE CON LE APPLICAZIONI E INFRASTRUTTURE ESISTENTI

I controlli di sicurezza possono richiedere l'integrazione con numerose applicazioni di business ed altre funzionalità di security, e da questo punto di vista i controlli di security as-a-service potrebbero offrire minori opzioni per

supportare un'integrazione estesa. Controlli di sicurezza con limitato supporto all'integrazione aumentano i costi di implementazione per gli utenti che devono creare soluzioni custom. Inoltre, dove i controlli di sicurezza as-a-service sono adottati per estendere le funzionalità di tecnologia di sicurezza implementata dall'utente, i service provider devono essere in grado di supportare un'amministrazione e un monitoraggio unificati sull'intero ambiente. Ciò perché controlli di security Cloud-based che richiedono processi di amministrazione duplicati riducono l'efficienza, innalzano il TCO per l'utente e accrescono le probabilità di un'efficacia ridotta a causa di una cattiva gestione. Dunque, i controlli di sicurezza che richiedono elevati livelli d'integrazione con applicazioni di business personalizzate o proprietarie sono meno indicati per essere erogati in modo efficace ed efficiente attraverso la nuvola.

CONTROLLO DEL PROCESSO

Adottare il modello Cloud-based significa esternalizzare la gestione dei servizi di IT security. Scegliere l'outsourcing comporta di conseguenza una certa perdita di controllo, anche se, come si è visto, occorre ricordare che vari vendor e service provider di servizi di sicurezza gestita consentono agli utenti aziendali di configurare, tramite portale Web, molte funzionalità e opzioni di amministrazione e reporting della piattaforma di security.

Le imprese con scarsa esperienza di outsourcing dell'IT sono improbabili candidate e a essere le prime utilizzatrici di controlli di sicurezza Cloud-based. Va altresì detto che le competenze IT necessarie per gestire questi processi possono anche essere messe a disposizioni dai partner certificati del fornitore che possono farsi carico di queste attività.

.4. BEST PRACTICE PER GESTIRE I DATI IN SICUREZZA

Le difficoltà di realizzazione di sistemi di monitoraggio della sicurezza dei dati variano a seconda del modello di Cloud computing scelto: SaaS (Software as a service), IaaS (Infrastructure as a service), PaaS (Platform as a service). Tuttavia vi sono alcune best practice applicabili in generale.

- Per cominciare, occorre stabilire che tipo di analisi è richiesta sui dati. Per alcuni casi d'uso, e in particolare per le offerte SaaS e PaaS, il monitoraggio di default della rete o dell'applicazione, fornito come parte dell'accordo di servizio con il Cloud provider, potrebbe essere sufficiente, anche se alcuni servizi, come quelli ALMaaS (Application lifecycle management as a service) o ASaaS (Application security as a service) non memorizzano i tipi di dati che devono essere monitorati.

- Le opzioni di monitoraggio della sicurezza a livello di dati vanno valutate nei progetti attuali e futuri, per assicurare che le piattaforme e i provider scelti forniscano gli appropriati livelli di controllo dell'analisi, commisurati ai rischi associati ai dati. Ciò è importante soprattutto per le tipologie di dati il cui trattamento è regolato da normative. Se i controlli del provider sono insufficienti, è meglio valutare i tool di terze parti, in modo da indirizzare adeguatamente i rischi.

- L'azienda utente deve assicurarsi che gli organismi incaricati delle verifiche, i dipartimenti legali e di controllo della conformità, e tutte le altre parti interessate, comprendano i rischi di un monitoraggio limitato della sicurezza dei dati nella Cloud. Queste figure devono concordare sull'idoneità della soluzione individuata, prima del passaggio alla sua effettiva implementazione, per evitare l'impatto su performance e costi causato da interventi a posteriori.

- È utile considerare lo stadio di maturazione dei Cloud security broker, o di terze parti in grado di fornire funzionalità aggiuntive di sicurezza, rispetto alle offerte standard dei Cloud service provider.

- Cercare e seguire le linee guida su come utilizzare le soluzioni e i tool nativi nella Cloud, le soluzioni di altri software vendor, o le API rese disponibili dai Cloud service provider per permettere agli utenti di sviluppare la propria soluzione.

- Nel caso in cui esistano due distinte piatta-

forme di monitoring, una on-premise e una nella public Cloud, è bene assicurarsi che ciascuna soluzione di monitoraggio si integri o comunichi con i sistemi di analisi, gli strumenti di risposta agli incidenti e i processi funzionanti a livello enterprise.

- Considerare i servizi di sicurezza Cloud-based in grado di agire come proxy, cifrare dati sensibili prima di memorizzarli nella Cloud, o monitorare l'accesso nella nuvola a tutte le informazioni.

GLI INCONVENIENTI DEL MODELLO SAAS

Nel sistemi di fornitura dei servizi Cloud basati sul paradigma SaaS (Software as a service), l'accesso ai dati non può avvenire in modo diretto, ma solo attraverso la specifica applicazione, e perciò non esiste una reale differenza fra monitoraggio di quest'ultima e monitoraggio dei dati.

La maggioranza dei fornitori di servizi SaaS produce report standard, basati sull'attività dell'applicazione: qui però, la sfida per l'utente è implementare funzionalità di monitoraggio e analisi in grado di osservare il comportamento degli addetti, per individuare e verificare a quali informazioni, record o documenti si accede per completare un dato lavoro.

Alcuni SaaS provider forniscono API (Application Programming Interface) utilizzabili per produrre strumenti di reporting e analisi personalizzati, ma scegliere questa strada implica difficoltà di sviluppo, e di standardizzazione rispetto ai servizi dei vari SaaS provider, tali da spingere a ritornare all'uso dei tool di monitoraggio nativi, messi a disposizione dal fornitore del servizio.

LA GIURISDIZIONE DEL DATO

Secondo il paradigma Cloud, tecnicamente, la memorizzazione delle informazioni nei data center può avvenire ovunque nel mondo, dunque anche in centri dati che risiedono in paesi con ordinamenti legislativi differenti, riguardo alla protezione a al trattamento dei dati, rispetto a quello di origine. In Italia fa testo il decreto legislativo 30 giugno 2003, n. 196, sul codice in materia di protezione dei dati personali, mentre a livello europeo il settore è disciplinato dalla direttiva UE 95/46/CE. Tuttavia nei paesi extraeuropei, e ad esempio negli Stati Uniti, vigono regolamentazioni diverse. Tale disomogeneità legislativa crea ambiguità giurisdizionali riguardo alle normative applicabili, specie quando, per questioni geografiche o territoriali, la figura del responsabile sul trattamento dei dati non risulta chiaramente individuabile. E in questo scenario, per un'azienda utente di servizi Cloud, negoziare ad esempio il rispetto della normativa italiana con un service provider extraeuropeo può rivelarsi oggettivamente arduo. Per tale ragione, prima di scegliere il fornitore a cui affidarsi, è bene leggere attentamente il contratto di servizio e tutte le clausole che contiene al riguardo

-5- LE DOMANDE DA FARE AL SERVICE PROVIDER

Per ridurre i rischi di impatto sul business causati ad esempio da eventi di violazione dei dati o interruzione dei servizi, prima di decidere se acquisire i servizi di IT security in modalità as-a-service, è meglio conoscere e valutare più a fondo i singoli Cloud service provider e come operano.
Molti di loro, infatti, non forniscono sufficiente trasparenza riguardo alle pratiche di sicurezza o alla conformità a determinate normative del settore. Ecco perché è necessario saper porre alcune domande chiave.

RETE

È il primo elemento critico. Al provider va chiesto ad esempio se richiede l'autenticazione a due fattori per il controllo amministrativo di server, router, switch e firewall. Se supporta tecnologie come Ipsec, o SSL (Secure Sockets Layer) con certificato a validità estesa (EV SSL), e se fornisce funzioni di ridondanza e load balancing (bilanciamento dei carichi di lavoro) per firewall, sistemi di prevenzione delle intrusioni (IPS) e altri componenti critici per la sicurezza.
Occorre sapere se esegue test di penetrazione esterna almeno trimestralmente, e audit di sicurezza interna della rete annualmente, in conformità con certificazioni come SAS 70 Type II.
È utile sapere se il service provider è in grado di mostrare requisiti documentati e procedure di audit per la sicurezza di rete, per avere garanzie che gli altri utenti non compromettano l'infrastruttura di servizi condivisa. Ancora, si può domandare se nel contratto e prevista la protezione contro attacchi di tipo DoS (Denial of service).

DATI E APPLICAZIONI

A questo livello, è bene sapere se il Cloud service provider riesamina la sicurezza delle applicazioni e il codice di supporto (Ajax, controlli ActiveX, Java applets) che sviluppa e utilizza.
Se esegue il monitoraggio e filtraggio dei contenuti, o applica tecnologie DLP (Data Loss Prevention); se possiede procedure documentate per la gestione della configurazione per tutte le applicazioni, inclusa l'installazione delle patch di sicurezza. Se il servizio Cloud implica la gestione di dati coperti da regolamentazioni o altri requisiti di conformità (Sarbanes-Oxley, PCI-DSS, ecc.) e se il service provider soddisfa i requisiti applicabili per la protezione di tali dati.

PIATTAFORMA E OPERATION

Riguardo alla prima, occorre verificare se il fornitore dei servizi Cloud dispone di policy documentate per l'irrobustimento (hardening) dell'infrastruttura virtualizzata che supporta i servizi. Se vengono fornite procedure validate per la gestione della configurazione, l'installa-

zione delle patch e la prevenzione del malware per tutti i server e PC che utilizzeranno il servizio Cloud in questione. Se esiste un insieme documentato di controlli che il service provider usa per assicurare la separazione dei dati e la sicurezza delle informazioni fra le applicazioni degli utenti.
Per quanto concerne le operation, il Cloud service provider dovrebbe anche eseguire periodici controlli sul personale che dispone di account amministrativi o di altri diritti di accesso privilegiato a server, applicazioni o dati degli utenti. E dovrebbe possedere privilegi di gestione come supervisore, e controlli di monitoraggio delle attività del database, per individuare comportamenti scorretti o sospetti degli impiegati con accesso amministrativo.
Il fornitore dei servizi Cloud dovrebbe anche poter mostrare un processo documentato per la valutazione degli allarmi di sicurezza provenienti dai vendor di sistemi operativi e applicazioni, schermando i sistemi fino a che non vengono installati patch e service pack di protezione.
Non va neppure dimenticata la necessità per il Cloud service provider di utilizzare funzionalità di monitoraggio della security, di gestione del registro di sistema, e tecnologie affidabili per lo storage delle informazioni sulle attività di audit o sui registri delle operazioni di sicurezza.
Ancora, il fornitore deve poter dimostrare l'esistenza di procedure consolidate per la gestione delle vulnerabilità, la prevenzione delle intrusioni, o la risposta agli attacchi.
Ma anche il possesso di piani collaudati per la gestione della continuità del business e delle operazioni di disaster recovery.

CONCLUSIONI

L'inarrestabile trend di espansione del Cloud Computing sta interessando anche i particolarmente critici e delicati servizi aziendali di sicurezza informatica (si veda il Cap. 1), come dimostrano i dati di diffusione del modello Cloud in tutte le realtà in cui le tecniche di protezione basate sulle classiche infrastrutture on-premise risultano difficoltose, inefficaci o troppo costose.
Far migrare i servizi di sicurezza IT nella nuvola consente alle imprese utenti di ottenere vantaggi (Cap. 2) soprattutto in termini di efficienza, efficacia, flessibilità e controllo dei costi (Opex contro Capex) legati alle attività di IT security.
Tuttavia, per ottenere pienamente tali benefici, si devono affrontare anche sfide (Cap. 3). Il punto essenziale è considerare con attenzione tutti i possibili elementi in grado di influenzare la qualità di erogazione dei servizi Cloud-based di sicurezza IT: in particolare, la banda e la disponibilità del servizio, i requisiti di scalabilità e personalizzazione delle funzionalità; le esigenze d'integrazione con le applicazioni e le infrastrutture già presenti, e anche il livello e la capacità di controllo che si vuol mantenere sulla configurazione e amministrazione di tali servizi nel Cloud.
Un'area chiave è il monitoraggio della sicurezza dei dati nella nuvola, in cui per la realizzazione dei sistemi è possibile seguire alcune best practice di validità generale (Cap. 4).
Infine, prima di optare per l'acquisizione dei servizi di IT security in modalità as-a-service è

sempre bene conoscere in profondità i diversi Cloud service provider e le loro specifiche offerte.
Soprattutto, è importante chiarire le politiche in materia di trasparenza, riservatezza e privacy nel trattamento dei dati. Inoltre bisogna valutare con attenzione il livello di conformità con le normative vigenti in merito alla gestione delle informazioni e ai piani di hardening e disaster recovery delle infrastrutture virtualizzate.

ICT4 E.GUIDE

BRIDGING THE GAP BETWEEN TECHNOLOGY & BUSINESS