

COMPLIANCE

NUOVE REGOLE SULLA PRIVACY: COSA CAMBIERÀ CON IL GDPR

Più responsabilità, anche penali, nuove restrizioni e un'uniformità a livello europeo solo al 70%.

Le ultime indicazioni confermano che entro luglio dovrebbe essere pubblicato il nuovo regolamento europeo sulla Privacy, dopodiché i Paesi interessati avranno due anni di tempo per adeguarsi alla nuova normativa.



In previsione di questi cambiamenti abbiamo intervistato un'esperta in materia, Paola Generali, managing director di GetSolution, società che dal 2003 si occupa di Privacy Law e di sicurezza dei sistemi informativi, per farci anticipare le novità.

pag.17-19

LA PAROLA AI PROTAGONISTI

LA SICUREZZA OLISTICA E INTEGRATA DI SNAM



Sulle difese adottate dalla società per la salvaguardia dei suoi asset tangibili e intangibili abbiamo intervistato Massimo Cottafavi, responsabile

Information Security & Business Continuity.

pag.05

LA PAROLA AI PROTAGONISTI

EASYSHIELD DI HITACHI DALLA COMPLIANCE ALLA CYBER SECURITY

La sicurezza IT nella nuova offerta che unisce le competenze del team italiano con la knowledge base e i Managed Security

Service dei SOC Hitachi Systems e le best practice di Above Security, acquisita lo scorso agosto.

pag.08



IN QUESTO NUMERO:

EDITORIALE

pag.3

• Le spinte al mercato della sicurezza

NEWS

pag.04

• Torna l'appuntamento con il Security Summit 2016

CYBER ATTACK

pag.10-11

• Cyber Intelligence: un passo avanti alle minacce

pag.12-13

• Per essere efficace la sicurezza va contestualizzata

pag.14-15

• Da cloud e IoT i principali timori per la sicurezza

SOLUZIONI

pag. 22-23

• Pc più sicuri con la verifica del Bios

pag. 24-25

• Come aumentare la sicurezza degli endpoint

pag. 26-27

• PMI nel mirino dei cyber criminali: le nuove soluzioni di Check Point

Le violazioni della sicurezza? Non sulla stampante.

Proteggi la tua rete con le stampanti più sicure al mondo.

Le nuove stampanti enterprise HP LaserJet con tecnologia JetIntelligence offrono la sicurezza di stampa più robusta del settore,¹ grazie a funzionalità integrate quali HP Sure Start con BIOS di auto-riparazione, la tecnologia di whitelisting e il rilevamento intrusioni durante l'operatività.

hp.com/go/printersthatprotect

A large HP printer is shown from a high angle. The main screen displays a statistic: 'Il 53% dei manager IT è consapevole della vulnerabilità delle stampanti ai crimini informatici.' The background of the screen shows a man in a yellow shirt standing in a server room. Below the main screen, there is a smaller touch screen displaying a dashboard with various charts and graphs. The printer is surrounded by various data visualization elements like spreadsheets and charts.

Il 53%
dei manager IT
è consapevole della
vulnerabilità delle
stampanti ai crimini
informatici.²

¹ Le stampanti più sicure al mondo e il massimo livello di sicurezza: sulla base di verifiche HP pubblicate nel 2015 sulle funzionalità di sicurezza integrate nelle stampanti della stessa categoria dei produttori concorrenti. Solo HP offre una combinazione di funzionalità di sicurezza per la verifica dell'integrità fino alle capacità di auto-riparazione del BIOS. Potrebbe essere necessario un aggiornamento dei service pack FutureSmart per attivare le funzionalità di sicurezza sui modelli HP LaserJet M527, M506, M577. Alcune funzionalità saranno disponibili come aggiornamento dei service pack HP FutureSmart su modelli di stampanti enterprise esistenti selezionati. Per un elenco dei prodotti compatibili visita: <http://h20195.www2.hp.com/V2/GetDocument.aspx?docname=4AA6-1178ENW>. Per maggiori informazioni, visita: hp.com/go/ljsecurityclaims.

² Ponemon Institute, "Annual Global IT Security Benchmark Tracking Study", marzo 2015.
© Copyright 2015 HP Development Company, L.P.

Le spinte al mercato della sicurezza



di Gaetano Di Blasio

Quando furono introdotte le prime norme in materia di privacy, si registrò un discreto impulso nel mercato della sicurezza. Quest'anno in molti si aspettano una spinta dall'approvazione del nuovo regolamento europeo, il GDPR (General Data Protection Regulation), che, però, sarà approvato definitivamente solo a luglio e, comunque, lascia due anni di tempo per gli adeguamenti eventualmente necessari. La spinta, che probabilmente ci sarà anche se l'Italia è tra i paesi in cui la normativa è più avanzata, potrebbe avere un impatto più significativo nel prossimo biennio.

Sulle novità relative al nuovo provvedimento trovate un'ampia disamina nelle pagine dedicate alla compliance, ma altri dettagli saranno ovviamente svelati all'imminente Security Summit di Milano, che, attenzione, cambia location.

L'appuntamento con gli amici esperti del Clusit sarà occasione anche per fare il punto sull'evoluzione dei sistemi di pagamento, alla luce della prossima direttiva PSD2.

È evidente che in questo contesto la sicurezza è fondamentale e, soprattutto, implicita.

La digitalizzazione di molti processi critici, come appunto i pagamenti, rappresenta un'opportunità di crescita forse più importante dei vari regolamenti. La sicurezza, infatti, diventa parte del processo, dunque una voce di costo tra le altre e, in definitiva, inseribile in una misura del ROI. Come ci insegnano i lavori svolti proprio in collaborazione con il Clusit per il progetto ROSI (Return On Security Investment), questa è una delle chiavi per creare sicurezza intrinseca by design accettata facilmente dal business.

È nell'automazione dei processi che va trovato spazio per la sicurezza e la sua crescita.

Numero 32
Tutti i marchi sono registrati
e di proprietà delle relative
società

Registrazione al tribunale
n.585 del 5/11/2010

Editore: Reportec srl

Direttore responsabile:
Gaetano Di Blasio

In redazione: Riccardo Florio,
Giuseppe Saccardi, Paola
Saccardi

Immagini: dreamstime.com -
www.securityebusiness.it

Reportec

SECURITY
& BUSINESS

TORNA L'APPUNTAMENTO CON IL SECURITY SUMMIT 2016

Dal 15 al 17 marzo si svolge a Milano l'evento dedicato alla sicurezza informatica in cui viene presentato il nuovo Rapporto Clusit che delinea lo stato dell'arte del settore in Italia

Torna a Milano l'appuntamento con il principale evento italiano dedicato alla sicurezza informatica che quest'anno si terrà dal 15 al 17 Marzo presso l'Atahotel Expo Fiera. La nuova location è stata scelta per rendere ancora migliore la fruizione della manifestazione, grazie alla presenza di spazi ampi e moderni dotati di luce naturale.

L'evento, che è arrivato all'ottava edizione, è organizzato dal Clusit (l'Associazione italiana per la sicurezza informatica) insieme all'agenzia di comunicazione e marketing

Astrea e prevede come in passato la partecipazione esperti e personalità di spicco nel settore ICT, così come rappresentanti del mondo delle istituzioni e gli stessi utenti di tecnologia.

Il programma dell'edizione 2016 è ricco e articolato e darà spazio a un centinaio di relatori che si alternano nel corso delle tre giornate, in cui sono previsti anche diversi momenti di dibattito e confronto ai quali il pubblico sarà chiamato a partecipare. Nel complesso l'agenda del Security Summit 2016, che prenderà il

via con la presentazione del Rapporto Clusit 2016 sulla sicurezza ICT in Italia (sessione plenaria di apertura martedì 15) prevede 7 tavole rotonde, 11 sessioni formative, 6 seminari e 20 atelier tecnologici.

I temi affrontati nel corso della tre giorni dagli esperti e rappresentanti delle istituzioni sono svariati: la prevenzione e gestione degli attacchi, il nuovo regolamento europeo sulla protezione dei dati personali, la sicurezza delle informazioni in ambito sanitario, le sfide dell'e-commerce, l'evoluzione dei sistemi di pagamento e le

coperture assicurative per i rischi relativi all'IT, cyberwar e cyber intelligence, sicurezza dei dispositivi mobile, Internet of Things.

La partecipazione a Security Summit 2016 consente inoltre di acquisire crediti CPE (Continuing Professional Education) validi per il mantenimento delle certificazioni CISSP, CSSP, CISA, CISM o analoghe richiedenti la formazione continua. L'iscrizione è gratuita e richiede l'accredito al sito www.securitysummit.it, dove sarà a breve disponibile il programma completo del convegno.





LA SICUREZZA OLISTICA E INTEGRATA DI SNAM

Sulle difese adottate dalla società per la salvaguardia dei suoi asset tangibili e intangibili abbiamo intervistato Massimo Cottafavi, responsabile Information Security & Business Continuity

di Gian Carlo Lanzetti

Come è organizzato il governo degli aspetti di information security e IT security all'interno del suo Gruppo?

Il Gruppo Snam ha posto sempre grande attenzione agli aspetti di tutela delle informazioni e delle infrastrutture tecnologiche a supporto del business. L'attuale modello di governo pone le proprie radici nel 2010, anno in cui è stata istituita una specifica funzione di Corporate Security. Fin da subito è stata istituita al suo interno una unità dedicata agli aspetti di Information Security, Business Continuity e Crisis management con l'obiettivo di sovrintendere, indirizzare e monitorare questi temi a livello di Gruppo. Tale unità mantiene forti relazioni con altre strutture aziendali, prima fra tutte quella dedicata agli aspetti di Sicurezza ICT, posizionata all'interno della Direzione ICT.

Dal momento che in un siffatto modello di governo la capacità di coordinamento è essenziale, un ruolo significativo ritengo sia quello ricoperto dall'Information Security Committee, un Comitato a valenza consultoria e decisoria espressamente dedicato alla condivisione e valutazione delle principali issue connesse alla gestione e tutela delle informazioni. Per sua stessa natura credo che l'Information Security Committee sia la diretta espressione del forte impegno del Gruppo nei confronti di questa tematica;

non va infatti sottovalutato che al suo interno siedono come membri permanenti tre primi riporti del vertice aziendale.

Viene attribuito un budget dedicato alle attività di information security?

Le unità preposte alla gestione della sicurezza possono fare affidamento su un budget, definito coerentemente con le specifiche esigenze rilevate nel corso delle analisi periodiche e tenendo conto delle eventuali esigenze di sicurezza che i nascenti progetti di business portano con sé.

Quale impatto ha avuto il tema della digital transformation sugli aspetti di difesa da minacce esterne ed interne?

La digital transformation impone alle aziende cambiamenti culturali e una rivisitazione a volte profonda dei processi interni. Per esempio, sebbene se ne parli da moltissimo tempo, è solo in epoca recente che principi e concetti spesso riassunti con il termine "sicurezza integrata" cominciano ad affermarsi realmente e a essere di uso comune. In altre parole, proprio per via dell'im-



Massimo Cottafavi - Snam



patto che la digital transformation sta avendo tanto sul modo di lavorare delle persone quanto sulle scelte di business, non è più possibile venire incontro alle reali esigenze di sicurezza di una determinata realtà aziendale operando sulla base di una compartimentazione delle responsabilità e delle competenze; non può per esempio esistere una sicurezza fisica slegata da una sicurezza informatica dal momento che, oggi, anche un asset fisico può risultare connesso digitalmente e per tale via risultare vulnerabile a forme di attacco impensabili in passato. La sicurezza deve necessariamente essere intesa in chiave olistica.

L'Osservatorio del Polimi dedicato alla Security ha rivelato la esistenza di un basso grado di consapevolezza delle organizzazioni italiane verso l'Information Security: voi vi identificate in questa indicazione oppure pensate di essere posizionati meglio?

Personalmente non credo che il vero problema sia rappresentato dal livello di consapevolezza raggiunto, ma da come tale consapevolezza viene tradotta in comportamenti attivi. Tanto per fare un esempio, chiunque è con-

sapevole che guidare una moto senza casco può esporre, oltre che a sanzioni, al rischio di seri danni fisici; malgrado questo alcune persone si ostinano a guidare senza casco, scegliendo consciamente di non tradurre in un comportamento virtuoso una consapevolezza che comunque hanno. Si tratta della stessa cosa che nella maggioranza dei casi accade quando un utente decide di usare password insicure o di annotarle nei pressi del PC, di lasciare il PC incustodito o di scaricare file "sospetti" che a volte provengono da indirizzi sconosciuti. Per le aziende ciò si traduce nella necessità di non limitarsi a organizzare campagne di sensibilizzazione e formazione, meglio se definite secondo criteri diversificati a seconda dello specifico target, ma anche di dotarsi di strumenti per monitorare gli effetti che tali iniziative hanno sui comportamenti attuati. Il gruppo Snam sta concentrandosi proprio su questo aspetto.

In ogni caso ritenete ci sia ancora molto da fare e se sì, al vostro interno, in quali direzioni?

Per definizione da fare ce n'è sempre, per la semplice ragione che non ci sarà mai un punto di arrivo. Le minacce sono eterogenee così come le tipologie di potenziali attaccanti. L'evoluzione tecnologica porta quotidianamente all'insorgere di nuove problematiche che prima non erano state prese in considerazione. In un contesto simile la vera sfida è rappresentata dalla capacità di superare il tradizionale approccio basato su una sicurezza "statica", vale a dire basata su analisi e rilevazioni periodiche, a vantaggio di un approccio "dinamico", incentrato cioè sulla capacità di intercettare e reagire



pressoché in real time a ogni cambiamento di contesto. Da questo punto di vista diventa essenziale mettere in campo capacità di threat intelligence.

Quali valutate saranno per voi le sfide prossime più importanti?

Certamente stiamo monitorando con attenzione l'evoluzione dei cosiddetti scenari cyber in modo che il modello organizzativo e i processi operativi di gestione della sicurezza risultino sempre in linea con le reali sfide che un'infrastruttura critica per il Paese deve saper cogliere. Al riguardo stiamo valutando con interesse e attenzione le indicazioni riportate all'interno del Framework Nazionale per la cybersecurity presentato di recente a Roma.

Security e Privacy sono due elementi congiunti o distinti della vostra strategia della Digital Security?

Il temi connessi alla tutela dei dati personali hanno oggettivamente una valenza diversa in un contesto opera-

tivo come quello all'interno del quale si muove il Gruppo Snam rispetto a quella che possono avere per società che si rivolgono al mass market (penso per esempio a telco e banche); cionondimeno le previsioni discendenti dalla normativa in materia di trattamento dei dati personali vengono prese in debita considerazione e non vengono vissute in alcun modo come antitetiche rispetto a quelle che possono essere le esigenze e le strategie di security.

Da ultimo come valutate i rapporti con i fornitori di tecnologie e cosa vi sentite loro di suggerire per una ottimizzazione delle risorse in campo su questo fronte?

I fornitori di tecnologie hanno un ruolo essenziale nell'ambito del disegno complessivo della sicurezza di un'azienda. Alcune volte però credo che garantiscano ai propri clienti un ritorno, in termini di valore aggiunto, inferiore a quello che potrebbero mettere in campo, focalizzandosi in maniera eccessiva sulla vendita di uno specifico prodotto o licenza. Dato il bagaglio esperienziale che portano con sé, non fosse altro per la possibilità che hanno, grazie alla loro conoscenza di molteplici realtà aziendali, di fornire benchmark e soluzioni alternative a fronte della medesima problematica, quello che mi aspetto è che si trasformino sempre più da venditori di tecnologie a consulenti a tutto tondo; in grado cioè di non proporre una soluzione standard ma di costruire insieme al cliente quella realmente indicata per rispondere alla sua esigenza, tenuto conto delle specificità e delle unicità dell'azienda che hanno di fronte.





EASYSHIELD DI HITACHI DALLA COMPLIANCE ALLA CYBER SECURITY

La sicurezza IT nella nuova offerta che unisce le competenze del team italiano con la knowledge base e i Managed Security Service dei SOC Hitachi Systems e le best practice di Above Security, acquisita lo scorso agosto

di Gaetano Di Blasio

«La sicurezza non dipende dalla tecnologia, ma dalla conoscenza», afferma Denis Cassinerio, Security BU & Sales North Italy Director di Hitachi Systems CBT, che aggiunge: «La sfida non consiste nell'aggiungere ulteriore tecnologia per aumentare il livello di controllo contro gli attacchi informatici, ma nella capacità di mettere a fattore comune le informazioni su come proteggersi, condividendole su scala mondiale, europea e locale».

Gli esperti della sicurezza l'hanno capito da tempo e le imprese ne sono sempre più convinte, mentre i governi sono, come spesso accade, in ritardo. Il problema, avverte Cassinerio, è che questo implica «la capacità di dialogare a livello di CERT nazionale con un protocollo comune di scambio di informazioni per comprendere lo stato d'evoluzione degli attacchi per fare fronte comune».

Per le aziende è diventata un'esigenza imprescindibile, ma non tutte sono strutturate per far fronte alla gestione della sicurezza internamente sul piano operativo e strategico, anche in termini di compliance. Una problematica che genera, secondo gli analisti di Gartner, un aumento del ricorso all'outsourcing sulla sicurezza.

«È una rivoluzione - afferma Cassinerio - che avrà sulle imprese lo stesso impatto che ha avuto sull'industria la macchina a vapore nel '700. Accompagnare le aziende in questo importante e articolato percorso di Security Risk

Management, permette alle imprese di rifocalizzarsi sul proprio core business, demandando così tutte le complessità tecnologiche, procedurali e di governance della sicurezza a partner specializzati e certificati come Hitachi».

Ma occorre un approccio corretto: «Oggi "sicurezza gestita" significa gestione del rischio», afferma Cassinerio in riferimento alla profonda conoscenza e capacità di analisi del team di specialisti di Hitachi Systems CBT.

Le migliori tecnologie sulla sicurezza

Nell'ambito della strategia di crescita in Italia e in Europa, Hitachi Systems CBT punta molto sulla Business Unit dedicata alla sicurezza, coerentemente con le priorità del gruppo che sta investendo in questa direzione. L'offerta EasyShield con il prefisso "Easy" sta a identificare i servizi che Hitachi ha predisposto per facilitare la gestione dell'ICT e della sicurezza per le aziende. «Lo scenario è noto: attacchi sempre più numerosi ed evoluti, fenomeni sempre più veloci e difficili da riconoscere. Occorrono competenze tecnologiche e di gestione. Le imprese sono messe sotto pressione su diversi fronti, dagli attacchi all'adeguamento normativo cui si aggiunge la nuova Regolamentazione EU in materia di privacy.

Affidarsi a un partner è la soluzione migliore per avere il meglio delle tecnologie e cedere la complessità IT concen-



Denis Cassinerio -
Hitachi Systems CBT



trandosi sul proprio core business. «Scegliere EasyShield vuol dire poter contare su un ampio spettro di soluzioni grazie anche ai Managed Security Service che permettono la cessione delle complessità tecnologiche a fronte di un elevato livello di protezione gestita. I clienti potranno così liberare risorse affidando a Hitachi la gestione delle attività di security analytics, per monitorare le minacce silenti già presenti in azienda, e di early warning per agire in modo preventivo», dichiara Cassinerio.

Sostanzialmente si tratta di un percorso strutturato verso la protezione del dato che avviene attraverso la gestione del ciclo di Security Risk Management, con un'adeguata realizzazione dei controlli di sicurezza, rispettando il principio di bilanciamento tra l'applicazione delle contromisure e la reale accettazione del rischio. Un approccio a 360 gradi che gestisce le esigenze di security, dalla compliance alla cyber security, ai servizi gestiti. Il panorama della sicurezza è ormai così articolato e complesso che non esiste un approccio unico e un servizio esaustivo capace di risolvere le minacce esterne. Per essere al sicuro è necessario dotarsi di strategie differenziate e flessibili.

Il know how di Hitachi Systems CBT è il risultato della potenzialità dei servizi di Above Security, attivo dal 1999 con SOC in Messico, Canada, Svizzera e a breve in USA, e dei SOC internazionali. Queste best practice internazionali sono preziose, non solo nella logica di information sharing, ma anche per la realizzazione del SOC italiano.

Inoltre, grazie alla piattaforma proprietaria Archangel di Above Security, i professionisti di sicurezza di Hitachi hanno un ulteriore accesso a tool, servizi e a capacità di response.

Oltre all'integrazione con i servizi e il supporto dei SOC internazionali di Hitachi Systems, la strategia mirata allo

sviluppo del business prevede un allargamento del portafoglio tecnologico attraverso delle partnership strategiche in ambito security.

L'obiettivo è aggiungere elementi di cyber security, dagli indicatori di compromissione attorno al perimetro dell'azienda all'erogazione di veri e propri piani di risposta agli incidenti e di threat prevention, veri e propri fattori differenzianti sul mercato. «Una velocità d'azione e copertura che possiamo garantire perché il nostro approccio alla sicurezza del dato parte dalla compliance e va a toccare aspetti relativi ai piani di gestione dell'informazione o ISMS o SGSI (Information Security Management System o Sistema di gestione della sicurezza Informatica). In questo modo supportiamo il cliente nella comprensione, adeguamento e implementazione del piano di gestione della sicurezza informatica nella sua continua evoluzione», spiega Cassinerio.

Le opportunità sono tante, soprattutto per il gran numero di medie imprese che hanno necessità di questo supporto. Aziende che hanno spesso sistemi di sicurezza maturi da ottimizzare e che possono ottenere notevoli vantaggi in un modello integrato con una collaborazione diretta con Hitachi Systems CBT, in particolare sul fronte SIEM (Security Information Event Management) con applicazione di SLA di intervento secondo esigenze diverse e un approccio tailor made. A ciò si aggiunge un'elevata esperienza e la capacità di erogare servizi in Cloud. In altre parole Hitachi Systems CBT si posiziona in un ruolo chiave per l'esperienza, le competenze e la conoscenza specifica della security che non può più essere relegata solo alla tecnologia, ma deve riguardare ambiti aziendali più ampi rientrando nelle priorità dei top manager di tutte le organizzazioni, conclude Cassinerio.

CYBER INTELLIGENCE: UN PASSO AVANTI ALLE MINACCE

I suggerimenti di Darktrace per anticipare le minacce e fare dell'Intelligence il punto centrale della propria cyber security

di Giuseppe Saccardi

Darktrace, una delle aziende più impegnate nell'ambito della Cyber Defense, ha fatto il punto sulle motivazioni per le quali è necessario attuare un cambio di prospettiva per quanto riguarda la cyber security. Il punto di partenza è che è ormai accettato che le violazioni della sicurezza, soprattutto in ambito aziendale, siano da considerare come 'inevitabili', e che il loro verificarsi sia più un discorso di 'quando' che di 'se'. Alla luce di questo cambiamento, l'approccio tradizionale basato su firme e regole che diventano obsolete dal momento che si riferiscono a minacce già individuate, mostra la sua inadeguatezza. Le aziende devono quindi essere proattive nei riguardi degli attacchi informatici, così come la 'Cyber Intelligence' deve guidare nel prendere decisioni quando le infiltrazioni sono nella loro fase iniziale e gestibile, in una finestra temporale che consenta di verificarne l'efficacia ed evitare che la situazione diventi critica.

Una considerazione, spiega Darktrace, va fatta proprio sul fattore tempo. Il tempo è una risorsa preziosa che manca spesso a chi viene attaccato. Le aziende lottano costantemente per rilevare le fasi iniziali di una infiltrazione, prima che vengano fatti danni quali il furto di dati su grande scala o l'interruzione di un servizio essenziale.

Invece le aziende si trovano coinvolte in una lotta contro il tempo per rimuovere e ridurre velocemente i danni finan-

ziari e d'immagine, al contrario dei mesi di preparazione e ricognizione che l'aggressore ha a disposizione prima di sferrare il suo attacco. Fintanto che il vantaggio rimane in mano all'aggressore le aziende attaccate saranno sempre sulla difensiva.

Ogni attacco inizia con una infiltrazione che a sua volta inizia con un cambiamento impercettibile nel normale ordine delle cose e s'ingrandisce fino a diventare una catena di eventi che messi insieme possono esercitare il controllo di un sistema remoto e metterne in pericolo i contenuti.

Occorre quindi iniziare a considerare il tempo in modo diverso, tentare di cogliere attività sospette nella finestra temporale compresa fra l'infiltrazione iniziale e i primi segnali di anomalia. All'interno dell'IT aziendale ci sono due fattori da tener presente:

Visibilità e comprensione: la visibilità su tutte le interazioni e comunicazioni digital è critica perché consente agli addetti della sicurezza di prendere le decisioni migliori basandosi sulla conoscenza dell'intero sistema. Avendo visibilità totale sull'andamento e il tipo di traffico gestito giornalmente nell'azienda, gli addetti della sicurezza sono in condizione di configurare al meglio la protezione della rete, identificare le vulnerabilità o i dipendenti infedeli e tenere effettivamente a freno in tempo reale le minacce informatiche.

Analisi intelligente e rilevamento anomalie: Avendo la conoscenza delle attività aziendali è possibile usare

nuove tecnologie per analizzarle ed avere una chiara visione di quale sia la normalità. I fondamentali progressi nella matematica probabilistica e nell'ambito del 'machine learning' hanno reso possibile questo approccio, usando una tecnologia che impara su base continua ciò che è normale e anomalo nell'ambito aziendale ed evidenzia anomalie su base probabilistica in tempo reale.

Le anomalie o le deviazioni da ciò che è stato identificato come normale sui sistemi, le reti e gli utenti devono essere autentiche e basate sulla comprensione dinamica dell'ambiente circostante. Un comportamento difforme spesso può essere affrontato in modo appropriato, ma solo se rilevato nelle sue fasi iniziali.

Cyber Intelligence' contro 'Threat Intelligence'

Una seconda considerazione fatta da Darktrace è terminologica. Il termine 'Threat Intelligence' viene usato per la raccolta e la condivisione di informazioni su minacce note. In altre parole si fa riferimento ad un database o insieme di dati da confrontare con gli allarmi di sicurezza rilevati in un'azienda, i log e altri dati forensici per capire se quanto rilevato è una minaccia oppure no.

Se quanto rilevato è riconducibile alle informazioni con-



tenute nella 'Threat intelligence' ciò può essere usato per proteggere l'azienda da attacchi simili

ancora in circolazione. Il difetto principale nel condividere informazioni riconducibili ad attacchi già avvenuti è che questo approccio 'a posteriori' non aiuta le aziende a difendersi dai nuovi attacchi di domani. Affinché questo funzioni è necessario che almeno un'azienda venga violata da ogni nuovo attacco per poterlo identificare, limitandosi a segnalare gli attacchi già subiti con la speranza che lo stesso si possa ripresentare.

Quindi la vera 'Cyber Intelligence' non è quella che identifica le minacce e i metodi di attacco già noti, ma si concentra sulla corretta comprensione di ciò che sta avvenendo in azienda con un livello di granularità tale da far emergere anche le azioni più subdole.

Per le aziende che vogliono essere proattive nei riguardi degli attacchi informatici queste domande, suggerisce Darktrace, sono critiche e richiedono azioni d'intelligence di elevata qualità e i riscontri di un'analisi avanzata e sensibile al contesto di un ampio spettro di fattori che contribuiscono all'eventuale attacco.

La 'Cyber Intelligence' deve guidare nel prendere decisioni quando le infiltrazioni sono nella loro fase iniziale e gestibile, in una finestra temporale che consenta di verificarne l'efficacia ed evitare che la situazione diventi critica.

PER ESSERE EFFICACE LA SICUREZZA VA CONTESTUALIZZATA

Analizzare il contesto è il cardine della sicurezza app-centrica. Il perché lo spiega Gad Elkin di F5

di Giuseppe Saccardi



Gad Elkin - F5 Networks

Una soluzione di sicurezza presa a sé stante può risultare non efficace. Quello che rappresenta il cardine della sicurezza, secondo Gad Elkin, Security Sales Director di F5 Networks per l'area EMEA, è la sua contestualizzazione. Vediamone assieme a Elkin i motivi.

Nonostante i tanti casi clamorosi raccontati dai media nel corso degli ultimi anni, osserva il manager di F5, le violazioni dei dati hanno dominato ancora una volta lo scenario della sicurezza nel 2015. Le aziende mobile, le catene alberghiere, gli enti federali e governativi, i rivenditori online e molte altre tipologie di aziende sono state prese di mira nel corso dell'ultimo anno. Nomi, indirizzi email, indirizzi fisici, informazioni sulle carte di credito, password, numeri di previdenza sociale, quasi tutte le informazioni personali, identificabili e sensibili, a cui riusciamo a pensare sono cadute almeno una volta nelle mani degli hacker.

Al di là dell'impatto economico immediato per le aziende colpite, ad esempio i costi da sostenere per far fronte ai vari rimborsi, questi attacchi possono avere anche ripercussioni pesanti sull'immagine dell'azienda; quante persone continueranno ad accordare la propria fiducia a un'azienda pur sapendo che potrebbe non essere in grado di proteggere adeguatamente i loro dati?

Ma quali sono i motivi per cui questi attacchi sono sempre più diffusi e hanno più successo? Si tratta, osserva

Elkin, di un riflesso della trasformazione del modo in cui le aziende oggi operano.

Attacco all'applicazione

Gli obiettivi principali degli attacchi oggi sono però le applicazioni stesse, perché è lì che sono ospitati i dati. In pratica, le applicazioni opererebbero come un gateway per i dati e sarebbero la porta che permette agli hacker di entrare. Altri fattori però si impongono. Le aziende sono sempre più mobile e cloud-based, per questo motivo le applicazioni contengono una quantità di dati crescente, cosa che le rende un bersaglio sempre più interessante per gli attacchi informatici. Dalla ricerca The State of Application Delivery 2016 è emerso ad esempio che il 39% delle aziende italiane utilizza più di 200 applicazioni ogni giorno e il 56% degli intervistati ritiene che le applicazioni mobile rappresenteranno il focus della spesa IT del 2016. Applicazioni che, inoltre, fino ad oggi risiedevano nel data center, il perimetro dove era necessario istituire le principali difese dal cyber crime. Oggi però, a causa della crescita del mobile e della comparsa del cloud, nella maggior parte dei casi, il data center non rappresenta l'elemento più vulnerabile. Ma cosa fare secondo F5 per proteggersi? Un approccio valido è pensare alla sicurezza a partire da quattro considerazioni:

Le organizzazioni si spostano sempre più verso il cloud

Cresce il BYOD e la percentuale di lavoratori che opera da remoto/mobile. Prevalgono il SSL, e di conseguenza molte applicazioni di sicurezza non hanno visibilità sul traffico crittografato e sulle minacce che si nascondono all'interno.

Gli attacchi sono sempre più sofisticati.

Tutti questi aspetti, e il quarto in particolare, rendono palese come l'approccio perimetrale non sia più adeguato. Oggi, il perimetro deve essere l'applicazione stessa, ovunque essa si trovi. È quasi come se la sicurezza dovesse tornare indietro ai principi della sua progettazione e abbracciarne uno che rappresenti una base solida in grado di aiutare le aziende a combattere anche le minacce più avanzate.

Attenti al contesto

La chiave, ritiene Elkin, è quindi una sicurezza app-centrica e il segreto perché questa abbia successo è il contesto, inteso come contesto dell'utente, del traffico e dell'applicazione.

Ma perché il contesto sarebbe rilevante per un'organizzazione? Ebbene, il contesto relativo all'utente, al traffico di dati e all'applicazione - come da quale piattaforma client viene effettuata la connessione, la collocazione geogra-

fica, la tipologia di browser utilizzata, il protocollo, l'applicazione a cui si accede - consente all'organizzazione di vedere con completezza tutto ciò che accade tra l'utente e l'applicazione. In sostanza, se un'organizzazione capisce quello che sta avvenendo sulla sua strada, avrà la capacità di prendere la decisione giusta e agire di conseguenza. Per proteggere un'applicazione bisogna necessariamente comprenderla, e questo è possibile solo attraverso la consapevolezza contestuale.

Focalizzare il proprio impegno sulla sicurezza delle applicazioni è un modo efficace, rimarca Elkin, di fermare le minacce e potrebbe rivelarsi anche più conveniente, perché permette di assegnare la protezione basandosi sul valore che l'applicazione ha per l'azienda, invece di cercare di proteggere tutto allo stesso modo. Proteggere l'applicazione, ovunque essa risieda, significherà garantire la sicurezza del business nel suo complesso.



DA CLOUD E IOT I PRINCIPALI TIMORI PER LA SICUREZZA

Partner Data e CoSoSys illustrano i timori delle aziende per la sicurezza dei dati nel 2016. Preoccupazioni per cloud, Wearable e Internet of Things

di Giuseppe Saccardi

Partner Data, società specializzata nella sicurezza IT, protezione del software, sistemi di identificazione e programmi di fidelizzazione, e CoSoSys, con cui Partner Data ha siglato un accordo di collaborazione a gennaio 2015, hanno evidenziato i maggiori timori delle aziende relativamente alla sicurezza dei dati nel 2016.

Secondo una ricerca condotta da CoSoSys, una delle maggiori preoccupazioni è costituita dal cloud, il cui mercato è peraltro in forte crescita e si ritiene crescerà dai 18.87 miliardi di dollari del 2015 ai 65.41 miliardi nel 2020.

I timori nella nuvola

Le statistiche relative a servizi cloud mostrano che queste aree costituiscono le maggiori preoccupazioni per la sicurezza dei dati aziendali. Infatti, oggi più che mai, App e dispositivi interconnessi sono parte integrante della vita quotidiana e i dati scambiati tra dispositivi e computer aziendali rendono le aziende sempre più vulnerabili.

Anche Servizi cloud come il file sharing e i social media sono tra i maggiori timori per molte organizzazioni a causa della rapida diffusione delle pratiche di carico/scarico di file tra collaboratori. Il più delle volte queste pratiche non sono autorizzate dall'IT aziendale che pe-

raltro, tramite una valida soluzione DLP (Data Loss Prevention), può limitare il trasferimento di dati solo verso indirizzi web affidati ed affidabili.

Lo Shadow IT, ovvero l'utilizzo di applicazioni e dispositivi non autorizzati dall'IT aziendale, preoccupa il 71% dei manager della sicurezza per il fatto che servizi non controllati possono causare seri problemi. Si calcola che il 72% degli impiegati utilizza servizi di file sharing non autorizzati dall'IT aziendale mentre il 7% delle aziende che non utilizza il Cloud è consapevole che lo Shadow IT si serve del Cloud al proprio interno.

La ricerca ha rilevato anche che un'altra grande preoccupazione è costituita dai wearable (oggetti indossabili interconnessi come gli smartwatch). Negli USA una persona su 5 possiede un wearable e nel 2019 si prevede la vendita di 148 milioni di unità.

Attenti al wearable

Uno studio condotto da PCW rivela che negli USA 860 utenti su 1.000 pensano che la tecnologia dei wearable li esponga alla violazione di dati, poiché le loro più intime informazioni (le ore di sonno, la frequenza dei battiti del cuore, le calorie consumate e i dati di business) vengono registrate e non è chiaro che fine facciano.

I produttori di wearable non hanno come priorità nel-

Shadow IT



Definizione di Gartner: Shadow IT si riferisce a dispositivi IT, applicazioni e servizi fuori dal controllo della organizzazione IT



dei responsabili della sicurezza IT sono in qualche modo preoccupati dello Shadow IT



delle aziende che bloccano l'uso del cloud sanno che app Shadow IT utilizzano al loro interno il cloud

lo sviluppo dei loro prodotti le funzioni di sicurezza ma si focalizzano sugli aspetti innovativi. I timori sulla sicurezza dei dati aumentano in quanto è facile accedere ai dati da dispositivi wereable persi o rubati poiché i dati non sono cifrati, protetti da PIN o da altri metodi di autenticazione.

Un rischio dall'IoT

L' Internet of Things (IoT), ovvero l'Internet applicato agli oggetti tramite etichette RFID, codici QR o altro, ha sicuramente segnato una svolta fondamentale in quest'epoca ma costituisce anche uno dei maggiori rischi per la sicurezza dei dati, specialmente se coinvolge grandi strutture come intere città. Il numero di dispositivi connessi a Internet cresce rapidamente e si pensa possa raggiungere i 50 miliardi nel 2020.

In caso di incidenti sulla sicurezza il disastro che può verificarsi ad esempio su una città basata su un sistema interconnesso può essere di proporzioni davvero enormi. Per strutture più piccole, come case d'abitazione o automobili, le vulnerabilità della sicurezza dei dati possono invece costituire una minaccia alla vita stessa. Vien da considerare che i timori sono quindi più che legittimi, sia come manager IT che cittadini.

Top Data Security Concerns for 2016+

Powered by EndpointProtector.com



Servizi Cloud



Il mercato del cloud si ritiene crescerà da 18.87 miliardi di USDS nel 2015 a 55.41 nel 2020



Più del 40% delle aziende utilizza Dropbox

Seguono, in quest'ordine: Microsoft One Drive, Google Drive, Box e Citrix ShareFile



di colletti bianchi utilizza servizi di file sharing non autorizzati



DE gustare

alla scoperta dei sapori d'Italia



NOTIZIE
ROAD TO DUBAI, LE ECCELLENZE ITALIANE SI PRESENTANO

**giornalisti,
enologi,
chef,
nutrizionisti,
esperti alimentari
vi promettono
un'esperienza
nuova**

01 GIUGNO 2015

La Toscana di Biella

Agricoltura biodinamica

Asparago in cucina



NOTIZIE
OLIO, FIRMATO PROTOCOLLO PER VALORIZZARLO



NOTIZIE
SARCHIO, SFOGLIETTE BIO PER TUTTI I GUSTI



NOTIZIE
DIETA MEDITER PREMIO GRUPPO



DE gustare
alla scoperta dei sapori d'Italia



Alla corte del RE

www.de-gustare.it

NUOVE REGOLE SULLA PRIVACY: COSA CAMBIERÀ CON IL GDPR

di Gian Carlo Lanzetti

Più responsabilità, anche penali, nuove restrizioni e un'uniformità a livello europeo solo al 70%. Un'ampia esame dei cambiamenti con Paola Generali di GetSolution

Le ultime indicazioni confermano che entro luglio dovrebbe essere pubblicato il nuovo regolamento europeo sulla Privacy, dopodiché i Paesi interessati avranno due anni di tempo per adeguarsi alla nuova normativa. In previsione di questi cambiamenti abbiamo intervistato un'esperta in materia, Paola Generali, managing director di GetSolution, per farci anticipare le novità. GetSolution è una società che dal 2003 si occupa di Privacy Law e di Sicurezza dei Sistemi Informativi, svolgendo progetti molto complessi presso clienti di medie e grandi dimensioni, sia italiani che internazionali. Ha maturato in particolare una specifica esperienza occupandosi di tematiche complesse quali big data, profilazione, anonimizzazione, pseudonimizzazione, dati aggregati, dati biometrici, dati genetici, trattamento di dati particolari su larga scala (gli attuali dati sensibili).

Quali sono, a suo avviso, i cambiamenti più importanti che il GDPR (General Data Protection Regulation) introdurrà in materia?

Senza dubbio i cambiamenti più rilevanti sono:

1. Le rilevanti responsabilità che ha l'incaricato del trattamento (quello che oggi è chiamato "responsabile del trattamento") rispetto a quelle attuali.
2. La possibilità da parte dell'incaricato del trattamento di subappaltare attività a un fornitore solamente a

seguito dell'ottenimento dell'autorizzazione da parte del Responsabile del Trattamento (quello che oggi è chiamato il Titolare del Trattamento).

3. La valutazione d'impatto (analisi dei rischi) come base sulla quale costruire la sicurezza delle informazioni attraverso l'implementazione di contromisure di sicurezza tecnologiche, procedurali e fisiche, è richiesta in particolare in particolare:

- Nel caso di una valutazione sistematica e globale di aspetti personali relativi a persone fisiche, basata sul trattamento automatizzato, compresa la profilazione, e da cui discendono decisioni che hanno effetti giuridici o incidono allo stesso modo significativamente su dette persone fisiche.
- Nel trattamento, sul larga scala, di categorie particolari di dati o di dati relativi a condanne penali e a reati di cui all'articolo 9 bis.
- Nel caso di sorveglianza sistematica di una zona accessibile al pubblico su larga scala.

La precisazione "in particolare" riportata nel comma 2 dell'articolo n. 33 non vuol dire che è obbligatoria solo nei 3 suddetti casi.

Ciò vuol dire che è obbligatoria per tutti anche perché nell'art. 30 che parla della Sicurezza del Trattamento, il



Paola Generali - GetSolution

Responsabile del Trattamento come anche l'incaricato del trattamento, devono mettere in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio.

Per fare questo l'unica soluzione è l'analisi dei rischi che permette di definire le adeguate contromisure di sicurezza tecniche e organizzative al fine di garantire la sicurezza del trattamento.

4. Le procedure di Data Breach da implementare in modo efficace ed efficiente, in quanto non solo è necessario notificare la violazione dei dati personali all'autorità di controllo competente, ma nel caso in cui la violazione presenti un rischio elevato per i diritti e le libertà delle persone fisiche, il responsabile del trattamento (quello che oggi è il Titolare) deve comunicare tale violazione all'interessato.

5. La possibilità da parte dell'interessato di chiedere al Responsabile del Trattamento e/o all'incaricato del Trattamento il risarcimento sia dei danni materiali che di quelli immateriali.

6. Il concetto di "By Default" e "By Design" sono nuovi a livello di formalizzazione, mentre mi permetto di dire che non sono nuovi come concetti "applicati o da applicare" anche se espressi diversamente nella normativa attuale. Quello che invece reputo molto interessante sottolineare sono due concetti che scaturiscono da questi due principi come anche ribaditi dall'art 30:

- La pseudonimizzazione
- L'anonimizzazione

Che sono due modalità che all'interno del Regolamento Generale vengono ribadite continuamente come strumenti fondamentali da utilizzare per garantire la sicurezza delle informazioni.

7. Le sanzioni di carattere amministrativo, ma non per gli elevatissimi importi dai 10.000.000 ai 20.000.000 euro e per le imprese sino al 4% del fatturato mondiale, che seppur rappresentando un'importante novità a mio avviso non è quella più significativa.

Ciò che rappresenta un cambiamento sostanziale e importantissimo sono le casistiche nelle quali sono applicate queste sanzioni, è veramente semplice incorrere in una di queste sanzioni.

8. Data Protection Officer vale a dire il Responsabile della protezione dei dati, è sicuramente una novità, tale figura corrisponde al "Privacy Officer" attuale con delle responsabilità certamente maggiori.

Inoltre indipendentemente dai casi in cui è obbligatorio avere il DPO, tenuto conto delle implicazioni riportate nei punti precedenti, ritengo che ogni azienda debba comunque valutare con molta attenzione se avvalersi di un DPO o meno in quanto l'applicazione del Regolamento Generale è complessa e la probabilità di incorrere in sanzioni è molto alta.

Ci sono due anni di tempo: cosa suggerisce alle aziende di fare nei due anni che intercorreranno dalla pubblicazione del Regolamento Generale sulla Data Protection alle prime verifiche che potranno essere svolte dalle autorità di controllo?

Le aziende avranno 2 anni dalla pubblicazione del Regolamento Generale sulla protezione dei dati personali per implementare tutti gli adempimenti previsti dal medesimo.

Quello che suggerisco di fare alle aziende sono 5 cose:
1. Innanzi tutto dopo la pubblicazione del Regolamen-

to Generale sulla Gazzetta Ufficiale dell'Unione Europea attendere 1 o 2 mesi prima di addentrarsi nell'implementazione in azienda del Regolamento, in



quanto ogni Autorità di controllo di ogni Stato Membro dovrà dare specifiche indicazioni in merito all'approccio da adottare relativamente all'implementazione degli adempimenti. Per cui verranno rilasciate delle linee guida da parte dell'Autorità di Controllo Italiana, come anche chiarimenti e delucidazioni. (Garante Privacy Italiano).

2. Ricercare una società di consulenza esperta e competente in ambito "Privacy" che possa seguire l'azienda nel percorso di passaggio al nuovo Regolamento che definirei "tortuoso", in quanto in questi due anni "di transizione" accadranno molte cose che dovranno essere seguite e gestite da consulenti molto esperti, quali per esempio:

- Il Garante della Privacy Italiano emanerà frequentemente e in modo continuativo Provvedimenti, Linee Guida, Chiarimenti, Modifiche di articoli del Regolamento in quanto previsto dal Regolamento stesso.
- Lo Stato Italiano dovrà legiferare su tutti gli aspetti di sua competenza, come per esempio le sanzioni di carattere penale per esempio.
- La Commissione Europea anch'essa potrà definire Linee Guida, Provvedimenti, Introdurre novità, integrazioni ecc..
- Verranno redatti singoli Codici di Condotta destinati

a specifiche tipologie di Responsabili e incaricati del Trattamento.

- Verranno identificati i soggetti che potranno certificare le aziende, attestando

il loro completo e corretto adempimento al Regolamento Generale e ovviamente anche la relativa norma certificativa.

Per cui è assolutamente necessario, anzi direi indispensabile per un'azienda individuare un fornitore di riferimento che possa sostenere l'azienda sia nell'implementazione del Regolamento ma anche seguirla e quindi guidarla in un panorama sia nazionale che internazionale ricco di contenuti in costante evoluzione.

3. Per l'implementazione degli adempimenti previsti dal Regolamento Generale partire "dal cuore" del medesimo: la valutazione d'impatto /analisi dei rischi:

- Nell'analisi dei rischi devono essere mappate in dettaglio tutte le categorie di dati personali che l'azienda tratta identificando finalità e modalità.
- Successivamente valuto la probabilità e i relativi impatti che potrebbero causare la perdita di riservatezza, disponibilità, integrità dei dati personali sia a livello aziendale ma anche nei confronti degli interessati.
- Calcolo il livello di rischio per i dati personali che ovviamente categorizzo, e definisco tutte le contromisure tecniche, organizzative e fisiche da implementare, come anche:
 - a. La necessità per l'azienda di avere un DPO,

anche se non strettamente obbligatorio

b. in base a quali criteri devo scegliere i fornitori, e cosa richiedere ai medesimi come contromisure di sicurezza, SLA, oltrenaturalmente al fatto che debbano essere adempienti al Regolamento Generale.

4. Le cose a mio parere da non fare:

- produrre centinaia di pagine di documentazione ridondante e inutile,
- scrivere “procedure complesse e impossibili da applicare”,
- prefissarsi obiettivi di sicurezza impossibili da raggiungere,
- blindare in modo indistinto l’azienda nel trattamento dei dati personali pensando così di garantire la sicurezza dei dati come anche l’adempimento al Regolamento Generale.

Tutto deve essere fatto in modo ponderato e soprattutto volto al raggiungimento della

massima efficacia ed efficienza per l’azienda nell’implementazione del Regolamento.

Teniamo inoltre in considerazione che davanti all’Autorità di Controllo oppure all’Autorità Giudiziaria l’azienda sia essa Responsabile del Trattamento che Incaricata del trattamento deve dimostrare, quindi presentare prove concrete che dimostrino che l’azienda è adempiente. Questo vuol dire per esempio scrivere poche procedure ma scritte bene e soprattutto efficaci, assicurandosi naturalmente che le medesime siano spiegate a chi le dovrà applicare e monitorata la loro applicazione.

Un’analisi dei rischi macchinosa che produce un “documento di 150 pagine” che nessun comprende piena-

mente, non comprova necessariamente che l’azienda ha implementato le adeguate contromisure di sicurezza. In quanto l’equazione tante pagine = ottima analisi dei rischi non è vera in assoluto.

5. L’azienda deve mantenere costantemente nel tempo la compliance al Regolamento Generale, e non sarà possibile implementarlo e poi dimenticarsene per qualche anno per poi riprendere “in mano” le cose, il cosiddetto mantenimento a elastico.

Il Regolamento è stato scritto anche in virtù di spingere le aziende a considerare il processo relativo alla gestione dei dati personali come un “di cui fondamentale” dell’azienda stessa e quindi gestito, migliorato, modificato costantemente nel tempo.

A suo avviso le aziende faticeranno a uniformarsi alla nuova disciplina e ritiene avranno realmente bisogno al loro interno di una figura dedicata alla Privacy?

A mio avviso, più che altro, ci sarà molta confusione, che molto probabilmente verrà in parte anche sollevata volontariamente da una parte del mercato dell’offerta.

Le argomentazioni su cui verrà fatta confusione saranno purtroppo tantissime e non riguarderanno solamente come implementare il Regolamento Generale, ma per esempio le Certificazioni previste dal Regolamento che potranno ottenere le aziende per dimostrare di essere adempienti al Regolamento Generale, delle quali tutto deve essere ancora deciso e definito.

Per cui sicuramente le aziende avranno delle rilevanti difficoltà a capire cosa fare, quando farlo, chi ascoltare

e di chi fidarsi.

Una figura dedicata alla privacy in moltissime realtà aziendali sarà indispensabile, proprio per progettare, creare e mantenere un percorso di adempimento al Regolamento efficace ed efficiente, che quindi si basi:

- Sulla valutazione attenta degli investimenti necessari
- Sull'evitare perdite di tempo.
- Sull'evitare duplicazioni.
- Sull'evitare di sbagliare a dare delle responsabilità a soggetti che non ne hanno le competenze.
- Sul raggiungimento di obiettivi di Efficacia ed Efficienza chiaramente definiti.

Le aziende dovranno, con tutte le loro forze, non farsi inghiottire da macchinismi offuscanti o da "canti delle sirene" ma dovranno ricercare, con un pò di fatica, di non fermarsi alle apparenze ma entrare in modo approfondito nel merito oggettivo delle cose.

Infine ritiene la nuova regolamentazione significativamente migliorativa rispetto alla precedente?

Il Nuovo Regolamento Generale è senza dubbio migliorativo rispetto al precedente, perché frutto anche dell'esperienza dell'applicazione dei singoli decreti le-



gislativi in ambito Privacy in essere ormai da anni nei singoli Paesi degli Stati Membri dell'Unione.

Ciò che però mi rammarica molto, è che l'obiettivo primario di uniformare la norma e di renderla uguale per tutti i Paesi appartenenti all'Unione Europea è stato raggiunto per il 70%, poiché il Regolamento stesso dà ampio margine di modifica del medesimo a ogni

singolo Stato Membro, anche su aspetti fondamentali.

In realtà non mi stupisce quanto suddetto, poiché è dal 2012 che sto seguendo l'iter internazionale politico/normativo relativamente alla stesura e approvazioni delle bozze del Regolamento Generale, e le discussioni a livello internazionale sono sempre state molto accese, in quanto le realtà aziendali come anche l'economia dei Paesi Europei sono molto diverse tra loro, e inoltre dobbiamo tenere in considerazione che del Gruppo di lavoro fanno parte anche gli Stati Uniti, che sono lì a rappresentare gli interessi delle loro Grandi Major, che sono trainanti sia per il loro mercato che per il mercato mondiale. Questo naturalmente andrà ad aggiungere ulteriore entropia nel trattamento dei dati personali all'interno dell'Unione Europea in quanto le aziende che operano in un contesto internazionale europeo dovranno comunque fare "i conti" con le differenze dell'Europa che saranno riflesse anche nel Regolamento Generale.

PC PIÙ SICURI CON LA VERIFICA DEL BIOS

Dell migliora la sicurezza del PC con la verifica BIOS e la tecnologia Advanced Threat Protection

di Giuseppe Saccardi

Dell ha annunciato la disponibilità della soluzione Endpoint Security Suite Enterprise. Il prodotto integra la tecnologia Cylance con l'uso dell'intelligenza artificiale e del machine learning per prevenire in modo attivo le minacce avanzate e il malware.

Inclusa nella soluzione, Dell ha inoltre annunciato la disponibilità di una funzione per la verifica post-boot del BIOS, che consente di mettere in sicurezza i propri dispositivi dagli attacchi di malware durante il processo di avvio. La soluzione sarà inserita nei PC Dell con l'acquisto della licenza Dell Data Protection | Endpoint Security Suite Enterprise.

In particolare, la nuova funzionalità di verifica del BIOS utilizza un ambiente Cloud sicuro per paragonare e verificare le singole immagini BIOS con i dati ufficiali presenti nel Dell BIOS lab. Poiché il test avviene in un ambiente esterno, in una piattaforma Cloud sicura, gli utenti, evidenzia la società, hanno la sicurezza che l'immagine post-boot non sia compromessa.

La verifica aiuta a estendere la sicurezza all'intero ciclo di vita del dispositivo e consente agli amministratori di avere una maggiore visibilità delle potenziali minacce. "La complessità sempre crescente degli attacchi ai BIOS, con nuove varianti di malware che si reinstallano nei BIOS stessi, porta alla necessità di sistemi di sicurezza sempre più sofisticati. L'esclusiva verifica

post-boot dei BIOS presenti nei PC commerciali Dell dà all'IT la sicurezza che i sistemi degli utenti siano costantemente protetti", ha commentato Brett Hansen, Executive Director, Data Security Solutions di Dell.

Disponibile da subito sui pc con chipset Intel

La funzione di verifica del BIOS sarà inizialmente disponibile sui PC Dell con chipset Intel di sesta generazione, tra cui il portfolio di PC Latitude recentemente annunciati al CES, e una selezione di PC Dell Precision, OptiPlex e XPS e tablet Dell Venue Pro. Grazie alla funzione, Dell rafforza la sicurezza dei propri PC aggiungendo la verifica BIOS alle funzioni di cifratura, autenticazione e protezione contro il malware.

La Dell Data Protection | Endpoint Security Enterprise è anche una suite di sicurezzache integra la tecnologia Cylance che utilizza l'intelligenza artificiale per proteggere i PC dalle minacce avanzate e dai malware, compresi gli attacchi zero-day e attacchi mirati quali il phishing e il ransomware.

Secondo i test di Cylance, riporta Dell, la soluzione offre un livello di protezione significativamente superiore, bloccando il 99% dei malware e delle minacce persistenti avanzate, con un'efficacia di gran lunga maggiore rispetto al 50% tipico delle soluzioni antivirus tradizionali.



Della suite Dell ha evidenziato i seguenti punti salienti:

- Nessuna firma: la tecnologia di protezione contro le minacce è basata sull'intelligenza artificiale e su modelli dinamici e matematici con un numero minimo di falsi positivi, che elimina la necessità di aggiornare costantemente le firme.
- Gestione e conformità consolidate: Endpoint Security Suite Enterprise minimizza i tempi di gestione della sicurezza degli endpoint, consentendo alle aziende di gestire tutti i componenti da remoto utilizzando una singola console che comprende report consolidati di status e di conformità. È inoltre conforme con gli standard PCI DSS, HIPAA HITECH e Microsoft per le solu-

zioni antivirus e anti-malware.

- Prevenzione attiva: la prevenzione del malware riduce notevolmente i costi di ripristino e i tempi di fermo macchina associati alla pulizia dei drive, creando una nuova immagine dell'hard disk e reinstallando il sistema operativo e i software applicativi.
- Maggiori prestazioni e sicurezza: Endpoint Security Suite Enterprise utilizza una minima parte delle risorse del Sistema, incluse la CPU e la memoria, normalmente associate all'uso degli antivirus e anti-malware tradizionali. Il rilevamento in locale senza la necessità di una connessione costante al cloud assicura che gli utenti mobili possano lavorare dove e come vogliono senza preoccupazioni.

COME AUMENTARE LA SICUREZZA DEGLI ENDPOINT

Intel Security ha reso più sicuri smartphone e notebook con un approccio volto a migliorare la protezione e ridurre i costi e l'impegno del personale IT

di Giuseppe Saccardi

Il problema della sicurezza degli endpoint, in una fase evolutiva dell'informatica aziendale e dei processi di business in cui dilagano sempre più dispositivi mobili, si diffonde lo smart working e un dipendente quando è fuori dall'ufficio ha non raramente con sé smartphone, tablet e notebook, costituisce uno dei problemi più seri per il reparto IT.

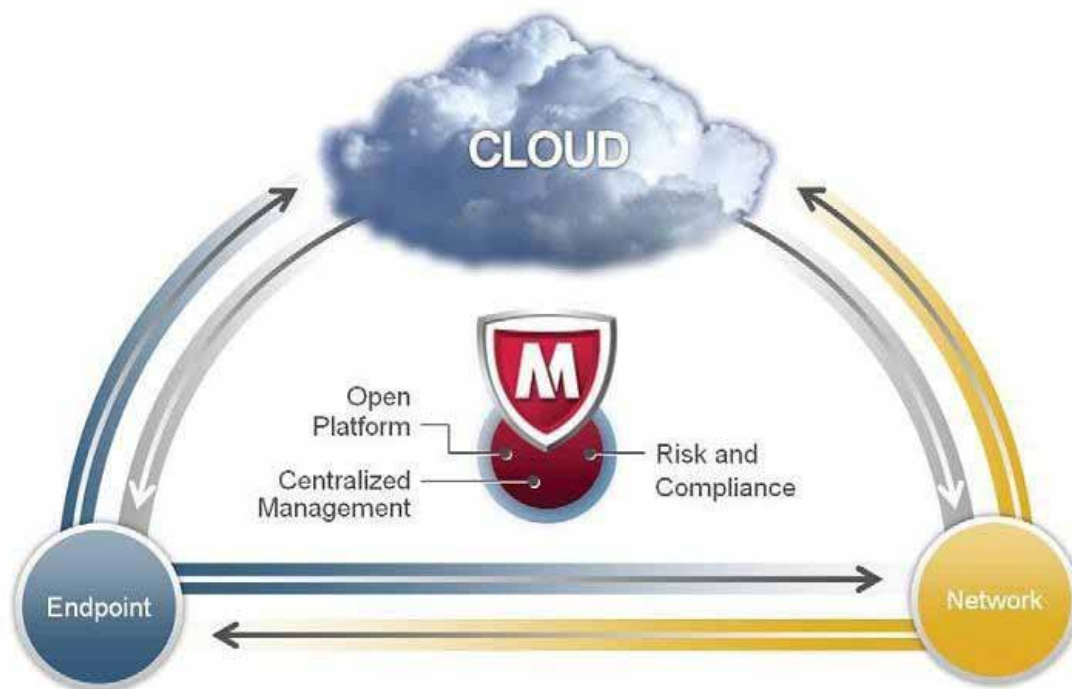
La protezione dei dati, delle comunicazioni, delle informazioni sensibili è non solo una necessità aziendale imprescindibile ma anche un preciso obbligo di legge in quanto tale ineludibile. Il problema è come affrontare tutto ciò senza appesantire i processi di business e in modo più trasparente possibile per l'utilizzatore dell'endpoint, che deve attenersi a modelli comportamentali precisi ma deve essere sgravato da problemi tecnici inerenti la gestione del rischio, delle minacce e quanto a questo correlato.

In sostanza, l'utilizzatore dell'endpoint, smartphone o tablet che sia, deve essere libero di fare il proprio mestiere, trattare i propri dati, trasmetterli e riceverli, accedere alle applicazioni business, eccetera, mentre è il reparto IT aziendale che deve garantirgli la sicurezza del contesto applicativo in cui opera.

Per molti sembra ieri ma sono passati ormai trent'anni da quando il personal computer ha iniziato ad essere di uso comune e ha trasformato il modo di lavorare e

lo stesso stile di vita. In successione sempre più rapida sono poi arrivati Internet, la banda larga, i telefoni cellulari e il cloud. Lavorare è diventato sempre più produttivo e la tecnologia ha dato indubbiamente un profondo contributo nell'aumentare l'efficienza aziendale. Ma come in tutte le medaglie il rovescio è costituito dalle crescenti minacce apportate alle informazioni e agli stessi sistemi, minacce in grado di carpire, alterare, usare fraudolentemente i dati riservati di un'azienda e causare danni economici e di immagine potenzialmente enormi. Quello a cui si assiste è una continua rincorsa tra nuove minacce e sistemi per bloccarle individuandole il prima possibile, e cioè prima che da minaccia potenziale si trasformino in danni reali a cui può essere difficile porre rimedio prima di aver subito significativi danni economici.

Nel corso del tempo, osserva ad esempio Intel, società che della sicurezza ha fatto uno degli aspetti salienti della propria vision tecnologica, non solo sono state migliorate e perfezionate soluzioni volte a contrastare i rischi, ma sono diventate anche facili da usare e hanno semplificato il compito di gestire le risorse di sicurezza di un'impresa. Ma più le aziende si digitalizzano, più diventa essenziale una gestione centralizzata, che però non deve andare a scapito della produttività come accade in strutture fortemente gerarchiche.



Orchestrare le policy e rendere sicuro l'endpoint

La chiave per gestire la sicurezza si basa per Intel su due elementi chiave, un efficiente orchestrator e la sicurezza dell'endpoint, due elementi che ha declinato nelle soluzioni, McAfee ePolicy Orchestrator (ePO) e Endpoint Security 10.1 (ENS 10.1), il cui obiettivo è di ridurre la complessità degli ambienti di sicurezza endpoint, migliorare le prestazioni e la visibilità sulle minacce avanzate e velocizzare le attività di rilevamento e bonifica. In essenza, le due soluzioni hanno tra gli obiettivi primari di certo quello di contrastare gli attacchi ma di farlo nel minor tempo possibile e soprattutto impegnando il minimo di risorse umane.

In questa ottica e vision di Intel, ePO rappresenta un unico punto di gestione che permette di consolidare le informazioni di sicurezza particolareggiate in arrivo da endpoint, dati, reti e più di 130 soluzioni di sicurezza di terze parti. La console centralizzata è poi il mezzo, evidenzia Intel, per ridurre drasticamente il tempo necessario per gestire le attività di security. Con ePO si può anche optare per una soluzione tradizionale di gestione in locale o per una basata su cloud.

La versione cloud è un approccio oramai ampiamente riconosciuto per semplificare la routine dei responsabili della sicurezza perché permette di disporre di aggiornamenti automatici della versione in uso e per far fronte alle mutevoli esigenze del proprio ambiente di sicurezza.

Per quanto concerne la sicurezza dell'endpoint, ha evidenziato Intel, la soluzione ENS 10.1 permette alle aziende di rispondere velocemente alle nuove minacce e di farlo con meno risorse. Si configura poi come un framework collaborativo per la protezione il cui obiettivo è di semplificare e rimuovere la complessità degli ambienti endpoint e consentire una maggiore visibilità sulle minacce avanzate oltre ad accelerare le attività di risposta, rilevamento e bonifica.

Sono dinamiche di collaborazione che ai fini pratici consentono di condividere le informazioni nei vari ambiti di prevenzione delle minacce, sicurezza web, firewall e moduli di intelligence delle minacce, cosa che si traduce in difese più intelligenti che cooperano al fine di migliorare il rilevamento e la risposta alle minacce avanzate.

PMI NEL MIRINO DEI CYBER CRIMINALI: LE NUOVE SOLUZIONI DI CHECK POINT

Analizziamo con David Gubiani i rischi corsi dalle Pmi e le caratteristiche delle nuove soluzioni lanciate con la linea 700

di Gaetano Di Blasio



David Gubiani - Check Point

Secondo un recente report di Check Point Software Technologies i danni economici derivanti da incidenti di sicurezza nelle piccole e medie imprese (Pmi) hanno superato i 100mila dollari l'anno. Un'altra indagine di mercato ha sottolineato che una piccola impresa su cinque è rimasta vittima del cybercrime.

Sono dati globali, ma in Italia? Lo chiediamo a David Gubiani, Security Engineering Manager di Check Point Italia, che pur non avendo «uno spaccato per paese che si possa considerare ufficiale», ci svela: «Dai dati che raccogliamo noi in Italia, presso i nostri clienti, ci rendiamo conto che le proporzioni sono pressoché identiche».

David aggiunge: «Le Pmi sono un target ideale per il cybercrime, in quanto il livello di sicurezza e la disponibilità di personale qualificato è sicuramente meno elevato delle imprese più grandi. Questo comporta un'esposizione al rischio maggiore e, di conseguenza, le Pmi tendono a essere le prime vittime di attacchi, spesso generici e condotti su larga scala».

Proprio per aiutare le piccole e medie imprese a colmare il divario tra l'entità degli attacchi cui sono sottoposte e le risorse per la protezione a loro disposizione, in Check Point Software Technologies hanno progettato le soluzioni della nuova linea 700.

Si tratta di un'evoluzione della linea 600, ma è solo l'ul-

tima delle appliance destinate alle Pmi. Abbiamo quindi chiesto a David di illustrarcene le caratteristiche, cercando di capire quali siano le novità più importanti e se ci siano caratteristiche espressamente sviluppate pensando alle piccole e medie imprese europee, facendo affidamento sul fatto che Check Point, pur essendo una delle più importanti aziende mondiali dedicate alla information security, nasce israeliana.

Partiamo quindi dall'osservare che tali soluzioni sono state carrozzate con hardware capace di raggiungere prestazioni di rete elevate a sufficienza da non penalizzare il traffico. Più precisamente, il costruttore dichiara capacità fino a 4 Gbps per la trasmissione attraverso il firewall e fino a 200 Mbps con tutte le funzionalità di threat prevention active.

David ci conferma: «Questo nuovo hardware affronta il problema delle performance in particolare. Storicamente, infatti, i firewall diminuivano il traffico quando tutte le funzioni di sicurezza erano attive, rallentando ulteriormente nel corso del tempo, e arrivando al punto di rendere necessaria la disattivazione delle funzioni di sicurezza per lasciare fluire il traffico».

È evidente che scegliere le prestazioni a scapito della sicurezza aumenta considerevolmente il rischio. Per questo l'esperto evidenzia con vigore: «Il nuovo hardware garantisce una sicurezza migliore senza impatto



sulle performance. Il risultato è una sicurezza più efficace, con la massima velocità di Internet». Di più: «La nuova linea 700 è anche dotata di WiFi 802.11ac e dovremmo aggiungere anche un modem VDSL incorporato in primavera», ci anticipa David, sottolineando che: queste caratteristiche sono molto richieste sul mercato europeo.

Le prestazioni sono solo uno degli aspetti considerati in fase di progettazione: «La linea di appliance per le Pmi è stata pensata con caratteristiche di gestione specifiche per quelle aziende che non hanno disponibilità di risorse in grado di gestire in maniera dedicata la sicurezza, quindi: facilità, velocità e automatismi adeguati», afferma sempre David, che continua: «Lato sicurezza sono state equipaggiate con lo stesso livello di funzionalità delle soluzioni enterprise, perciò nulla è lasciato al caso e una Pmi può, con un rapporto qualità prezzo adeguato, portarsi in casa una soluzione top class».

In particolare: «Questo design offre alle Pmi un ulteriore vantaggio, ovvero la possibilità di sfruttare, come le grandi aziende, la soluzione Threat Cloud, per ottenere aggiornamenti e feedback in tempo reale. Il tutto, out of the box.», precisa il manager italiano.

A giudicare dalle informazioni forniteci da David e dai dati dichiarati dal produttore, la linea 700 sembra realmente un'ottima soluzione per una piccola e media impresa italiana, anche considerando i prezzi consigliati in fase di lancio per le due varianti: 499 dollari per

la soluzione 730, da 100 Mbps, e 799 dollari per la soluzione 750, da 200 Mbps. Resta opzionale il WiFi 802.11ac e non è ancora noto il

prezzo dell'opzione VDSL.

Le nuove soluzioni si affacciano su un mercato estremamente vasto. Le Pmi, infatti, sarebbero il 90% delle aziende nel mondo, riportano presso Check Point citando stime della Banca Mondiale, che in questa categoria contano tanto il piccolo negozio quanto "complessi team internazionali". Chiaramente questi ultimi sono più sensibili del fruttivendolo all'angolo riguardo la sicurezza informatica, ma troppe Pmi tendono a sottovalutare i rischi che corrono.

Afferma Gabi Reish, vice president of product management di Check Point: «Non solo i cybercriminali sfruttano mezzi sempre più sofisticati per sottrarre dati, ma sempre più spesso prendono di mira lo spirito imprenditoriale dei reparti IT delle piccole aziende».

La linea 700 fornisce un livello di protezione avanzato e Reish ne approfondisce alcune caratteristiche, a cominciare dalle funzionalità pre-installate che comprendono firewall, VPN, intrusion prevention, antivirus, antispam, application control, Url filtering e la possibilità di attivare il monitoraggio della sicurezza per la propria rete.

In particolare, grazie al Security Management Portal di Check Point e al servizio Cloud Management SMB, Check Point e i suoi partner possono offrire protezione e performance 24 ore su 24.

shaping tomorrow with you

FUJITSU

The Innovation Engine

Trasforma l'IT
con il Business-Centric
Computing

L'infrastruttura IT delle aziende deve essere adeguata alle priorità del business, garantire risultati sostenibili e consentire una continua innovazione.

Grazie alle soluzioni Business-Centric Computing è possibile allineare la capacità di calcolo alle esigenze aziendali e rendere l'elaborazione e l'analisi dei dati più veloce e più efficiente che mai.

Inoltre, Windows Server 2012 R2 garantisce maggiore flessibilità e agilità per la virtualizzazione, gestione, archiviazione, connettività di rete, infrastruttura desktop virtuale, accesso e protezione dei dati, piattaforma Web e applicazioni.

INFO » <http://business-datacenter.it.fujitsu.com/>

NUMERO VERDE » 800 466 820

E-MAGAZINE » <http://tech4green.it>



Windows Server