Serie “Executive”

Elementi di sicurezza essenziali per i CIO

Accogliere l’innovazione con fiducia

IBM

Ogni giorno, nuovi flussi di informazioni entrano nelle aziende, consentendo di eseguire analisi basate su valori aggiornati al minuto e di prendere decisioni più intelligenti. Mai come prima, dipendenti e clienti sono interconnessi in una moltitudine di tecnologie. Tuttavia, la proliferazione e sovrapposizione delle reti pone forti sfide per la sicurezza. La complessità è vertiginosa e i possibili punti di attacco quasi illimitati. I CIO (Chief Information Officer) devono scontrarsi con frustrazioni e problematiche in misura sempre crescente. E’ possibile garantire un alto livello di sicurezza nell’era dell’iper-connessione? La risposta è sì, ma ciò richiede cambiamenti radicali nei processi e nei comportamenti. IBM ha implementato la propria strategia interna identificando i dieci elementi essenziali necessari a garantire la security intelligence nel 21esimo secolo.

Alle prime luci dell’alba, al proprio risveglio a New York, il Vice Presidente commerciale scende dal letto, prende lo smart phone e scopre che sta emergendo una grande opportunità in Malesia. La notizia scatena una serie di comunicazioni a cascata. Prima di colazione, sei membri del Global Team sono in teleconferenza, uno di loro via Skype a Stoccolma. Tre clienti chiamano dai telefoni cellulari. Nel corso della giornata, gli scambi di email si susseguono intersecandosi da ogni parte del mondo, circa la metà sulla rete aziendale, altri su Gmail e Yahoo. In serata, a New York, l’affare è concluso. Nelle ore successive, alcuni partecipanti si scambiano messaggi amichevoli su LinkedIn.

Il 91%

degli utenti di smart phone aziendali si collega alla posta elettronica aziendale, ma solo ad uno su tre viene richiesta l’installazione di un software per la sicurezza mobile.

Fonte: Kaspersky Labs
http://usa.kaspersky.com/sites/usa.kaspersky.com/files/Enterprise%20Mobile%20Survey.pdf

E’ ormai noto che i manager, oggi, sono in grado di riunire risorse umane e gigabyte di dati in un istante, e utilizzarli per prendere decisioni più rapide e di gran lunga più informate. Tuttavia, sono proprio i punti di forza di queste reti interconnesse – la loro velocità e apertura, facilità di accesso in tutto il mondo – a creare, al contempo, una miriade di vulnerabilità. Pertanto, garantire la sicurezza della rete aziendale diventa un compito sempre più complesso, la cui difficoltà cresce esponenzialmente al passo con l’aumento di informazioni che affluiscono da migliaia di dispositivi e attraverso lo scoring di servizi web pubblici. Secondo lo studio condotto Kaspersky Labs, il 91% degli utenti di smart phone aziendali si collega alla posta elettronica aziendale, ma solo ad uno su tre viene richiesta l’installazione di un software per la sicurezza mobile. In un simile ambiente, l’accesso è facile per tutti gli attori coinvolti – comprese, fin troppo spesso, le organizzazioni criminali.

Le cerchie criminali attualmente si pongono come obiettivo principale i PC collegati ad Internet e i dispositivi mobile. Attaccando i dispositivi con malware difficile da rilevare, ampliano le loro basi di azione. Per i ladri, le reti aziendali sono ricche di tesori digitali, comprese password, user ID, segreti aziendali e dati personali. Gli intrusi digitali, inoltre,

puntano ad asset strategici, da sedi governative ministeriali a reti di comunicazione. Per alcuni, l’obiettivo è compromettere le attività di business. Secondo le stime di Gartner, dal 20 al 30 percento dei PC di consumatori è stato compromesso da botnet e malware utilizzabili come infrastrutture per le attività criminali. Dato che molte aziende stanno considerando l’uso aziendale dei dispositivi personali, il potenziale di attacco assume proporzioni allarmanti.

Il 20–30%

dei PC di consumatori ospita malware e lavora part-time per i criminali.

Fonte: http://www.computerweekly.com/opinion/CW-Security-Think-Tank-How-to-prevent-security-breaches-from-personal-devices-in-the-workplace

Un unico computer infetto può provocare gravi danni. Attualmente, uno degli esempi più drammatici è Stuxnet, un worm altamente sofisticato studiato per danneggiare il software e le apparecchiature industriali. Nella primavera del 2009, il worm ha iniziato a diffondersi in tutte le macchine, principalmente concentrate in Iran. Presumibilmente, qualcuno lo aveva introdotto attraverso un thumb-drive contaminato. Sviluppato per attaccare macchine target dotate di programma software Siemens, il worm ha mandato in tilt numerosi sistemi industriali.

Le lezioni apprese dai leader della sicurezza aziendale sono chiare. Se un worm riesce ad introdursi in settori fortemente protetti in Iran e altrove, potrebbe essere molto più semplice identificare una breccia in un ambiente caratterizzato da una forza lavoro di professionisti attivi in tutto il mondo che utilizzano Twitter, Facebook, soluzioni testuali e Skype. Inoltre, se un worm è in grado di danneggiare l’apparecchiatura industriale, altri non potrebbero forse interrompere intere supply chain, reistradare il traffico e compromettere le reti elettriche, solo per citare alcune delle possibili catastrofi? Per dirlo con un’unica parola: sì.

Per affrontare queste sfide crescenti, le aziende hanno bisogno di una **nuova categoria di leader della sicurezza.** Naturalmente questi leader dovranno conoscere le innumerevoli minacce tecnologiche, ma dovranno altresì comprendere questioni di natura strategica. Quali informazioni devono essere ampiamente condivise? Chi dovrà avere accesso a determinate informazioni preziose e in che modo saranno protette? Nel loro insieme, le sfide tecniche e strategiche creano un livello di complessità vertiginoso. E, mentre si diffonde la tentazione di rispondere a tale complessità con soluzioni altrettanto complesse, i dirigenti lungimiranti hanno capito che tale escalation è insostenibile, fuori portata e, in ultima analisi, inutile.

L’unica soluzione è cambiare, a livello radicale, il modo in cui le aziende operano. Il punto di partenza consiste nell’ **espandere la mission della sicurezza aziendale,** dallo staff tecnico con le proprie macchine ad ogni singolo individuo all’interno dell’azienda, nonché a tutti gli attori che intraprendono business con l’azienda stessa. Si tratta dell’unica soluzione possibile, dato che visto che ogni persona rappresenta una potenziale violazione, ognuno deve costituire altresì una componente integrante della soluzione.
In definitiva, il successo verte sulla creazione di una consapevolezza forte e persistente: **una cultura di consapevolezza del rischio.**

La cultura di consapevolezza del rischio richiede qualcosa di più della tecnologia aggiornata e si estende ben oltre le best practice. Tale cultura rappresenta un nuova prospettiva, nella quale l’approccio pragmatico verso la sicurezza informa ogni decisione e procedura, a tutti i livelli aziendali. Essa deve ridefinire il modo in cui le persone gestiscono le informazioni, dai dirigenti di livello C agli stagisti estivi. All’interno di tale cultura, le procedure per la sicurezza dei dati diventano una sorta di “seconda natura”, proprio come avviene quando si allacciano le cinture di sicurezza o quando si conservano i fiammiferi in un luogo sicuro.

Tale cultura rappresenta un nuova prospettiva, nella quale l’approccio pragmatico verso la sicurezza informa ogni decisione e procedura, a tutti i livelli aziendali.

Questa decisione non è prorogabile. La sicurezza aziendale sta raggiungendo rapidamente un punto critico. Consideriamo gli elementi che la compongono. Nella classe criminale, i professionisti hanno preso il posto dei dilettanti e ciò contribuisce ad aumentare le minacce. Contemporaneamente, le aziende hanno aumentato la produttività ed hanno favorito l”empowerment’ dei lavoratori, con un’ampia distribuzione di fiumi di dati digitali su attività, marketing, vendite e servizio clienti. Ciò moltiplica la vulnerabilità. Inoltre, dato che ora le aziende gestiscono il proprio business quasi completamente in formato digitale, le conseguenze di un attacco possono compromettere l’intero assetto aziendale. In sintesi: i ladri sono più competenti, dispongono di innumerevoli porte e finestre digitali attraverso le quali accedere, e il valore interno che potrebbe essere compromesso è inestimabile.

Se da un lato la posta in gioco è altissima, dall’altro la via verso la sicurezza può sembrare scoraggiante e confusa. Nonostante i prodotti e servizi per la sicurezza non manchino sul mercato attuale, i nostri clienti riferiscono spesso di essere frustrati da un mercato della sicurezza che sembra vacillare, passando da una cattiva notizia all’altra, cercando di dare risalto alla recente crisi della sicurezza o ai requisiti di compliance. Molti non sanno da dove cominciare o in cosa credere, descrivendo spesso la sicurezza e la compliance come un investimento di valore non quantificabile o che apporta un ritorno sugli investimenti (ROI) di dubbio valore e di scarsa convenienza. Questa confusione genera spesso indecisione, o, ancora peggio, la decisione di rinunciare all’innovazione basata sul timore.

Proteggere un’azienda rappresenta sicuramente un’ardua impresa, che non è mai completa. Inoltre, cambiare una cultura è difficile. Ma questo tipo di azione è indispensabile. Un elevato livello di sicurezza è il costo che bisogna pagare per restare nel business, e raggiungerlo è possibile.

IBM cerca costantemente di trovare l’equilibrio tra innovazione necessaria e l’esigenza di controllare il rischio. La risposta completa dell’azienda comprende tecnologia, processi e misure politiche e consta di dieci pratiche essenziali. Nel corso dei prossimi mesi, distribuiremo una serie di white paper nei quali potrete apprendere tali pratiche più nel dettaglio. Per il momento, di seguito è riportato un breve riepilogo:

Elementi di sicurezza essenziali

1. Creare una cultura di consapevolezza del rischio

Il concetto è elementare. Ogni singola persona può infettare l’azienda, facendo clic su un allegato di dubbia provenienza o non installando una patch di sicurezza sullo smart phone. Pertanto, l’impegno volto alla creazione di un’azienda sicura deve riguardare tutti. Creare una cultura di consapevolezza del rischio implica la definizione dei rischi e degli obiettivi e la comunicazione degli stessi. Ma il cambiamento importante è di carattere culturale. Si pensi alla reazione istintiva – all’orrore – che molti provano nel vedere un genitore che chiacchiera al telefonino mentre il proprio bambino attraversa da solo la strada. Lo stesso tipo di intolleranza dovrebbe esistere, a livello aziendale, quando i colleghi restano indifferenti di fronte alle questioni che riguardano la sicurezza. I dirigenti, chiaramente, devono promuovere incessantemente questo cambiamento con un approccio dall’alto verso il basso, implementando al contempo gli strumenti necessari a tracciare il progresso.

2. Gestire gli incidenti e reagire

Poniamo che si verifichino due incidenti simili, uno in Brasile e l’altro a Pittsburgh. Tali incidenti possono essere collegati. Ma senza la security intelligence necessaria ad identificare il legame che li collega, un pattern importante, che potrebbe indicare un potenziale incidente, potrebbe passare inosservato. E’ necessario pertanto un impegno a livello aziendale volto ad implementare funzionalità di intelligent analytics e risposta automatizzata. La creazione di un sistema automatizzato e unificato consentirà all’azienda di monitorare le proprie operazioni e di reagire tempestivamente.

3. Proteggere il posto di lavoro

I cyber-criminali sono alla costante ricerca di punti vulnerabili. Ogni singola stazione di lavoro, computer portatile o smart phone fornisce una potenziale apertura che espone ad attacchi nocivi. Le impostazioni su ciascun dispositivo non devono essere affidate a singoli individui o gruppi autonomi. Esse devono essere interamente soggette ad una gestione e implementazione centralizzata . Inoltre, i flussi di dati all’interno dell’azienda devono essere classificati, ognuno con il proprio profilo di rischio e devono essere istradati esclusivamente alla cerchia di utenti corrispondente. Proteggere la forza lavoro significa dissipare il caos e sostituirlo con la fiducia.

4. Sicurezza sin dalla progettazione

Immaginate cosa succederebbe se le aziende automobilistiche producessero le auto senza cinture di sicurezza o airbag, e li aggiungessero in un secondo momento, a seguito di situazioni allarmanti o incidenti. Sarebbe insensato ed eccessivamente costoso. Allo stesso modo, una delle principali vulnerabilità dei sistemi informatici – nonché spreco di denaro – deriva dall’implementazione prima dei servizi e poi dell’aggiunta delle funzionalità di sicurezza a seguito di un ripensamento. L’unica soluzione consiste nel realizzare la sicurezza sin dall’inizio e nell’eseguire regolarmente test automatizzati per tracciare la conformità. Questo processo consente inoltre di risparmiare denaro. Se la realizzazione di una funzionalità di sicurezza nell’applicazione costa un extra di €49,5, aggiungerla successivamente può costare fino a 100 volte di più, ovvero €4.958.

5. Mantenere il software aggiornato

Succede sempre così. Le persone continuano ad usare i vecchi programmi software perché li conoscono e si sentono a proprio agio nell’utilizzarli. Tuttavia, la gestione degli aggiornamenti in una combinazione di software può essere pressoché impossibile. Inoltre, le aziende di software , a volte, smettono di produrre le patch per i vecchi programmi. I cyber criminali sanno fin troppo bene queste cose. In un sistema sicuro, gli amministratori possono tener traccia di ogni programma in esecuzione, possono essere certi che sia aggiornato e possono disporre di un sistema completo per istallare aggiornamenti e patch non appena sono disponibili.

6. Controllare l’accesso in rete

Consideriamo la criminalità urbana. Mantenere l’ordine pubblico sarebbe molto più facile se tutti i veicoli della città fossero dotati di un radio tag univoco e viaggiassero solo su alcune arterie di grande traffico, circondate da sensori. Lo stesso vale per i dati. Per le aziende che instradano i dati registrati attraverso punti di accesso monitorati, il rilevamento e isolamento del malware sarà di gran lunga più semplice.

7. La sicurezza nel cloud

Il cloud computing promette altissimi livelli di efficienza, ma può presentare alcuni rischi. Migrando alcuni servizi IT nel cloud computing, l’azienda entra in contatto con molti altri ambienti, ed eventualmente anche con scammer esperti. Visto da questa prospettiva, il cloud è come un hotel nel quale una determinata percentuale di clienti è affetta da peste bubbonica. Per sopravvivere in questo ambiente, gli ospiti devono disporre degli strumenti e delle procedure necessari per isolarsi dagli altri e per monitorare possibili minacce.

8. Monitorare l’intero ecosistema

Poniamo che un cliente abbia bisogno di accedere al sistema. In che modo assicurarsi che abbia le credenziali giuste? Si possono lasciare su un notepad? Possono essere inviate per sms? Simili improvvisazioni contengono dei rischi. La cultura della sicurezza aziendale deve estendersi oltre le mura aziendali e definire best practice tra clienti e fornitori. Si tratta di un processo simile al controllo qualità introdotto nella scorsa generazione. La logica è la stessa: la sicurezza, come l’eccellenza, devono essere diffuse in tutto l’ecosistema. Gli effetti nocivi della negligenza in un’azienda possono danneggiare interi settori della società.

9. Proteggere i gioielli dell’azienda

Da qualche parte, nel forziere, sono nascosti i gioielli più preziosi dell’azienda, quali, ad esempio, i propri dati scientifici e tecnici, o forse alcuni documenti riguardanti possibili fusioni ed acquisizioni, o magari si tratta di informazioni finanziarie private di clienti. Ogni azienda dovrebbe stilare un inventario, riservando un trattamento speciale ai dati critici . Ogni voce prioritaria dovrebbe essere protetta, tracciata e codificata, se da essa dipende la sopravvivenza dell’azienda. E, in alcuni casi, potrebbe.

10. Tracciare l’identità

Poniamo che un consulente venga impiegato full time. Dopo sei mesi ottiene una promozione. Un anno dopo, un concorrente sopraggiunge e lo assume. In che modo il sistema tratta questa persona nel corso del tempo? In primo luogo deve darle accesso limitato ai dati, quindi deve aprire un maggior numero di porte prima di revocare tale accesso alla fine. Questo significa gestire il ciclo di vita dell’identità e costituisce un elemento cruciale. Le aziende che non gestiscono adeguatamente tale ciclo di vita operano all’oscuro e sono vulnerabili all’intrusione. Questo rischio può essere risolto implementando sistemi meticolosi per identificare le persone, gestire i permessi e revocarli alle dimissioni.

In che modo accogliere l’innovazione con fiducia?

Il giusto equilibrio tra gestione dei rischi e promozione dell’innovazione

Partecipa alla conversazione

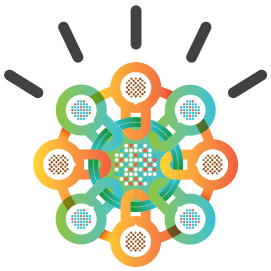
Per leggere ulteriori articoli, conoscere maggiori dettagli o condividere le proprie opinioni con altri leader della sicurezza partecipa a **ibm.com/smarter/cai/security**.

L’autore

Kristin Lovejoy è Vice President of IT Risk, Office of the CIO, IBM. L’autrice è reperibile al seguente indirizzo **klovejoy@us.ibm.com**.

Informazioni sull’IBM Centre for Applied Insights

L’IBM Centre for Applied Insights integra una profonda conoscenza dei contenuti e know-how analitico per assistere i clienti nell’individuazione di nuovo valore . Il Centro conduce ricerche e realizza risorse e strumenti con un orientamento pragmatico per stimolare le aziende all’azione.



IBM Italia S.p.A.
Circonvallazione Idroscalo
20090 Segrate (MI)
Italia

CIE03116-ITIT-00