



Prevenire e gestire gli incidenti: gli Emergency Response Services di IBM



Avvertenze
Pubblicato nel 2014

Tutti i marchi contenuti in questo white paper sono registrati e di proprietà delle relative società. Tutti i diritti sono riservati. Va notato che le informazioni contenute possono cambiare senza preavviso; le informazioni contenute sono reputate essere corrette e affidabili anche se non sono garantite. La descrizione delle tecnologie non implica un suggerimento all'uso dell'una o dell'altra così come il parere espresso su alcuni argomenti da parte di Reportec è puramente personale.

Copyright Reportec – 2014
www.reportec.it

Indice

Prevenire e gestire gli incidenti: gli Emergency Response Services di IBM	5
Uno scenario ad alto tasso di pericolo	6
<i>Metodologia Cyber Security Intelligence Index</i>	<i>6</i>
Un costo da valutare	8
Cost of Data Breach. Global Study	10
<i>La metodologia del “Cost of Data Breach Study. Global Study”</i>	<i>10</i>
Gli IBM Emergency Response Services	12
<i>Una suite di servizi</i>	<i>12</i>
<i>Un supporto esterno</i>	<i>13</i>



Prevenire e gestire gli incidenti: gli Emergency Response Services di IBM

La costante pressione delle minacce informatiche impone scelte strategiche. È opportuno attivare una protezione multilivello, come stratificati sono gli attacchi.

Soprattutto, però, una protezione basata sugli effettivi rischi che un attacco andato a buon fine comporta.

Il che solleva questioni fondamentali: quali sono questi rischi?

Quanto ci costa una violazione alla sicurezza? È sufficiente prevenire?

Questo white paper traccia uno scenario attraverso i risultati del "Cost of Data Breach Study: Global Study" del Ponemon Institute e del Cyber Security Intelligence Index 2014 di IBM, che confronta i dati derivanti dal monitoraggio di miliardi di eventi sulla sicurezza con quelli ricavati dalle attività di risposta o indagine forense su incidenti dovuti agli attacchi informatici.

Infine, vengono analizzate le caratteristiche del servizio in abbonamento IBM Emergency Response Services, che mette a disposizione un team per prevenire le minacce, mitigare i rischi e rispondere alle emergenze.

Quando valutiamo l'acquisto di una porta blindata, il venditore ci chiede quanto tempo vogliamo che debba metterci lo scassinatore per entrare. Non mette in dubbio la capacità di quest'ultimo nel superare la barriera, ammettendo implicitamente di non poterci assicurare la totale salvaguardia dei nostri beni.

Analogamente, nessuno potrà garantire al 100% la sicurezza dei dati, ma si può ridurre il più possibile l'esposizione alle minacce e ridurre i rischi che un attacco andato a buon fine comporterebbe. Occorre, però, valutare tali rischi con attenzione, sia per predisporre la protezione più efficace rispetto alla propria esposizione sia per investire in maniera oculata rispetto al valore di quello che si deve proteggere. È facile concordare che non conviene spendere per la protezione più di quanto vale ciò che si vuole proteggere. D'altro canto, se si valuta con attenzione quali siano i rischi, si comprende che "il gioco vale la candela", perché in ballo può esserci la reputazione, se non addirittura la sopravvivenza stessa, della propria azienda.

Uno scenario ad alto tasso di pericolo

Il report Cyber Security Intelligence Index 2014 fornisce una panoramica accurata delle principali minacce degli ultimi anni, analizzando in dettaglio il volume degli attacchi, i settori maggiormente coinvolti, le tipologie prevalenti degli attacchi e dei loro autori.

I dati raccolti riguardano il 2013, anno in cui si sono verificati clamorosi attacchi a grandi realtà statunitensi, scoprendo nuovi tipi di vulnerabilità "integrate". È iniziata, del resto, l'era del machine to machine e sono sempre di più le connessioni tra dispositivi che il reparto IT non prende in considerazione.

L'esempio forse più eclatante in tal senso, riguarda Target, un'importante catena di supermercati statunitense. I cybercriminali sono riusciti a penetrare nel sistema di monitoraggio dei frigoriferi, gestito da un fornitore esterno, che ne controllava lo stato, pronto a intervenire prima che si verificassero guasti. Da qui hanno ottenuto l'accesso alla rete, arrivando a intercettare i dati sulle carte di pagamento trasmesse dal sistema di casse al gestionale centrale.

Non è chiaro quanti dati siano stati copiati, né se questi fossero realmente utilizzabili, perché esistevano altri livelli di protezione, a cominciare dalla crittografia e dalla separazione dei diversi elementi componenti i numeri della carta. Gli esperti di IBM calcolano che, in media, una carta di credito viene venduta sul mercato nero a un prezzo variabile tra 25 e

100 dollari, a seconda delle informazioni disponibili oltre al numero della carta, come il codice di sicurezza CSV, la conoscenza del limite di utilizzo o la data di scadenza.

Si sono verificati diversi incidenti nel retail (bersaglio privilegiato perché vi si fa ampio uso di carte di paga-

mento): secondo il Cyber Security Intelligence Index, sono stati rubati i dati di oltre 110 milioni di carte di credito.

Il numero di attacchi è in aumento, sempre secondo l'analisi del Cyber Security Intelligence Index. In particolare, è stato determinato che nel



La security intelligence consente di ridurre il rischio. Con le analisi degli eventi di sicurezza, gli strumenti di IBM hanno ridotto 16.856 attacchi a 109 incidenti. In media, il numero annuale di attacchi di sicurezza sostenuti nel 2013 dai clienti IBM è sceso a una media di quasi 17mila contro i 73mila del 2012. (Fonte IBM)

METODOLOGIA CYBER SECURITY INTELLIGENCE INDEX

Il Cyber Security Intelligence Index ha considerato i dati forniti da IBM Managed Security Services derivanti dal monitoraggio di miliardi di eventi all'anno sui dispositivi dei clienti, tra i quali sono stati selezionati quelli relativi agli incidenti rilevati in 133 paesi. A questi sono stati aggiunti i dati ottenuti dalle indagini forensi. Infine sono state poste domande (quali qual è il panorama attuale delle minacce? Che tipo di attacchi sono stati lanciati? Quanti attacchi hanno causato incidenti che hanno richiesto un'indagine?) a un campione di clienti.

Poiché i profili dei clienti differiscono in modo significativo in base alla dimensione e al settore di industria, i dati del report sono stati adattati per descrivere un'organizzazione di medie dimensioni con 1.000/5.000 dipendenti (anche se i clienti di IBM sono tipicamente aziende di dimensioni più grandi) e con in media 500 dispositivi di sicurezza.

2013, in media, le aziende hanno dovuto affrontare oltre 91 milioni di eventi di sicurezza: il 12% in più del 2012. In parte quest'aumento si spiega anche con la continua crescita di dati, reti, applicazioni e delle innovazioni tecnologiche che li supportano. Va, però, registrato anche l'incremento degli obiettivi per potenziali attacchi.

Il dato è impressionante e rende definitivamente chiaro che 91 milioni di eventi l'anno non possono essere gestiti manualmente, come si faceva con i primi firewall e come in molti ritengono di poter fare con strumenti di correlazione di prima generazione.

Gli esperti di IBM hanno invece dimostrato come strumenti di analytics e di correlazione avanzati sono in grado di filtrare tali volumi di dati e ridurre sensibilmente i rischi. Anzi, il crescere degli eventi e dei dati relativi aiuta a raffinare l'analisi e a gestire gli eventi con maggiore efficienza.

Un costo da valutare

Come visto i guadagni associati ad attività di cybercrime sono notevoli e, di converso, elevati sono i danni economici per le imprese. Non sappiamo quali sono stati i costi effettivi per Target, certo l'impatto sull'immagine è stato notevole.

Ma non è solo questo a dover preoccupare, perché ci sono diversi aspetti che vanno considerati, oltre il furto dei dati sensibili. In particolare la criticità del "post evento". Solo le ore spese per valutare i danni e le contromisure da prendere per evitare che si ripeta l'incidente sono un costo non indifferente.

In generale, nella valutazione dell'impatto di un incidente di sicurezza occorre prendere in considerazione la reputazione del brand, la fiducia dei clienti, la perdita dei dati aziendali, la produttività dei collaboratori, la disponibilità operativa, gli audit normativi e i costi di adeguamento del sistema per la sicurezza.

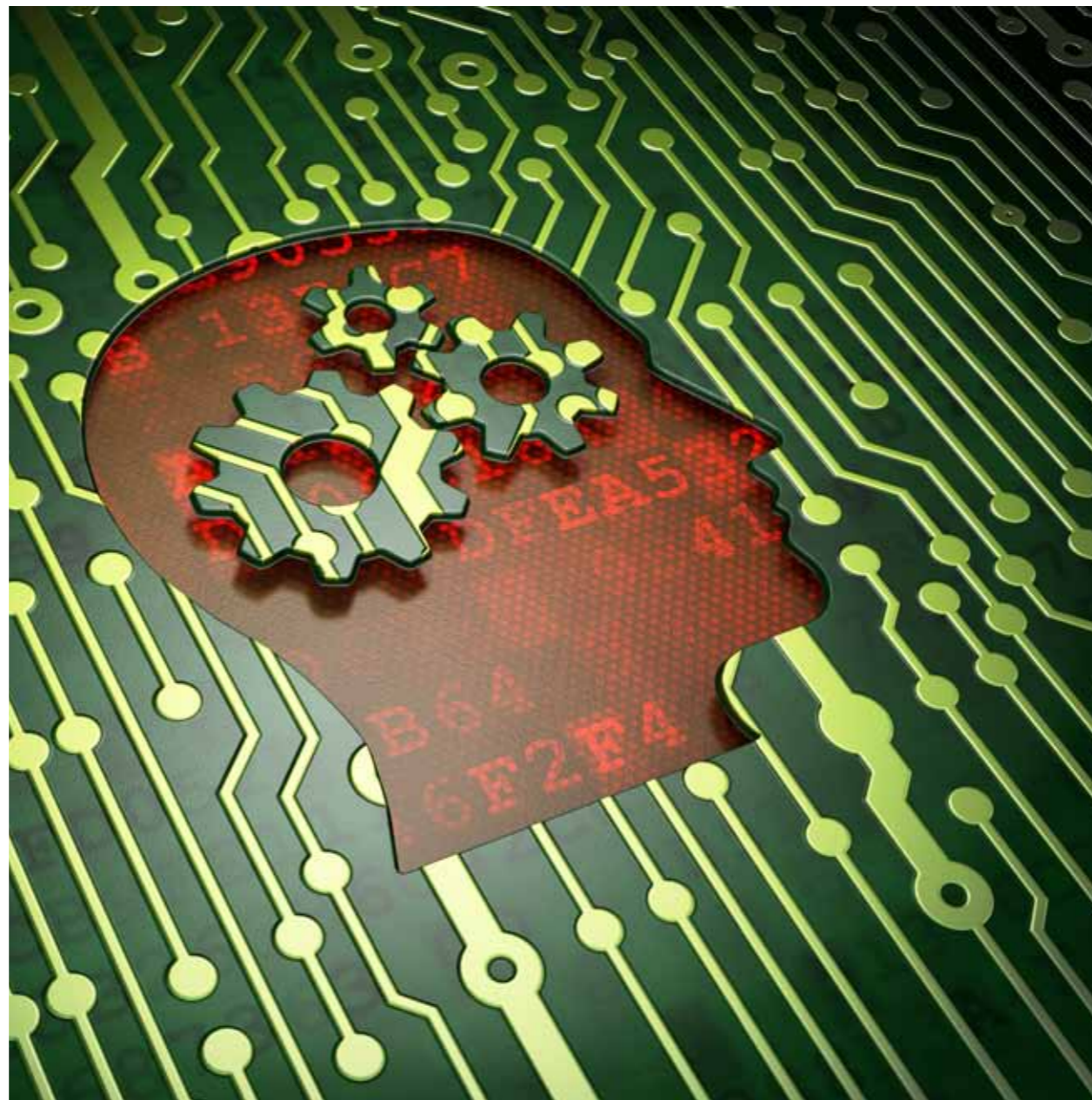
Per aiutare le imprese a valutare il proprio rischio, il Ponemon Institute ha realizzato il Cost of Data Breach Study: Global Study. Questo ha calcolato che il costo totale medio per una violazione dei dati è aumentato del 15%, raggiungendo 3,5 milioni di dollari, secondo le stime dei manager intervistati. Il costo medio sostenuto per ogni record smarrito o rubato contenente informazioni sensibili e confidenziali è aumentato di oltre il 9% da 136 dollari nel 2013 a 145 dollari nel 2014.

Va sottolineato che tale costo varia molto tra i diversi paesi. Molte di queste differenze di costo posso-

no essere attribuite ai tipi di attacchi e minacce che le organizzazioni affrontano, nonché alle normative e leggi in materia di protezione dei dati vigenti nei rispettivi paesi. Per avere un'idea: il costo medio stimato in Germania e negli Stati Uniti è rispettivamente di 195 e 201 dollari, ben superiore alla media.

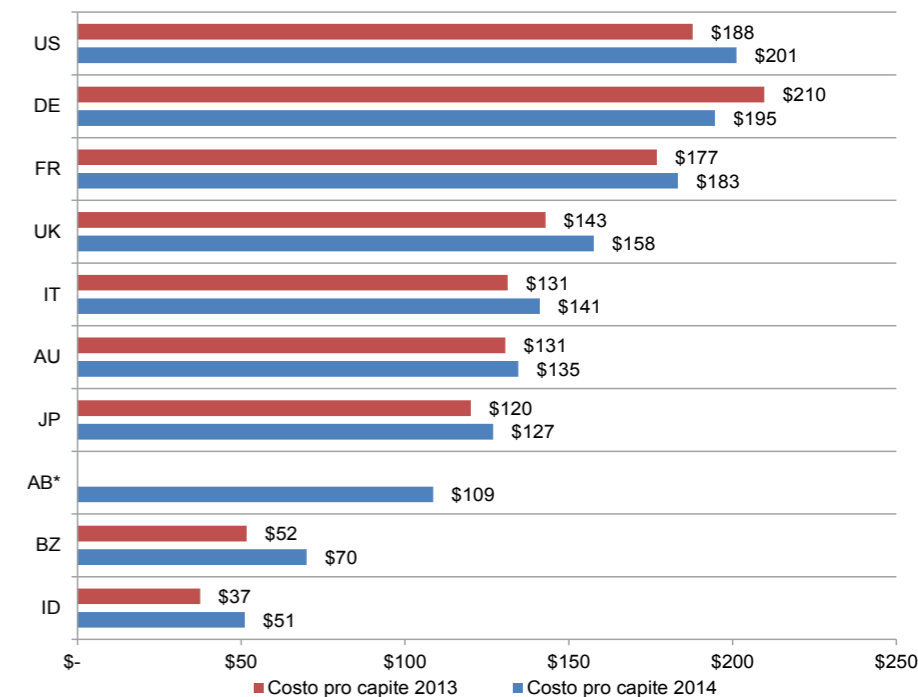
Dall'altro lato ci sono Brasile e India, dove il costo medio è valutato ri-

spettivamente 70 e 51 dollari. L'Italia è più o meno a centro classifica, con un costo medio stimato che è passato dai 131 dollari del 2013 ai 141 dollari del 2014. Peraltro, per comprendere i termini della questione va considerato anche il valore assoluto, cioè considerare il numero di record che sono stati trafugati. In Italia, per esempio, questi sono stati dichiarati in numero pari a 19.034.



Il costo pro capite medio delle violazioni dei dati nel corso di due anni. Per costo pro capite medio s'intende il costo totale delle violazioni dei dati diviso per il numero di dati smarriti o rubati.

Legenda: AU = Australia; BZ = Brasile; FR = Francia; DE = Germania; ID = India; IT = Italia; JP = Giappone; AB = Emirati Arabi Uniti e Arabia Saudita; UK = Regno Unito; USA = Stati Uniti. (Fonte: Ponemon Institute)



Gli analisti del Ponemon Institute hanno anche misurato le cause delle violazioni, che per la maggior parte (41%) sono dovute a un vero e proprio attacco criminale o comunque malevolo. In pratica, compromissioni attraverso malware, ma anche azioni mirate da parte di cybercriminali in possesso di informazioni riservate, ottenute attraverso tecniche di phishing, social engineering e SQL injection.

Il 30% è stato invece determinato dal comportamento negligente di dipendenti o collaboratori esterni, mentre il restante 29% è stato imputato a malfunzionamenti dei sistemi (che includono errori sia nei processi IT sia in quelli di business). Osservando le dinamiche degli attacchi, peraltro, si comprende che il fattore umano è una componente determinante, non solo perché causa diretta del 30% delle violazioni, ma anche perché in parte respon-

sabile anche negli altri casi. Spesso, infatti, l'infezione da malware avviene per l'ingenuità del dipendente che apre un link in un mail malevola. Inoltre, non sono rari i casi in cui un dipendente risulta vittima di social engineering perché non adeguatamente informato sulla sensibilità di alcune informazioni.

A tal proposito, vale la pena sottolineare il dato riportato dal Cyber Security Intelligence Index di IBM: nel 2013 per oltre il 95% degli incidenti analizzati il fattore determinante è stato l'errore umano. Quello più diffuso è stato l'apertura di un allegato infetto o di un URL non sicuro. Altri errori comuni sono configurazioni errate di sistema, gestione inadeguata delle patch, utilizzo di nomi e password predefiniti, password facili da individuare, perdita di laptop o dispositivi mobili e divulgazione di informazioni regolamentate mediante l'uso di indirizzi e-mail non corretti.

Cost of Data Breach. Global Study

Secondo la nona edizione della ricerca "Cost of Data Breach Study", condotta a livello mondiale dal Ponemon Institute e pubblicata a Maggio 2014, il costo totale medio per la violazione dei dati a livello mondiale è aumentato del 15% in un anno, raggiungendo i 3,5 milioni di dollari.

Di seguito riportiamo i principali risultati ricavati dallo Studio Global Cost of Data Breach:

- Il costo sostenuto per ogni record perso o rubato, contenente informazioni riservate e sensibili, è aumentato di più del 9%, toccando i 145 dollari.
- Le violazioni più onerose si sono verificate negli Stati Uniti e in Germania, con un costo rispettivamente di 201 e 195 dollari per dato compromesso. Le violazioni dei dati meno costose sono state in India e Brasile, rispettivamente pari a 51 e 70 dollari.
- Le cause principali cui addebitare le violazioni dei dati variano da paese a paese e possono influire sul costo della violazione. I paesi nella regione Araba e la Germania hanno avuto un maggior numero di violazioni dei dati causate da attacchi malevoli o di organizzazioni criminali. L'India ha avuto il maggior numero di violazioni dei dati causate da anomalie di sistema o di processo. L'errore umano è stato la causa più comune nel Regno Unito e in Brasile.

- Le violazioni dei dati più onerose sono state quelle causate da attacchi malevoli o di organizzazioni criminali. Gli Stati Uniti e la Germania hanno sostenuto i costi più elevati.
- L'approccio alla sicurezza è stato essenziale per ridurre il costo della violazione dei dati. In media, le aziende che hanno dichiarato di avere un solido livello di sicurezza sono riuscite a ridurre il costo addirittura di 14 dollari per dato.
- L'integrazione della gestione della business continuity ha ridotto il costo della violazione dei dati, in media, di quasi 9 dollari per dato.
- La nomina di un Chief Information Security Officer (CISO) alla guida di un team di gestione della violazione dei dati ha ridotto il costo di una violazione di oltre 6 dollari per dato.
- I Paesi che hanno perso il maggior numero di clienti in seguito a una violazione dei dati sono stati la Francia e l'Italia. Le aziende nella Regione Araba e in Brasile hanno subito la perdita di clienti minore.
- La probabilità per un'azienda di subire una violazione dei dati che coinvolga 10mila o più dati riservati è del 22% nell'arco di due anni. I Paesi che hanno la maggiore probabilità di subire una violazione dei dati sono India, Brasile e Francia.

Come già emerso nei precedenti studi Cost of Data Breach, la causa più comune per una violazione dei dati risulta l'attacco malevolo da parte di soggetti interni all'azienda o di un'organizzazione criminale.

L'obiettivo della ricerca, come spiega Larry Ponemon, presidente e fondatore del Ponemon Institute, è quello di aiutare le imprese a indirizzare i propri investimenti in sicurezza, ma anche di fornire un orientamento sulla probabilità che le imprese hanno di subire una violazione dei dati e sui possibili interventi per ridurre le conseguenze finanziarie.

In questa nona edizione è stato anche chiesto alle figure professionali coinvolti nelle aziende quali sono le preoccupazioni maggiori sugli incidenti di sicurezza, quali investimenti stanno effettuando e l'eventuale esistenza di una strategia al riguardo.

Di seguito sono riportati alcuni dei risultati chiave:

- Le minacce più grandi per le aziende partecipanti alla ricercasono il malware e i tentativi di accesso non autorizzato subiti. Secondo lo studio, queste due minacce sono in aumento.
- Solo il 38% delle aziende ha una strategia di sicurezza per proteggere la propria infrastruttura IT. Una percentuale più elevata (45%) ha in essere una strategia di sicurezza per proteggere il proprio patrimonio di informazioni.
- Codice maligno e probe subiti hanno registrato il massimo aumento. Le aziende stimano che dovranno confrontarsi con una media di 17 codici maligni e 12 probe subiti ogni mese. Gli incidenti

legati agli accessi non autorizzati sono rimasti sostanzialmente invariati e le aziende stimano che dovranno confrontarsi con una media di 10 incidenti di questo tipo ogni mese.

- La maggior parte delle aziende (50%) ha scarsa o nessuna fiducia rispetto all'adeguatezza degli investimenti effettuati in risorse umane, processi e tecnologie per affrontare le minacce potenziali ed effettive.
- Idealmente, le aziende vorrebbero investire 14 milioni di dollari nei prossimi 12 mesi per realizzare la propria strategia di sicurezza. Tuttavia, nell'arco dei prossimi 12 mesi, le aziende prevedono di disporre in media di circa metà di tale cifra, ovvero 7 milioni di dollari, da investire in strategia di sicurezza.

LA METODOLOGIA DEL "COST OF DATA BREACH STUDY. GLOBAL STUDY"

Lo studio annuale di Ponemon "Cost of Data Breach Study" è basato sulla raccolta di informazioni dettagliate sulle conseguenze finanziarie causate dalla violazione di dati. Ai fini di questa ricerca, viene considerata "violazione dei dati", un incidente in cui dati sensibili, protetti o riservati vengono persi o rubati e messi a rischio.

Per la ricerca è definito record compromesso quello che identifica il soggetto le cui informazioni sono state perse o rubate in una violazione dei dati.

Il Ponemon Institute ha condotto 1.690 interviste con professionisti dell'IT, della compliance e della sicurezza delle informazioni, in rappresentanza di 314 organizzazioni, nei 10 Paesi seguenti: Stati Uniti, Regno Unito, Germania, Australia, Francia, Brasile, Giappone, Italia, India e, per la prima volta, la regione araba (un insieme di organizzazioni degli Emirati Arabi Uniti e dell'Arabia Saudita).

Tutti gli intervistati sono figure che, per ruolo, conoscono le violazioni dei dati subite dalle rispettive organizzazioni e i costi associati alle relative risoluzioni. Tutte le organizzazioni partecipanti hanno subito violazioni dei dati, da un livello minimo di circa 2.400 record compromessi a poco più di 100mila.

I dati in valore sono stati espressi in dollari, convertendo le valute dei vari paesi coinvolti in quella degli Stati Uniti.

Gli IBM Emergency Response Services

Molte imprese posseggono eccellenze nel loro settore di attività, ma fanno fatica a mantenere livelli altrettanto elevati di preparazione anche in ambiti altamente specializzati come quello della sicurezza informatica. Ambito in cui esistono aree di specificità in cui occorre un'esperienza che solo chi segue e gestisce numerose e variegata realtà può possedere.

I cybercriminali dispongono di risorse enormi e si sono organizzati, realizzando una vera e propria attività di ricerca e sviluppo per produrre attacchi informatici sempre più sofisticati. La vendita di kit preconfezionati attraverso il Deep Web, inoltre, hanno accresciuto notevolmente la frequenza degli attacchi.

A peggiorare la situazione contribuisce anche la pervasività delle nuove tecnologie, legate al cloud, ai dispositivi mobile e ai social media, che hanno praticamente eliminato i confini della rete e contribuiscono ad aumentare le vulnerabilità.

Ecco perché IBM propone gli Emergency Response Services, che, attraverso la formula dell'abbonamento mettono a disposizione 24 ore su 24 il supporto di un team di sicurezza a livello globale. Il team aiuta le imprese con servizi di gestione degli incidenti e risposte per neutralizzare gli attacchi, nonché servizi proattivi per prevenirli.

I team di IBM mettono a disposizione supporto e strumenti avanzati di analytics, che aiutano a pianificare

una strategia di difesa, a individuare le violazioni e, dunque, a reagire con la necessaria rapidità.

Non meno importanti sono le azioni da intraprendere dopo che l'incidente è avvenuto, a cominciare dall'analizzare la causa principale per una più efficace prevenzione. Occorre poi ripristinare il più rapidamente possibile i sistemi coinvolti ed evitare che incidenti simili possano causare danni futuri.

Infine, ma non ultimo per importanza, occorre gestire correttamente i requisiti di conformità alle normative.

Una suite di servizi

L'abbonamento può includere diversi servizi, a seconda delle esigenze specifiche di ciascuna impresa.

Il primo servizio, che si può considerare di partenza, è un Workshop di pianificazione, che consiste in un laboratorio di una giornata per raccogliere le informazioni, rivedere il piano di sicurezza esistente e i processi previsti. Infine, si analizza come rispondere e gestire i dati in un ipotetico scenario di attacco.

Inoltre nell'offerta base del servizio è incluso anche l'abbonamento a

120 ore all'anno di servizi proattivi e di risposta in caso di emergenza.

Una parte delle ore sottoscritte per l'abbonamento, possono essere utilizzate per ottenere dagli esperti di IBM una valutazione delle vulnerabilità esistenti oppure la definizione di un "Combined Security Incident Response Plan" (CSIRP).

È inoltre possibile effettuare una simulazione dei processi e delle procedure per la risposta agli incidenti identificando eventuali problematiche o criticità nascoste.

Un terzo servizio incluso nell'abbonamento è la possibilità di aggiornare

trimestrali e di supporto remoto. Per esempio, è possibile condurre un check delle minacce in corso, su base mensile, per tutta la durata dell'abbonamento. In questo caso sarà a disposizione un Incident Manager o un analista dedicato, per raccomandazioni e assistenza relativamente agli incidenti di sicurezza. Un quarto servizio, incluso nell'abbonamento, prevede la disponibilità illimitata 24 ore su 24 a rispondere a una dichiarazione di emergenza. Viene lanciato l'allarme contattando il servizio telefonico o il manager dedicato, che provvedono ad avviare le

procedure iniziali di triage. Infine, è disponibile un servizio altamente specializzato attraverso l'accesso all'IBM X-Force Threat Analysis Service (XFTAS). Questo valuta la situazione globale delle minacce online e fornisce analisi e informazioni aggiornate per una gestione proattiva della sicurezza.

Un supporto esperto

Le finalità dell'IBM Emergency Response sono di aiutare le imprese a ridurre l'impatto di un incidente di sicurezza e ad accelerare il ritorno alla normalità. Per questo si inizia con il supporto nella definizione di un sistema di protezione efficace ed efficiente.

Sviluppando una strategia CSIRP e valutando un sistema di risposta alle emergenze le imprese possono affrontare con maggiore serenità un eventuale incidente di sicurezza.

Punto di forza di questa suite di servizio è senza dubbio la competenza dei team di IBM. Sulla sicurezza informatica, questi possono inoltre contare su best practice, attività di ricerca e capacità a livello globale.

L'efficacia degli interventi si basa su un'esperienza maturata affrontando numerosi casi di violazioni in tutto il mondo, sia all'interno di IBM stessa sia per altre organizzazioni. Competenze non solo tecniche, che vanno dal mainframe agli smartphone, ma anche relative alla giurisprudenza digitale.

APPROFONDISCI



