NUOTARE CON GLI SQUALI

Valutazione della maturità della sicurezza e best practice per fronteggiare la concorrenza

INTRODUZIONE

La gestione aziendale del 21o secolo è simile al tentativo di nuotare in mezzo agli squali. Sussiste infatti un pericolo evidente: gli elementi più minacciosi diventano giorno dopo giorno sempre più potenti, organizzati e collaborativi. Occorre imparare a nuotare nel mare della trasformazione digitale, uno dei problemi più scottanti per gli attuali CEO, avvalendosi di capacità specifiche per operare all'interno di un ambiente infestate da squali.

Le tecnologie di trasformazione digitale (Big Data/analytics, cloud computing, mobilità e social business) costringono a spostare le applicazioni e i dati aziendali fuori dai sicuri controlli perimetrali di endpoint e reti, riducendo la visibilità e il controllo per i professionisti della sicurezza. Le aziende stanno nuotando in acque torbide e le protezioni adottate finora non sono più sufficienti..

Evitare la trasformazione digitale è impossibile. A tale scopo, è sufficiente ricordare il destino di aziende come Blockbuster e Borders, incapaci di adattarsi al cambiamento e alle relative implicazioni. Occorre piuttosto un cambiamento drastico in termini di approccio tecnologico e mentalità strategica. In questo documento si suggeriscono le best practice sviluppate dalle aziende che hanno adottato un approccio più maturo nei confronti della sicurezza. Occorre una nuova mentalità per sopravvivere in questo contesto ed essere in grado di rispondere agli attacchi.

UTILIZZO DI QUESTO DOCUMENTO

Il presente documento offre informazioni sulle caratteristiche e sulla maturità della sicurezza nel mercato, identificando alcune best practice per migliorare questo aspetto nella vostra azienda. Inoltre, il documento evidenzia gli elementi in grado di accelerare l'innovazione e aumentare maggiormente i livelli di maturità delle aziende. Infine, forniremo alcuni suggerimenti in grado di offrirvi un vantaggio rispetto alla concorrenza, informazioni provenienti da una ricerca condotta nell'estate del 2016 fra 500 responsabili della sicurezza in Francia, Germania, Italia, Spagna e Regno Unito.

SICHERHEITSREIFEGRAD VERGLEICHBARER UNTERNEHMEN

In base alla ricerca, condotta fra 500 responsabili della sicurezza, IDC ha suddiviso il mercato in cinque categorie di maturità, che è possibile ordinare in questo modo partendo dai livelli più bassi:

ad-hoc
opportunistic
repeatable
managed
optimised.

Le aziende si distribuiscono attraverso la tipica curva a campana indicata in figura 1.

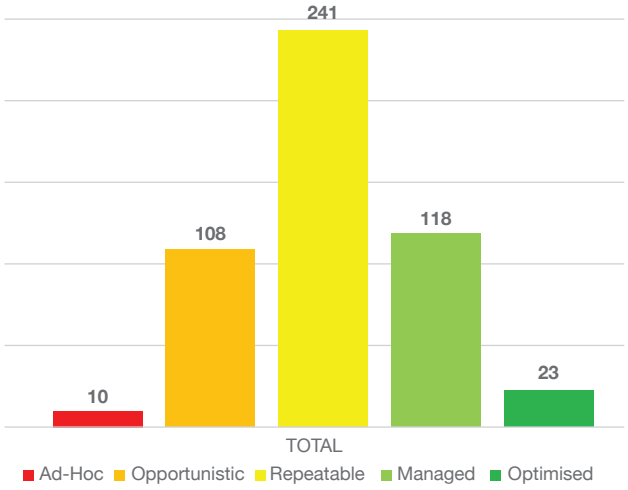

Figura 1

Source: IDC, 2016

Sono davvero poche le aziende che si trovano nella parte bassa del grafico dell'approccio alla sicurezza e un numero altrettanto esiguo di aziende si trova nella parte alta. Gran parte si trova invece in una posizione intermedia. Per nuotare in un mare infestato da squali, dovrete superare i concorrenti e adottare best practice adeguate. La sezione successiva del presente documento indicherà le best practice più efficaci per il settore della sicurezza.

BEST PRACTICE DI SICUREZZA

Tradizionalmente, le tecnologie della sicurezza ambivano a proteggere le aziende dalle minacce conosciute. È possibile tenere sotto controllo questo tipo di minacce collocando dispositivi, applicazioni e dati alle spalle della rete di sicurezza costituita da firewall, controlli perimetrali dei dispositivi e livelli di rete. Tuttavia, esistono due tendenze in grado di rendere insufficiente questi modelli di sicurezza preventiva come unico sistema di difesa:

- La trasformazione digitale sta spostando applicazioni e dati aziendali fuori dal perimetro aziendale e dalla visibilità e dal controllo da parte dei team di sicurezza interni alle aziende.
- Le minacce hanno raggiunto una dimensione senza precedenti. Ogni giorno vengono create oltre un milione di nuove varianti di malware, rendendo impossibile identificare velocemente le minacce e sviluppare difese tradizionali in grado di contrastarle.

In poche parole, occorrono nuovi approcci aziendali per identificare e rispondere alle minacce sconosciute, nonché per bloccare quelle note. Occorre una sicurezza proattiva in grado di individuare i potenziali indicatori di compromissione e porre rimedio alla situazione senza attendere un attacco palese. Ciò richiede un cambiamento radicale in termini di mentalità relativa alla strategia di sicurezza. A tal scopo, viene fornita un'analisi degli elementi che limitano l'efficacia della sicurezza in base ai livelli della maturità, consultabile in figura 2.

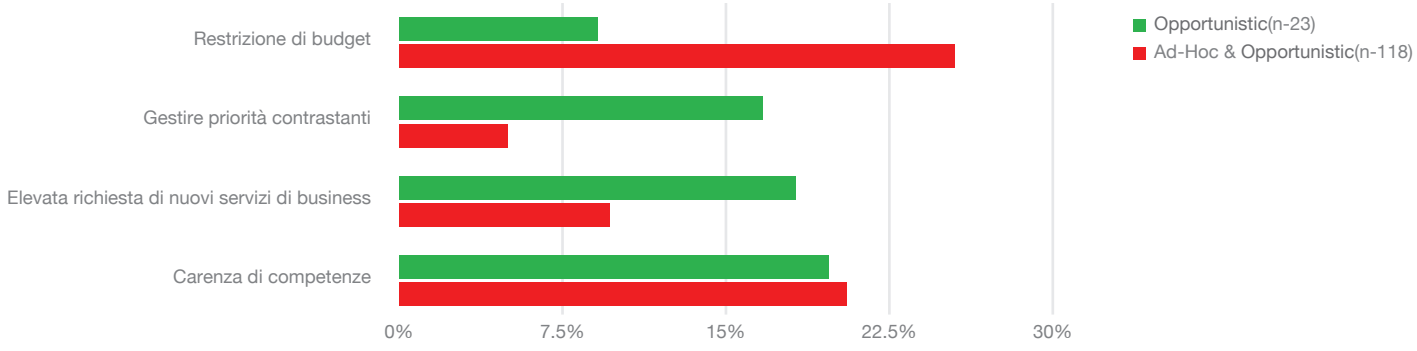

Figura 2

Source: IDC, 2016

Alcuni elementi comuni riguardano tutti i livelli di maturità. In particolare, costi e disponibilità di competenze rappresentano i limiti principali. Ciò non rappresenta una sorpresa alla luce della carenza globale e persistente di competenze nel settore della sicurezza. Tuttavia, è importante valutare le preoccupazioni generate dalla disponibilità di informazioni relative alle best practice.

Le pressioni economiche e le lacune in termini di competenze sono i problemi principali per le aziende con livello di maturità inferiore. Invece, ai livelli caratterizzati da una maggiore maturità, le aziende vantano un equilibrio ottimale fra i suddetti settori e argomenti come la gestione delle priorità in conflitto e il supporto della domanda di nuovi servizi aziendali. Ciò evidenzia un importante cambio di passo in termini di mentalità: le best practice della sicurezza devono prendere in considerazione le esigenze aziendali.

Una volta compiuto questo passo, le aziende devono analizzare il significato di tutto ciò in termini di approcci concreti alla sicurezza, soprattutto per quanto riguarda l'abbandono dei modelli di sicurezza reattivi in favore di quelli proattivi. All'atto pratico, come indicato nella figura 3, esistono due tendenze legate alla maturità delle imprese. La maturità è direttamente proporzionale all'implementazione e alla pianificazione delle tecniche di natura proattiva e inversamente proporzionale all'utilizzo di metodi di sicurezza non proattivi.

Adozione di una sicurezza proattiva in base al livello di maturità

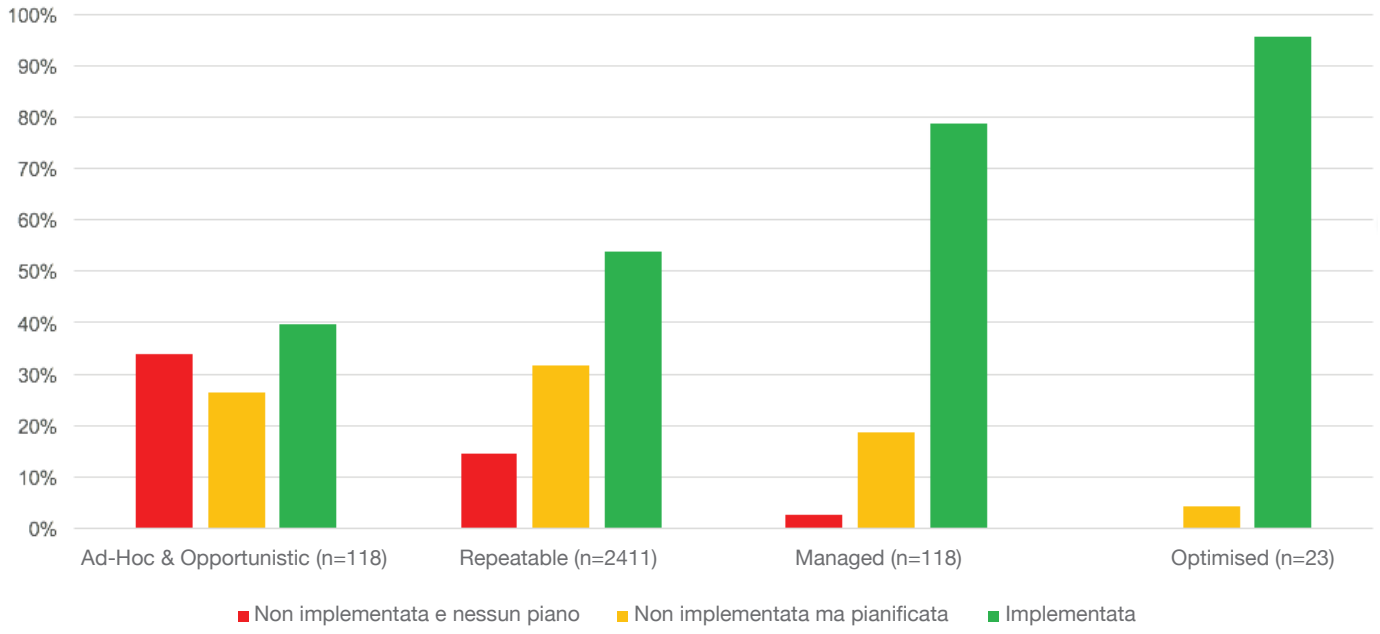

Figura 3

Source: IDC, 2016

Secondo la ricerca, le principali tecnologie di sicurezza aziendali in grado di agevolare l'approccio proattivo comprendono la threat intelligence, l'intelligenza artificiale e l'analisi euristica del comportamento degli utenti. Quanto più una azienda impiega tecnologie come l'intelligenza articificiale e gli algoritmi euristici, tanto più può dirsi matura nella gestione della sicurezza.Anche se gli approcci di sicurezza proattivi consentono di aumentare il livello della maturità in termini di sicurezza, si tratta di tecnologie che comportano anche una serie di problemi.

Ad esempio, le tecniche proattive richiedono la raccolta e il monitoraggio dei registri comportamentali e operativi su una scala molto più ampia. Alla luce delle pressioni sulle risorse finanziarie subite dai team di sicurezza, occorre intavolare una discussione sulle tecniche in grado di ridurre il carico delle risorse interne. Secondo le best practice, esistono due modelli potenziali.

OUTSOURCING

Anche se la sicurezza delle aziende è un aspetto complesso, la tendenza generale è indirizzata al controllo interno di questo elemento. Le motivazioni che spingono a questo tipo di approccio sono diverse. Per le aziende appena nate, la sicurezza viene considerata un'attività critica: qualsiasi tipo di esternalizzazione potrebbe ridurre la visibilità e il controllo dei team interni sulla sicurezza. I service provider di sicurezza gestita (Managed security services provider, MSSP) hanno dispensato grandi promesse non sempre rispettate. Infine, i team di sicurezza interni potrebbero considerare l'utilizzo di fornitori di terze parti come un'ammissione del proprio fallimento e un riconoscimento dell'impossibilità di svolgere questo compito in maniera autonoma.

Tuttavia, in un mondo totalmente connesso, le imprese non possono contrastare le minacce in maniera indipendente. Ciò vale soprattutto per le imprese europee dotate di risorse limitate in termini di sicurezza e quando le terze parti offrono un supporto eccellente attraverso modelli di erogazione industrializzati, su scala globale e con personale di elevata competenza. Pertanto, i MSS diventano un aspetto molto importante per le aziende che intendono applicare best practice di sicurezza.

Anche se in grado di ridurre le pressioni sulle risorse interne aziendali,i MSS non sono l'unica risposta possibile al problema. Secondo le ricerche IDC, al posto dell'esternalizzazione totale è consigliabile bilanciare erogazione interna e MSS in modo da soddisfare gli obiettivi aziendali e il profilo di rischio di un'impresa. La presenza di risorse interne per la gestione della sicurezza è un elemento importante per la conoscenza dell'impatto strategico delle decisioni aziendali sulla sicurezza (e viceversa). Essendo sempre più legata alla gestione dei rischi e alle organizzazioni nel loro complesso, la sicurezza è divenuta una caratteristica essenziale delle best practice per la gestione aziendale e delle metodologie di protezione.

AUTOMAZIONE

Oltre ai MSS, l'automazione è un altro modello chiave a disposizione delle aziende per ridurre la pressione sulle risorse e compensare lo squilibrio fra trasformazione digitale ed evoluzione del panorama delle minacce. L'automazione consente di gestire e implementare operazioni di sicurezza gestibili attraverso soluzioni tecnologiche. Il coinvolgimento del personale interno aiuta a conservare la visibilità e il controllo della sicurezza.

Questo processo avrà conseguenze con l'affermazione dell'intelligenza artificiale e del cognitive computing a livello di sicurezza in modo da ridurre ulteriormente la pressione sulle risorse e demandare il processo decisionale alle macchine. Tuttavia, almeno per il momento, le best practice richiederanno ancora una certa supervisione umana per garantire il funzionamento delle macchine o l'esclusione dei dispositivi automatizzati dalle decisioni più importanti.