CRITTOGRAFIA PERVASIVA

Un nuovo paradigma per la protezione

INTRODUZIONE

> *"Sono un hacker professionista da più di 15 anni. Vado alla ricerca dei problemi di cybersecurity nella tecnologia per rendere quest'ultima più sicura. Ma dopo averlo fatto per tanti anni, mi sento frustrato. Vedo sempre gli stessi problemi. Non ci sono miglioramenti. E nonostante facciamo sempre più affidamento sulla tecnologia, questa diventa sempre meno sicura."*
>
> Cesar Cerrudo, professional hacker e CTO di IOActive Labs

Il volto mutevole dell'informatica riflette il modo in cui le organizzazioni e le persone si connettono, in misura sempre più ampia, tramite Internet.

Tutte le organizzazioni sfruttano la tecnologia, anche una pompa di benzina che accetta pagamenti con carta di credito. La necessità di incorporare dati e processi protetti non è più un requisito per le sole grandi aziende, ma è diventata una componente tecnologica essenziale per organizzazioni di tutte le dimensioni. La sicurezza in un mondo virtualizzato, connesso a Internet e orientanto al cloud come quello odierno, è una sfida crescente e complessa per le *aziende*, non solo per l'IT.

Proteggere il ciberspazio è molto difficile. L'espansione a livello globale delle sedi da cui possono operare i criminali è la sfida meno impegnativa. La crescente integrazione tra ciberspazio e mondo fisico ha creato molte più opportunità per furti, danneggiamenti e alterazioni. Gli obiettivi emergenti si moltiplicano con lo sviluppo di nuove associazioni tra il mondo cibernetico e quello fisico. Ridurre le vulnerabilità e minimizzare le conseguenze nelle complesse reti cibernetiche sono due obiettivi sempre più difficili da raggiungere.

Il trend è in fase di accelerazione e le sfide si fanno imponenti. L'approccio base alla sicurezza si sta dimostrando poco adeguato rispetto alla natura aggressiva dell'ambiente. Occorre un cambio di paradigma e occorre farlo presto.

Solitaire Interglobal Ltd. (SIL) monitora gli aspetti del business e della sicurezza da più di 21 anni. La raccolta di informazioni mediante Global Security Watch (GSW) offre continuamente informazioni sulle tendenze e sui rischi a migliaia di organizzazioni. Per creare in modo efficace una panoramica globale e completa dei rischi e delle opportunità offerte, SIL guarda alla sicurezza in modo olistico. Questa visione include un'ampia prospettiva della sicurezza, focalizzata su quattro aree principali. Queste possono essere classificate, in genere, come:

- Dati: accesso (lettura, copia) o manipolazione[1]
- Sicurezza dei processi: capacità di eseguire, ostacolare, manomettere

[1] *La sicurezza dei dati include una qualche forma di accesso alle informazioni aziendali, come la lettura o l'acquisizione di una copia di contenuti specifici. La manipolazione dei dati di un'azienda si ha quando le informazioni vengono modificate o eliminate per cambiarne il contenuto e alterare la relazione di attributi ed entità.*

- Area architetturale: proprietà intellettuale, come modello di business, struttura del processo, metadati
- Area fisica: accesso alle sedi fisiche o alle attrezzature[2]

Per formare le basi di questo recente studio, SIL ha analizzato i dati di ricerca provenienti da organizzazioni reali, integrandoli con informazioni dettagliate su minacce e sicurezza tratte dal Global Security Watch (GSW). Non sorprende che i cambiamenti nei tipi, nell'ambito e nella velocità delle minacce negli ultimi anni continuino ad accelerare a livelli mai visti prima.

GSW è un servizio per associati che ha seguito l'evoluzione dettagliata delle minacce alla sicurezza e del loro effetto sulle imprese, su base mondiale, per 21 anni. Attualmente raccoglie le informazioni riportate da più di 8,9 milioni di organizzazioni. I dati forniti da GSW rappresentano una fonte approfondita di informazioni sulle minacce da una prospettiva di business che fornisce input allo studio, costruita sulla base di informazioni provenienti da situazioni reali. Sebbene GSW raccolga l'impronta delle minacce e altri meccanismi dettagliati, l'attenzione principale riguarda l'impatto sull'attività aziendale, sulle risorse organizzative e sui costi di prevenzione e correzione.

Riepilogo dei risultati

Un riscontro significativo dei dati di GSW, integrati da oltre 62.000 analisi mirate sulla sicurezza, effettuate da SIL negli ultimi due anni, è che, sebbene alcune organizzazioni siano a conoscenza delle incursioni di sicurezza, molte invece non lo sono, o lo sono solo parzialmente. Inoltre, oltre il 91,3% delle organizzazioni esaminate non erano a conoscenza delle ramificazioni complete del crimine informatico perpetuato, a cui erano sottoposte. Tutte le revisioni e le analisi richieste da queste organizzazioni hanno dimostrato che l'ambito delle vulnerabilità è stato ignorato o solo parzialmente riconosciuto dalle funzioni di business della loro organizzazione. La scoperta più sorprendente è stata che la gran parte di queste organizzazioni *non era a conoscenza del numero totale di incursioni effettive*[3] nei loro sistemi.

Aumentando il pericolo, molte di queste incursioni non si sono limitate a un singolo episodio, ma hanno aperto la porta della sicurezza per un periodo di tempo significativo. Un esempio può essere visto analizzando un riepilogo pubblicato circa le violazioni HIPAA fino al dicembre 2015.

> *"Più del 10% delle 1.135 principali violazioni HITECH, al 17 ottobre 2014, erano continue e non attribuibili a eventi univoci, con un periodo che andava da più di 1 giorno a 2.891 giorni. Analizzando questi dati più in dettaglio, è stato scoperto che:*
> *-- 4 violazioni sono durate più di 2.000 giorni*
> *-- 7 violazioni sono durate tra 1.000 e 1.500 giorni*
> *-- 10 violazioni sono durate tra 500 e 1.000 giorni*
> *-- 35 violazioni sono durate tra 100 e 500 giorni."*

Fonte: Melamedia, LLC analysis of Office of Civil Rights Data, 2015

Periodi estesi in presenza di incursioni attive possono avere un effetto decisamente negativo sull'operatività aziendale. Le aziende possono soffrire di una riduzione

---

[2] *In questo documento non tratteremo la sicurezza fisica.*

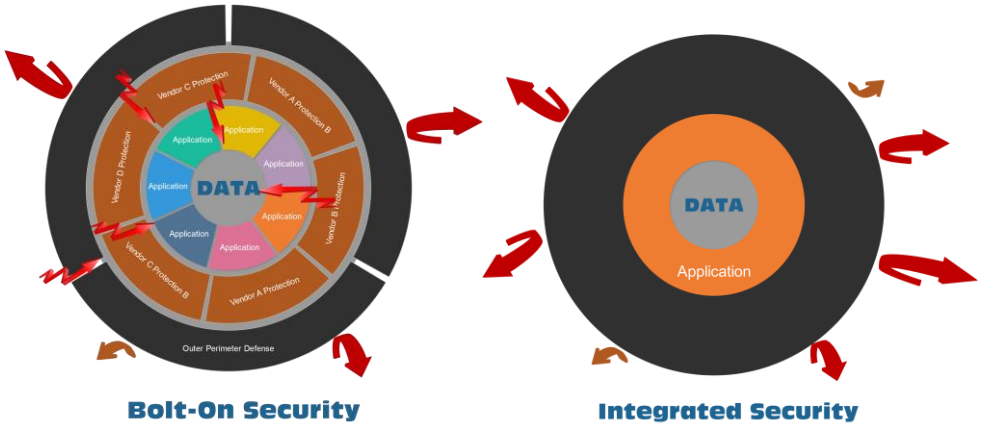
[3] *Le incursioni vanno a buon fine nel panorama IT aziendale e comprendono l'intrusione o la violazione iniziale e ogni successivo furto, distruzione o blocco (dati, ricerca o acquisizione, DoS ecc.).*

media del 16,2%-63,7% nei profitti lordi e nella valutazione, nel caso in cui le incursioni durino più di 3 mesi.

Con l'accelerazione della distribuzione del cloud, l'aumento delle applicazioni rivolte verso l'esterno espone l'infrastruttura organizzativa a una base di utenti più ampia e meno controllata. Le mutevoli esigenze del mercato spingono le organizzazioni ad adottare cicli di progettazione e implementazione più rapidi. Ciascuno di questi nuovi set di utenti, ciascuna nuova applicazione, aumenta la possibilità che un'incursione di sicurezza vada a buon fine.

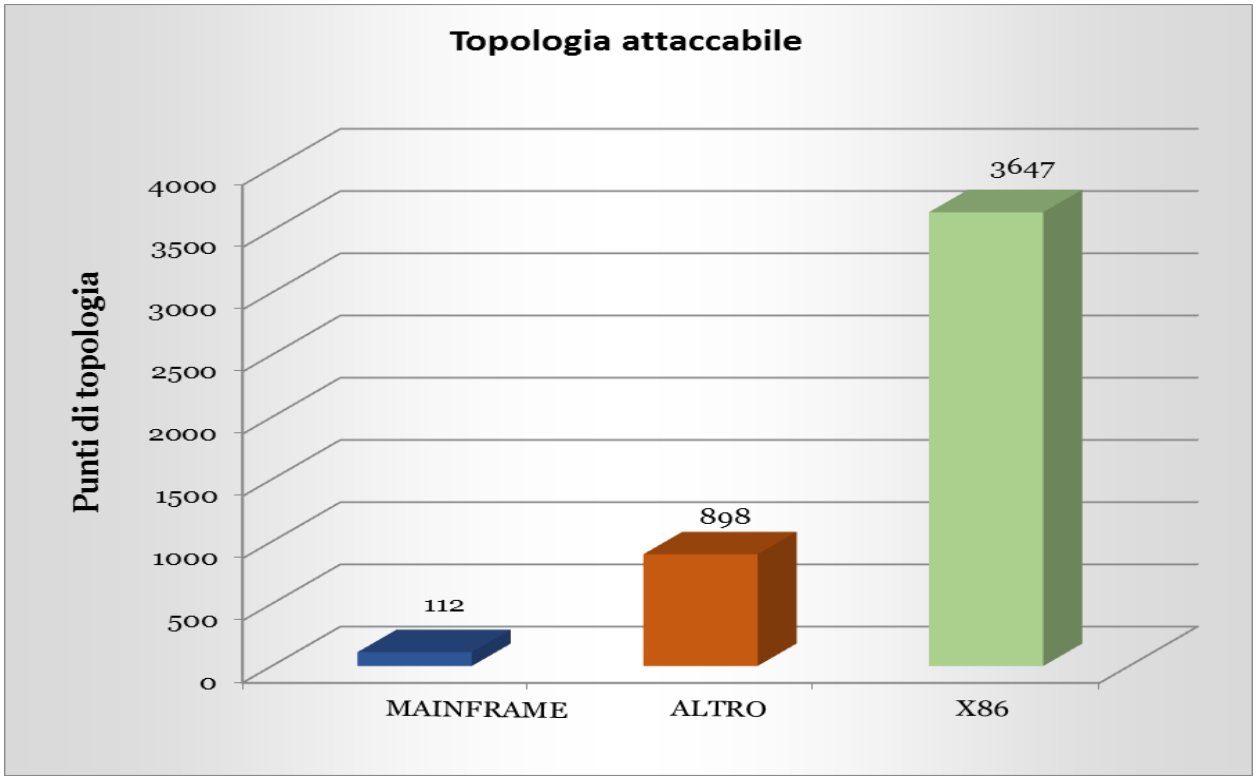
Quando la reattività tattica include l'aggiunta di strati di sicurezza e di salvaguardia, l'architettura risultante inizia a somigliare a una cipolla, con strati su strati, destinati a fornire sicurezza aggiuntiva. Tuttavia, in realtà, i livelli stessi possono creare ulteriori punti di topologia attaccabili.

Ciascun punto in cui una soluzione parziale viene collegata a un'altra rappresenta un obiettivo in più per un hacker esperto. Più complessi sono i livelli, più attaccabile risulta la topologia. Questa vulnerabilità fa parte di un profilo di rischio di sicurezza, che viene utilizzato sempre più dalle compagnie di assicurazione, per determinare l'esposizione di un'organizzazione a danni informatici significativi.



L'aumento nell'utilizzo di software di virtualizzazione pone maggiormente l'enfasi sulla sicurezza. Ognuna di queste macchine virtuali (VM) crea nuovi punti di vulnerabilità e aumenta la complessità della sfida riguardante la sicurezza. Poiché sempre più organizzazioni adottano e sviluppano soluzioni di cloud ibrido, la crescente domanda di pratiche di sicurezza reattive e resilienti deve crescere ed evolversi di pari passo.

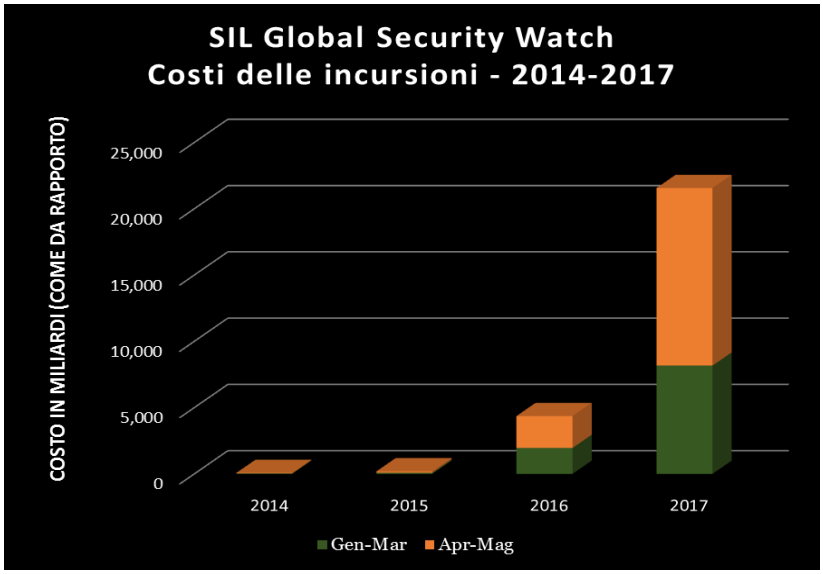
La topologia attaccabile varia molto tra le diverse architetture di base. Un'analisi generale di un gruppo composto da oltre 115.000 aziende ha illustrato questa differenza, come possiamo vedere qui.

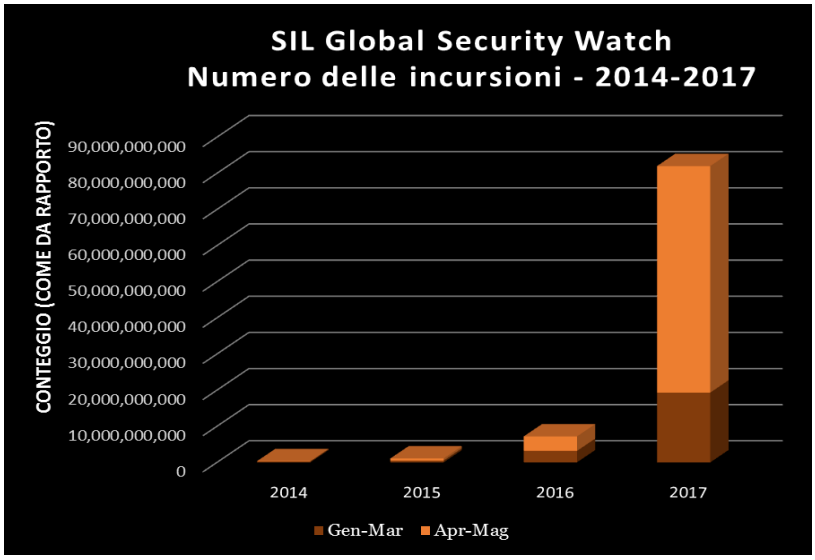


Questa differenza significativa deriva dalla struttura di base e dalla strategia realizzata dietro l'architettura della piattaforma, dal design dei chip, dal sistema operativo, dal metodo di integrazione degli stack.

Un'analisi dettagliata delle incursioni segnalate negli ultimi quattro anni mostra l'aumento esponenziale del numero di incursioni e dei costi associati ai danni.

Nota: SIL raccoglie dati su implementazioni di produzione reali. Ciò fornisce un punto di vista reale, piuttosto che teorico, delle pratiche operative, dei comportamenti e delle metriche, che non sono soggette a dichiarazioni dei fornitori o benchmark artificiali.





Non è solo il numero degli attacchi a essere cambiato. Negli ultimi 20 anni, è cambiato notevolmente anche il volto delle incursioni. Se due decenni fa la sicurezza aveva a che fare principalmente con il controllo degli accessi, oggi la topologia delle minacce è molto più complessa.

Uno dei vettori di minaccia in più rapida crescita è l'attacco ransomware. In questo tipo di attacco, l'incursione blocca file, directory e altri componenti del sistema. Al proprietario viene chiesto di pagare per ottenere un codice di sblocco, che non sempre funziona.

> *"Quest'anno siamo stati colpiti da 5 grandi ondate di problemi di sicurezza. Alcuni erano malevoli, altri pure estorsioni. Abbiamo speso più di 1 milione di dollari per ripristinare i nostri web server e ancora non siamo sicuri di come gli hacker siano riusciti a raggiungerli. Gli attacchi ci sono costati clienti, molto tempo e denaro. Non è una bella sensazione, proprio per niente."*
>
> CFO - Azienda manifatturiera di medie dimensioni

Confronto delle piattaforme di sicurezza

La misurazione della sicurezza è di tipo riflessivo, in quanto viene valutata in base all'assenza di disagi e problemi. Le falle di sicurezza sono molto visibili, mentre il successo passa inosservato. Per costruire una comprensione delle metriche riflettenti associate alla sicurezza, IBM ha chiesto a SIL di condurre indagini, raccogliere dati ed eseguire analisi, per fornire una chiara comprensione dei vantaggi e dei relativi costi che si possono vedere, quando le organizzazioni implementano la piattaforma mainframe IBM Z nella loro architettura IT, rispetto ad altre architetture di piattaforma. Questa analisi è stata rivolta principalmente al valore della sicurezza dal punto di vista del business, affinché chi ha il ruolo di fornire le direttive aziendali possa comprendere il vantaggio delle offerte IBM Z security nella valutazione delle soluzioni di sicurezza.

Durante questo studio, sono state esaminate attentamente le principali caratteristiche comportamentali del software e dell'hardware attraverso un gran numero di sistemi reali di clienti (più di 9.602.000). Tutti questi clienti hanno implementato la sicurezza nell'ambito dei loro ambienti di produzione, ma con diverse combinazioni di metodi e meccanismi di security. Sono comprese organizzazioni tenute a supportare standard regolamentati e di mercato per la sicurezza delle informazioni, come HIPAA, PCI, SOX ecc. Le informazioni contenute nei report sui clienti e la massa di dettagli realmente reperibili sono preziosi, in quanto forniscono una comprensione realistica, piuttosto che teorica, per come l'uso di diversi tipi di sicurezza possa influire sul cliente.

Oltre 81 milioni di data point su attività di incursione dettagliate e l'impatto di GSW forniscono una base di costo e di esposizione prevedibile, fondamentale per comprendere la sicurezza e la protezione degli asset nel mercato di oggi.

Nella raccolta e nell'analisi dei dati oggetto di studio, sono state estrapolate diverse caratteristiche. Queste caratteristiche influenzano la capacità, l'efficienza e l'affidabilità dell'ambiente protetto. Inoltre, è stata esaminata la sinergia fra sicurezza e operazioni di business. Il comportamento rappresentato è stato proiettato e modellato in opzioni possibili per la distribuzione. Per creare questa comprensione, occorre molto più delle pure e semplici performance di un server, poiché la sicurezza deve proteggere, senza ostacolarli, i processi e le operazioni aziendali. Anche se i requisiti di capacità e gli effetti del throughput dei sistemi di sicurezza sono importanti, la loro possibilità di tradursi in termini di business è più in linea con il mercato odierno. La prospettiva di business comprende una miriade di fattori, tra cui affidabilità, livelli di sicurezza, livelli di personale, costo totale della sicurezza (compreso il ripristino) e altri effetti. Questo si collega direttamente alle decisioni che responsabili IT, CTO e direzione aziendale devono prendere ogni giorno.

Prospettive e visioni

Dall'analisi emergono due categorie di prospettive e visioni. La prima prospettiva è correlata alle rispettive categorie di attività e prestazioni, che includono:

- Efficienza operativa
- Efficacia della sicurezza
- Rischio per l'IT
- Resilienza e agilità

Ciascuna di queste aree apre le porte a un altro livello di prospettiva. All'interno di questo livello, l'importanza e l'attenzione differiscono in base alla parte dell'organizzazione che sta valutando le sfide e le ramificazioni della sicurezza. Ci sono due campi principali in questa struttura di sensibilizzazione e responsabilità, uno di business e uno tecnico. Mentre il lato tecnico è la visione tipica della creazione e della gestione della sicurezza, il crescente ambito della sfida e il cambiamento dei vettori della criminalità informatica hanno spostato la responsabilità primaria della sicurezza al business.

In ultima analisi, l'IT è progettata per supportare le funzioni di business. Una delle fonti primarie dei dati di studio è la visione della sicurezza da parte della gestione aziendale di un'organizzazione, sia a livello dirigenziale che di line-of-business. I modelli di funzionamento delle organizzazioni oggetto di studio sono raggruppati in tutte le quattro aree di confronto, per identificare la loro influenza sulle metriche di business. Ognuna di queste metriche di business ha una differenziazione misurabile e significativa quando viene analizzata la soluzione di sicurezza di IBM Z, che dovrebbe essere presa in considerazione nel pensiero critico dell'organizzazione.

Nello studio sono rappresentati anche gli aspetti tecnici della sicurezza. Il fatto che queste siano responsabilità più tradizionalmente appartenenti all'IT, non riduce la loro importanza in un mondo di cybersecurity in evoluzione.

Molte delle categorie propongono risultati che riguardano sia il punto di vista del business che quello tecnico. La complessità del punto di vista, dell'autorità, delle necessità del business e della responsabilità, sono elementi tipici della sfida molto complessa che oggi le organizzazioni si trovano ad affrontare. Questo studio fornisce un'articolazione basata sui dati di alcuni dei componenti di questa sfida.

Le metriche granulari sintetizzate per tipo di piattaforma nello studio mostrano come un criterio di successo specifico sia diverso nella popolazione generale degli implementatori. Queste metriche sono ampie in copertura e toccano aree di considerazione finanziaria, nonché di qualità organizzativa. Sono presentate con brevi definizioni e con l'effetto netto focalizzato dell'implementazione di ciascuna piattaforma. Per essere utili in una gamma di settori diversi, tutte devono essere normalizzate su base di unità di lavoro[4] e categorizzate in livelli per dimensione aziendale (piccola, media, grande e molto grande). La misura di base è stata definita in base all'azienda media, in modo che tutte le altre metriche si basino su una variazione da quel setpoint standard. Le implementazioni incluse in questo studio sono state limitate a quelle in produzione.

EFFICIENZA OPERATIVA

L'efficienza operativa è la capacità di un'impresa di consegnare prodotti o servizi ai propri clienti o partner nel modo più redditizio, garantendo al contempo standard di qualità elevati. L'efficienza operativa può essere considerata come il rapporto tra l'input per eseguire un'operazione aziendale e l'output guadagnato dall'impresa. Quando si migliora l'efficienza operativa, il rapporto di input/output diventa più favorevole. Gli input sono tipicamente basati sul denaro (costo), sulle persone (numero di dipendenti oppure Full Time Equivalent, FTE) o su tempo e sforzi.

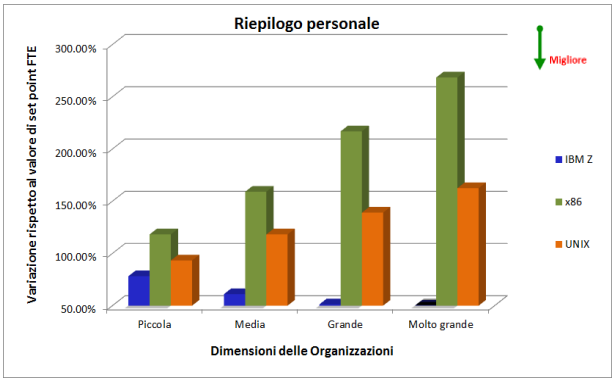
Quando la sicurezza viene vista da una prospettiva di efficienza operativa, i contributi sono tratti da queste aree specifiche. La difficoltà nel misurare l'efficienza operativa della sicurezza deriva dalla sua forma incorporata. L'analisi di SIL ha esaminato diverse aree di importanza distinte, tra cui:

- Carico di personale
- Spese mirate attraverso aggregazione del TCO
- Carico di lavoro

In queste aree, occorre trattare sia le informazioni aziendali che quelle tecniche. Tuttavia, le metriche derivate dai dati formano modelli diversi per la valutazione del business rispetto a quella tecnica. Le misure permettono ai diversi gruppi di strategizzare e controllare aspetti della sicurezza che si allineano con gli obiettivi appropriati per la loro responsabilità organizzativa.

PERSONALE

Un fattore sottostante che si palesa in molte altre aree è l'efficienza dell'interfaccia tra l'amministratore della sicurezza e l'infrastruttura. Comprende componenti software, hardware e sistemi operativi, e il conseguente effetto sui livelli di personale. Con l'aumento dell'efficienza dei livelli di personale, aumenta la produttività. Lo sforzo necessario per eseguire lo stesso compito nell'ambito della sicurezza è diminuito in modo tale che ogni membro del personale di sicurezza è più produttivo.



[4] *La base di unità di lavoro è stata definita utilizzando gli standard pubblicati dell'International Function Point User Group e si basa sull'analisi dei punti funzionali (FP).*

L'efficienza di tutti i componenti specifici che forniscono tale influenza sulla user experience è difficile da suddividere in metriche diverse da confronti eccessivamente dettagliati, che perdono di efficacia in virtù del grado di dettaglio. Una visione generale dei gruppi di sforzo del personale in FTE è stata riesaminata per fornire una metrica generale per il confronto tra le piattaforme. La media complessiva per lo sforzo del personale di sicurezza è stata inclusa nel grafico come un'altra misurazione di confronto. Questa media aggrega tutti i report, indipendentemente dalle dimensioni.

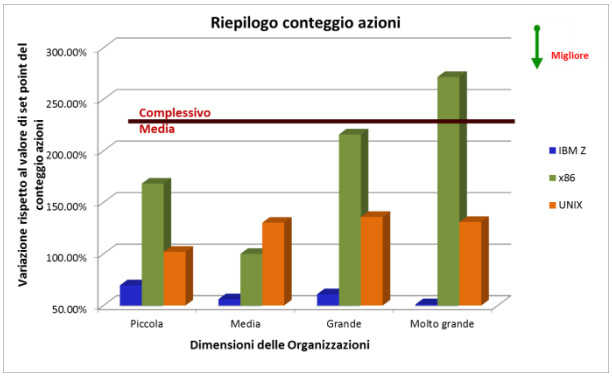
I livelli di sforzo messi a confronto sono quelli necessari per mantenere un ambiente "gold standard" per ogni gruppo di sistemi operativi. Il carico di lavoro sui sistemi è stato normalizzato a livelli identici per mantenere lo stesso campo di confronto di livello definito nei precedenti confronti. Il set point per il confronto è il valore mediano del campo complessivo rispondente, poiché per i componenti di sicurezza sono disponibili moltissime opzioni.

> *"Rispetto a tre anni fa, sulla piattaforma z (sic) eseguiamo il quadruplo del lavoro. Nel frattempo abbiamo due persone in meno, ma le persone rimaste riescono ancora a gestire tutto il lavoro.*
>
> *Se mettiamo questo valore a confronto con l'aumento negli altri gruppi di piattaforme, dovremmo avere almeno dieci volte il numero di persone attuale per gestire il carico."*
>
> CIO - Grazie azienda di servizi finanziari

Poiché diverse architetture di sicurezza hanno set diversi di standard di implementazione, è importante tenere in considerazione il rigore di questi standard quando si esaminano i livelli di personale. Il livello di personale di sicurezza notevolmente inferiore per la distribuzione e l'utilizzo di IBM Z è direttamente attribuibile alla natura integrata dello stack operativo Z. Questo è particolarmente importante quando un'organizzazione cresce o se un'organizzazione sta seguendo un percorso verso un modello di consegna di servizi cloud. IBM Z richiede l'88,35% di tempo di personale in meno rispetto alle altre alternative.

Una parte fondamentale di questa efficienza operativa è rappresentata dal numero di attività manuali e dal tempo necessario per eseguire tali attività. Le attività conteggiate e temporizzate sono quelle che devono essere attuate dal personale di sicurezza al fine di raggiungere lo stesso livello di due diligence, attività proattiva e modifiche reattive. Per comprendere appieno le differenze tra le piattaforme, SIL ha ricevuto informazioni dettagliate di acquisizione di video e azioni da oltre 620 clienti. Questi dati sono stati assemblati in un quadro di tempistiche e attività, analizzati per rilevare catene causali e efficienze, utilizzati per costruire un confronto degli sforzi richiesti dalle diverse piattaforme. I dati di confronto vengono normalizzati per fornire un campo di gioco uniforme, come discusso altrove in questo documento. Il confronto di attività e tempistiche risultante può essere visto nei seguenti grafici.

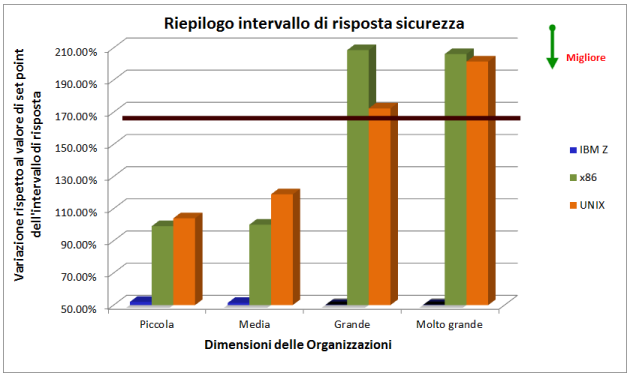
Le attività di sicurezza variano in modo significativo in base alla piattaforma sottostante e alle dimensioni dell'organizzazione. In generale, più grande è l'organizzazione, più complesse ed eterogenee dovranno essere le pratiche di sicurezza. Il tipo di piattaforma aggiunge un'altra dimensione a questo sforzo in aumento. Confrontando il numero di base delle azioni che devono essere eseguite per mantenere gli standard di sicurezza, il



numero di attività che devono essere eseguite manualmente dal personale di sicurezza IBM Z è sostanzialmente inferiore a quello degli altri gruppi di piattaforme. Gli studi su tempo e movimento mostrano che le soluzioni di sicurezza Z richiedono l'*81,17%* di attività in meno per implementare livelli di protezione standard. L'incorporazione di meno attività nelle responsabilità del personale, ne aumenta in modo significativo la produttività. Consente anche di ridurre il livello di FTE da mantenere nell'arena della sicurezza, richiedendo un numero notevolmente inferiore di cambiamenti di contesto, elemento che a sua volta riduce il rischio.

"I security technical officer responsabili delle nostre piattaforme Z hanno il tempo per completare tutte le loro attività, comprese quelle proattive. Questo non vale per coloro che supportano i nostri ambienti UNIX e Wintel. E il motivo non è una differenza di dedizione o di tempo. Semplicemente, è più semplice ed efficiente proteggere Z che non le altre piattaforme."

Direttore della sicurezza - Azienda manifatturiera di medie dimensioni



Vi è un'influenza corrispondente sugli intervalli di tempo necessari per realizzare obiettivi di sicurezza. Il grafico mostra l'impatto sui tempi di risposta per le modifiche di sicurezza. Questa metrica mostra l'agilità della sicurezza intrinseca associata ai gruppi di piattaforme. I tempi di risposta più bassi qui documentati indicano una risposta più veloce, che nel mondo della sicurezza significa ridurre al minimo i danni di un'incursione. Gli intervalli di tempo inclusi in questa somma sono quelli che fanno parte della normale progettazione, manutenzione e comportamento proattivo. Le attività e gli intervalli che fanno parte dell'indagine sulle incursioni non sono inclusi in questa visualizzazione.

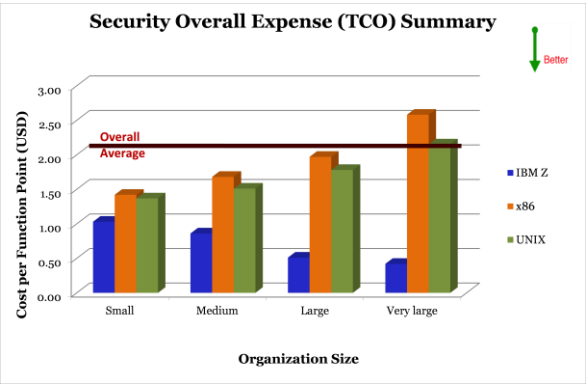
L'intervallo di attività per le normali attività gold standard per il personale di sicurezza dimostra che esistono notevoli vantaggi, sotto l'aspetto dei livelli di personale, per le implementazioni di Z. Le stesse attività standard su Z consumano fino all'*81,66%* di tempo in meno rispetto a quelle eseguite su altre piattaforme.

"La sicurezza sul mainframe è l'area meno problematica nella nostra organizzazione. Spesso ci dimentichiamo di avere un gruppo di sicurezza sul mainframe, in quanto ci causa i minimi problemi."

CIO - Gruppo finanziario di medie dimensioni

COSTO TOTALE DI PROPRIETÀ

Il costo totale di proprietà (TCO) fornisce una delle principali metriche aziendali per l'efficienza operativa. Questa metrica di alto livello aggrega tutte le spese all'interno dell'organizzazione che contribuiscono a qualsiasi aspetto dell'implementazione della protezione. In questa parte dell'analisi dello studio sono riassunte tutte le spese che hanno contribuito alla protezione degli asset. La sicurezza fisica è esclusa, ma tutti



gli altri aspetti sono inclusi. Ancora una volta, i progetti e le relative spese sono stati normalizzati secondo la base standard. Ciò consente di mettere a confronto in modo più preciso le piccole e grandi organizzazioni, e le relative spese.

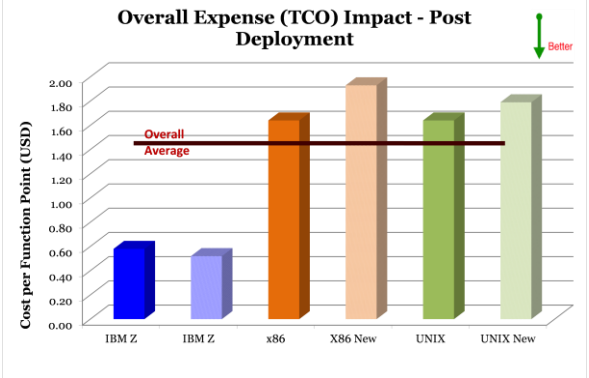
L'isolamento del TCO per la pratica di sicurezza è impegnativo in quanto la sicurezza è sempre più incorporata in tutti gli aspetti delle operazioni dell'organizzazione. Normalizzando il TCO in base a una definizione di unità di lavoro standard, come i punti funzione, è possibile effettuare un confronto accurato ed evidenziare il trend. I modelli di spesa mostrano tendenze crescenti per alcuni tipi di piattaforme, in quanto la complessità dell'implementazione cresce. Questo è un trend contraddittorio per IBM Z. Un andamento decrescente della spesa unitaria si traduce nell'efficienza di scala, in cui lo sfruttamento del quadro e della base consente di ottenere un modello economico di investimento finanziario. Come si evince dal grafico di accompagnamento, la spesa per le implementazioni di sicurezza Z sono ridotte fino all'83,72% rispetto a quelle delle altre piattaforme. Questo deriva parzialmente dalla combinazione di base di sicurezza architettata e piattaforma altamente scalabile. L'efficienza di questa sinergia è dimostrata dal fatto che, mentre si carica più pesantemente l'architettura, si ottnere un calo notevole nel costo dell'unità di lavoro. Questa situazione si ha ogni volta in cui l'architettura è progettata per ambienti altamente scalabili, ma si nota più generalmente solo nell'hardware. In questo caso, la comunanza di progettazione per la scalabilità è presente sia nell'hardware fisico che nel sistema operativo.

> *"Il nostro mainframe IBM ha un costo molto inferiore rispetto alle altre attività che effettuiamo come azienda. Negli ultimi tre anni i costi si sono abbassati, nonostante il nostro reparto finanziario continui a dirci che sono troppo alti. Io ribadisco che il costo complessivo è inferiore perché abbiamo meno problemi, meno personale e meno probabilità di incappare in problemi."*
>
> CFO - Distributore di grandi dimensioni

La scalabilità architettata è particolarmente importante quando i sistemi diventano più complessi, ad esempio quando aumentano gli utenti, il BYOD prolifera, oppure vengono implementate applicazioni cloud estese e ad accesso multiplo. L'escalation nell'adozione del cloud e l'aumento della distribuzione delle applicazioni nel cloud hanno reso più difficile mantenere una sicurezza reattiva. La forma dell'implementazione del cloud condiziona anche le sfide di sicurezza. Che il cloud distribuito sia privato, pubblico, di comunità o ibrido, le pratiche di sicurezza devono evolversi costantemente.

I vantaggi del bilanciamento del controllo e dell'accessibilità per l'uso di cloud ibridi sono stati meglio compresi e l'adozione di questa forma di distribuzione cloud ha reso il cloud ibrido l'opzione di implementazione più diffusa. Esso rappresenta uno degli scenari più complessi per la sicurezza poiché devono essere protette tutte le architetture della piattaforma.

Nelle situazioni in cui la sicurezza viene gestita con una serie di componenti di protezione addizionali o quando la principale governance della sicurezza risiede esclusivamente nell'applicazione distribuita, il confronto della spesa complessiva s'innalza significativamente con l'aggiunta di nuovi servizi. Nel seguente grafico è illustrato questo tipo di effetto. I progetti inclusi in questa parte dell'analisi mostrano l'impatto a breve termine dell'acquisizione di sicurezza. In tutti questi casi, queste 16.027 organizzazioni hanno aggiunto un'unica applicazione cloud alle



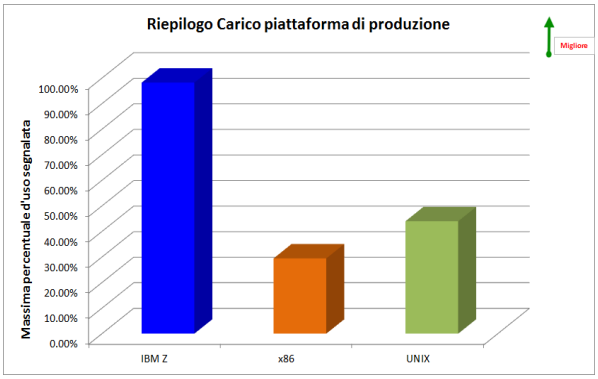
implementazioni cloud esistenti. Le implementazioni hanno interessato cloud privati, pubblici e ibridi e sono state progettate per più di 1.000 utenti.

Il TCO basato sui punti funzione mostra la differenza di spesa a breve termine presente al momento dell'acquisizione. L'impatto sul costo complessivo delle unità di lavoro mostra l'influenza sul business che la tecnologia presenta. Il carico di lavoro aggiuntivo ha permesso alla distribuzione IBM Z di diffondere un costo stabile per la sicurezza su un numero maggiore di punti funzione, senza aggiungere alcuna spesa significativa. Altri gruppi di piattaforme richiedevano ulteriori spese per quanto riguarda le licenze ecc. L'impatto medio prima della singola distribuzione aggiuntiva del cloud riduceva le implementazioni di Z in media del *14,02%,* mentre le altre piattaforme mostravano un aumento fino al *19,62%*. Il grafico riepilogativo illustra la media per ciascuno dei gruppi architettonici. I dati sottostanti per i singoli progetti sono notevoli in quanto nessuna delle implementazioni IBM Z ha mostrato un aumento di TCO per punto funzione, anche se due di esse hanno mostrato un impatto nullo. Le altre architetture hanno dimostrato risultati individuali con un aumento compreso tra il *2,9% e il 38,4%*. Il modello di impatto è significativo se viene preso in considerazione nel contesto di un'attività in espansione che mira al cloud, espandendo i dispositivi utente distribuiti e affrontando importanti nuove offerte di servizi.

La comunicazione del costo e dell'impatto effettivo della sicurezza rappresenta un'altra sfida. L'articolazione di un business case per i miglioramenti e le espansioni della sicurezza è un tema di discussione frequente, nonché oggetto di contestazione da parte dei professionisti della sicurezza in tutto il mondo. L'impatto dei costi della sicurezza come aspetto dell'efficienza operativa non è chiaramente compreso dalla maggioranza dei dirigenti aziendali. In un pool di dati raccolti nel 2015 e 2016, che comprendeva oltre 9,5 milioni di dirigenti aziendali, meno dell'11% aveva visto un business case per le spese di sicurezza. Meno dello 0,9% di queste persone ha affermato di comprendere la derivazione di costi di sicurezza, economie di scala e spese proiettate. Purtroppo, meno del 35% delle persone responsabili per le decisioni aziendali strategiche riteneva che il proprio personale di sicurezza comprendesse come proiettare o calcolare i costi. Tutto ciò contribuisce a una situazione in cui la riduzione o l'aumento delle assegnazioni dei costi dei carichi di lavoro sono inaspettate e non apprezzate. Alla luce di questa mancata visione, la direzione esecutiva non riesce a comprendere l'efficienza scalabile delle implementazioni di sicurezza di IBM Z.

CARICO DI LAVORO

La misurazione del TCO è, principalmente, una metrica aziendale. Include le caratteristiche fondamentali della scalabilità dell'architettura per espandere e sfruttare meglio la spesa. Tuttavia, la metrica si riferisce alla scalabilità e alla resilienza nella sua forma grezza. La gestione delle risorse di sicurezza si basa sul controllo del tempo impiegato dal personale e sul costo incorporato dell'infrastruttura e del software necessario per mantenere la pratica di sicurezza. L'architettura scalabile e resiliente della piattaforma costituisce la base per un utilizzo efficiente del tempo e del denaro. Una piattaforma più scalabile consente di eseguire meno progetti di implementazione e aumentare notevolmente la capacità delle risorse IT necessarie per sostenere l'attività. Pertanto,



una piattaforma altamente scalabile che richiede poche attività per distribuire un carico di lavoro aggiuntivo aumenta l'efficienza operativa del gruppo di servizi IT.

Una dimensione della scalabilità e della resilienza di distribuzione è il livello al quale può essere caricata un'architettura di base, prima di ottenere prestazioni poco affidabili e poco omogenee. La capacità di utilizzare una percentuale più elevata della capacità teorica massima di una macchina si traduce in una riduzione dei costi e dei rischi. Il carico massimo di produzione, riportato dal gruppo oggetto di studio, è stato utilizzato per articolare la fiducia dei responsabili dell'esecuzione di operazioni senza intoppi, nella capacità della piattaforma di mantenere un carico di lavoro. I carichi di lavoro che hanno raggiunto un livello superiore, ma che sono durati meno di 10 minuti, sono stati omessi da questa analisi.

> *"Quando ci avete chiesto come funzionano normalmente i nostri sistemi, non solo abbiamo inviato i dati ma in realtà li abbiamo anche analizzati. Non mi sono reso conto che il carico medio sulle nostre piattaforme Wintel era inferiore al 14% mentre il nostro mainframe funziona costantemente al 98% o oltre. Non ho mai capito fino a che punto questa piattaforma fosse più efficiente. In qualche modo avevo dato per scontato che tutti i sistemi funzionassero allo stesso livello. D'ora in poi guarderò meglio quale applicazione viene ospitata, e dove."*
>
> COO - Grande organizzazione del settore sanitario

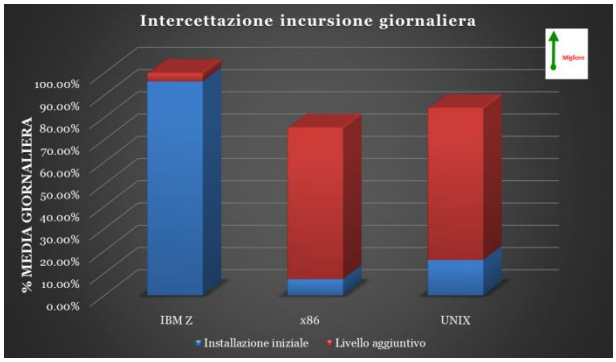
EFFICACIA DELLA SICUREZZA

Per esaminare l'area di efficacia della sicurezza, SIL ha trovato confronti misurabili in una combinazione di metriche oggettive e soggettive. Le metriche oggettive comprendevano la capacità delle misure di sicurezza di catturare e prevenire incursioni, sia quelle segnalate che quelle rilevate dagli audit dettagliati. Le informazioni contenute in questa misurazione si applicano sia al lato tecnico che a quello business di un'organizzazione, in quanto la quantità di incursioni può essere tradotta, in gran parte, nell'effetto che hai sui profitti.

Ognuna di queste aree fornisce una certa differenziazione, fondamentale per la soluzione di cybersecurity IBM Z.

RESISTENZA ALLE INCURSIONI

La principale metrica sul successo della security è il numero di incursioni catturate, neutralizzate o a cui è stato impedito di causare qualsiasi forma di danno. Le incursioni aggregate in questa metrica non includono quelle bloccate da firewall e da dispositivi di sicurezza aggiuntivi. Sono state coneggiate invece solo quelle bloccate dalla soluzione di sicurezza presente sulla piattaforma. Questi numeri sono stati normalizzati dal conteggio reale di VM residenti su una piattaforma, poiché ogni VM rappresenta un'entità logica separabile. Questa è una metrica indicativa poiché non è stata effettuata nessuna modifica per il numero di utenti all'interno di ciascuna VM.



Il livello di blocco delle incursioni fornito dall'installazione iniziale per ciascuna delle piattaforme costituisce la base per qualsiasi protezione aggiuntiva richiesta o installata. Questo grafico

mostra la sicurezza fornita dall'installazione iniziale e dal livello supplementare, espressa in percentuale di incursioni che sono state bloccate. Sulla base delle installazioni iniziali, le soluzioni di sicurezza IBM Z di base hanno fornito fino a *13,21 volte* il livello di intercettazione rispetto alle piattaforme alternative. Inoltre, la soluzione Z fornisce una base, una protezione fondamentale che supera il 92,1%, anche senza gli elementi supplementari necessari per le architetture alternative.

I livelli aggiuntivi di protezione sono applicazioni aggiuntive, tattiche e tecniche ecc., che variano da organizzazione a organizzazione, ma basate sulla sorveglianza, sulla posizione e sulla governance individuale della sicurezza. Livelli più elevati di requisiti di security supplementari indicano un aumento degli sforzi da parte del software e del personale di sicurezza.

La combinazione di capitale intellettuale e servizi automatizzati, unitamente al design architetturale delle soluzioni di sicurezza informatica IBM Z, comporta l'intercettazione di una percentuale significativamente maggiore di incursioni. La piattaforma Z fornisce un'intercettazione delle incursioni di base fino al *20,74%* migliore della sicurezza combinata della base aumentata con sforzi (estesi, competenti e rigidi) per tattiche, tecniche e procedure di sicurezza supplementari fornite dalle piattaforme alternative.

Ulteriori informazioni sull'efficacia della soluzione di sicurezza richiedono un'analisi più approfondita. I servizi di sicurezza iniziano con la base dell'architettura, che include tutti i componenti hardware, software e middleware. Su di essi vi sono, a livelli, le politiche organizzative, le procedure, la posizione e la governance. Mentre questi elementi possono essere misurati rispetto alle migliori pratiche correnti e considerati come aspetti di differenziazione chiave, questo studio si basa sull'esame delle soluzioni di fornitori che combinano hardware, software e middleware per piattaforme, compresi i sistemi operativi.

> *"Non ho idea del perché ci siano meno problemi di sicurezza con la piattaforma z. So semplicemente che non ne abbiamo. Il personale di sicurezza continua a raccontarmi di questo e di quello, ma il succo è che tutto funziona. L'ultima volta che abbiamo avuto un problema con la sicurezza su quella piattaforma, abbiamo scoperto che qualcuno aveva rubato la password di qualcun altro. L'ultima volta che ho avuto un problema su una piattaforma diversa è stato circa un'ora fa. Chiedetemi quale preferisco!"*
>
> CIO - Distributore di grandi dimensioni

La natura della sicurezza incorporata di Z è notevolmente diversa da quella creata con soluzioni di protezione addizionali. Con un più ampio gruppo di interfacce da mettere in sicurezza, la protezione dei dati e dei processi aziendali è più vulnerabile quando viene definita a livello di dispositivo. Una strategia più efficace attira il controllo e la definizione delle politiche verso un punto più centralizzato. Lo stack di sicurezza Z integrato e incorporato fornisce un notevole vantaggio in questo settore.

Un altro fattore di complessità, pertinente a un esame dell'efficacia comparativa della sicurezza, è l'aumento del mobile computing. Con la crescita esponenziale delle connessioni e degli hotspot pubblici, un contributo crescente al rischio di sicurezza deriva dalle politiche, dalla governance e dall'efficacia di questi punti di accesso sconosciuti. Se la soluzione di sicurezza è progettata per essere distribuita, anziché amministrata centralmente, il profilo di rischio dell'applicazione e dei suoi dati aumenta in modo significativo. In questo tipo di topologia sempre più comune, la soluzione Z presenta vantaggi architetturali. Per queste implementazioni flessibili, il

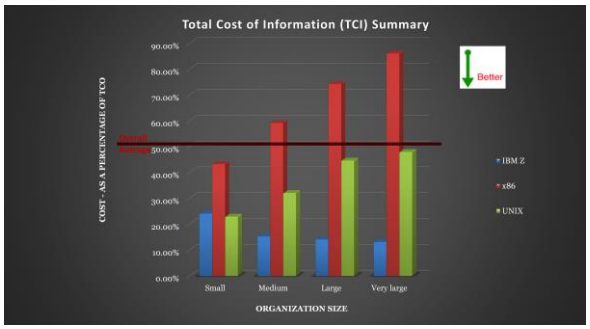
profilo di rischio SIL imposta il livello di rischio della piattaforma Z a meno di 1/20 di una delle soluzioni alternative.

COSTI E SPESE

I costi connessi alla sicurezza includono sia la metrica tradizionale del TCO, che la metrica più recente del costo totale delle informazioni (TCI), che fornisce una visione espansa dei contributi di costo all'interno di un'organizzazione Il TCO è composto dalle spese necessarie per operare in continuità. Le categorie di costo in questa metrica comprendono il personale operativo dell'IT, il supporto applicativo, i servizi esterni per completare il personale operativo o risolvere i problemi, le spese di alimentazione e raffreddamento, la manutenzione, le licenze hardware e software e lo spazio fisico.

Il TCI è una metrica che ridefinisce le spese organizzative per quanto riguarda il sostegno e la protezione delle risorse organizzative dell'IT e della proprietà intellettuale (IP). Queste includono dati, processi aziendali, ricerca, struttura applicativa e altre proprietà intellettuali. Le spese incluse in questa metrica includono l'infrastruttura che tiene e distribuisce le risorse, il personale, l'alimentazione, il raffreddamento, le misure di sicurezza ecc., che mantengono le attività protette e in esecuzione. Questa metrica tiene conto degli impatti negativi della perdita e dei danni delle IP e delle opportunità perse, ad esempio per DoS e tempi di inattività. La metrica che meglio riflette l'impatto e l'influenza della sicurezza IT all'interno di un'organizzazione è il TCI, in quanto crea una comprensione della metrica riflettente della sicurezza.

Quando si esamina il TCI per diverse architetture, ci sono diversi modi per riassumere le relative caratteristiche. Poiché esiste un'ampia varianza nelle dimensioni delle implementazioni delle infrastrutture, il riepilogo basato sul valore complessivo di risorse IT e IP è statisticamente vago. Una base di confronto normalizzata esprime il TCI come percentuale del TCO. I risultati di questa analisi sono mostrati nel grafico.



Le implementazioni di IBM Z mostrano fino all'*84,83%* di riduzione del TCI su un'ampia gamma di aziende di dimensioni diverse. Poiché questa metrica è un fattore di spinta chiave per i nuovi costi di implementazione, il fattore più basso rafforza l'efficienza nella scalabilità tipica delle implementazioni Z. Il confronto sul TCI include il costo della disponibilità, l'effetto delle incursioni e le metriche di inattività, in modo tale che non sia necessario tenere conto di una vista aggiuntiva. Il differenziale tra le soluzioni si basa in gran parte su tre contributi, nelle aree dei:

- Costi del personale
- Costi dovuti agli effetti dell'incursione
- Componenti aggiuntivi all'architettura dell'infrastruttura

I costi per il personale e l'infrastruttura sono auditabili, mentre il costo degli effetti delle incursioni è una combinazione di importi oggettivi e soggettivi proiettati. In tutti i casi, i costi sono tratti direttamente dai report dei clienti e non sono stati modificati, ma semplicemente aggregati e mediati in tutta la base di studio.

I costi associati alle configurazioni di sicurezza IBM Z sono inferiori alle opzioni di protezione x86 e UNIX, sia sulla base delle spese tradizionali, che sui costi riflettenti dovuti a incursioni. Ciò rappresenta la differenza tra stack di sicurezza altamente integrati rispetto alle aggiunte tipiche di altre architetture, che creano maggiore suscettibilità e vulnerabilità.

FATTORI DI RISCHIO DI SICUREZZA

Il rischio di sicurezza può essere definito come il potenziale con il quale una determinata minaccia sfrutta con successo le vulnerabilità di un processo, o di un asset, o di un gruppo di attività, causando danni all'organizzazione o ai clienti che serve. Viene misurato come combinazione della probabilità del verificarsi di tale evento e delle relative conseguenze. SIL crea i profili di rischio che sono costruzioni attuariali utilizzate per fornire una visione consolidata del rischio complessivo di un'organizzazione. Questo include il contributo del rischio individuale proveniente da applicazioni, interfacce, strutture di gestione, aspetti di social engineering ecc. Ai fini del profilo del rischio in una distribuzione di sicurezza, le principali dimensioni del profilo di rischio sono:

- Pool sperimentale dell'attività di incursione
- Costi di incursione
- Esposizione

Il nuovo scenario nel mondo dell'IT ha dettato un cambiamento di prospettiva per chiarire le opzioni dal punto di vista della gestione. Alcuni degli effetti delle incursioni segnalati dai clienti sono:

- Perdita di servizio
- Perdita del cliente a causa della mancanza di fiducia
- Modifiche non strategiche all'architettura
- Recupero di dati mancanti o danneggiati
- Perdita di capitale intellettuale esclusivo

Questi effetti hanno elementi di probabilità e costi e si riferiscono direttamente alle pratiche di sicurezza organizzativa.

> *"Diversi attacchi ci hanno allontanato dai clienti, hanno comportato elevati costi di correzione e hanno avuto altre influenze assai negative. Questa esperienza ci ha fatto perdere la fiducia da parte dei clienti. Stiamo spostandoci velocemente verso un MSP che esegue parte del workload su un grande mainframe, visto che sembra essere l'unico posto sicuro in cui lavorare in questi giorni".*

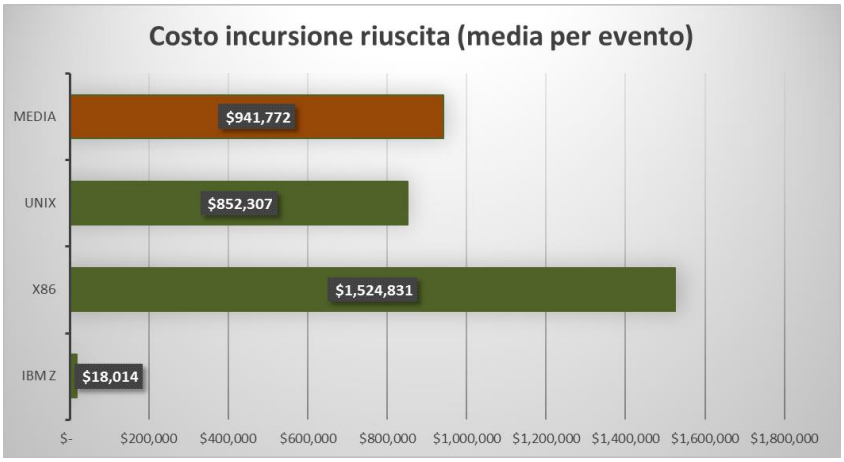
Direttore - Azienda di distribuzione di medie dimensioni

COSTI DI INCURSIONE

L'incursione può essere definita come un ingresso riuscito nel panorama di un'organizzazione. Questo ingresso può assumere la forma di un furto, una distruzione o un blocco. Le attuali protezioni devono coprire una varietà più ampia di punti di accesso rispetto a quelli necessari per la sicurezza, a livello dell'intera piattaforma. In questa situazione, deve essere in atto il controllo di tutti gli aspetti dell'elaborazione. Molte installazioni governative e sicure richiedono protezione per l'assegnazione e la gestione delle principali sfere dell'IT: I/O, accesso alla rete, gestione della memoria e accesso generale.

In alcuni casi di incursioni di sicurezza, i costi per un'organizzazione possono richiedere molto tempo per essere valutati. Un esempio di ritardata realizzazione dell'impatto è quando viene rubata una ricerca di proprietà. La perdita dell'IP esclusivo può avere un impatto significativo sul mercato.

La media dei costi associati a un'incursione indica l'esposizione relativa alle diverse tecnologie. Purtroppo, nel mercato si è creato un clima di "perdita accettabile", a causa dei costi medi di tutta la moltitudine di incursioni minori. Questo ha creato un precedente di negligenza nella definizione e nel controllo della sicurezza, che ignora l'esposizione reale alle incursioni più grandi e più gravi. Quando un'organizzazione è condizionata a tollerare perdite "gestibili" ripetute, lascia le sue informazioni e le sue attività in uno stato vulnerabile e maturo per danni maggiori.



Il costo medio di un'incursione sta aumentando, così come la velocità di tale aumento. Una parte di ciò deriva dall'ampliamento delle applicazioni in cloud, dove più persone e dati possono essere influenzati da incursioni durante ciascun periodo di tempo. L'altro fattore da considerare è che i responsabili delle incursioni stanno migliorando e diventando più aggressivi nei loro attacchi. Ciò indica un crescente livello di minaccia che dovrebbe essere preso in considerazione quando si selezionano componenti IT.

Il costo medio di un'incursione è influenzato da una moltitudine di caratteristiche. La velocità e l'efficacia del rilevamento, la capacità di isolare l'incursione affinché non provochi ulteriori danni, il livello approfondito di correzioni ecc., sono tutti fattori che influenzano l'impatto finanziario generale.

Il costo per incursione sostanzialmente più basso per la piattaforma Z dimostra la sinergia di tutti questi fattori. Nel complesso, la correzione sulle implementazioni di sicurezza Z è in media del *98,82%* inferiore rispetto alle piattaforme alternative. Da un punto di vista leggermente diverso, le organizzazioni spendono in media *84,65 volte* di più per risolvere i danni delle incursioni su piattaforme diverse da IBM Z.

Il costo necessario per ottenere diversi livelli di sicurezza è notevole. Per comprendere questi fattori, le diverse forme di sicurezza possono essere suddivise in livelli di controllo:

- Aziendale normale
- Processi riguardanti carte di credito
- Banking
- Sanità
- Ricerca
- Difesa

Basandosi su funzionalità ed elementi di controllo critici, fattori ponderati in modo uniforme, le diverse piattaforme forniscono una copertura di sicurezza riepilogata nella tabella seguente. Questa configurazione esamina solo le funzionalità di protezione fornite con l'installazione iniziale, poiché le opzioni aggiuntive possono essere applicate a qualsiasi configurazione di protezione.

Sicurezza coperta in modo nativo per piattaforma

Descrizione del livello di sicurezza	IBM Z	x86	UNIX
Azienda standard	100.00%	18.16%	30.26%
Procedura con carta di credito	99.00%	11.04%	18.28%
Settore bancario	94.00%	5.26%	10.22%
Settore sanitario	100.00%	3.24%	8.51%
Settore ricerca	92.50%	2.86%	4.16%
Settore difesa	85.54%	0.26%	1.86%

Durante le attività di studio separate, il SIL ha condotto una serie di analisi delle vulnerabilità su un gruppo di utenti casuali. In totale, sui clienti totali coinvolti nello studio principale, sono stati presi in analisi 14.625 utenti durante l'analisi delle vulnerabilità SIL. La maggior parte di quei clienti non sono consapevoli del fatto che i loro sistemi sono stati attaccati. In generale, alcune delle organizzazioni erano consapevoli delle violazioni della sicurezza. Tuttavia, la scoperta più straordinaria è stato il numero di organizzazioni soggette a violazioni della sicurezza senza che ne fossero al corrente. Durante questa serie di controlli casuali delle vulnerabilità, è emerso che 8.2061 organizzazioni erano state soggette a processi di estrazione da parte di soggetti estranei, che erano ancora attivi, rubando informazioni e influenzando i processi in tempo reale.

Il numero di incursioni rilevate è stato significativamente più elevato rispetto ai livelli inizialmente noti. Gli esiti di molte incursioni potrebbero non essere scoperti per molto tempo, specialmente fino a quando gli effetti del furto dell'IP non diventa evidente.

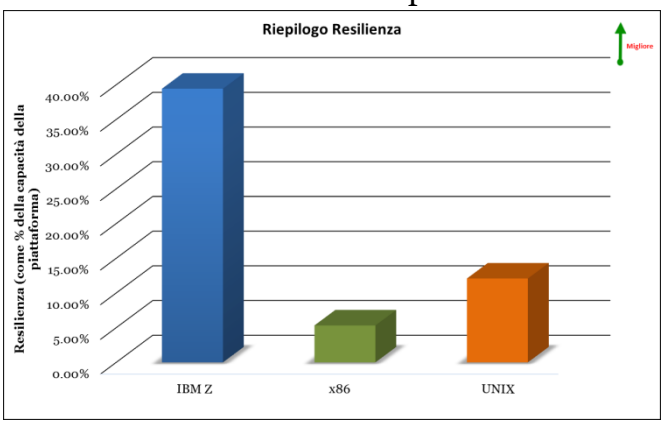
La longevità delle incursioni è cresciuta di pari passo con il crescente livello di sofisticatezza degli attacchi. Nell'analisi delle incursioni effettuate sugli utenti residenti, senza che questi sospettassero alcunché, citata in precedenza, è stata presa in analisi la longevità del tipo di attività criminale oggetto dell'attacco. È stato determinato che una percentuale superiore al 31,19% delle incursioni parassitiche esisteva da oltre due anni. Circa il 43.28% di tali incursioni era stato attivo per un periodo oscillante tra uno e due anni. Un altro 23,16% di tali attacchi era rimasto attivo sui sistemi per un periodo compreso tra tre e 12 mesi. Il resto dei casi emersi era suddiviso tra incursioni di breve durata e altri attacchi dei quali non era possibile stabilire la data di inizio, in quanto precedente all'adozione di misure di monitoraggio adeguate. Le implementazioni Z si sono fatte notare per non aver mai figurato nell'elenco delle piattaforme attaccate.

> *"Circa quattro mesi fa abbiamo acquisito un'azienda come parte del nostro impegno in ambito M&A. Una delle principali ragioni per cui abbiamo effettuato la fusione è stata quella di poter utilizzare alcuni dei loro IP. Subito dopo aver avviato la razionalizzazione dei sistemi, abbiamo scoperto che la piattaforma era stata infettata con numerosi spyware installati nei sistemi interni. Ora il nostro staff legale sta lottando per determinare se ciò può comportare la nostra uscita dall'accordo, in quando il valore dell'IP è stato messo in serio pericolo da queste minacce. Si tratta di un problema enorme.*
>
> CIO - Very Large Biologic Organisation

Questo tipo di vulnerabilità estese con attività criminali coperte comporta il massimo livello di esposizione per le organizzazioni. Capire gli effetti di tali minacce per le aziende è difficile quando queste vengono alla fine scoperte, in quanto il lungo periodo di esposizione alla minaccia lascia l'organizzazione aperta a perdite significative per la fiducia dei clienti, con il rischio di importanti azioni legali e processi di risanamento prolungati.

RESILIENZA E AGILITÀ

I principali fattori in una piattaforma orientata alla sicurezza sono la resilienza della stessa, che le consente di gestire livelli e forme di attacchi anche imprevedibili, unitamente alla velocità con cui il sistema reagisce ad attacchi e minacce emergenti. La resilienza dell'implementazione può essere vista come la capacità di gestire richieste di risorse impreviste senza alcun malfunzionamento della piattaforma nel suo complesso. Sono stati osservati casi estremi, con crash dei sistemi in caso di attacchi concentrati di tipo Denial Of Service (DoS). Le implementazioni più resistenti fanno affidamento su capacità ed elasticità di hardware e sistemi operativi. La resilienza è una metrica tipica nella valutazione dell'acquisto di hardware e dell'implementazione dei sistemi operativi. La tabella allegata mostra le valutazioni combinate relative ai livelli di resistenza dei gruppi della piattaforma. Il valore di resilienza indicato è il risultato dei risultati registrati e notificati dello sfaldamento dei punti di interruzione associati alla piattaforma di produzione utilizzata per lo studio. Il punteggio è espresso sottoforma di percentuale del carico di lavoro e rappresenta la quantità di coda generata e di stress tollerabile da algoritmi di invio, meccanismo di buffering e altri componenti, senza che ciò abbia influssi negativi sul funzionamento complessivo del sistema.

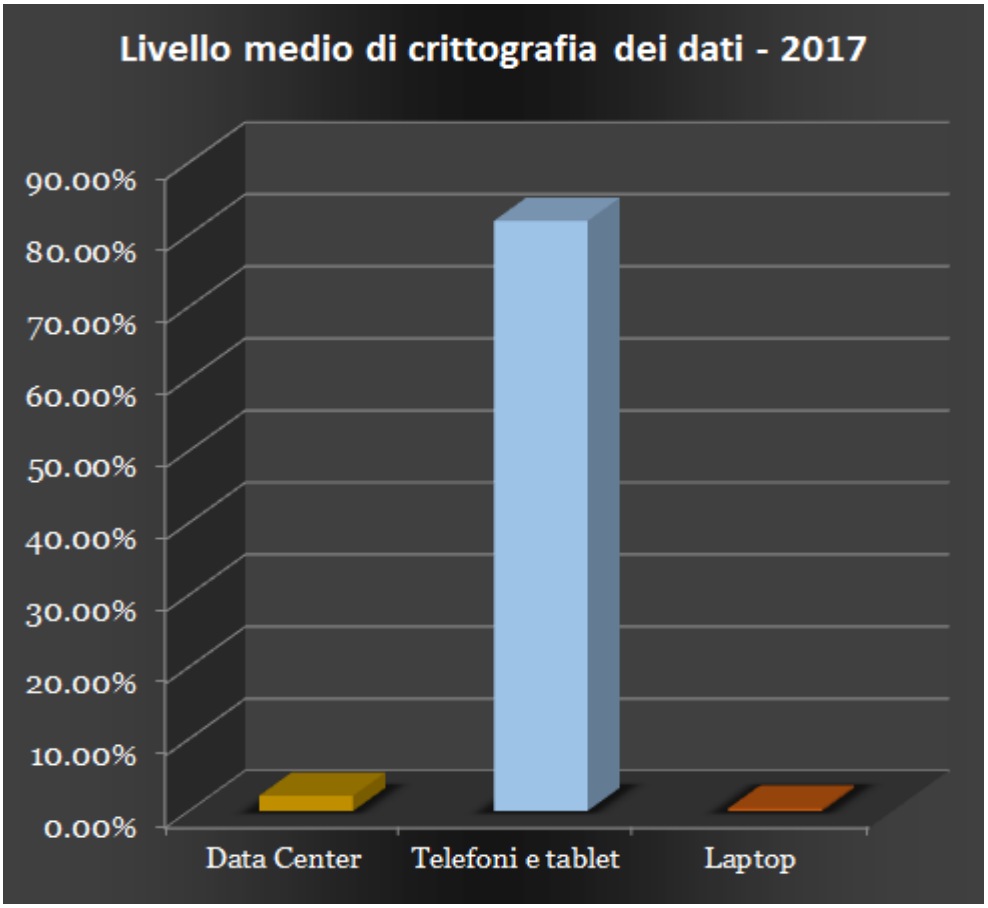


Esiste una sostanziale differenza tra la resilienza delle installazioni basate su dispositivi Z e le soluzioni concorrenti. La resilienza media fatta registrare dalle implementazioni IBM Z è fino a *7,41 volte* rispetto a quella delle altre opzioni. Ciò si traduce in una minore necessità di ricorrere a complessità tecniche per la soluzione IT, e ciò contribuisce a ridurre i TCO e i TCI citati nelle sezioni precedenti di questo articolo.

CRITTOGRAFIA PERVASIVA

I dati dei clienti e dell'azienda stessa rappresentano una risorsa chiave. Si tratta di una risorsa inestimabile, in quanto rappresentano l'elemento chiave che offre un vantaggio di mercato e costituisce il capitale intellettuale di ogni azienda. La crittografia ha rappresentato finora uno dei metodi principali per proteggere i dati in quanto, una volta crittografati, si eliminano tutte le vulnerabilità e la possibilità per gli hacker di accedere ai dati. Ma molte di queste risorse dati sono attualmente prive di qualunque protezione.

La prospettiva è differente in altre aree della comunicazione dati. La piattaforma per i dispositivi mobili è stata realizzata sulla base di un concetto di privacy che integrava la crittografia fin dalla fase iniziale di progettazione. Il confronto tra differenti livelli di crittografia è illuminante.



Questa scheda riepilogativa illustra le differenze di base tra l'approccio IT mainstream e quello adottato invece per le piattaforme di comunicazione mobile. Dal momento che l'industria delle telecomunicazioni ha compreso fin dall'inizio l'importanza della crittografia nel settore delle comunicazioni mobili, circa l'82% del traffico in transito su tale piattaforma è crittografato, mentre solo il 2,13% dei dati aziendali che risiedono nei data center è crittografato. L'assenza di crittografia sulle preziose risorse aziendali interne archiviate presso i data center o su computer portatili è costituisce una grave lacuna.

Secondo i dati di SIL GSW, meno del 3,5% degli 11,2 miliardi di dati violati durante gli ultimi tre anni erano protetti dalla crittografia. Di fatto, ciò significa che non appena il sistema viene violato, le informazioni in esso contenute sono totalmente vulnerabili agli attaccanti. La perdita di fiducia da parte di clienti e partner è comprensibile, dato che questa mancanza di lungimiranza può portare a gravi violazioni della privacy.

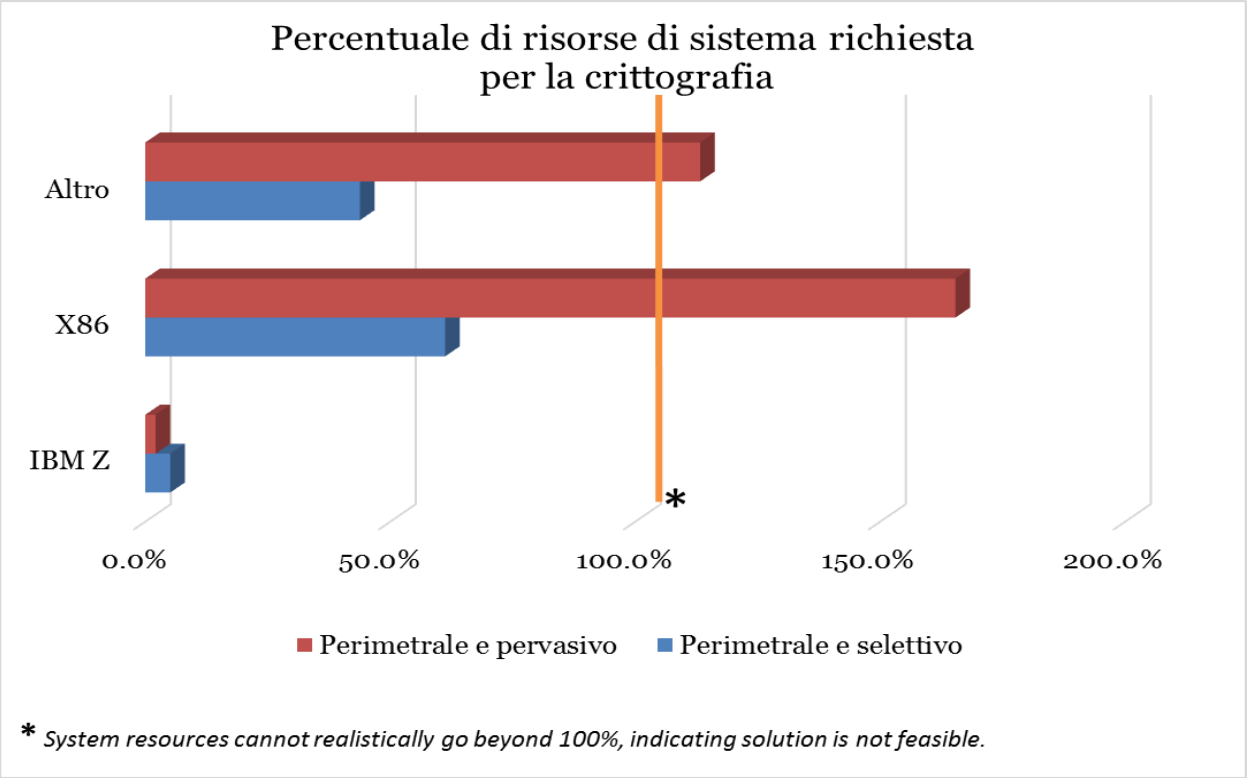
Esistono svariate ragioni che spiegano il ridotto utilizzo della crittografia. I costi in termini di tempo e capacità di sistema hanno incoraggiato le aziende a concentrarsi su tecniche di protezione del perimetro di sistema e sulla crittografia selettiva. Con le difese perimetrali che attualmente utilizzano fino al 61,2% della capacità complessiva della piattaforma, con una tendenza a crescere, è necessario passare a un cambio di paradigma.

Un recente progresso un termini di aspetti fondamentali relativi all'ambiente di elaborazione promette di fare una notevole differenza sul mercato. Il cambiamento risiede nella transizione dell'attuale crittografia utilizzata dai sistemi IBM Z, che passa da un modello selettivo a uno pervasivo. Questa significativa modifica nella struttura di base della piattaforma di elaborazione e gli effetti che essa sortirà sulla sicurezza, causeranno un effetto altamente disruttivo nel settore.

Il concetto di fondo non è quello di introdurre un livello decisionale che consente di scegliere se applicare o meno la crittografia. Invece, sarà possibile adottare la crittografia come funzione integrata all'interno dei normali processi di elaborazione.

L'assenza di decisioni associate alla crittografia selettiva costituisce un ulteriore risparmio in termini di costi complessivi e una riduzione delle complessità associate all'uso della crittografia nell'attuale contesto di mercato.

La principale barriera verso l'uso della crittografia su larga scala è finora stata rappresentata dal costo di tale tecnologia e dai carichi prestazionali che tale processo impone alle piattaforme di elaborazione. Tuttavia, secondo le organizzazioni che hanno elaborato lo studio, le soluzioni aggiuntive che sono state implementate, hanno causato una crescita tale della capacità di sistema, da richiedere fino al 61% del carico di sistema per il solo processo crittografico. Ciò si traduce in notevoli costi infrastrutturali, effetti negativi sulle prestazioni, ecc.



* *System resources cannot realistically go beyond 100%, indicating solution is not feasible.*

Gli attuali requisiti delle risorse crittografiche sono chiaramente illustrati in tabella sopra. La transizione verso la crittografia pervasiva mette in evidenza alcune delle differenze fondamentali in termini di architettura. Mentre le piattaforme Z sfruttano la loro capacità di crittografia pervasiva in blocco a costi ridotti, altre architetture evidenziano un significativo incremento in termini di costi operativi. Al fine di abilitare le architetture non Z per l'uso della crittografia pervasiva, sarebbe necessario implementare un'enorme topologia distribuita. Analizzando il carico medio per ciascuna piattaforma presa in esame dal gruppo di studio, l'implementazione richiederebbe un numero di server fino a ***12,2 volte*** superiore rispetto all'attuale numero.

Un tale incremento dei sistemi che compongono la piattaforma comporterebbe un sostanziale incremento dei costi operativi. Tutto ciò avrebbe un impatto notevole sulle organizzazioni che decidono di adottare questa soluzione, con un sostanziale incremento dei costi relativi ad hardware, software e personale. Questa soluzione consentirebbe di risolvere il problema relativo alla crittografia pervasiva, ma non risolverebbe comunque il problema associato alle architetture che richiedono il retrofitting con soluzioni aggiunte in un secondo momento.

Seppure non utilizzante le ultimissime tecnologie, l'architettura Z offre funzioni di crittografia che consentono di ottenere maggiore efficacia a fronte di costi ridotti. La soluzione offre un livello di protezione e sicurezza oltre ***8,5 volte*** superiore, con un ***costo inferiore del 93%*** in termini di costi complessivi, con una ***riduzione dello***

sforzo richiesto pari all'81%. Anche in questo caso di tratta tuttavia di crittografia selettiva, che comunque consente di mitigare almeno la disperata necessità di garantire la protezione dei sistemi.

L'impatto complessivo derivante dalla maggiore velocità del motore crittografico e dalla capacità di crittografare i dati in blocco da vita a una soluzione pervasiva, in grado di offrire una velocità ***18,4 volte superiore a 1/20 del costo delle altre soluzioni***.

Sebbene la crittografia pervasiva sia implementabile sui mainframe Z, attualmente tale funzionalità non può essere implementata in nessun'altra architettura. La più restrittiva architettura, associata alle soluzioni x86, richiederebbe una capacità 7,32 *volte* superiore rispetto all'attuale capacità richiesta per l'esecuzione dei carichi di lavoro necessari per utilizzare la crittografia pervasiva si un singolo server. I requisiti per questo tipo di soluzione richiedono numerosi miglioramenti di differenti aspetti di tali piattaforme alternative, tra cui quelli legati al design dei chip, agli elementi di base del sistema operativo e a quelli associati ad altre limitazioni di capacità interna della piattaforma. Tali progressi rappresentano cambiamenti a lungo termine in termini di design dei chip e dei processi di produzione, con tempi di implementazioni tipici di due o tre anni, a condizione che sia possibile creare la tecnologia di base richiesta.

Se tale obiettivo non viene raggiunto, allora non è possibile soddisfare le esigenze associate alle funzioni di crittografia pervasiva su tali piattaforme. I sistemi che risiedono su tali piattaforme continueranno a operare con profili di rischio ed esposizione elevati, richiedendo eccessive quantità di tempo da parte del personale, unitamente a elevatissimi costi e consumi di risorse organizzative.

L'applicazione della crittografia a livello pervasivo offre una significativa riduzione della percentuale della piattaforma da dedicare ai processi di sicurezza. Nel caso dell'organizzazione presa in esame in un recente studio SIL, è emerso che le aziende che adottano la crittografia pervasiva sulle piattaforme IBM Z possono conseguire una riduzione dei costi generali di elaborazione pari al 91,7%.

Inoltre, l'esposizione ai crimini informatici è oggi talmente elevata che la mutevole base di costo deve includere anche la sostanziale possibilità di attacchi informatici in grado di danneggiare le risorse aziendali.

Carichi di lavoro e velocità di reazione sono elementi fondamentali quando si tratta di sicurezza. Tanto rapidamente un'organizzazione è in grado di reagire alle minacce, quanto minore è la possibilità che gli attacchi riescano ad arrecare danni. La velocità di risposta è fattore chiave non solo al fine di evitare eventuali effetti avversi, ma anche per minimizzare l'impatto. Nel confronto tra crittografia selettiva e quella pervasiva, nell'ambito dello stesso studio, l'87,2% delle incursioni non avrebbe richiesto alcuna reazione, in quanto l'uso del modello basato sulla crittografia pervasiva avrebbe automaticamente mitigato gli effetti della minaccia.

E per gli attacchi avrebbero potuto richiede un'azione correttiva, la velocità di risposta si è dimostrata notevolmente superiore nel caso del modello basato sulla soluzione pervasiva. La ridotta complessità dell'architettura di sicurezza si traduce in un numero inferiore di comandi richiesti per risolvere lo stesso tipo di problema. Nei test, la velocità di risposta ha richiesto solo il 14,2% del tempo richiesto dal modello basato sulla crittografia selettiva.

Anche la porzione di topologia esposta agli attacchi viene ridotta. Con un numero inferiori di punti esposti ad attacchi all'interno dei vari layer, è possibile affrontare le minacce con un approccio più olistico e meno complesso. Tale ridotta complessità può anche ridurre significativamente il rischio di future intrusioni. La porzione di topologia esposta agli attacchi, misurata durante il test e comparata a quella di un gruppo di clienti di dimensioni piccole e medie, è passata da una media di 2.423 punti attaccabili a soli 196. Ciò si traduce in una riduzione complessiva delle minacce ***pari al 92%***.

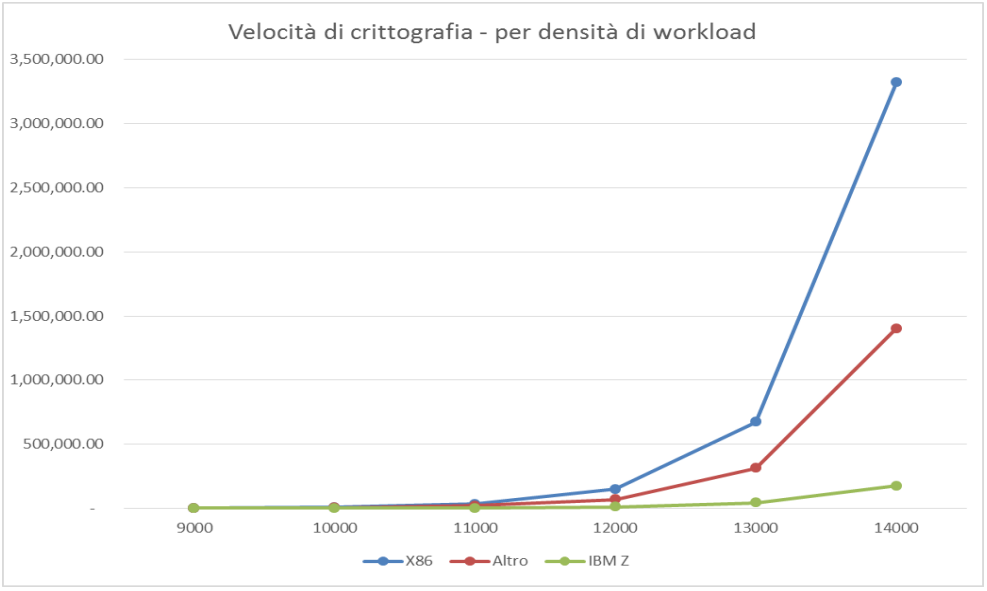
Utilizzando un modello pervasivo, SIL ha esplorato il rischio di incursioni e il livello di esposizione, mediante un sistema di misurazione misto e meccanismi di simulazione, utilizzati per testare la nuova tecnologia. Assegnando lo stesso numero di aspetti di protezione ai dati, e mettendo a confronto un modello basato su selettivo e uno pervasivo, è stato possibile dimostrare che la combinazione tra numero inferiore di operazioni manuali e accresciuta velocità consentiva di ottenere una riduzione dei costi fino all'81,63% rispetto alle soluzioni x86, in base a differenti fattori.

Con l'eliminazione della proliferazione delle piattaforme, una sfida che oggi interessa molteplici aziende, i risparmi vanno oltre i semplici costi della piattaforma. I vantaggi si estendono alla quantità di personale richiesto per la gestione dei sistemi, eseguire i test di sicurezza e gestire le varie risorse associate alla sicurezza. La riduzione del personale rappresenta un aspetto ancora più importante rispetto a quello legato ai sistemi. Nei casi delle attuale piattaforme Z, che già oggi richiedono una quantità di personale di sicurezza inferiore dell'80% rispetto alle piattaforme tradizionali, l'uso della crittografia pervasiva consentirebbe di mantenere la quantità di personale costante, mentre nel caso delle piattaforme alternative il numero di addetti dovrebbe crescere sostanzialmente su base annuale.

In tale tipologia di ambiente, l'approccio pervasivo alla crittografia è giustificato dai costi. Se il mercato dovesse incentivare una transizione verso tale tecnologia, gli sforzi dei produttori verso le soluzioni fisse potrebbero essere orientati in modo tale da concentrarsi sulle modifiche architetturali chiave necessarie per adottare la crittografia pervasiva come elemento integrato dell'architettura. Tali modifiche possono porre maggiori complessità per determinate architetture.

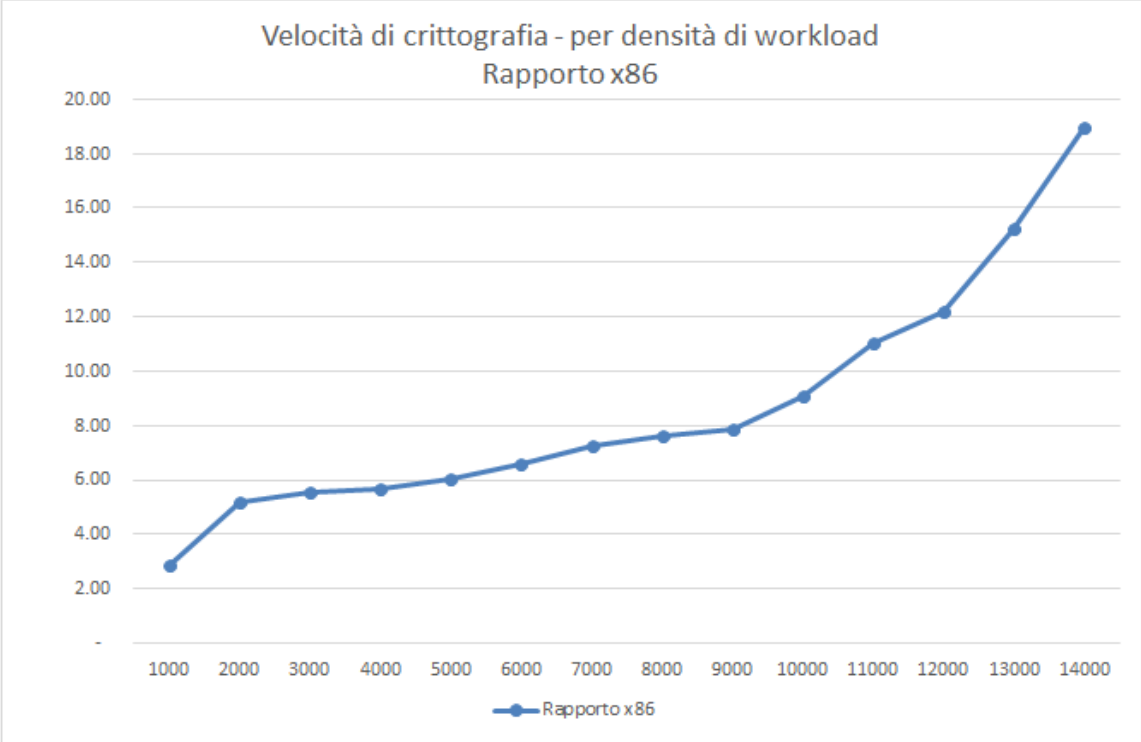
Mentre l'architettura mainframe IBM è in grado di garantire transazioni individuali a una velocità 2,87-3,24 volte superiore rispetto alle piattaforme x86, l'adozione della tecnologia pervasiva consente di incrementare notevolmente tali moltiplicatori. Dato che il flusso di attività che caratterizza il modello pervasivo consente di gestire blocchi di transazioni come elementi unitari, anziché come processi crittografici individuali, il risparmio in termini di capacità sono notevoli, e ciò ha positive ripercussioni sulla velocità.

Questo approccio alla crittografia conferisce livelli straordinari di velocità al motore crittografico, con velocità di crittografiche fino a 18,4 *volte* superiori rispetto alle piattaforme alternative. L'efficienza influisce anche sui costi. I costi operativi risultanti dall'adozione della crittografia pervasiva costituiscono una percentuale compresa tra il 5,1% e l'8,0% dei costi richiesti dalle altre piattaforme alternative; un risparmio notevole.



La piattaforma IBM offre ulteriori risparmi laddove le altre piattaforme non sono in grado di offrire la scalabilità necessaria a far fronte all'espansione della domanda. Il rapido deterioramento delle prestazioni in tali casi è notevole e rende qualunque soluzione non basata sulla piattaforma IBM Z non sostenibile. La densità delle richieste di crittografia tendono a saturare rapidamente la capacità delle altre piattaforme, rendendole incapaci di garantire tempi di reazione adeguati, con insostenibili tempi di attesa per il completamento delle operazioni richieste. Un tale impatto rende difficile conseguire gli obiettivi corrispondenti agli accordi sul livello del servizio (SLA) e alle aspettative sulle prestazioni. Come illustrato nel grafico seguente, tanto maggiore è la densità delle richieste, quanto più elevati saranno i costi complessivi generati dai motori dell'altra piattaforma. Una quantità maggiore di risorse disponibili viene utilizzata per l'elaborazione di tali processi e delle attività di sistema. Quando la domanda di funzionalità di crittografia pervasiva raggiunge un livello sufficientemente elevato, l'intero sistema rallenta fino a bloccarsi del tutto.

La differenza di comportamento tra le risposte offerte dalle differenti architetture possono essere osservate nella tabella riassuntiva di cui sotto.



Il rapido decadimento delle prestazioni sulle piattaforme x86 è indicativo delle limitazioni che affliggono le attuali architetture. L'aggiunta di processori o threading aggiuntivi offre solo miglioramenti marginali, con piccole quantità di parallelizzazione. Sfortunatamente, questo è un approccio autolimitante, dato che l'incremento dei costi complessivi generati da ciascun thread aggiuntivo annulla rapidamente i miglioramenti iniziali conseguiti in altre aree.

SIL ha deciso di esplorare a fondo questo complesso problema, analizzando in dettaglio le attività degli ultimi 14 mesi di 117.000 organizzazioni. In ciascuna di queste situazioni, è stato creato un ambiente emulato, che è stato poi utilizzato su base quotidiana sulla base delle informazioni fornite dal cliente.

Il modello è stato inizialmente sottoposto a stress test, assicurandosi che fosse in grado di replicare i risultati registrati durante i processi di gestione dei carichi di lavoro registrati durante i processi di produzione reali. Una volta verificata l'accuratezza dei dati, i carichi di lavoro e le attività associate sono stati trasferiti a un mainframe simulato, utilizzando prima la crittografia selettiva e poi quella pervasiva.

Successivamente, il medesimo carico delle attività è stato comparato in tutte e tre le situazioni. Dai test è emerso che, nessuno degli 1,16 miliardi di incursioni catturate e registrate dai clienti partecipanti, avrebbe avuto successo se attuata contro un sistema IBM Z con funzionalità di crittografia pervasiva attive.

Il modello di crittografia selettiva ha indicato un notevole livello di protezione, bloccando il 92,1% delle incursioni. Tuttavia, la crittografia selettiva si è anche rivelata più lenta e ha utilizzato una maggiore quantità di capacità di sistema. L'efficienza della crittografia è risultata notevolmente migliore con il modello pervasivo.

Questo tipo di protezione offre vantaggi diretti in termini di redditività aziendale. Le incursioni registrate da questi clienti durante i 14 mesi, hanno causato costi pari a 1,3 miliardi di dollari. Tali costi includono le perdite di tempo dei sistemi, i costi del personale, quelli di correzione dei problemi causati e le perdite associate alle azioni intraprese per mitigare gli effetti negativi sulle quote di mercato. La crittografia pervasiva avrebbe permesso di evitare le conseguenze degli 1,16 miliardi di attacchi rilevati nell'arco dei 14 mesi e i relativi 1,3 miliardi di dollari in costi associati a tali attacchi.

L'adozione di tale modello consente quindi di ridurre il profilo di rischio delle organizzazioni e delle applicazioni. Dato che un numero crescente di aziende di assicurazioni richiede accantonamenti finanziari basati sui profili di rischio operativi e di quelli delle applicazioni, qualunque elemento che contribuisce a ridurre il rischio può avere un significativo impatto finanziario sulle aziende. Numerose assicurazioni chiedono alle aziende di implementare questi accantonamenti finanziari come parte integrante dei budget IT. Questo trend ha avuto inizio circa setto o otto anni fa, e attualmente si sta espandendo. Attualmente, il fattore di rischio per l'architettura mainframe è fino all'80% inferiore rispetto ai sistemi basati farm di calcolo x86 e su altre architetture. Questa percentuale è calcolata in base al budget IT complessivo, dato che tutti gli aspetti associati all'ambiente di calcolo sono influenzati dagli attacchi e dagli altri problemi associati alla sicurezza. Nel caso di un'organizzazione con un budget IT di 12 milioni di dollari, la differenza in termini di accantonamenti finanziari, risulterebbe essere di 764.400 dollari per le piattaforme x86, a fronte di soli 160.524 dollari per la piattaforma IBM Z.

Un aspetto di particolare interesse è stato quello associato alle incursioni basate sul furto delle chiavi crittografiche. I dati rubati facevano parte dell'accoppiata pubblica e privata utilizzata nel settore per garantire la sicurezza delle attività all'interno della piattaforma. Questa minaccia è stata completamente eliminata attraverso il modello della crittografia hardware, integrato nella soluzione Z. Dato che non è necessario alcun handshaking per l'accoppiata, nessun attacco a tale piattaforma è andato a buon fine durante i 14 mesi dello studio.

E dato che l'impatto dei furti delle altre chiavi crittografiche ha causato danni per 6.587.500 dollari, nell'arco di tempo preso in esame dallo studio, tale salvaguardia rappresenta un altro vantaggio sostanziale per le soluzioni basate sul modello pervasivo.

MANAGED SERVICE PROVIDER (MSP)

Questo tipo di crittografia sortisce anche un notevole effetto sui provider di servizi cloud, o su qualunque MSP. Le architetture cloud comportano anche una serie di rischi aggiuntivi legati alla natura stessa dell'architettura. Qualunque tipo di memoria o risorsa condivisa espone la macchina nel suo complesso a potenziali danni, causati non solo da problematiche intrinseche di sicurezza interna, ma anche al rischio di attacchi esterni. Talvolta definito come "sideways hacking", l'isolamento offerto dal mainframe, unito alle funzionalità di crittografia completa integrata, può avere un impatto notevole su clienti, MSP e redditività dell'azienda. E dato che spesso gli MSP sono legati a contratti con tariffe bloccate, qualunque attacco riconducibile alla responsabilità dell'MSP va a influenzare radicalmente la redditività netta. In tali casi, la crittografia pervasiva consente di modificare questo problema e il relativo profilo di rischio.

EVENTI RECENTI

Durante il periodo preso in considerazione dallo studio SIL, si sono verificati numerosi eventi nel mondo della sicurezza che presentano analogie con il tipo di problematiche che possono essere risolte mediante la crittografia. È stato rilasciato un virus attivo in grado di simulare un attacco ransomware. In realtà si trattava di una vera e propria arma, realizzata per distruggere. I danni derivanti da questo attacco sono stati estesi e ingenti.

L'attacco ha coinvolto governi, ospedali, aeroporti e aziende, che hanno subito gravi danni. L'attacco ha generato costi di lungo periodo che non sono ancora stati calcolati, e le cui conseguenze si sentiranno ancora per molti anni. Tuttavia, il punto più importante è che questo tipo di attacco può accadere e accadrà nuovamente. Il tipo di crittografia utilizzato da questa nuova tecnologia, unito ai componenti integrati dell'architettura Z, sarebbe stato in grado di arrestare tale attacco, in quanto la capacità del virus di corrompere il file di controllo rappresenta proprio uno degli elementi che caratterizzano la protezione offerta dalle piattaforme Z, che pertanto sarebbero state immuni a tali attacchi.

In pratica, utilizzando i sistemi Z sarebbe stato possibile risparmiare i trilioni di dollari spesi per fare fronte alla minaccia, e le persone che hanno subito danni fisici, oltre alle aziende che hanno subito le conseguenze negative degli attacchi sarebbero state al sicuro. Questo rappresenta un cambiamento fondamentale e profondo del paradigma del settore nell'ambito della sicurezza.

In questo momento, non esiste nessun'altra architettura chip in grado di supportare il modello basato sulla crittografia pervasiva. Ciò è dovuto alle limitazioni tecniche in termini di larghezza di banda e overhead. Si tratta di una sfida per quelle architetture che necessitano di implementare tali funzionalità, che rappresentano oramai un'assoluta necessità per il settore.

EFFETTI NETTI

Il TCO relativo alla crittografia richiederà alle aziende di valutare i loro budget IT. Dato che la maggior parte del budget IT viene calcolato sulla base dello sviluppo delle applicazioni, con una percentuale allocata compresa tra 41,5% e 68,2%, nel caso delle organizzazioni prese in esame dallo studio, qualunque modifica che consenta di ridurre tale percentuale ha un effetto immediato sulla redditività aziendale.

Assegnando alla crittografia il ruolo di elemento fondamentale centrale ai fini della sicurezza di un ambiente di elaborazione, anziché implementare modifiche a posteriori delle applicazioni per abilitare le funzioni crittografiche, l'effetto netto sui budget IT sarebbe una riduzione di circa il 22,1%.

CONCLUSIONI

"Il significato delle implicazioni di ciò è che gli attacchi informatici dovrebbero essere considerati come un atto di guerra, dalla prospettiva dell'azienda. Mercoledì, segretario generale della NATO, Jens Stoltenberg, ha dichiarato che un attacco informatico potrebbe causare l'attivazione dell'Articolo 5, quello che stabilisce i principi di attivazione della difesa collettiva in ambito NATO".

Luke Graham |@LukeWGraham, venerdì, 30 giugno 2017 | 9:50 AM ET,
Tech Transformers, A CNBC Special Report

L'attuale versione della piattaforma IBM Z offre un sostanziale vantaggio in termini di prestazioni dei TCO, prestazioni e rischi, rispetto alle altre piattaforme attualmente disponibili sul mercato. L'attuale livello di crittografia selettiva

disponibile, e quello di resistenza della piattaforma nativa alle minacce comuni, fornisce alle organizzazioni un livello di protezione integrata di base notevole.

Tuttavia, la diffusione della crittografia pervasiva cambia radicalmente non solo il livello di salvaguardia di cui la piattaforma Z può disporre, ma rappresenta anche un cambio di paradigma per il settore in generale. Questo cambio di paradigma rappresenta una sfida per qualunque prodotto concorrente attualmente disponibile sul mercato.

Le aziende che svolgono la loro attività commerciale online e quelle che sono passate a un modello cloud sono particolarmente sensibili verso il tema della sicurezza informatica. La sicurezza dei dati aziendali e del capitale intellettuale aziendale sta rapidamente diventando un elemento centrale, in un mondo sempre più connesso. Questo crescente livello di integrazione implica maggiori complessità, in quanto le organizzazioni fanno fatica a proteggere i loro margini di mercato e, di conseguenza, i loro margini finanziari. IBM Z vanta una lunga tradizione nel campo della protezione delle risorse e delle implementazioni ad alta sicurezza. E, grazie alla maturità acquisita è possibile offrire funzionalità non presenti in altre soluzioni di virtualizzazione, incluse quelle che controllano la sicurezza di accessi e processi.

La sezione sottostante illustra alcuni degli aspetti fondamentali emersi dallo studio.

Riepilogo

Categoria	*Commento*	*Quick Byte*
Velocità di risposta	Le medesime attività standard effettuate sulla piattaforma Z consumano un tempo di clock fino all'85,80% rispetto alle altre piattaforme.	La piattaforma Z offre anche una maggiore reattività di risposta alle minacce per la sicurezza.
Rischio	I set dei profili di rischio SIL per la piattaforma Z sono inferiori a 1/20 rispetto a quelle delle altre soluzioni.	Il rischio per la sicurezza è significativamente inferiore con le installazioni basate sulla piattaforma Z.
Efficacia della sicurezza	Calcolando sulla base dell'installazione iniziale, la soluzione di sicurezza basata sulla piattaforma Z offre un livello di rilevamento delle minacce fino a 8,5 volte superiore rispetto alle soluzioni alternative, con un conseguente risparmio del 93% in termini di costi complessivi, a fronte di uno sforzo inferiore dell'81%.	La piattaforma IBM Z offre l'ambiente più sicuro per gli ambienti dedicati alle applicazioni.
Efficacia della sicurezza	Le piattaforme Z offrono funzionalità di rilevamento degli attacchi di base con un livello di efficacia fino al 20,74% superiore rispetto alle piattaforme alternative, con un livello di sicurezza completo.	La sicurezza di base offerta dalle piattaforme Z è più efficiente di quella offerta dalle soluzioni aumentate offerte dalle piattaforme alternative.
L'impegno del personale	Studi dedicati in materia di tempistiche e spostamenti indicano che le soluzioni di sicurezza Z richiedono una percentuale di interventi inferiore dell'81% inferiore per l'implementazione dei livelli di protezione standard.	IBM Z richiede quantità di personale inferiori per la messa in sicurezza.
Risanamento	I costi di risanamento delle implementazioni di sicurezza Z sono inferiori del 98,82% rispetto alle altre piattaforme alternative.	Riparare i danni causati alla sicurezza ha un costo inferiore per le piattaforme Z.
Total Cost of Security Ownership	Il TCO per le implementazioni di sicurezza Z può essere ridotto fino all'83,72% rispetto alle altre piattaforme.	Le piattaforme Z offrono un migliore ritorno sui tuoi investimenti sulla sicurezza.
Costo totale delle informazioni	Le implementazioni IBM Z offrono TCI inferiori dell'84,83%, con organizzazioni di varie dimensioni	La gestione delle informazioni sulla piattaforma Z ha costi inferiori.
Crittografia pervasiva	L'architettura mainframe IBM è in grado di offrire funzionalità di crittografia fino a 18,4 volte più veloci a un costo pari al 5% rispetto a quello delle altre piattaforme.	IBM Z trasforma la crittografia pervasiva in una realtà concreta.
Fondo di mitigazione dei rischi	Nel caso di un'organizzazione con un budget IT di 12 milioni di dollari, la differenza in termini di accantonamenti finanziari, risulterebbe essere di 764.400 dollari per le piattaforme x86, a fronte di soli 160.524 dollari per la piattaforma IBM Z.	Il ridotto profilo di rischio delle piattaforme Z si traduce in minori costi degli accantonamenti finanziari allocati per le assicurazioni sulle minacce informatiche.
Una soluzione esclusiva	Attualmente, IBM Z è l'unica architettura in grado di supportare il modello basato sulla crittografia pervasiva.	IBM Z offre funzionalità crittografiche senza eguali.

La mutevole natura delle aziende che operano online sta diventando sempre più fluida. Cambiamenti sempre più rapidi, attacchi attivi e una sempre maggiore complessità dei ruoli associati alla gestione dei rischi, rappresentano una un complesso mix di pericoli e opportunità.

Nell'analisi appena completata da SIL, lo scopo originario era quello di esaminare l'impatto nel mondo reale della sicurezza aziendale offerta dall'architettura della piattaforma. A tale fine, SIL ha messo a confronto le principali architetture IBM Z, UNIX e x86.

I risultati dello studio hanno avuto un profondo impatto nel settore.

SOLITAIRE INTERGLOBAL LTD.

Solitaire Interglobal Ltd. (SIL) è un provider di servizi che vanta una lunga esperienza nel settore della modellazione applicata nell'ambito delle previsioni sulle prestazioni. Fondata nel 1978, SIL sfrutta le tecnologie AI e soluzioni matematiche proprietarie sul calcolo del caos per effettuare analisi predittive e delineare scenari forensi. Le analisi effettuate da SIL offrono a oltre 5.900 clienti in tutto il mondo funzionalità di definizione del profilo di rischio in tempo reale, analisi delle cause di fondo, impatti ambientali, gestione capacità, tendenze di mercato, analisi dei difetti, analisi sull'efficienza delle applicazioni Fourdham, identificazione dinamica delle risorse organizzative, nonché analisi granulare di costi e spese. SIL offre anche servizi di certificazione RFP che consentono ai produttori di fornire servizi alle organizzazioni governative e alle aziende di tutto il mondo.

Numerosi fornitori di hardware e software commerciali e governativi collaborano con SIL per ottenere la certificazione delle capacità prestazionali e delle limitazioni delle loro gamme di prodotti. SIL collabora anche con questi produttori al fine di migliorare i throughput e la scalabilità delle installazioni dei clienti, generando profili di rischio e altre strategie finalizzate alla mitigazione dei rischi. Negli ultimi decenni, SIL è stata coinvolta nella definizione degli standard industriali e delle certificazioni delle prestazioni, effettuando una raccolta di informazioni attiva per l'OPMS (Operational Characterisation Master Study), con l'incarico di acquisire una migliore comprensione dei costi organizzative delle piattaforme IT-centriche e delle loro caratteristiche comportamentali. L'OPMS ha continuato negli anni a costruire il database euristico di SIL, che attualmente contiene oltre 475 petabyte di informazioni. L'accresciuta base statistica ha continuato a migliorare l'accuratezza delle previsioni e delle analisi fornite da SIL, fino a raggiungere livelli di accuratezza ineguagliati nel settore. Nel complesso, SIL esegue oltre 2 milioni di modelli all'anno, offrendo i suoi servizi ai suoi clienti sottoscrittori, nonché fornendo soluzioni ad-hoc per clienti occasionali.

NOTE SULLA METODOLOGIA

Al fine di comprendere l'impatto delle piattaforme Z come parte integrante dell'infrastruttura IT delle aziende, e il loro effetto sull'esperienza d'uso da parte dei clienti, sono stati prese in esame varie tipologie di piattaforme. Lo studio ha poi comparato la relativa differenza in termini di comportamento di funzionamento per ciascun fatto, come il numero totale di interruzioni, ecc., per comprendere a fondo gli effetti netti delle varie piattaforme. Sono stati osservati gli effetti relativi a prestazioni generali, capacità, consumi e altre metriche aziendali.

L'approccio adottato da SIL utilizza una lista e fattori di correlazione associati al comportamento operativo durante la produzione, utilizzando sistemi e attività aziendali reali. Per gli scopi prefissi dall'indagine, sono stati osservati, registrati e analizzati 9.602.042 modelli di configurazioni, al fine di fornire solide prove in grado di suffragare i risultati ottenuti. Sono stati poi rilevati i dati relativi all'esperienza dell'utente, per compararli con quelli relativi alle varie piattaforme. Sono stati analizzati e comparati oltre 6,3 milioni di feedback dei clienti, poi comparati con i dati sugli ambienti IT, e quindi integrati nello studio. Utilizzando una grande quantità di dati reali su clienti e di settore è stato possibile acquisire una migliore comprensione del comportamento delle piattaforme nel mondo reale. I dati rilevati da questi sistemi sono poi stati utilizzati per creare una proiezione realistica degli attuali problemi e dei vantaggi operativi. I dati comportamentali relativi ai sistemi sono stati poi analizzati per isolare le caratteristiche dell'architettura in termini di prestazioni lorde e in termini di effetti aziendali netti.

Dato che una parte dello studio esamina l'impatto delle tecnologie emergenti sulle prestazioni complessive, sui costi e i rischi di un significativo numero di aziende, sono stati condotte dettagliate emulazioni operative con i dati forniti dai clienti. L'emulazione ha testato l'ambiente virtuale delle organizzazioni oggetto dello studio per un periodo di 14 mesi, seguendone le attività quotidiane, in base ai dati forniti dai partecipanti. I risultati di questo esercizio sono stati inclusi nei risultati presentati in questo articolo.

In una situazione come quella presentata da questo studio, SIL utilizza una metodologia che integra l'acquisizione dei dati operativi, incluse le informazioni estremamente dettagliate sulle attività del sistema. Si noti che tutte le informazioni sono state fornite dai clienti, e ricavati direttamente dalle loro piattaforme di produzione. È essenziale capire che nessuno dei dati utilizzati dallo studio è stato ottenuto da benchmark artificiali o mediante test costruiti ad arte. Ciò in quanto il valore dello studio deriva dalla comprensione dei processi operativi reali condotti presso le aziende, piuttosto che da un concetto basato sulla semplice percezione di ciò che avviene in un contesto reale. Pertanto, le ottimizzazioni effettuate presso questi siti derivano da dati relativi a situazioni reali, e non a configurazioni ottenute mediante benchmark artificiali. Dato che l'obiettivo di questa analisi non era limitato a definire le differenze tra sistemi operativi o hardware con differenze minime, le varie versioni sono state combinate tra loro, evidenziando solamente le differenze complessive tra le principali architetture. Tale approccio offre una panoramica più generale della strategia adottata delle singole architetture.

Al fine di supportare la natura olistica di questa analisi, lo studio ha elaborato analisi e informazioni relative a installazioni, settori, località e produttori differenti. Qualunque studio di questo tipo evidenzia una certa sovrapposizione dei dati, come nel caso in cui una data azienda utilizza prodotti di differenti produttori. In tali casi, il totale delle percentuali discrete può superare il 100%. Nel caso di organizzazioni basata su implementazioni multi-layer, come quelle distribuite su molteplici località geografiche o che utilizzano classificazioni industriali multiple, sono state analizzate mediante suddivisioni discrete dei feedback forniti per ciascuna metrica. Un filtraggio aggiuntivo è stato effettuato per eliminare quelle piattaforme che non apparivano conformi alle best practice. Dato che numero di malfunzionamenti, scarse prestazioni e costi elevati che caratterizzano molte delle installazioni prese in esame non sono associati alle scelte fatte in materia di hardware o software, tali progetti sono stati rimossi dalla base di analisi dello studio.

Il campione preso in esame dallo studio include i settori manifatturiero (26,55%), quello della distribuzione (19,87%), della sanità (4,67%), quello al dettaglio (12,83%), quello finanziario (22,16%), il settore pubblico (6,54%), quello delle comunicazioni (3,88%) e un gruppo misto (3,50%).

Lo studio include anche varie regioni geografiche, con il Nord America rappresentante il 32,05% delle aziende incluse nello studio, seguito da Sud e Centro-America con il 10,58%, l'Europa con il 33,62%, l'Asia-Pacifico e l'Asia con il 15,62% e l'Africa con il 4,74%, oltre a un ulteriore 3,38% di organizzazioni che hanno fornito informazioni ma che non fanno parte delle succitate regioni geografiche.

Dato che strategie e vantaggi offerti tendono a variare in base alle dimensioni delle organizzazioni, SIL ha adottato un ulteriore categorizzazione, suddividendo le aziende oggetto dello studio in piccole, medie, grandi e grandissime. Queste categorie includono il numero di dipendenti e il fatturato annuo lordo di ciascuna azienda. Il numero del personale moltiplicato per il fatturato lordo genera una metrica utilizzata come fattore di analisi. In base alla definizione fornita, una piccola azienda deve avere meno di 100 dipendenti e un fatturato lordo inferiore ai 20 milioni di dollari, oppure un valore pari a 2.000, ottenuto calcolando 100 (numero di dipendenti) X 20 (importo del fatturato lordo). Un'azienda con 50 dipendenti e un fatturato lordo di 40 milioni di dollari verrebbe considerata anch'essa come l'azienda di cui sopra, e sarebbe quindi catalogata come azienda di piccole dimensioni. Le categorie assegnate da SIL sono le seguenti: 2.000 (piccola azienda); 10.000 (azienda di medie dimensioni); 100.000 (azienda di grandi dimensioni) e 1.000.000 (azienda di grandissime dimensioni).

I dati forniti in questi studio sono stati raccolti come parte di un processo di raccolta dati e supporto sistemi in tempo reale, a cui SIL partecipa fin dal 1978. Il personale del cliente ha effettuato tutti i test presso i siti SIL dislocati presso la sede del cliente. I risultati dei test sono stati inviati a SIL mediante i normali punti di raccolta dati sicuri utilizzati da tali clienti fin dall'inizio della collaborazione con il servizio di supporto SIL. Non appena ricevute le informazioni presso i punti di ricezione dati sicuri, il processo standard di elaborazione dati AI di SIL ha preparato i dati in formato standard, rimuovendo ogni riferimento ai dati personali dettagliati del cliente. I dati cosi scremati sono stati inseriti nei sistemi per l'analisi e l'elaborazione dei risultati.

RICONOSCIMENTO ED ESONERO DELLE RESPONSABILITÀ

Questo documento è stato sviluppato con il finanziamento di IBM. Sebbene il documento utilizzi materiale disponibile pubblicamente e proveniente da vari fornitori, tra cui IBM, non riflette necessariamente le posizioni di tali fornitori sui temi in esso affrontati.

ZSL03452-ITIT-00