WHITE PAPER

L'importanza della **sicurezza dei dati**

SCALE TO WIN

INFINIDAT

Le sfide

Il 2017 non è stato un anno facile per essere un CIO / CISO e il 2018 non sembra mostrare alcun segno di miglioramento in tal senso. Con così tante violazioni di dati in grado di rovinare un'intera carriera nel solo 2017 (Equifax, Uber, Yahoo per citare solo alcuni casi) e con requisiti normativi più rigorosi in tutto il mondo, i CIO / CISO hanno la responsabilità societaria di rivedere il loro approccio alla sicurezza dei dati.

Oltre al rispetto delle normative, le organizzazioni hanno la responsabilità nei confronti di clienti e azionisti di proteggere i dati e minimizzarne l'esposizione non soltanto agli attacchi esterni ma anche ai dipendenti. Nel 2017, il metodo più comune di violazione dei dati è stato l'invio di phishing a dipendenti interni delle società (vedi il 2017 Data Breach Investigation Report). Ciò rende tali dipendenti involontariamente complici nella violazione dei dati: oltre l'80% dei cyber attacchi andati a buon fine hanno avuto un elemento umano critico. Il professionista non IT che riceve un'email dal suo migliore amico colpito e apre un allegato, il dipendente che accede a un sito infetto e crea una falla nel perimetro di sicurezza. Per quanto non esista una protezione del 100%, ci sono però regole di buon senso per ridurre il rischio.

Ci sono due termini da tenere in mente quando vogliamo proteggere i dati dagli hacker:

> ***"La superficie di attacco di un ambiente software è la somma dei diversi punti (i "vettori di attacco") nei quali un utente non autorizzato (l'"aggressore") può tentare di accedere ai dati o estrarre dati da un ambiente. Tenere la superficie di attacco il più piccola possibile è una misura base di sicurezza."*** *(Wikipedia)*

Se un'organizzazione tratta i suoi dati come la fonte del suo vantaggio competitivo e comprende quanto essi siano sensibili per i suoi clienti, come dovrebbe minimizzare la superficie di attacco e in che modo gli AFA (All Flash Arrays) lo stanno impedendo?

Quando l'organigramma detta il metodo di sicurezza

Le legge di Conway ci ha insegnato ormai che la struttura organizzativa spesso incide sui risultati / progettazione più di qualsiasi altro fattore. Nell'ambito della sicurezza questo principio è molto semplice: se il CISO e il responsabile storage hanno un buon rapporto, molto probabilmente i dati saranno criptati nello storage layer e la casella "crittografia" spuntata.

Lo storage inoltre è il "percorso a minore resistenza" in quanto gli array di storage possono attivare la crittografia istantaneamente senza riduzione delle prestazioni.

Ma la crittografia a livello di storage aiuta la vostra superficie di attacco? Un po' sì. Essa lascia non criptati TUTTI gli altri strati tra l'utente attraverso l'applicazione e l'infrastruttura e quei dati attraversano la rete non protetti.

Dove dovremmo allora criptare i dati?

Pensatela in questo modo – più in alto nella catena si trovano i dati personali o sensibili, più strati vengono protetti. Ciascuna linea della tabella seguente rappresenta un possibile strato che può essere criptato e ciascuna colonna una superficie di attacco.

Notato quanto poco protegga la crittografia a livello di storage?
Eppure essa rappresenta un metodo di sicurezza dati comunemente usato (e spesso l'unico).

Dove è usata la crittografia	**✓ Chi può vedere i dati?** **⚠ Chi può causare accidentalmente una violazione?**						
	App Admin	OS Admin	DBA	VM Admin	Network Admin	Storage Admin	Backup Admin
Applicazione	⚠	✓	✓	✓	✓	✓	✓
Applicazione OS	⚠	⚠	✓	✓	✓	✓	✓
Database	⚠	⚠	⚠	✓	✓	✓	✓
VM Encryption	⚠	⚠	⚠	⚠	✓	✓	✓
Fabric (Data in flight)	⚠	⚠	⚠	⚠	✓	⚠	⚠
Storage	⚠	⚠	⚠	⚠	⚠	⚠	⚠
Backup	⚠	⚠	⚠	⚠	⚠	⚠	⚠

In che modo gli all flash array aumentano la vostra superficie d'attacco?

Per quanto la maggior parte degli AFA (se non tutti) offrano una crittografia a livello di disco, essa rappresenta l'unico livello di crittografia da essi consentita. Se i dati sono criptati altrove, gli AFA non possono effettuarne la riduzione e la loro intera economia crolla. Gli AFA devono affidarsi alla riduzione dei dati (in un rapporto compreso tra 3:1 e 6:1) per minimizzare il sovrapprezzo a un punto in cui sia accessibile.

Quando "ottimale" incontra fattibile

QUESTO APPROCCIO OTTIMALE ALLA SICUREZZA DEI DATI È SPESSO LIMITATO DALLA REALTÀ PREESISTENTI:

- Quell'applicazione vecchia di dieci anni che non offre alcuna crittografia e assistenza
- Quell'applicazione critica per l'azienda la cui manutenzione richiede un anno
- Quel proprietario di applicazione che si rifiuta di spendere del tempo per criptare i dati

Quando il gioco si fa serio, spesso è necessario fare dei compromessi per accelerare l'adozione della sicurezza dei dati. Molti opteranno per criptare questi ambienti nei livelli più bassi dello stack (DB / VM / OS) al fine di adempiere ai requisiti societari e di regolamentazione. Questo approccio è spesso necessario per rispettare delle scadenze. Tuttavia, vale la pena limitare il numero degli approcci separati per evitare spese generali elevate.

Si deve inoltre osservare che tutte queste alternative hanno lo stesso effetto: distruggere le capacità di riduzione dati degli AFA e aumentare il loro costo totale di proprietà.

Benefici aggiuntivi della crittografia ai livelli superiori dello stack

DISTRIBUZIONE DEL CARICO DI LAVORO E PERFORMANCE

Ad eccezione dei Self Encrypting Drive (SED), la crittografia richiede un po' di potenza della CPU. Uno stack IT ha sempre più host che array di storage; spostare la task della crittografia dei dati a un livello più elevato dello stack comporta una maggiore distribuzione del carico di lavoro, riducendo quest'ultimo a livello dei singoli dispositivi e, pertanto, migliorando la performance generale.

GRANULARITÀ

Più alto è il livello della crittografia nello stack, migliore è la granularità: un'applicazione può soltanto criptare Informazioni Personali Identificabili (PII) in quanto "capisce" il contesto / significato dei dati. Anche questo porterà a minori spese generali.

Se andiamo a un livello inferiore - il Database Administrator (DBA) può fornire un table space criptato e un table space non criptato e collocare i dati giusti nello spazio giusto. Per quanto meno granulare, è comunque meglio che criptare un intero VM o LUN.

CLOUD READINESS

Spostare la crittografia ai livelli più alti dello stack è un prerequisito per qualsiasi migrazione al cloud nel caso in cui i dati debbano mantenere lo stesso livello di protezione, anche sulla rete (WAN). I dati criptati possono spostarsi o entrare nel cloud in sicurezza senza necessità di ulteriori meccanismi di sicurezza (quale la gestione della crittografia a livello di cloud).

FACILITÀ DI INTEGRAZIONE

Integrare i livelli OS, DB o hypervisor ha un vantaggio: ci sono pochi flavor di ciascuno di essi, a fronte di molte applicazioni nell'ambiente. Da un punto di vista delle operazioni, ciò può ridurre la complessità.

CALL TO ACTION

- Pianifica la protezione dei dati della tua azienda
- Imposta una deadline per le nuove applicazioni da progettare con la crittografia sin dal primo giorno
- Forma sviluppatori di applicazioni in-house su metodologie security-by-design
- Analizza le applicazioni esistenti e trova il modo giusto, per la tua azienda, di proteggere i dati
- Crea un piano di transizione per crittografare le applicazioni legacy con dati riservati o sensibili