SOPHOS
Security made simple.

Decifrare il codice: una guida semplice alla cifratura

Di **Anthony Merry**, Director of Product Management, Data Protection

Il successo di un'azienda dipende sempre maggiormente dalla sua abilità di utilizzare a proprio vantaggio i dati di cui dispone. Sia che si tratti di incrementare il fatturato o di incentivare la redditività, le aziende contano sui dati per aumentare le vendite, favorire l'innovazione dei prodotti, acquisire clienti in un mercato specifico e ottenere un vantaggio competitivo. I dati sono preziosi, ma possono diventare pericolosi se finiscono nelle mani sbagliate.

I casi di violazione dei dati compaiono nei titoli dei notiziari quasi tutti i giorni, eppure solamente una piccola percentuale degli attacchi informatici è rivolta a organizzazioni di grandi dimensioni quali Sony, Anthem, o il governo statunitense. Se la vostra è una piccola-media impresa (PMI), anche i vostri dati si trovano nell'occhio del mirino. Più di 700 milioni di record sono stati compromessi nel 2014, e il 53% dei casi confermati di perdita di dati si è verificato in aziende con meno di 1000 utenti*, secondo un report compilato da Verizon[1]. Nessuna azienda o istituzione al mondo può ritenersi immune al furto dei dati, indipendentemente da posizione geografica, dimensioni e settore.

La sicurezza IT si dedica principalmente alla difesa di oggetti fisici (server, desktop e laptop, dispositivi mobili), ma le aziende dovrebbero concentrarsi maggiormente sulla protezione dei dati contenuti in questi computer. Con il proliferare dei dati e l'esigenza di accedere ai dati ovunque e in qualsiasi momento, la cifratura sta rapidamente guadagnando terreno come il migliore punto di partenza per avviare una strategia di protezione efficace.

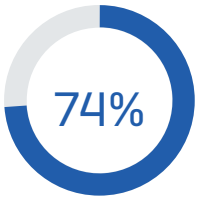
Nonostante la dura e fredda realtà delle statistiche dei casi di violazione e perdita accidentale dei dati, molte aziende esitano a implementare la cifratura. Perché? In parte è perché da diverso tempo la cifratura sembra essere circondata da una serie di falsi miti, che includono le seguenti affermazioni:

- La cifratura è troppo difficile da installare e da gestire
- La cifratura limita la performance di laptop, desktop, server e applicazioni

Oltre a questi falsi miti comuni, implementare una strategia di protezione dei dati che includa la cifratura può essere molto impegnativo e generare confusione, come in questi esempi:

- Avete bisogno di utilizzare la cifratura ovunque si trovino dati, ovvero su: dischi, file, cartelle, dispositivi removibili, dispositivi mobili e servizi di cloud storage?
- Quali sono le migliori prassi per l'implementazione della cifratura?
- Come occorre procedere per proteggere tutti i dati importanti, senza interferire con le consuete attività dell'azienda?

Questo white paper si propone di sfatare tutte le paure e dissipare la confusione che circonda la cifratura. Dimostra come le aziende possano procedere verso il futuro con una strategia di cifratura efficace, in maniera semplice, pratica, e fattibile. Cominciamo quindi con il dire tutta la verità su alcuni falsi miti.

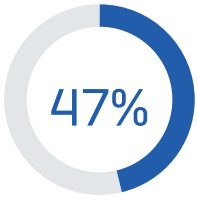


Percentuale di aziende di piccole dimensioni caduta vittima di una violazione dei dati nel 2015[2]

I falsi miti della cifratura

Falso mito: La cifratura serve solo alle aziende che devono ottemperare a requisiti di conformità specifici che prescrivono l'uso della crittografia per legge.

Verità: I dati sono preziosi per qualsiasi tipo di organizzazione, e in quanto tali devono essere protetti. Possono includere informazioni sui clienti (nominativi, indirizzi e-mail, dati di carta di credito), informazioni finanziarie interne o della concorrenza, dati dei dipendenti, proprietà intellettuale, e molto altro ancora. In pratica, i dati sono come il denaro: possiedono un valore e devono essere protetti di conseguenza. Le aziende devono sempre e comunque cifrare i dati di natura sensibile, sia che ciò sia o meno un requisito legale.



Percentuale delle violazioni dei dati dovuta a un attacco malevolo/ criminale, +42% rispetto all'anno scorso[3]

* In aziende dalle dimensioni conosciute

Falso mito: **La cifratura è troppo complicata e richiede troppe risorse.**

Verità: La cifratura dei dati può essere molto semplice da implementare e gestire. Il segreto è capire quali sono i tipi di dati da cifrare, dove siano situati, e chi debba aver diritto di accedervi. Inoltre, optando per una soluzione di cifratura next-gen che cifra tutti i file per impostazione predefinita, si semplifica ulteriormente la protezione dei dati come routine quotidiana per tutti i dipendenti.

Falso mito: **La cifratura è troppo pesante per la performance di database e applicazioni.**

Verità: La performance di applicazioni, database, server e reti è una delle priorità principali per responsabili IT e utenti finali. Se realizzata e implementata correttamente, oltre a garantire la protezione dei dati più critici su tali sistemi, la presenza della cifratura comporta un impatto molto basso sulla performance, tanto da risultare impercettibile agli occhi degli utenti.

Falso mito: **La cifratura non aumenta il livello di protezione dei dati salvati nel cloud.**

Verità: È più sicuro salvare nel cloud dati cifrati che non cifrati. Sapete dove vengono archiviati i vostri dati nel cloud? Chi vi può accedere veramente? Le risposte a queste domande spezzano un'ulteriore lancia a favore della cifratura dei dati da caricare sul cloud, con chiavi di cifratura controllate da voi stessi.

Falso mito: **La cifratura dei dati è più importante della gestione delle chiavi.**

Verità: Senza un'adeguata gestione delle chiavi, la cifratura è inutile. Sono troppe le aziende che non sono in grado di gestire le proprie chiavi di cifratura, in quanto tali chiavi vengono o salvate sullo stesso server dei dati cifrati, oppure su un provider di servizi cloud che ne effettua la gestione. Sarebbe assurdo quanto chiudere la propria automobile a chiave, lasciando le chiavi nella portiera.

Falso mito: **Se i dati sono cifrati, è impossibile che vengano rubati.**

Verità: La cifratura non impedisce il furto o lo smarrimento dei dati, ma ne garantisce la sicurezza, rendendoli illeggibili e inutilizzabili. Optate per una soluzione di cifratura che offra una prova concreta che i dati erano stati cifrati.

Capire la cifratura: Come funziona

La cifratura è un metodo che codifica i messaggi in un formato che risulta illeggibile per gli utenti non autorizzati. La crittografia (l'arte e la scienza alla base della cifratura) utilizza algoritmi per trasformare dati leggibili (testo in chiaro) in dati in un formato illeggibile (testo crittografato).

Senza entrare troppo nei dettagli, potrebbe essere utile pensare a questo esempio: cifrando i dati, questi ultimi vengono archiviati come quando si conserva del denaro in una cassaforte, per cui occorre una chiave per aprire la cassaforte e accedere al denaro.

Esistono vari modi diversi per utilizzare la cifratura, ma per le aziende esposte al rischio di perdita dei dati, due ambiti molto importanti da conoscere sono la cifratura completa del disco e la cifratura a livello dei singoli file.

Per cifratura completa del disco (Full-Disk Encryption, FDE) si intende la cifratura di un disco intero

Full-disk Encryption

Per cifratura completa del disco (Full-Disk Encryption, FDE) si intende la cifratura di un disco intero, piuttosto che di file specifici, al livello del settore sotto il File System. In altre

parole, vengono cifrati tutti i contenuti dell'hard disk fisico del dispositivo.

La FDE offre la protezione più adeguata quando un dispositivo non è attivo (spento oppure in modalità di sospensione), in quanto garantisce la protezione dei dati "inattivi". La FDE viene considerata la prima linea di difesa in una strategia di protezione dei dati, e ha come obiettivo principale la messa in sicurezza dei dati nell'eventualità in cui un dispositivo venga smarrito o rubato.

Per cifratura dei file si intende la cifratura di singoli file specifici

Con la FDE, tutti i file salvati su un computer o dispositivo digitale verranno automaticamente cifrati (protetti). Tuttavia, non appena un file lascia il disco (ad es. se dovesse essere inviato per e-mail, copiato su un'unità removibile o caricato nel cloud), non è più protetto dalla FDE.

Cifratura dei file

Per cifratura dei file si intende la cifratura di singoli file specifici. Si immagini ad esempio di avere due documenti in un computer. È possibile scegliere di cifrarne uno, ma non l'altro. A differenza della cifratura del disco, che cifra automaticamente tutti gli elementi salvati all'interno del disco, con la cifratura dei file occorre impostare regole e criteri che determinino i tipi di file da cifrare.

A differenza della FDE, i file cifrati rimangono cifrati dopo aver lasciato il disco o il dispositivo. Un file cifrato può essere condiviso tramite e-mail, pur continuando a garantirne la sicurezza. Lo stesso vale per la copia di un file cifrato su un supporto removibile oppure nel cloud. Ciò viene talvolta definito come protezione di dati in uso e dati in transito.

Con la cifratura dei file, occorre impostare regole per semplificare il processo. È ad esempio possibile implementare la cifratura per impostazione predefinita di tutti i documenti Word, ma non delle immagini.

Le moderne soluzioni di cifratura next-gen introducono il concetto della cifratura sempre attiva. Essenzialmente, ciò significa che tutti i file vengono automaticamente cifrati per impostazione predefinita. Gli utenti non devono più assumersi la responsabilità di decidere quali elementi cifrare e, anche se i file possono essere decifrati secondo necessità, viene sempre garantita una posizione iniziale di massima sicurezza.

Implementazione di una strategia di cifratura

Secondo un report del Ponemon Institute[4], alla domanda che chiede quale sia la principale sfida di pianificazione e implementazione in una strategia di cifratura dei dati, i partecipanti hanno risposto come segue:

56%	Percentuale dei partecipanti che dichiara che sia scoprire dove si trovino i dati di natura sensibile all'interno dell'organizzazione
34%	Percentuale dei partecipanti che dichiara che sia classificare i dati da cifrare
15%	Percentuale dei partecipanti che dichiara che la sfida più difficile sia educare gli utenti ad adoperare correttamente la cifratura

La cifratura è la base su cui impostare qualsiasi strategia di protezione dei dati. Prima di poter trasformare una strategia in un piano attuabile, occorre porsi le seguenti domande:

1. **Come avviene il processo di entrata e uscita dei dati nella vostra azienda?** Ricevete e-mail con file in allegato? Ne inviate? Ricevete dati su chiavette USB o altri tipi di supporti rimovibili? Come procede la vostra azienda per salvare e condividere internamente ed esternamente grandi quantità di dati? Utilizzate servizi di archiviazione nel cloud, come DropBox, Box, OneDrive, ecc? E adoperate dispositivi mobili e tablet? Secondo un sondaggio condotto da Sophos, gli utenti che fanno uso delle tecnologie adoperano in media 2,9 dispositivi ciascuno. Come agire per tenere sotto controllo i dispositivi che hanno accesso ai dati aziendali? Occorre cercare una soluzione di cifratura realizzata per adattarsi al modo in cui vengono adoperati i dati, e a come questi ultimi vengono trasferiti all'interno dell'azienda.

   Esempio di un caso di utilizzo: Con il sempre più elevato numero di PMI che utilizzano i servizi di cloud storage, occorre una soluzione che protegga la condivisione dei dati nel cloud, e che garantisca pieno controllo sulle chiavi di cifratura.

   Occorre una soluzione di cifratura dei dati in grado di difendere i dati, indipendentemente da dove ne avvenga l'accesso, senza ulteriori complicazioni per gli utenti finali. La cifratura deve essere come un angelo custode, e l'utente non deve accorgersi della sua presenza.

2. **Come vengono utilizzati i dati dalla vostra azienda e dai vostri dipendenti?** Quali sono i loro flussi di lavoro e come agiscono per incrementare i livelli di produttività durante le normali mansioni quotidiane? Quali strumenti, dispositivi o app utilizzano? Possono essere potenziali vettori di perdita dei dati?

3. **Chi ha diritto di accedere ai vostri dati?** Questa domanda può essere vista sia da un punto di vista etico che normativo. In alcuni casi, gli utenti non dovrebbero avere accesso a certi tipi di dati, per via di questioni etiche (ad es. dati di risorse umane e informazioni relative agli stipendi). Esistono leggi sulla protezione dei dati valide a livello internazionale, che stabiliscono che l'accesso ai dati debba poter essere consentito solamente a chi ne abbia bisogno per svolgere le proprie mansioni; a chiunque altro, l'accesso andrebbe negato. I vostri dipendenti hanno accesso solamente ai dati di cui hanno bisogno per svolgere il proprio lavoro, oppure a molti più dati rispetto a quelli strettamente necessari?

   Esempio di un caso di utilizzo: Gli amministratori IT tendono ad avere diritti illimitati di accesso ai dati e alle infrastrutture informatiche. È necessario che un amministratore IT possa accedere ai dati di risorse umane di tutti i dipendenti, oppure ai documenti del reparto legale che trattano delle cause legali in corso? In una società ad azionariato diffuso, è necessario che i dipendenti che non appartengono al reparto finanza possano accedere ai più recenti dati finanziari?

4. **Dove si trovano i dati?** Sono archiviati centralmente e situati per la maggior parte in un data center? Interamente ospitati nel cloud? Salvati su laptop e dispositivi mobili dei dipendenti? Secondo un sondaggio a cura di Tech Pro Research, il 74% delle aziende permette, o intende permettere, ai dipendenti di adoperare i propri dispositivi mobili in ufficio, a scopo lavorativo (BYOD). Inoltre, i dipendenti lavorano anche da casa o mentre si trovano in viaggio. Si portano appresso dati aziendali di natura sensibile, contenuti all'interno dei dispositivi, e ciò aumenta il rischio che si verifichino perdite

dei dati e violazioni della conformità. Si pensi a quanto sarebbe facile accedere a informazioni riservate sulla vostra azienda, se lo smartphone di un dipendente dovesse essere smarrito o rubato.

Ciascuna organizzazione è un caso a sé, per cui non esiste una strategia di protezione adatta a tutte le situazioni. La vostra strategia di protezione dei dati deve essere progettata in base ai seguenti fattori: le esigenze dell'azienda, il tipo di dati con cui ha a che fare la vostra organizzazione, e normative locali/di settore, e le dimensioni dell'azienda.

Sebbene molte di queste decisioni varino da organizzazione a organizzazione, è presente una costante valida per tutte: occorre educare i dipendenti.

È essenziale che i dipendenti capiscano come rispettare la conformità con una strategia di protezione dei dati chiaramente definita, e devono sapere come adoperare la cifratura. Occorre stabilire esplicitamente quali sono i dati a cui possono accedere, come deve avvenire l'accesso, e come possono agire per proteggere questi dati. È particolarmente importante accertarsi di poter sia fornire che gestire la cifratura in modo tale che non abbia alcun impatto sui flussi di lavoro dell'azienda. La natura umana esita ad accogliere favorevolmente i cambiamenti, per cui la vostra strategia di protezione dei dati deve prevedere un programma di sensibilizzazione e formazione.

Scegliere una soluzione

La richiesta di indicare quali siano le funzionalità più importanti per le soluzioni basate sulle tecnologie di cifratura ha restituito i seguenti risultati[5]:

62%	Percentuale dei partecipanti che dichiara che sia la possibilità di effettuare la distribuzione nel cloud e on-premise
53%	Percentuale dei partecipanti che dichiara che i fattori più importanti siano performance e latenza
51%	Percentuale dei partecipanti che dichiara di conferire la priorità più elevata alla gestione delle chiavi

Quelli che seguono sono alcuni aspetti fondamentali da tenere presente durante la scelta della migliore soluzione di sicurezza per la vostra azienda:

Facilità d'uso: Una soluzione di cifratura deve essere semplice ma completa. Il prodotto di cifratura deve essere facile da impostare e da distribuire, con una console di gestione intuitiva.

Multipiattaforma: Optate per una soluzione che offra tutti i tipi di cifratura, incluse cifratura completa del disco e cifratura dei singoli file, su sistemi operativi di vario genere, come ad es. Windows, Mac, Android e iOS.

Adattabilità: La soluzione ideale protegge i dati senza interferire con il flusso di lavoro dell'azienda, e senza incidere negativamente sulla produttività. Deve essere la soluzione di cifratura a doversi adattare al flusso di lavoro dell'azienda, e non il contrario.

Approvazione da parte di entità indipendenti: Verificate che qualsiasi azienda

selezionate per rispondere alle vostre esigenze di cifratura offra ampio supporto e goda dell'approvazione indipendente di analisti di settore, recensori e clienti.

Scalabilità: Man mano che cresce, la vostra azienda ha bisogno di una soluzione scalabile, in grado di crescere con voi. Inoltre, deve consentire la gestione delle chiavi e l'implementazione dei vostri criteri di protezione dei dati con la massima facilità.

Prova di conformità: Se dovesse accadere il peggio, dovrete essere in grado di dimostrare che i vostri dati erano protetti. Se operate in un mercato verticale o in un'area geografica in cui sono in vigore leggi o normative specifiche per la tutela dei dati, gli auditor avranno bisogno di prove che dimostrino che i dati erano cifrati.

La nuova Sophos SafeGuard Encryption

Sophos SafeGuard è la pluripremiata soluzione di cifratura next-gen by Sophos. È **sempre attiva** e cifra i contenuti sin dal momento della loro creazione, per cui potrete sempre partire da una posizione di massima sicurezza. **Synchronized Encryption** difende proattivamente i dati, convalidando continuamente l'utente, l'applicazione e l'integrità della sicurezza di un dispositivo, prima di concedere accesso ai dati cifrati. E tutto ciò avviene in maniera **invisibile** agli occhi degli utenti, per garantire una collaborazione trasparente e sicura. Inoltre, Sophos SafeGuard semplifica il rispetto della conformità alle normative sulla tutela dei dati, pur senza interferire con il lavoro degli utenti.

Sophos SafeGuard offre la migliore soluzione di cifratura attualmente disponibile sul mercato:

- 'Breakout Star' nella Forrester Encryption Wave del 2015[6]
- Leader del Quadrante magico di Gartner negli ultimi 7 anni[7]
- Premio TechTarget Readers' Choice del 2014 come migliore soluzione di cifratura del 2014
- Test indipendenti hanno decretato Sophos Encryption la soluzione più veloce e con minore impatto sulla performance

Per saperne di più, visitare www.sophos.it/encryption.

Conclusione

Esistono troppe aziende che non adoperano la cifratura in maniera diffusa, per via dell'impressione che la cifratura sia troppo complicata. La cifratura è in realtà piuttosto semplice: quando i dati sono cifrati, sono protetti, e risultano illeggibili in caso di furto o smarrimento di un dispositivo.

La cifratura non è mai stata più indispensabile. Dipendenti in mobilità, un cybercrimine dotato di risorse sempre più sofisticate, e la crescita del mercato nero per il commercio dei dati sono tutti fattori che indicano che le informazioni di natura sensibile sono oggi più che mai esposte a enormi rischi.

L'implementazione di una strategia di protezione dei dati impostata sulla cifratura comincia dal capire il motivo per cui la cifratura è essenziale, e come può essere utile nel vostro caso in particolare. Implementando una soluzione di cifratura che sia semplice potrete avere la tranquillità e la certezza che i vostri dati rimangono sempre e comunque protetti.

Declinazione di responsabilità

Gartner non appoggia alcun vendor né prodotto o servizio citato all'interno delle sue pubblicazioni di ricerca e non suggerisce agli utenti delle tecnologie in questione di scegliere solamente i vendor che abbiano ottenuto le valutazioni più elevate. Le pubblicazioni di Gartner riflettono solamente le opinioni dell'organizzazione, e non devono pertanto essere considerate come affermazioni di fatto. Gartner rinuncia a qualsiasi garanzia, implicita o esplicita, in merito a questa ricerca, incluse le garanzie sulla commerciabilità o sull'idoneità a un particolare scopo.

1. Verizon. (2015). 2015 Data Breach Investigations Report
2. PwC. (2015). 2015 Information Security Breaches Survey
3. Ponemon Institute. (2015). 2015 Cost of Data Breach Study: Global Analysis
4. Ponemon Institute. (2015). 2015 Global Encryption & Key Management Trends Study
5. Ponemon Institute. (2015). 2015 Global Encryption & Key Management Trends Study
6. Forrester Research, The Forrester Wave™: Endpoint Encryption, Q1 2015, redatto da Chris Sherman, 16 gennaio 2015
7. Gartner Magic Quadrant for Mobile Data Protection, John Girard, 8 ottobre 2015

Osservatela in azione

Scoprite di più su Sophos SafeGuard, e osservatela in azione, visitando sophos.it/encryption

Preventivo

Richiesta di preventivo senza obbligo di acquisto

Vendite per l'Italia:
Tel: (+39) 02 94 75 98 00
E-mail: sales@sophos.it

21/10/16 WPIT (DD-2467)

SOPHOS