SOPHOS
Security made simple.

Cifratura next-gen: La strategia Sophos

La perdita dei dati continua a essere un serio problema per le aziende di qualsiasi genere: nessuna al mondo è immune, indipendentemente da ubicazione geografica, dimensioni o settore di attività. Secondo Privacy Rights Clearinghouse, mentre la metà dei casi di violazione dei dati avvenuti nel 2014 era dovuta a hacking o malware, al secondo posto si trovava la diffusione accidentale dei dati (16%).

Allo stesso tempo, anche l'ambiente di lavoro ha subito enormi cambiamenti negli ultimi anni. Le aziende del giorno d'oggi devono proteggersi contro la perdita dei dati (accertandosi di rispettare le leggi sulla protezione dei dati), pur offrendo ai propri dipendenti la garanzia di poter mantenere i più alti livelli di efficienza possibili nel competitivissimo ambiente commerciale moderno.

La strategia della cifratura di ultima generazione (next-gen) adottata da Sophos è appositamente realizzata per soddisfare queste esigenze. Il presente documento descrive i motivi per cui la cifratura next-gen è un must, descrivendone la modalità operativa e dimostrando come Sophos semplifichi per le aziende di qualsiasi dimensione il processo di messa in sicurezza dei dati, pur garantendo ai propri utenti piena libertà e controllo.

Lo stato attuale

L'ambiente lavorativo attuale è molto diverso da quello di cinque o dieci anni fa. Vi sono differenze significative nel panorama dei dispositivi e delle minacce. Diamo un'occhiata ai due cambiamenti principali che hanno avuto un enorme impatto sulla protezione dei dati.

Non sono i dispositivi a essere mobili, siete voi

Il tipico utente finale ha in media tre dispositivi. Mentre un tempo venivano utilizzati computer desktop e talvolta laptop, il panorama si è esteso in modo tale da includere tablet e dispositivi mobili. Pensate ai vostri utenti finali. È molto probabile che abbiano un laptop e un dispositivo mobile; altri utenti avranno anche un tablet o due.

Spesso i dispositivi mobili contengono la stessa quantità, se non di più, di informazioni di natura sensibile di un laptop. Sono anche molto più facili da smarrire. Ciò significa che la potenziale superficie di attacco è in aumento, poiché gli utenti dispongono di un maggior numero di dispositivi che contengono dati.

La tipica forza lavoro è mobile, e vuole mantenere gli stessi livelli di produttività anche quando si trova in viaggio. La produttività significa fondamentalmente poter accedere ai dati aziendali sul dispositivo desiderato, da qualsiasi luogo e in qualsiasi momento.

È mezzanotte, avete idea di dove si trovino i vostri dati?

Sapete dove vengono archiviati i dati aziendali? Sono situati su server, desktop, laptop, dispositivi mobili, tablet, dispositivi di archiviazione removibili e anche su provider di cloud storage. I dati aziendali di natura sensibile si trovano all'esterno del tradizionale perimetro di rete dell'azienda, e ciò è in primo luogo perché il concetto di limite del perimetro aziendale è ormai obsoleto.

Come si può definire un limite per il perimetro aziendale se i dati si trovano su vari dispositivi mobili e soluzioni di cloud storage diverse? Questi dispositivi possono essere non gestiti, oppure trascorrere ben poco tempo all'interno della rete aziendale. Oppure, nel caso dei provider di servizi di cloud storage, è possibile che non sappiate neppure dove vengano fisicamente archiviati i dati, e chi vi possa accedere. Da tutto ciò deriva l'esigenza di proteggere i dati ovunque gli utenti decidano di conservarli.

Definire la strategia della Synchronized Encryption next-gen

Nell'elaborare la nostra strategia di cifratura di ultima generazione, abbiamo preso in analisi diversi ambiti nei quali i clienti rischiano di subire gravi danni in caso di perdita o violazione dei dati, che potrebbero causare l'inosservanza delle normative in vigore. La nostra strategia prende in considerazione i seguenti ambiti:

1. L'impatto del furto o dello smarrimento dei dispositivi
2. La modalità d'uso dei dati da parte degli utenti
3. La diffusione accidentale dei dati a causa di un errore umano
4. Gli attacchi di hacking o malware
5. La semplicità

Sebbene anche gli attacchi mirati (che sono diversi da quelli opportunistici, che utilizzano, ad esempio, malware o phishing) possano essere inclusi nell'elenco, la possibilità statistica che una piccola o media impresa cada vittima di un attacco mirato è piuttosto bassa. A meno che la vostra non sia un'azienda di grandi dimensioni, come Sony o Target, oppure che vi occupiate di informazioni estremamente specializzate o di natura particolarmente sensibile, i malintenzionati non sono disposti a investire le risorse necessarie per sferrare un attacco mirato.

L'impatto del furto o dello smarrimento dei dispositivi

L'utente medio possiede tre dispositivi, che possono tutti essere facilmente smarriti o rubati. Può capitare di perdere il telefonino sul treno mentre ci si reca al lavoro, oppure di dimenticare inavvertitamente il laptop ai controlli di sicurezza aeroportuale nella fretta di prendere un volo. I dispositivi sono piccoli, e possono sempre capitare disgrazie. La cifratura completa del disco serve a proteggere i dati a riposo, e rappresenta un'ottima prima linea di difesa. Tuttavia, non basta per proteggere i dati aziendali, se si osserva il comportamento degli utenti moderni.

La modalità d'uso dei dati da parte degli utenti

Osservate i vostri utenti per un'ora e prestate attenzione a come adoperano i dati. Li creano (in forma di documenti, presentazioni, ecc.), e copiano i file su condivisioni di rete, chiavi USB o servizi di cloud storage. L'utente finale lavora con i file, e i file vengono trasferiti tra vari dispositivi e opzioni di cloud storage diverse. In situazioni del genere, la protezione dei dati è un must.

Semplice errore umano

Siamo esseri umani. Rischiamo tutti di commettere errori. È capitato a tutti di creare un'e-mail, allegare il file sbagliato e inviare il messaggio per errore (oppure di mandare il file giusto al destinatario sbagliato). Vi sono vari esempi di come un semplice errore umano possa causare la perdita o la violazione dei dati. I browser web e i client di posta sono ottimi esempi di strumenti di produttività che vengono utilizzati dagli utenti finali per condividere i dati, ma che rischiano di esporre accidentalmente i dati aziendali al cloud o a occhi indiscreti.

Attacchi di hacking o malware

L'analisi svolta nel 2014 da Privacy Rights Clearinghouse sui casi di violazione dei dati ha classificato i vari tipi di violazione, scoprendo che hacking e malware costituiscono il 51% dei casi di violazione dei dati. Il malware è in costante aumento, sia dal punto di vista della quantità che della complessità. Ciò vale anche per il furto dei dati tramite attacchi opportunistici. Non ci si può fidare del malware, e occorre senza dubbio evitare che possa accedere ai dati cifrati.

La semplicità

La cifratura agisce in maniera ottimale quando nessuno si accorge che c'è. Offre una protezione discreta e silenziosa, senza interferire con le attività dell'utente finale. Si consideri ad esempio l'HTTPS. La S sta per "sicuro", e indica che tutte le comunicazioni tra il browser e i siti web sono cifrate. Tuttavia, la maggior parte degli utenti non nota quasi mai la differenza quando visita un URL.

La cifratura deve essere facile da usare sia per gli amministratori che per gli utenti finali, per poter raggiungere alti livelli di consenso generale.

La nuova Sophos Next-Gen Encryption

La strategia ci cifratura next-gen adottata da Sophos si basa su due asserzioni:

1. Tutti i dati creati da un utente finale sono importanti e devono essere protetti (cifrati). Questa parte della strategia è nota come cifratura "sempre attiva", oppure cifratura per impostazione predefinita.

2. La cifratura deve essere persistente, indipendentemente da dove un file venga salvato, copiato o trasferito.

La cifratura viene generalmente considerata come uno dei metodi migliori per proteggere i dati. Sia che l'utente stia creando un documento che descrive una nuova idea per un brevetto, o un foglio elettronico che delinea un nuovo concetto aziendale, si tratta sempre e comunque di dati importanti, e tali dati devono essere cifrati in maniera automatica e trasparente. Non si dovrebbe lasciare a un utente la responsabilità di decidere se cifrare o meno un file, secondo l'importanza che ritiene debba essere attribuita al file in questione. In realtà, è possibile fare in modo che gli utenti non si rendano neppure conto che i dati sono cifrati. Con questo approccio, gli utenti possono mantenere i consueti livelli di produttività e proteggere i dati senza modificare i normali flussi di lavoro.

Una volta cifrato, il file deve rimanere in questo stato. Qualsiasi cosa accada al file, indipendentemente da eventuali spostamenti, copiature, processi di rinomina, e dalla sua ubicazione all'interno o all'esterno del dispositivo, la cifratura deve essere persistente. Se un utente dovesse smarrire accidentalmente un file, tale file verrà smarrito nella sua forma cifrata, e ciò lo renderà inutile/illeggibile per chiunque non sia autorizzato a visualizzarlo.

E la DLP?

Quando si considera la protezione dei dati, spesso si pensa alla prevenzione contro la perdita/fuga dei dati (Data Loss/Leakage Prevention, DLP). DLP e cifratura hanno sempre avuto un rapporto interdipendente. Sebbene la DLP possa essere un'ottima tecnologia, esistono molti esempi di aziende che, una volta investite quantità elevate di tempo o denaro in una strategia di DLP, non la implementano. Il problema è la complessità del processo. Occorre applicare regole per i dati, che magari non sono ancora state create. Un problema comune è l'eccessiva severità delle regole impostate dagli amministratori, che genera un carico di lavoro molto elevato, dovuto ai falsi positivi. Spesso capita anche che gli amministratori rendano le regole troppo permissive, e ciò causa la fuoriuscita dei dati dall'azienda, nonostante sia presente un sistema di DLP. Sophos sta rivoluzionando la DLP, rimuovendo la necessità di classificare i dati. Questa semplificazione è di grandissimo aiuto sia per gli utenti finali che per gli amministratori.

Ciò non significa che la DLP non sia importante. La DLP svolge pur sempre un ruolo essenziale nella cifratura next-gen. Tuttavia deve essere un'eccezione, piuttosto che la regola. Quando gli utenti desiderano decifrare i dati, la rimozione della protezione da un file è una decisione consapevole. Ed è questo il momento ideale per eseguire, facoltativamente, le regole di DLP. Se non vengono segnalati allarmi, l'utente è in grado di decifrare il file, in quanto non è presente alcun elemento ritenuto sensibile. Tuttavia, in presenza di un segnale di allarme, la richiesta di decifratura del file viene negata. Questo approccio è un modo estremamente affidabile per garantire che i file continuino a essere cifrati. Oltre a tutto ciò, tutte le richieste di decifratura di un file vengono sottoposte ad audit e inserite nel log.

L'adozione di questo approccio semplifica notevolmente la DLP e riduce i requisiti di elaborazione, in quanto la valutazione delle regole di DLP diventa un'eccezione (ovvero viene effettuata solamente in fase di decifratura dei dati).

Synchronized Encryption

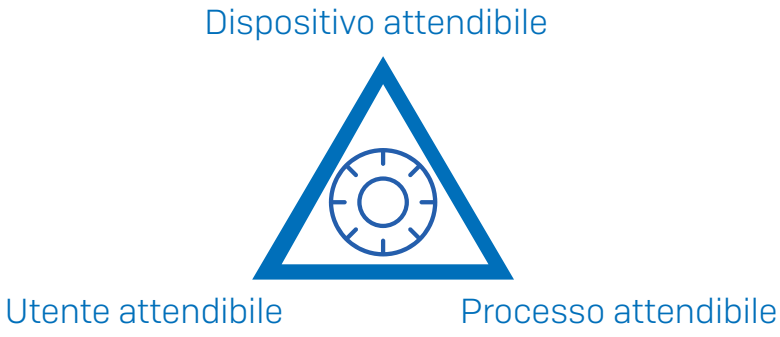
Presupponendo che tutti i dati degli utenti siano cifrati, il secondo elemento da proteggere in ordine di importanza sono le chiavi di cifratura che hanno cifrato i dati.

Le chiavi di cifratura si basano sul principio fondamentale che solamente dispositivi, app e utenti attendibili debbano avere diritto di accedere ai dati cifrati.

Per applicare questo principio, Sophos integra il know-how e l'efficacia dei prodotti Sophos Endpoint e Sophos SafeGuard Encryption (SafeGuard), al fine di trasformare la cifratura in una tecnologia di protezione contro le minacce. Il prodotto Endpoint continuerà a svolgere il proprio compito in maniera eccellente, determinando lo stato di sicurezza e di integrità del computer, e stabilendo se i processi in esecuzione siano o meno attendibili. Anche il prodotto di protezione dei dati continuerà con le attività per cui è stato realizzato, cifrando i dati e proteggendo l'accesso alle chiavi.

Per stabilire quando rilasciare le chiavi e autorizzare l'accesso ai contenuti cifrati, triangoliamo e sincronizziamo i dati relativi a identità dell'utente, dispositivo e applicazione/processo.

Per essere considerato attendibile e poter accedere ai dati cifrati, l'utente deve utilizzare un dispositivo attendibile, essere un utente attendibile, e adoperare un processo o un'applicazione ritenuta attendibile per l'accesso ai dati.



Occorre rispettare tutte e tre queste condizioni, per poter accedere alla chiave di cifratura e visualizzare i dati.

In quasi tutti i casi, un utente finale aziendale che è legittimo sarà in grado di accedere ai dati in maniera trasparente da un dispositivo attendibile (ovvero un dispositivo fornito in dotazione dall'azienda) e con applicazioni attendibili. Se una o più di queste condizioni non dovesse essere soddisfatta, l'accesso alla chiave di cifratura verrà negato e l'utente potrà vedere il file cifrato, ma senza essere in grado di visualizzarne i contenuti. In questo modo, anche se il malware per il furto di dati dovesse riuscire a esfiltrare un file protetto, tale file sarà inutile senza la chiave di accesso.

Dispositivo attendibile

Vi sono diversi modi per stabilire se un dispositivo sia attendibile. Ad esempio, lo può essere se su di esso sono installati i giusti prodotti Sophos. Oppure se l'agente Sophos Endpoint ha valutato il sistema, rilevandone lo stato come integro (Heartbeat™ verde). Inoltre, un dispositivo attendibile può essere un dispositivo mobile che viene gestito dalla soluzione di EMM dell'azienda, e che, in quanto tale, ne rispetta il criterio di sicurezza. In alternativa, è possibile per l'amministratore definire esplicitamente un sistema come non attendibile, come ad es. quando viene utilizzato da collaboratori esterni.

Se un laptop Windows o Mac si trova in uno stato di infezione attiva, e l'endpoint è in fase di rimozione del malware, con tutta probabilità il sistema non deve essere ritenuto attendibile. Per quanto riguarda dispositivi mobili quali iPhone o Android Phone, i dispositivi non devono essere considerati attendibili neanche quando non rispettano il criterio di conformità aziendale (ad es. nel caso di jailbreaking o mancanza di una password per il blocco dello schermo).

Utente attendibile

Proprio come per i dispositivi, vi sono anche vari modi per stabilire se un utente debba o meno essere considerato attendibile. Può esserlo in base all'identità, oppure semplicemente se effettua correttamente l'accesso al sistema. Vi sono casi di utilizzo, come ad es. quando un dipendente smette di lavorare per un'azienda, nei quali gli utenti possono accedere al dispositivo, ma senza disporre di accesso ai dati cifrati.

Processo attendibile

Sophos Endpoint svolgerà il ruolo principale nel determinare se un processo sia o meno attendibile. I dettagli specifici di tale processo, con o senza Sophos Endpoint, non rientrano nell'ambito di applicazione di questo documento.

Genericamente, per logica interna, PUA (applicazioni potenzialmente indesiderate), malware, virus, browser web o client di posta non vengono ritenuti attendibili. Tuttavia, vi sono altri tipi di applicazioni, come ad es. i programmi torrent, a cui le aziende possono istintivamente impedire l'accesso ai dati cifrati. I browser web e i client di posta vengono considerati inattendibili per impostazione predefinita, in quanto costituiscono modi in cui gli utenti possono accidentalmente condividere o smarrire dati importanti. Ciò aiuta a proteggere i sistemi dai problemi causati dal semplice errore umano.

Perché si parla di processi e non di applicazioni? In primo luogo, si tratta di garantire agli utenti finali la possibilità di mantenere gli stessi livelli di produttività. Bloccando esclusivamente i processi che non si comportano adeguatamente, si consente a tutti i processi attendibili di eseguirsi in maniera indisturbata.

Diamo un'occhiata a tre esempi di processi, che non sono né malware né virus, per determinarne l'attendibilità.

1. **Notepad**

   Notepad è un'applicazione semplice e autosufficiente. Può essere ritenuta attendibile perché è semplice e non contiene alcuna attività di tipo malevolo. Siccome Notepad viene considerata un'applicazione attendibile, può accedere alle chiavi di cifratura. Ciò consente di implementare la cifratura per impostazione predefinita dei documenti creati con Notepad, e la visualizzazione in chiaro dei documenti di testo cifrati.

2. **Internet Explorer**

   Internet Explorer è noto per essere stato oggetto di attacchi di exploit in passato, ed è un metodo comunemente utilizzato per distribuire malware sui dispositivi. In quanto tale, non viene considerato attendibile per impostazione predefinita. Siccome Internet Explorer non è attendibile, non può accedere alle chiavi di cifratura, per cui potrà effettuare l'accesso ai file soltanto nel loro formato cifrato. Non può né aprire né visualizzare i contenuti dei file, ma può caricare un file cifrato su un servizio di condivisione di file basato sul cloud.

3. **Microsoft Word**

   Microsoft Word può essere sia attendibile che non attendibile. Word può presentare un comportamento adeguato ed essere ritenuto attendibile, per cui quando un utente adopera Word per creare un documento, può essere cifrato per impostazione predefinita. L'utente può semplicemente fare doppio clic sui file cifrati per leggerli e modificarli. Il processo è completamente trasparente, perché Word viene ritenuto attendibile per l'accesso alle chiavi di cifratura allo scopo di cifrare/decifrare processi in background. Tuttavia Word può anche essere infettato con malware come i virus delle macro, e quando ciò avviene Word non può più essere considerato attendibile per l'accesso alle chiavi di cifratura, per cui non sarà in grado di leggere i dati cifrati.

Questi sono solamente tre esempi del processo di determinazione dell'attendibilità, e da essi emerge il bisogno del monitoraggio costante dell'integrità dei sistemi con la Synchronized Encryption.

Monitoraggio continuo dell'integrità prima di conferma l'attendibilità

In generale, è consigliabile che una tecnologia di protezione dei dati svolga il monitoraggio continuo dello stato di sicurezza, integrità e attendibilità delle applicazioni/dei processi di sistema. L'obiettivo è garantire agli utenti finali alti livelli di produttività, pur mantenendo protetti i dati. Come già discusso, se un processo non viene considerato attendibile, potrà accedere a un file solamente in formato cifrato, senza poter adoperare la chiave di cifratura per decifrarne i contenuti. Nella maggior parte dei casi, gli utenti non si rendono conto di questa operazione. Tuttavia, se il processo è malevolo, come nel caso del malware, è ovvio che non dovrebbe neppure essere eseguito. E se il sistema si trova in uno stato di infezione attiva, non deve essere considerato attendibile. L'attendibilità dei processi è la prima reazione allo stato di integrità, ma anche lo stato di sicurezza complessiva del sistema gioca un ruolo fondamentale nella strategia di reazione.

Torniamo al concetto del garantire agli utenti la possibilità di mantenere alti livelli di produttività. Occorre impedire ai processi non attendibili di accedere ai dati in chiaro, e bloccarne l'esecuzione. Tuttavia, nel caso in cui vi siano ad esempio due documenti Word aperti (il primo dei quali contiene un documento importante e sicuro sul quale state lavorando, e il secondo un file inviato da un amico o un collega), se uno di questi due documenti dovesse rivelarsi malevolo, occorre bloccare solamente il processo di Word che rappresenta un pericolo. L'utente deve poter continuare a mantenere la consueta produttività lavorando sul documento Word sicuro.

Se il sistema dell'utente dovesse essere infettato in maniera grave da uno o più malware la cui disinfezione è in corso, come ultima risorsa la Synchronized Encryption può revocare temporaneamente le copie locali delle chiavi di cifratura. La revoca delle chiavi garantisce che niente nel sistema possa decriptare file o dati. Ciò incide sulla produttività dell'utente, in quanto questi non potrà accedere ai dati cifrati, ma è proprio questo il punto. Si vuole veramente concedere a un utente (e alle applicazioni o processi che utilizza) l'accesso a dati cifrati da un sistema infetto? Ovviamente no. Una volta disinfettate la o le infezioni di malware, e una volta ripristinata e confermata l'integrità del sistema, le chiavi di cifratura vengono restituite al sistema, e l'utente potrà quindi godere nuovamente dei consueti livelli di produttività.

Un processo non attendibile è pericoloso?

Se un processo non è attendibile, significa che rappresenta un pericolo? Non necessariamente. Vi sono diversi casi di utilizzo nei quali è desiderabile concedere a un processo l'accesso ai file, ma solo in formato cifrato. Gli utenti possono ad esempio utilizzare un client di posta come Outlook per inviare un allegato. Il client di Outlook non è attendibile, ma può accedere ai file in formato cifrato per svolgere funzioni legate a consegna e allegati. Una volta raggiunto il destinatario, Outlook si affida a un'applicazione attendibile quale Word o Excel per aprire l'applicazione. Questo processo è completamente invisibile agli occhi dell'utente, e allo stesso tempo gli allegati sono cifrati e quindi protetti durante l'invio.

Questo esempio dimostra anche perché il concetto della Sophos Synchronized Encryption è ben diverso dal whitelisting delle applicazioni. Con il whitelisting, è possibile che un'applicazione inserita nell'elenco possa essere attendibile per l'esecuzione, ma ciò non significa che debba disporre di accesso ai dati cifrati. Con la Synchronized Encryption si determina se un'applicazione attendibile che viene eseguita abbia il giusto livello di attendibilità richiesto per poter visualizzare la versione in chiaro dei dati cifrati.

Synchronized Encryption senza Sophos Endpoint

Per usufruire di tutti i vantaggi di Sophos Synchronized Encryption, i clienti devono utilizzare sia Sophos Endpoint che Sophos SafeGuard. Ma come cambia questo concetto in assenza del prodotto Sophos Endpoint? Tutta la logica di cui sopra rimane pur sempre valida, ma la verifica dello stato di integrità del sistema e dell'attendibilità dei processi smette di essere dinamica e diventa statica. Il prodotto SafeGuard non può rilevare il malware, per cui occorre un metodo diverso per valutare lo stato di integrità del sistema. L'attendibilità dei processi si basa poi su una strategia che è più simile a un elenco di processi privi di nomi sicuri, che gli amministratori definiscono come attendibili. Per impostazione predefinita, qualsiasi voce contenuta in tale elenco non è attendibile.

Opzioni di collaborazione con la cifratura next-gen

Gli utenti finali hanno bisogno di collaborare tra di loro, sia all'interno che all'esterno di un'azienda, per poter svolgere le comuni mansioni lavorative e per mantenere adeguati livelli di produttività. La cifratura next-gen garantisce che tutti i dati creati sono protetti, e che l'accesso a tali dati viene concesso solamente a elementi attendibili. Come si svolge la collaborazione a questo punto? Anche in questo caso, l'obiettivo principale è permettere agli utenti di mantenere i consueti livelli di produttività e i normali flussi di lavoro. Procediamo ora a osservare in maniera più dettagliata queste due categorie.

Collaborazione interna

La collaborazione interna è in realtà l'esperienza più semplice e trasparente. Tutti gli utenti interni dell'azienda hanno accesso alle chiavi di cifratura. Tutti i dati creati vengono cifrati. Vengono condivisi in formato cifrato, e chiunque può accedervi.

1. **John crea e salva un documento Word.** Desidera l'opinione di Judy. Quando John salva il documento, viene salvato e cifrato automaticamente (cifratura per impostazione predefinita). John non deve svolgere alcuna azione in particolare per cifrare il documento Word.
2. **John apre Outlook e crea una nuova e-mail** avente come destinatario Judy. Agendo secondo il consueto flusso di lavoro, John allega il file all'e-mail. Digita il messaggio e lo invia. Outlook è un client di posta e, generalmente, non viene considerato attendibile. Siccome non è cifrato, viola uno dei tre pilastri (non è un processo attendibile). Quando Outlook legge il documento Word per allegarlo, il file viene allegato in formato cifrato.
3. **L'e-mail viene quindi inviata a Judy**, che riceve e apre l'e-mail di John. Il file allegato all'e-mail nella cartella della Posta inviata di John è cifrato. Il file allegato all'e-mail nella cartella di Posta in arrivo di Judy è cifrato. Il file allegato è cifrato durante l'invio da John a Judy.
4. **Judy fa doppio clic sul documento Word** allegato all'e-mail e lo apre in maniera trasparente in Word, dove Judy può ora revisionare il testo e inserire commenti. Outlook non è un'applicazione attendibile, per cui quando salva il documento su un percorso per i file temporanei, il file si troverà nel suo stato attuale, ovvero quello cifrato. Outlook lancia quindi Word, richiedendo l'apertura del file temporaneo appena creato. Word è attendibile, e ha accesso alla chiave. Siccome Judy è un'utente attendibile, il dispositivo di Judy è attendibile e MS Word è attendibile, il documento potrà essere decifrato per la lettura, e visualizzato nel formato corretto e in chiaro per Judy.

   Inoltre, se Judy dovesse leggere questa e-mail da un dispositivo mobile protetto con Sophos Mobile Control, avrà la possibilità di salvare l'allegato cifrato in Secure WorkSpace (e nel contenitore cifrato); siccome questo contenitore cifrato ha la stessa chiave, Judy potrà visualizzare i contenuti senza metterne a repentaglio la sicurezza.

Né John né Judy devono modificare il proprio normale comportamento, e tutte le loro interazioni sono cifrate. La loro esperienza è trasparente, e possono collaborare senza alcun problema.

Collaborazione esterna

La collaborazione esterna subisce dei cambiamenti quando tutti i dati vengono cifrati. Gli utenti possono collaborare esternamente in due modi, ovvero tramite:

1. Protezione con password (incapsulamento in un file HTML5)
2. Decifratura

Collaborazione esterna con un file decifrato

Vi sono casi di utilizzo in cui conviene condividere i dati in formato decifrato. Ne sono un esempio le informazioni pubbliche, quali gli opuscoli. Si tratta di informazioni pubbliche che sono accessibili a chiunque, per cui la decifratura non rappresenta un problema. La decifratura dei dati è l'unico momento in cui la cifratura next-gen si troverà "a tu per tu" con l'utente finale. L'utente deve infatti confermare di essere conscio del fatto che sta prendendo la decisione consapevole di decifrare il file in questione.

L'utente dovrà prendere la decisione consapevole di decifrare il file prima di inviarlo. Come discusso in precedenza, il file può opzionalmente essere sottoposto a un'analisi di DLP per verificarne i contenuti, e se non viene sollevato alcun allarme, il file verrà decifrato. Inoltre la cifratura, o in questo caso la decifratura, è persistente, per cui rimarrà nello stesso stato. L'intero processo viene inserito nel log e sottoposto ad audit, per consentire all'amministratore di monitorare eventuali comportamenti malevoli da parte dei dipendenti. Una volta decifrato il file, è possibile proseguire secondo il normale flusso di lavoro.

Collaborazione esterna con un file protetto da password

Cosa succede se si desidera inviare un contratto in maniera sicura a un destinatario esterno, ma occorre consentire a tale destinatario la possibilità di decifrare e utilizzare il file, senza sapere se questi abbia a disposizione un software di cifratura?

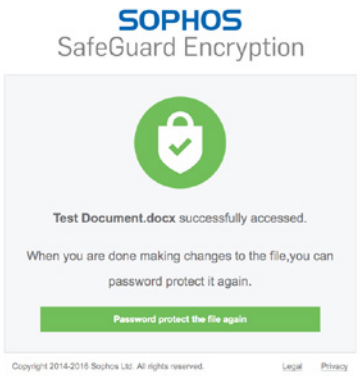
L'utente deve semplicemente creare un file protetto da password e impostare una password. Essenzialmente, il software ri-cifra il file contenente il contratto (che chiameremo contract.doc) con la password assegnata dall'utente, e lo incapsula in un wrapper HTML5. Il processo crea un file che si chiama contract.html. Occorre comunicare la password al destinatario. Il risultato è un singolo file HTML che può essere interpretato da qualsiasi browser su cui è abilitato HTML5 e su tutti i sistemi operativi. Il singolo file HTML è composto da tre parti ben distinte:

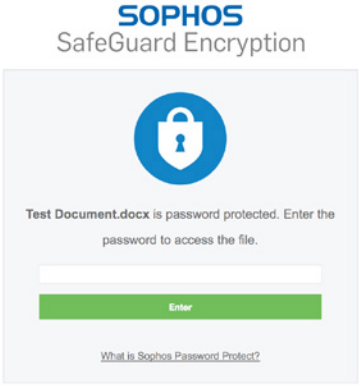
1. Il livello di presentazione (ciò che l'utente vede nel browser web quando apre il file)
2. Il codice per decifrare il payload allegato
3. Il file cifrato (contract.doc in questo esempio)

L'utente invia quindi al destinatario un'e-mail con contact.html, invece di contract.doc. Quando il destinatario fa doppio clic sul file HTML nel proprio client di posta, verrà aperta una finestra del browser che richiede l'inserimento della password. Presupponendo che venga inserita la password corretta, il browser eseguirà il codice per decifrare il file, e quest'ultimo verrà salvato localmente sul computer del destinatario in formato non cifrato.

Ciò permette l'invio del file riservato in formato cifrato, per poi consentirne la decifratura quando viene aperto dal destinatario.

Se il destinatario deve restituire un file aggiornato, il wrapper HTML può anche essere utilizzato come contenitore. Il destinatario deve semplicemente aggiornare il file e trascinarlo nella schermata HTML. Questo processo crea una collaborazione bidirezionale sicura con un utente esterno che non possiede Sophos SafeGuard Encryption.





Semplificare la vita agli utenti finali

Per semplificare la vita agli utenti finali, Sophos offre varie funzionalità, come ad es. un plugin per Outlook, in grado di rilevare i messaggi e-mail inviati all'esterno dell'azienda e contenenti un allegato. Può quindi comunicare all'utente che sta per inviare un file cifrato, e chiedere quale delle opzioni desidera selezionare per la collaborazione esterna. In questo modo può anche adottare le dovute misure. Alternativamente, è possibile concedere a un amministratore la facoltà di specificare, mediante l'uso dei criteri, un'azione predefinita da svolgere in maniera automatica.

Accesso ai dati su piattaforme multiple

Per consentire agli utenti finali di mantenere gli stessi livelli di produttività, questa funzionalità di cifratura next-gen deve essere eseguita su tutti i dispositivi più comunemente adoperati dagli utenti. Questa funzionalità è compatibile con Windows, OS X, iOS e Android.

Abbiamo accennato in precedenza che gli utenti hanno in media tre dispositivi a testa. In caso di una grave infezione di malware sul computer Windows di un utente, questo computer viene isolato e considerato non attendibile. L'utente può tuttavia continuare a utilizzare e mantenere gli stessi livelli di produttività sui propri Mac o iPad, sia che si trovi in ufficio o in viaggio. Quando un dispositivo viene compromesso, è pur sempre un inconveniente, ma almeno in questo modo l'utente ha la possibilità di utilizzare un dispositivo diverso.

Protezione next-gen dei dati contro le minacce

Con Sophos i clienti possono raggiungere livelli superiori di sicurezza quando uniscono la cifratura next-gen alla nostra vasta gamma di prodotti per la sicurezza sincronizzata. Se un cliente ha Sophos Endpoint più Sophos UTM/Firewall e Sophos SafeGuard, tutte e tre le soluzioni agiranno in sincronia non solo per offrire una soluzione in grado di rilevare e rimuovere le minacce in maniera più efficace, ma anche per garantire che i dati cifrati siano inaccessibili alle minacce. Ecco la sicurezza di ultima generazione per la vostra azienda.

Conclusione

La cifratura next-gen rivoluziona i paradigmi della protezione dei dati. L'uso della cifratura sempre attiva al posto della tradizionale cifratura di file/cartelle solleva gli utenti finali dall'onere di decidere quali siano i dati importanti e gli elementi da cifrare. Di conseguenza, l'intero sistema diventa più semplice per l'utente finale, in quanto i file vengono cifrati/decifrati in maniera automatica e trasparente, senza modificare il normale flusso di lavoro. La Synchronized Encryption protegge i dati contro le minacce, revocando le chiavi dai sistemi infetti e negando l'accesso alle applicazioni non attendibili o malevole. Tutto ciò garantisce livelli costanti di produttività per gli utenti, mentre i dati (e l'azienda) rimangono protetti.

Più di 100 milioni di utenti in 150 paesi si affidano a Sophos, per la migliore protezione contro minacce complesse e perdita di dati. Sophos si impegna a fornire soluzioni di protezione completa facili da distribuire, gestire e utilizzare, che garantiscono il più basso TCO (Total Cost of Ownership) del settore. Sophos offre soluzioni all'avanguardia per cifratura, sicurezza per endpoint, web, e-mail, dispositivi mobili, server e rete - tutti basati sul supporto dei SophosLabs: la nostra rete internazionale di centri di analisi e prevenzione delle minacce. Per saperne di più, visitate: www.sophos.it/products.

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

01/08/2016 WP-IT (NP)