CRITTOGRAFIA SOFTWARE E CONFORMITÀ NORMATIVA: SOLUZIONI MENO COSTOSE E RISCHI DI SICUREZZA PIÙ ELEVATI

REQUISITI NORMATIVI E DI CONFORMITÀ

In precedenza, la sicurezza dei dati era un aspetto relegato ai soli reparti IT. Tuttavia, a causa delle continue violazioni ai danni degli utenti, i governi mondiali hanno iniziato a imporre alle aziende requisiti sempre più stringenti per crittografare e proteggere tutti i dati che consentono di identificare le persone.

Dallo standard HIPAA nel settore sanitario, al regolamento GDPR in ambito EMEA e a quello CCPA in California, la crittografia delle classi di dati protetti viene resa obbligatoria mediante regolamenti. Le organizzazioni incaricate della conformità si sono moltiplicate esponenzialmente negli ultimi 3 anni o più. Ciò a causa del moltiplicarsi delle sanzioni e delle cause legali associate a tale problema.

A causa di tali cambiamenti, i reparti IT hanno iniziato a trovarsi in difficoltà nello stare al passo con sicurezza e costi crescenti. Durante la pandemia causata dal virus COVID, i budget vengono utilizzati per hardware aggiuntivo e investimenti in firewall, a detrimento delle misure finalizzate a implementare la crittografia dei dati.

Di fatto, la crittografia software basata su soluzioni come Microsoft BltLocker® o software di gestione degli endpoint di aziende come Symantec, McAfee o altri provider simili, è in costante crescita. Alcune aziende e consumatori utilizzano anche drive USB di tipo standard con drive integranti "partizioni sicure", come quelle fornite da provider specifici.

CRITTOGRAFIA E DATI IN TRANSITO

Dipendenti e consumatori hanno la necessità di avere i loro dati sempre con se. Per fare ciò esistono svariate opzioni come:

1. Servizi Cloud: Una soluzione ideale, in quanto consente di accedere ai dati da qualunque dispositivo connesso a internet. Tuttavia, la flessibilità ha un prezzo. Lo storage dati su cloud non consente all'utente di controllare i suoi dati o quelli dell'azienda, con il potenziale rischio che i server cloud in cui tali dati risiedano vengano violati o infiltrati.
2. Drive USB standard: Sebbene l'uso di un drive USB appaia più sicuro, il rischio di violazione dei dati in caso di smarrimento del drive è notevole. Per esempio, non è infrequente sentire storie di drive USB persi e ritrovati da terzi con informazioni riservate al loro interno, oppure di cassetti pieni di drive USB persi e mai restituiti.
3. Drive USB con crittografia hardware, USB: Questi drive USB sono dotati di architetture personalizzate che integrano un controller crittografico integrato e controllo degli accessi. I dati vengono crittografati con il protocollo crittografico più sicuro, ossia AES -256 bit in modalità XTS, unitamente ad altre misure di sicurezza finalizzate a mitigare attacchi fisici o verso il firmware. Questi drive sono realizzati da aziende specializzate in dispositivi di sicurezza e, sebbene più costosi rispetto i drive USB tradizionali, offrono una maggiore sicurezza dei dati. I drive con certificazioni FIPS 197 o FIPS 140-2 di livello 3 possono aggiungere straordinari livelli di protezione e sicurezza.
4. Drive USB standard con crittografia software: Al fine di operare in conformità con i requisiti di sicurezza normativi, è possibile utilizzare soluzioni di crittografia software con BitLocker o altre soluzioni simili. Si tratta di soluzioni accettabili e dai costi relativamente ridotti che utilizzano la medesima crittografia AES-256 XTS.

Non deve sorprendere il fatto che nella maggior parte dei casi aziende e industrie tendono a optare per la quarta opzione, ossia la crittografia software. Ciò principalmente perché la crittografia software come BitLocker o altre soluzioni di sicurezza dei dati sono "gratuite".

TUTTAVIA, LA CRITTOGRAFIA SOFTWARE NON È CONFORME ALLE NORMATIVE VIGENTI

Per i professionisti della sicurezza aziendale, la crittografia software è in grado di offrire esattamente le stesse funzionalità delle più costose soluzioni basate su drive USB con crittografia hardware. Ma si tratta veramente della soluzione più indicata? Con budget ridotti, le aziende stanno optando per la crittografia software a fini di conformità normativa, inconsapevoli di alcuni importanti aspetti negativi associati alla crittografia basata su software.

Qual è il problema con i drive USB dotati di crittografia software? I data at rest (dati a riposo) e quelli in transito non sono sempre e comunque crittografati con tecnologia AES-256 XTS? In generale, la risposta è si. Il problema è che: La crittografia software è considerata "crittografia rimovibile".

Come sarebbe a dire "rimovibile"? Significa che un drive con crittografia software può essere soggetto a disattivazione della crittografia da parte degli utenti?

La risposta è affermativa. Gli utenti possono rimuovere la funzione di crittografia software dai drive USB. Ci si potrebbe chiedere, perché farlo? Semplicemente perché lo possono fare e perché desiderano poter accedere ai loro file senza necessità di utilizzare una password, oppure perché hanno dimenticato la password ma necessitano dei dati contenuti nel drive USB.

COME RIMUOVERE LA CRITTOGRAFIA SOFTWARE DA UN DRIVE USB

Per gli utenti che non desiderano inserire password complesse o di altro tipo, l'accesso ai dati è semplice:

1. È sufficiente connettere un drive con crittografia software a un computer
2. Formattare il drive
3. Una volta completata la formattazione, la crittografia è rimossa
4. Copiare i file con informazioni segrete o confidenziali nel drive per un facile accesso

Si tratta di un'operazione semplice per gli utenti che utilizzano un computer non soggetto a restrizioni. I reparti IT hanno implementato restrizioni in termini di comandi utilizzabili sui computer aziendali, ma la stessa procedura può essere attuata anche su qualunque computer non aziendale.

A fini di conformità, la semplicità di disattivazione della crittografia dati si traduce nel fatto che un drive precedentemente fornito dall'azienda in forma crittografata è ora privo di tale funzione, anche se i dati crittografati che erano stati archiviati sul drive sono ora persi per sempre dopo la disattivazione della funzione crittografica con il metodo indicato sopra (le chiavi crittografiche sono associate ai dati). Qualunque dato archiviato sul drive dopo la disattivazione della funzione crittografica sono considerati non sicuri e potenzialmente non conformi, e ciò può causare violazioni di regolamenti come HIPAA, GDPR, CCPA e altri.

LE CONSEGUENZE DELLA PERDITA DI DRIVE NON CRITTOGRAFATI

Se il drive USB fornito da una data azienda viene perso e poi ritrovato, anche se l'azienda non è inizialmente consapevole ma lo scopre successivamente attraverso social media, l'evento costringe l'azienda a rispettare specifici requisiti di conformità, tra cui:

1. La necessità di condurre un'indagine forense per identificare i dati andati persi
2. Determinare se l'evento comporta violazioni di tipo legale, di concerto con il dipartimento legale
3. Determinare se è necessario inviare notifiche ai clienti

Ed è a questo punto che la perdita di un singolo drive USB può diventare estremamente costosa. Con parcelle per servizi legali che ammontano a migliaia di euro all'ora, tali processi di conformità possono causare migliaia e migliaia di euro di spese, oltre al potenziale rischio di sanzioni pecuniarie, cause legale intentate dai clienti e dal altri soggetti, e all'imbarazzo causato dalla diffusione dei dati.

Quando la crittografia software viene considerata un'alternativa fattibile in virtù dei costi ridotti, spesso non si tengono in conto i rischi di cui sopra e le potenziali conseguente economiche.

Ma esiste anche un altro rischio associato all'uso di drive USB non crittografati su reti aziendali. Si tratta di una minaccia nota come "BadUSB". BadUSB è una classe di malware che è stata utilizzata spesso da attori maligni per violare i firewall aziendali e introdurre malware nelle difese informatiche di una data azienda, attraverso dispositivi di storage USB.

BadUSB

Quando un drive USB viene connesso a un computer, il controller del chipset del computer avvia una procedura di handshake con il controller del drive USB mediante il firmware. Questo scambio avviene a valle dei sistemi operativi come Microsoft/macOS/Linux e quindi prima che questi rilevino la connessione del drive USB al computer. Ciascun drive USB è dotato di un firmware che viene eseguito quando il drive viene collegato a una porta USB.

Attori maligni hanno capito che è possibile infettare un computer mediante un malware attraverso la procedura di handshake, sostituendo il firmware eseguito sul drive USB con un firmware maligno che inietta il malware nel computer target quando questo comunica con il drive USB. Un drive USB standard non dispone di alcuna funzione di sicurezza sul firmware interno eseguito dal controller e pertanto un drive USB tradizionale viene tramutato in drive BadUSB maligno con il fine di penetrare attraverso i firewall e violare le difese informatiche dei sistemi attaccati.

Numerose aziende cercano di bandire l'uso dei drive USB sui loro sistemi, oppure anche riempire le porte USB con resina epossidica. Tuttavia, si è rilevato che specifiche categorie di dipendenti necessitano di trasportare i dati con loro mediante drive USB. Per esempio, alcuni dirigenti che desiderano portare i dati al lavoro o per consentirne l'uso a consulenti legali o finanziari che non operano su un cloud aziendale; collaboratori esterni che necessitano di tali dati per lavoro ma non possono accedere ai database aziendali; analisti finanziari che devono rispettare pressanti scadenze nella compilazione dei loro rapporti mensili con la necessità di operare su fogli di lavoro da casa.

Come indicato dall'analisi precedente, esiste un notevole rischio associato all'uso di drive USB standard con soluzioni di crittografia software. A prima vista, una soluzione che appare economica, si rivela essere anche potenzialmente pericolosa e costosa. Solo il costo di una consulenza di 2 o 3 ore con un avvocato e relativa a potenziali violazioni dei dati, annulla qualunque risparmio derivante dall'uso di soluzioni economiche.

I DRIVE DOTATI DI CRITTOGRAFIA HARDWARE SONO LA SOLUZIONE MIGLIORE PER LA CONFORMITÀ NORMATIVA

Cosa rende i drive USB dotati di crittografia hardware la soluzione migliore per le applicazioni associate alla conformità normativa:

1. I drive USB sono dotati di funzioni di crittografia hardware sempre attiva: Gli utenti non sono in gradi di disattivare la funzione crittografica, resettare le regole della password (anche in termini di lunghezza minima e complessità) e disabilitare o alterare il numero di tentativi di inserimento password non validi impostati automaticamente. A differenza della crittografia software, che non limita il numero di tentativi di inserimento password mediante attacchi con dizionari software, le versioni hardware limitano il numero di tentativi, bloccando i dati quando vengono effettuati 10 tentativi errati di inserimento password, o spesso anche un numero inferiore. Questa funzione è estremamente sicura nell'era dei supercomputer.
2. I drive con crittografia hardware utilizzano anche controller con funzioni di crittografia premium e sono dotati di svariate funzioni di sicurezza: Anche se non sempre riveliamo tutte le contromisure di sicurezza adottate, esistono misure specifiche che garantiscono la protezione contro gli attacchi BadUSB. In fabbrica, quando viene caricato il firmware sui drive con crittografia hardware, vengono utilizzati esclusivamente firmware firmati digitalmente. Ciò significa che quando tali drive USB crittografati vengono connessi a un computer, il controller crittografico effettua prima di tutto una verifica dell'integrità del firmware attraverso la firma digitale ed effettua il caricamento solo una volta effettuata tale verifica. Qualunque tentativo di sostituire il firmware causa il blocco del drive che non sarà più in grado di funzionare, eliminando qualunque minaccia.
3. I drive USB dotati di crittografia hardware possono anche essere dotati di ID prodotto (PID) personalizzate per un'azienda specifica: Questi drive di classe premium possono integrare un identificatore digitale programmato al loro interno. In tal modo, quando il drive viene connesso a un firewall aziendale interno o esterno, viene identificato come drive aziendale. Per esempio, se un dipendente perde un drive aziendale e acquista un modello identico in un negozio al dettaglio, il nuovo drive, seppure esternamente identico, non sarà autorizzato ad accedere alla rete aziendale. Questa personalizzazione aggiunge un livello di sicurezza ulteriore ai drive USB.
4. I drive con crittografia hardware consentono di risparmiare denaro in maniera rapida: La sola riduzione o eliminazione dei potenziali rischi ripaga i clienti dai costi sostenuti per il loro acquisto in brevissimo tempo.

Kingston è il leader mondiale nella produzione di drive USB crittografati e offre famiglie di drive dotati di varie funzionalità e varie fasce di prezzo. Contattate direttamente Kingston per discutere in che modo possiamo aiutarvi a mantenere la conformità con le soluzioni USB crittografate per dirigenti, dipendenti, collaboratori esterni e altre figure professionali.