Perché i drive USB sono ancora importanti nell'attuale contesto?

#KingstonIsWithYou

Perché i drive USB sono ancora importanti nell'attuale contesto?

Prefazione e contenuti

In un mondo digitale in cui il 60% dei dati aziendali globali viene archiviato sul cloud[1], discutere della rilevanza di una tecnologia storage utilizzata da quasi trent'anni può sembrare strano. Tuttavia, dalla sua introduzione, questa tecnologia si è evoluta costantemente e continua a farlo ancora oggi.

Sono oramai lontani gli anni in cui i drive USB rappresentavano solo un modo per connettere file, drive e applicazioni. Le moderne soluzioni non solo vantano migliori velocità di trasferimento, ma rappresentano anche alternative di storage affidabili e sicure spesso indispensabili. Ma perché i drive USB sono ancora importanti, quando le soluzioni di storage basate sul cloud sembrano offrire pressoché gli stessi vantaggi?

Questo eBook spiega il ruolo dei drive Flash USB in un mondo dominato dalle soluzioni cloud. Con il supporto di alcuni dei principali esperti del settore, spiegheremo in che modo le moderne organizzazioni utilizzano i drive USB, discutendo del loro ruolo rispetto alle soluzioni dotate di crittografia software, ambienti di storage indipendenti e di funzioni di sicurezza dati degli endpoint.

Indice dei contenuti	Pagine

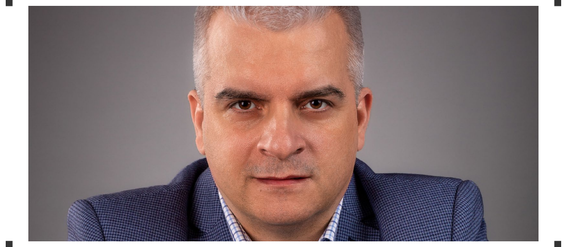
Perché i drive USB sono ancora importanti nell'attuale contesto?

Collaboratori

Questo eBook è stato realizzato con il contributo di tre esperti in IT e tecnologie emergenti.

Rafael Bloom

Rafael ha trascorso la sua carriera operando in vari ruoli dirigenziali nei settori delle tecnologie di prodotto, delle comunicazioni di marketing e nello sviluppo aziendale. L'attività della sua azienda di consulenze è incentrata sulle nuove sfide associate ai cambiamenti tecnologici e normativi in ambito organizzativo, dei prodotti e delle comunicazioni. Questo tipo di attività, caratterizzata da elevata interdisciplinarità, implica il possesso di conoscenze nei settori della governance e della conformità in termini di design, privacy dei dati e tecnologie emergenti, come AdTech, tecnologie mobili e 5G, IA e machine learning.



Tomasz Surdyk

Con i suoi 24 anni di esperienza nella sicurezza IT del settore amministrativo, Tomasz è una figura di spicco in materia di sicurezza informatica, cybersecurity e dati personali. Nella sua carriera ha gestito reti e sistemi ICT in cui vengono elaborate informazioni segrete e dati personali all'interno di amministrazioni pubbliche, oltre che nella NATO e nell'UE. Da diversi anni Tomasz è titolare di un'azienda specializzata nell'implementazione di soluzioni di sicurezza finalizzate ad accrescere la sicurezza di dati aziendali e dati personali.

David Clarke

David è considerato uno fra i primi 10 influencer nella classifica redatta da Thompson Reuter ("Top 30 most influential thought-leaders and thinkers on social media, in risk management, compliance and reg-tech in the UK") e figura anche nella Top 50 degli esperti globali di Kingston Technology. In passato, David ha rivestito numerosi ruoli nell'ambito della gestione della sicurezza , come Global Head of Security Service Delivery ed Head of Security Infrastructure per svariate aziende Global FTSE 100.

L'avvento dei drive flash USB

Quando il primo drive USB (Universal Serial Bus) fu lanciato sul mercato, oltre vent'anni orsono, la compatibilità pressoché universale di tale tecnologia rivoluzionò il settore informatico. Grazie alla capacità di mettere a disposizione degli utenti molteplici dispositivi, lo standard USB si è evoluto rapidamente, offrendo velocità di trasferimento notevolmente più elevate, una porta USB 3.0 e funzionalità ancora maggiori, con il lancio del primo drive Flash USB, nel 2000.

Da allora, la tecnologia ha fatto passi da gigante in termini di capacità di storage mobile e di capacità di adeguarsi alle moderne esigenze di sicurezza. L'attuale trend del settore si concentra verso drive USB progettati per impieghi specifici. Sotto il profilo aziendale, la diffusione dello smart working, l'uso dei servizi cloud e le sfide poste dalla sicurezza informatica, stanno portando il settore verso soluzioni più efficaci. Oltre a ciò i requisiti normativi richiedono che i dati siano memorizzati e secondo metodi conformi. Tali pressanti requisiti spesso si uniscono alla necessità di utilizzare sistemi distribuiti e complessi installati su base locale oppure su cloud.

Bisogna poi tenere in considerazione i volumi crescenti di dati strutturati e non strutturati, come documenti, email, foto, video, e metadati, che aggiungono complessità al soddisfacimento di esigenze di storage aziendale sempre più complesse.

Ma se tali esigenze possono essere soddisfatte dallo storage su cloud, qual è il ruolo e la rilevanza dei drive USB nell'attuale panorama aziendale?

> **Molti pensano ai drive USB come soluzioni obsolete oppure troppo semplici in quanto il loro utilizzano il passato era considerato come una sorta di dispositivo economico, a basse prestazioni e caratterizzato da bassi livelli di sicurezza. - Rafael Bloom**

Storage portatile che soddisfa le crescenti esigenze del mercato

La vecchia idea che vedeva i drive USB come soluzioni per lo storage portatile, è stata sostituita dalla concezione dei drive USB come soluzioni di storage ad alte prestazioni in grado di proteggere i dati per utilizzi personali e funzioni di backup su base locale, con funzionalità in grado di offrire funzioni aggiuntive per la protezione e la confidenzialità dei dati. Questo aspetto può assumere notevole importanza nel caso di applicazioni che prevedono il trattamento di dati particolarmente sensibili ai requisiti di conformità come i dati relativi alle risorse umane dati finanziari dati medici, sicurezza della proprietà intellettuale (IP) e tutte le informazioni che consentono l'identificazione personale (PII). Inoltre, questa generazione di dispositivi offre velocità di trasferimento elevate, grandi capacità di storage, funzionalità di backup e di sicurezza che possono essere utilizzate per:

- L'archiviazione di informazioni normative che richiedono la distribuzione manuale
- L'archiviazione di documenti legali e finanziari che devono essere consegnati o stampati fuori dagli uffici o da località remote
- Qualunque ambiente ostile in cui il ransomware può rappresentare una minaccia
- Trasferimento dei dati verso sistemi di stampa non dotati di funzionalità di rete

In qualità di produttore leader di soluzioni USB crittografate Kingston Technology si è tenuta al passo con le crescenti esigenze del settore, Realizzando soluzioni come Kingston IronKey™ S1000. I migliori drive USB crittografati del settore sono conformi ai più rigidi standard di sicurezza, con la capacità di proteggere i dati confidenziali attraverso soluzioni di crittografia XTS-AES a 256-bit e chip crittografici dotati di solide funzionalità antimanomissione. Inoltre tali drive sono dotati di certificazione FIPS 140-2 di Livello 3. Ciò significa che tali dispositivi sono sono formalmente certificati come dispositivi hardware crittografici per l'utilizzo in contesti governativi negli Stati Uniti; ciò ne fa una soluzione ideale per qualunque organizzazione che necessita di gestire dati riservati in tutta sicurezza e tranquillità.

questi drive USB con crittografia hardware offrono soluzioni di gestione sicura dei dispositivi indipendentemente dal fatto che i dati siano archiviati su base locale o sul cloud. L'uso di soluzioni di storage dati crittografati conformi che siano anche semplici da utilizzare senza alcun software aggiuntivo consente anche di liberare tempo prezioso per il personale IT, con soluzioni progettate per un'implementazione semplice ed efficiente.

Storage portatile che soddisfa le crescenti esigenze del mercato

Archiviazione e backup sono altri due ambiti in cui i drive USB possono essere utilizzati per proteggere le risorse digitali a lungo termine, indipendentemente dai servizi cloud offerti da terze parti. Sebbene sia vero che i trasferimenti di grandi volumi di dati possono essere gestiti con maggiore semplicità mediante applicazioni cloud, i dati IP proprietari possono ancora essere sufficientemente sensibili da richiederne l'archiviazione su dispositivi USB sicuri crittografati scollegabili dalla rete internet in tutta sicurezza.

Ci saranno sempre circostanze in cui un'organizzazione ha bisogno che i dati siano logicamente e fisicamente sotto il proprio controllo, soprattutto quando si utilizzano unità crittografate. Esistono casi in cui lo storage su dispositivi HDD/SSD tradizionali non può essere crittografato. In tali casi, l'utilizzo di drive USB crittografati esterni, come il Kingston IronKey D300S consente di risolvere questo problema. Questo drive flash USB è dotato di crittografia hardware che utilizza lo standard XTS 256-bit AES (Advanced Encryption Standard), che è uno standard di cifratura a blocchi in grado di crittografare blocchi dati da 128-bit. E quando sopraggiunge la necessità di crittografare dati con criteri ancora più rigidi lo standard AES utilizza la modalità di cifratura a blocchi XTS, che è in grado di garantire una migliore e più resiliente protezione dei dati rispetto alle altre modalità.

> Secondo me, i drive flash USB vengono ancora utilizzati e rappresentano un elemento integrante nell'ambito della sicurezza dei dati. Tra gli altri utilizzi tali drive vengono anche utilizzati per il trasferimento rapido di informazioni tra dispositivi differenti, nonché per garantire un adeguato livello di protezione dei dati archiviati. - Tomasz Surdyk

Crittografia: Crittografia hardware e software a confronto

Passando osservare in che modo i dati vengono crittografati, è possibile affermare che la crittografia hardware rappresenta rappresenta una soluzione più sicura è semplice da gestire rispetto alla crittografia software Ciò perché il processo di crittografia viene tenuto separato dal resto del sistema host e ciò rende più difficile qualunque tentativo di intercettazione o manomissione. La gestione centralizzata a livello di dispositivi consente di controllare i drive attraverso la rete LAN interna e le connessioni Internet e costituisce uno strumento eccellente per:

- La definizione di regole di utilizzo della crittografia USB per soggetti singoli o gruppi
- Monitorare l'attività dei file, per meglio tracciare l'ingresso e l'uscita dei file dall'organizzazione
- Fornire funzioni di backup dei contenuti remoto per il trasporto di dati critici
- Effettuare la disabilitazione da remoto di dispositivi quanto un dispositivo USB va perso oppure compromesso
- Eseguire il reset da remoto delle password quando queste vengono dimenticate

Quando i drive autorizzati vengono correttamente gestiti secondo questo processo, si minimizzano i rischi che i dati in essi contenuti vengano copiati o condivisi in maniera illegale. Inoltre, i moderni drive USB con crittografia hardware sono dotati di numerose funzionalità extra che contribuiscono a impedire l'accesso e la lettura di dati e messaggi ai soggetti non autorizzati.

> **Credo che la crittografia hardware sia notevolmente superiore rispetto a quella software. La crittografia hardware quella software sono caratterizzate da notevoli differenze in termini di vulnerabilità agli attacchi brute force. I dispositivi dotati di crittografia hardware sono più resistenti agli attacchi brute force.**
> **- Tomasz Surdyk**

Crittografia: Crittografia hardware e software a confronto

Sebbene molte aziende siano più inclini ad acquistare dispositivi dotati di crittografia software in ragione dei costi inferiori, tale decisione può spesso rivelarsi svantaggiosa. Le soluzioni basate su crittografia software condividono le medesime risorse di crittografia del dispositivo host con altri programmi. Pertanto, la sicurezza di tali dispositivi dipende direttamente dalla sicurezza del computer e spesso richiede aggiornamenti software che, se non effettuati con regolarità, espongono a vulnerabilità. I drive USB dotati di crittografia software possono essere soggetti anche a attacchi di tipo brute force per periodi di tempo illimitati, che tentano di indovinare la password e non ci sono soluzioni adeguate in grado di fare fronte a tali attacchi basati sull'uso di dizionari in grado di testare milioni di combinazioni di caratteri in periodi di tempo brevissimi.

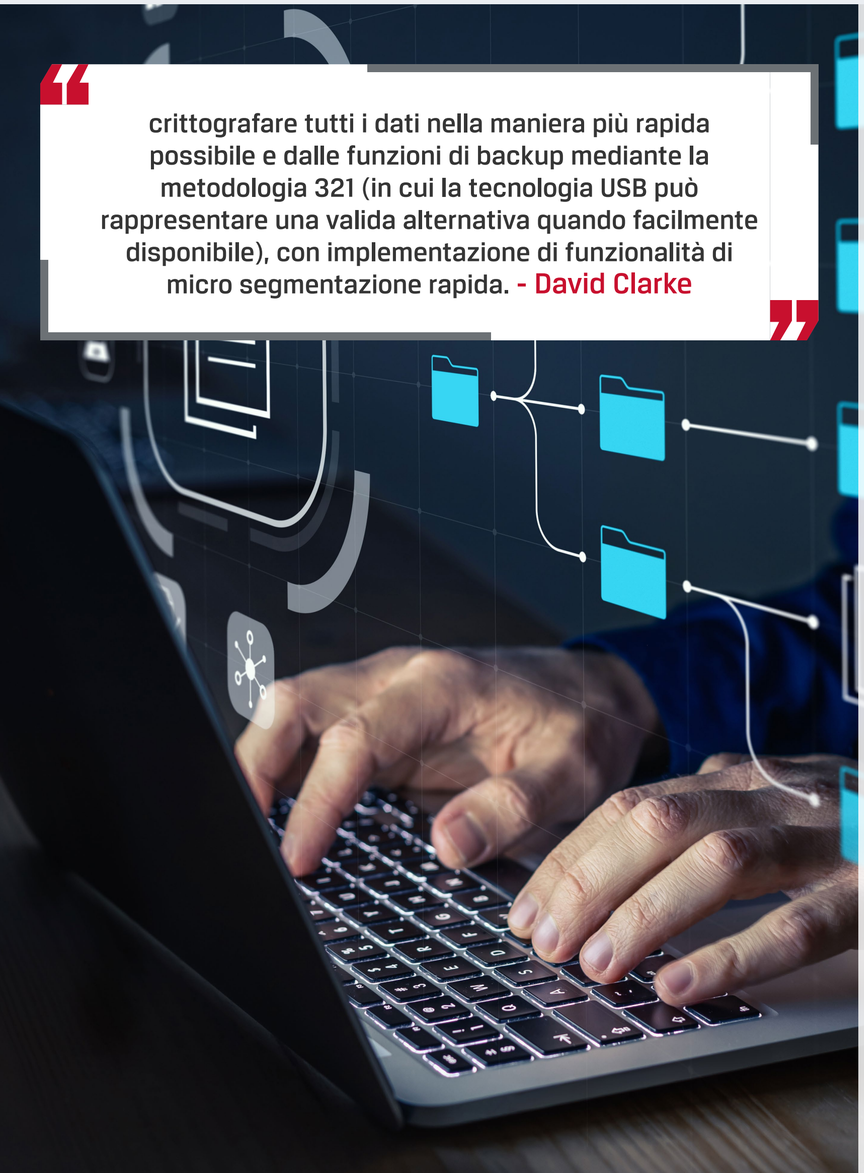
Inoltre, la crittografia software è anche soggetta a rimozione. Qualunque dipendente dotato di un drive crittografato che utilizza la crittografia software può copiare i dati, formattare il drive USB causando la rimozione della funzione di crittografia. Tali dati possono successivamente essere copiati nuovamente sul drive, che può essere utilizzato senza alcun problema di autenticazione anche su piattaforme e sistemi operativi differenti.

Come abbiamo citato in precedenza, la crittografia hardware è una "crittografia" fisica e, di conseguenza, lo storage dei dati crittografati avviene in maniera indipendentemente rispetto ai sistemi host utilizzati. Ciò garantisce un livello di protezione aggiuntivo in caso di compromissione dei sistemi host.

Tale aspetto non può essere sottovalutato, in particolare quando si tratta di applicazioni in settori come quello finanziario, della sanità o governativi. Ciò in quanto regolamenti specifici come l'HIPAA (Health Insurance Portability and Accountability Act), e PCI DSS (Payment Card Industry Data Security Standard), spesso hanno requisiti estremamente rigidi per quanto riguarda la crittografia di informazioni sensibili.

Garantire la conformità a tali regolamenti mediante l'utilizzo di dispositivi dotati di solide funzioni di crittografia hardware consente alle organizzazioni di evitare onerose sanzioni, cause legali e gravi danni alla reputazione. Sebbene i drive dotati di crittografia hardware siano ancora più costosi rispetto ai più economici drive USB di tipo commerciale, i costi legali associati a potenziali violazioni dei dati contenuti in un drive USB possono facilmente superare i costi necessari per acquistare centinaia di drive. Ciò a causa delle spese associate alla necessità di ricorrere a centinaia di ore di consulenze e supporto legale.

La crescente necessità di proteggere i dati sensibili



> crittografare tutti i dati nella maniera più rapida possibile e dalle funzioni di backup mediante la metodologia 321 (in cui la tecnologia USB può rappresentare una valida alternativa quando facilmente disponibile), con implementazione di funzionalità di micro segmentazione rapida. - David Clarke

Quando si tratta di protezione dati sensibili contro perdite e furti, ogni organizzazione ha l'obbligo di garantire che i dispositivi utilizzati dispongano di adeguate funzioni di sicurezza. È anche importante tenere in considerazione che sebbene esista una miriade di minacce informatica in costante evoluzione, il livello di maturità digitale e le capacità di gestione dei dati degli endpoint da parte degli utenti, rimangono comunque un elevato fattore rischio quando non affrontate in maniera adeguata. Le minacce di natura interna che includono le perdite di controllo sui dati, lo smarrimento di dispositivi storage USB, la trasmissione di dati all'esterno degli ambienti sicuri, l'utilizzo di drive USB non crittografati e la condivisione di password, può essere il risultato di una carenza di attenzione da parte degli utenti finali. Ognuna di queste situazioni può essere evitata con adeguati corsi di formazione, educazione e drive USB di tipo adeguato.

> L'organizzazione dovrebbe disporre di una chiara mappatura dei dati, includendo anche il livello di importanza e/o sensibilità dei dataset, con un piano che prioritizzi prima di tutto i dati più importanti, sia rimuovendo i collegamenti fisici a tali dati, oppure facendo in modo tale che la fonte dei dati sia irrintracciabile. La capacità di isolare i sistemi colpiti in maniera rapida rappresenta un elemento chiave e in tale senso disporre di un piano già documentato e testato costituisce un fattore vitale. - Rafael Bloom

La pianificazione è una struttura di comunicazione ben collaudata svolgono anch'esse un ruolo fondamentale nella gestione di potenziali minacce esistenziali. Le moderne minacce informatiche normalmente prendono di mira i punti deboli delle organizzazioni.

Il momento migliore per sviluppare un piano di adozione di drive USB protetti da crittografia è sicuramente prima di averne bisogno. Tale approccio consiste nell'integrare i drive USB crittografati e le regole associate come parte integrante della strategia di sicurezza complessiva della vostra organizzazione. L'assenza di piani e linee guida per la gestione dei drive USB crittografati lascia le aziende completamente allo scoperto contro minacce e rischi di qualunque tipo, inclusa la mancata conformità a normativa e regolamenti come la direttiva GDPR (General Data Protection Regulation), e specificamente con l'articolo 32, che prevede la crittografia dei dati sensibili.

> Utenti che elaborano dati sensibili. La perdita di tali dati accresce il livello di responsabilità e influisce negativamente sull'immagine e sulla sicurezza dell'azienda. Al fine di proteggere i dati sensibili è necessario ricorrere a svariate soluzioni di sicurezza tra cui la crittografia dei dati. - Tomasz Surdyk

Sicurezza dei dati finanziari sensibili

Unitamente alle implicazioni intrinseche per la sicurezza, è anche necessario osservare standard di conformità in materia di storage dati e backup. Alcune di queste prassi, come la necessità di gestire e implementare programmi di ritenzione dati, sono piuttosto comuni attraverso verticalizzazioni, mentre altre, come la migrazione dei dati aziendali verso il cloud, sono trattati in maniera estremamente differente.

In numerosi settori verticali, come quello dei servizi finanziari sono stati implementati regolamenti che hanno reso obbligatoria la gestione adeguata dei dati. Cio è particolarmente vero anche nel settore bancario, tradizionalmente estremamente avverso all'adozione di soluzioni di backup e storage di terze parti e nel quale molti insistono ancora nell'utilizzare infrastrutture di gestione dati di tipo proprietario.

Le istituzioni finanziarie sono anche tenute a conformarsi a una crescente lista di regolamenti standard in materia di sicurezza dei dati, come SOX (Sarbanes-Oxley Act) e la direttiva GDPR (General Data Protection Regulation). Tuttavia, con il crescente numero di dipendenti appaltatori esterni, cresce il rischio di perdite di dati e con ciò la mancata conformità a regolamenti e direttive imposti da tali normative standard.

La realtà è che qualunque sforzo di garantire la conformità può essere vanificato con estrema semplicità quando il personale che opera da remoto non riesce a salvaguardare la propria identità digitale, quella dei dispositivi portatili utilizzati per il loro lavoro, i dati dei clienti e i dati finanziari che recano con se. Ecco perché un numero sempre crescente di organizzazioni sta passando verso soluzioni di sicurezza mobili come I drive USB crittografati Kingston IronKey, per proteggere le loro identità digitali e le applicazioni indipendentemente dal luogo in cui i dipendenti le utilizzano.

> **Quando si considerano le mutazioni dei trend complessivi verso soluzioni IT più distribuite e la crescente scalabilità dell'infrastruttura cloud, è semplice osservare come la maggior parte delle industrie e la stragrande maggioranza delle piccole e medie imprese, non siano più preoccupate di gestire sale server refrigerate in proprio. - Rafael Bloom**

Accesso sicuro ai dati medici dei pazienti

Il settore della sanità e un altro di quelli in cui la sicurezza dei dati svolge un ruolo fondamentale. In questo caso le informazioni dei pazienti sono maggiormente esposte al rischio di furti con violazioni che hanno visto esporre 45,67 milioni di registrazioni dei pazienti nel 2021, il volume annuale totale più elevato dal 2015[2]. Quando si tratta di storage e backup dei dati, i dati dei pazienti rappresentano le informazioni mediche più sensibili e complete che consentono agli operatori del servizio sanitario di trattare i loro pazienti in tutta sicurezza.

Tali dati possono includere qualunque tipo di informazione, dai file delle cartelle cliniche elettroniche dei pazienti (EHR), Ai test medici, alle fotografie e alle immagini radiografiche, fino ai file amministrativi che includono dati su salari, assicurazioni dei pazienti e, infine, i dati sui fornitori. Dovendo far fronte a un crescente numero di dipendenti che operano da remoto e a un mercato della sanità globale che sta attraversando un periodo di grandi cambiamenti e trasformazioni, non deve sorprendere che la sicurezza dei dati sia in cima alla lista delle preoccupazioni dei provider di servizi sanitari.

> **Con il caso del ransomware che costituisce una minaccia in costante crescita, ogni organizzazione che gestisce dati sensibili è costretta a tenere in considerazione in che modo garantire la continuità operativa in condizioni di estremo rischio. - Rafael Bloom**

Inoltre l'incapacità di anticipare rischi e operare in conformità a rigidi regolamenti come HIPAA (Health Insurance Portability and Accountability Act) e HITECH (Health Information Technology for Economic and Clinical Health Act), possono causare violazioni dei dati con conseguenti ingenti costi per il settore sanitario, minando ulteriormente la fiducia di pazienti, partner e organismi di regolamentazione.

Grazie a soluzioni come la gamma di drive USB crittografati IronKey di Kingston, le organizzazioni del settore sanitario possono definire regole specifiche per password, utilizzo delle applicazioni, funzioni di ripristino, e tante altre funzionalità per drive multipli o migliaia di drive, operando da una singola console di gestione centralizzata. Gli operatori che operano da remoto e quelli che operano in campo possono usufruire della capacità di supportare un maggior numero di pazienti, grazie all'uso di soluzioni semplici e intuitive che eliminano la necessità per il personale di installare driver o altro software per la gestione sicura dei dati memorizzati. Tutto ciò mentre utenti e amministratori sono in grado di impedire l'accesso ai loro dati in maniera semplice e rapida indipendentemente da dove si trovano.

Il ruolo dei drive USB in un futuro scandito dallo storage cloud

> **Lo storage dei dati su cloud rappresenta il presente ma anche il futuro. Sostengo ancora che la sicurezza dei dati mediante dispositivi fisici, per esempio mediante l'uso di drive USB crittografati, rappresenti ancora la soluzione migliore. Gli utenti non hanno il controllo totale di ciò che accade nel cloud. Tuttavia, gli utenti possono controllare i dati contenuti nei driver USB crittografati in quanto tali dati sono archiviati e messi in sicurezza dagli utenti stessi. L'accesso a tali supporti è garantito esclusivamente agli utenti che li possiedono. - Tomasz Surdyk**

Ora che i vantaggi dei drive USB appaiono chiari, è il momento di analizzare qual è il ruolo il loro ruolo nel futuro dello storage cloud?

Fino a un decennio fa, i drive USB venivano utilizzati prevalentemente come strumenti per il trasferimento l'archiviazione di dati in maniera semplice pratica. Tuttavia, in virtù dell'impatto dei nuovi modelli di lavoro ibrido e la crescente diffusione di team di dipendenti distribuiti, il cloud attualmente garantisce un accesso più rapido semplice da molteplici dispositivi ai dati archiviati. Ciò sebbene i drive flash fossero in passato immensamente popolari in virtù del fatto che garantivano un'estrema praticità di trasporto dei file. Attualmente i servizi di storage su cloud garantiscono una maggiore portabilità dei file.

Tuttavia, lo storage cloud è caratterizzato ancora da numerose limitazioni. La tecnologia cloud richiede una connettività di rete, che non sono limita quando e in che modo i file possono essere sottoposti a backup o trasferiti, ma comporta anche rischi aggiuntivi per la sicurezza. Pertanto, quando un'azienda impone al personale l'utilizzo del cloud virgola non è necessariamente in grado di controllare da dove avviene l'accesso ai dati. Quindi, il semplice atto di accedere a una rete VPN mediante una connessione Wi-Fi personale o pubblica, espone gli utenti a rischio di violazioni e aggressioni da parte degli hacker. Inoltre, i servizi cloud rappresentano un'opportunità unica per hacker e altri operatori maligni, in quanto la maggior parte del malware (61%) viene ora distribuita mediante applicazioni cloud[3].

> **Pertanto è importante tenere in considerazione ciò che accade quando il cloud non è disponibile, gli scenari in cui dati devono essere disponibili al 100% e nei casi in cui lo storage a lungo termine espone a vulnerabilità. - David Clarke**

Il ruolo dei drive USB in un futuro scandito dallo storage cloud

La crittografia USB d'altro canto può essere ottenuta sia mediante soluzioni hardware, sia mediante soluzioni software. La crittografia basata su hardware, esente da software, rappresenta il metodo più efficace per fornire protezione contro gli attacchi informatici. Si tratta di una soluzione eccellente e non complessa per garantire la protezione contro violazioni dei dati ed è in grado di rispettare gli standard di conformità, garantendo una sicurezza assoluta in termini di protezione dei dati, in tal modo aiutando le organizzazioni a gestire in tutta tranquillità qualunque tipo di minaccia, con una riduzione dei rischi.

Dato che si tratta di dispositivi totalmente indipendenti, i drive USB con crittografia hardware non richiedono elementi software sul computer host. Nessuna vulnerabilità software consente di eliminare il rischio di attacchi brute-force, sniffing e attacchi hash alla memoria. I drive USP dotati di crittografia software sono anche esposti a un rischio aggiuntivo, dettato dal fatto che gli utenti possono disabilitare la funzione crittografica semplicemente formattando il drive su un computer qualunque per poi utilizzare lo stesso drive per l'archiviazione di dati sensibili non protetti.

I drive USB dotati di crittografia hardware offrono anche caratteristiche fisiche straordinarie in termini di sicurezza di dati. Tali dispositivi consentono di definire i criteri di accesso da parte di utenti amministratori virgola e possono integrarsi con le soluzioni endpoint locali preesistenti. Tale caratteristica ne fa una soluzione efficiente ed economica per l'impiego in numerosi scenari in cui lo storage cloud non sarebbe adatto oppure non rappresenterebbe un'alternativa altrettanto efficace. Esempi di tali casi possono includere quelli in cui dati necessitano di archiviazione su dispositivi che non sono collegati in rete, oppure file che devono restare riservati, oppure ancora file a cui è necessario accedere anche in assenza di collegamenti in rete.

> **Se si considerano i dati come appartenenti a due categorie, rispettivamente "dati caldi" o "dati freddi", in base al loro livello e frequenza di utilizzo su base quotidiana per le varie organizzazioni, può essere una soluzione più efficiente archiviare i "dati freddi" sul cloud, utilizzando invece dispositivi di storage USB locali per i "dati cosiddetti" a caldo, quando continuità operativa e prestazioni elevate rappresentano l'aspetto più importante per lo svolgimento di una particolare funzione o di processi business critical. - Rafael Bloom**

Riepilogo

Benché non sia possibile prevedere l'introduzione delle innovazioni future, siamo in grado di offrire una gamma al vertice di drive USB, che mettono a disposizione degli utenti un'ampia gamma dinamica di soluzioni crittografate in grado di soddisfare qualunque requisito di protezione dei dati su dispositivi mobili. Dai drive USB dotati di tastierini alfanumerici con protezione mediante pin di semplice utilizzo fino alle soluzioni dotate di funzioni crittografiche con certificazione FIPS 140-2 di Livello 3, per garantire il più elevato livello di protezione crittografica unitamente a funzionalità antimanomissione; oppure ancora soluzioni dotate di tecnologia Superspeed USB 3.1 senza alcun compromesso in termini di sicurezza. Tutti i prodotti della gamma IronKey di Kingston sono progettati per soddisfare le esigenze dei clienti con una gamma di drive USB che garantisce elevata potenza massima efficacia nel trasporto dei dati e un'ampia gamma di soluzioni di storage dati mobili.

Il nostro team di esperti specializzati è pronto ad assistervi durante ogni fase del vostro percorso di selezione e acquisto delle soluzioni di storage dati, offrendo un supporto affidabile nella scelta della soluzione di storage più adatta alle vostre esigenze.

Possediamo le competenze e le capacità tecniche necessarie ad aiutarvi a garantire la sicurezza delle informazioni riservate in totale conformità con i nuovi regolamenti, indipendentemente dal fatto che dobbiate definire un piano USB crittografato, selezionare i migliori drive USB per le vostre esigenze aziendali, oppure ancora definire e implementare specifiche regole di sicurezza. Offrendo un servizio altamente personalizzato, ci stiamo impegnando a fornire prodotti che siano in grado di supportare le priorità dello storage dati dei clienti, consentendo loro di mantenersi al passo con i vorticosi cambiamenti senza precedenti che caratterizzano l'attuale contesto del settore aziendale globale.

Informazioni su Kingston

Grazie ai suoi 35 anni di esperienza, Kingston è in grado di individuare e risolvere efficacemente le problematiche di gestione dei dati mobili, consentendo al personale di lavorare con facilità e in sicurezza ovunque, senza impatti negativi sulle aziende.

1. Statista - https://www.statista.com/statistics/1062879/worldwide-cloud-storage-of-corporate-data
2. SC Magazine - https://www.scmagazine.com/analysis/breach/breaches-exposed-45-67m-patient-records-in-2021-largest-annual-total-since-2015
3. Infosecurity Magazine - https://www.infosecurity-magazine.com/blogs/cloud-services-top-of-mind-phishers

#KingstonIsWithYou