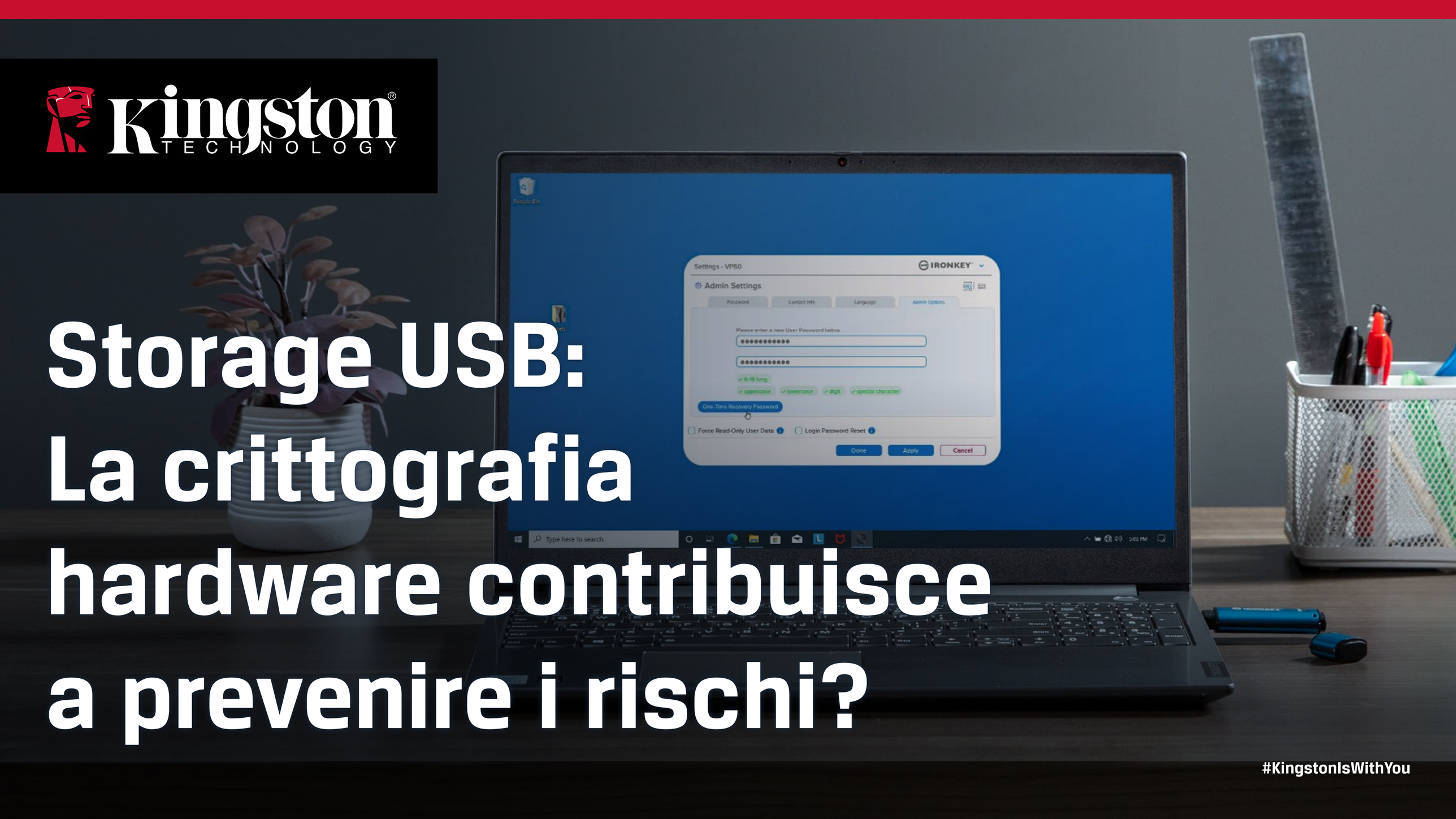
Storage USB: La crittografia hardware contribuisce a prevenire i rischi?



#KingstonIsWithYou

Storage USB: La crittografia hardware contribuisce a prevenire i rischi?

Prefazione e contenuti

La sicurezza informatica rappresenta una preoccupazione crescente per le aziende. Tuttavia, molte aziende non sono adeguatamente informate e preparate a fronteggiare le minacce informatiche. Negli Stati Uniti solo il 50% delle aziende ha implementato un piano di sicurezza informatica; tra queste, il 32% non ha aggiornato tale piano dall'inizio della pandemia scatenata dal virus COVID-19, che ha portato molte aziende ad adottare modelli di lavoro ibridi secondo UpCity. E la frequenza degli attacchi informatici sta crescendo su scala globale. Il numero di aziende interessate da attacchi ransomware è cresciuto dal 37% del 2020 al 66% del 2021[1].

La compromissione della sicurezza informatica può avere effetti devastanti sulle aziende. Oltre ai costi monetari derivanti dagli attacchi informatici bisogna tenere in conto le perdite di dati , la compromissione della sicurezza, e gli effetti negativi sulla reputazione delle aziende sia a breve che a lungo termine.

Uno dei vettori più comuni per l'inoculazione di minacce informatiche è costituito dai drive USB. Questi dispositivi sono universalmente diffusi in molte aziende in virtù della loro semplicità di utilizzo. Infatti, basta collegarli a qualunque dispositivo compatibile per poterli utilizzare. Tuttavia, è esattamente tale semplicità di utilizzo che rende i drive USB vulnerabili agli attacchi; è sufficiente un drive rubato per consentire a un attore maligno di accedere a dati potenzialmente sensibili. Ed è proprio qui che entra in gioco la crittografia, che può svolgere un ruolo importante per garantire la sicurezza dei drive USB, consentendone l'utilizzo e mitigando i rischi posti dalle minacce informatiche, sia per i singoli soggetti, che per le aziende. In questo eBook forniamo risposte alle seguenti domande:

- Perché i drive USB crittografati sono così importanti per proteggere i dati contro gli attacchi informatici?
- Quali sono i punti deboli e le vulnerabilità per le aziende?
- Quali sono le misure che si possono adottare per proteggere i dati delle aziende?

Indice dei contenuti	Pagine

Storage USB: La crittografia hardware contribuisce a prevenire i rischi?

Collaboratori

Questo eBook e stato creato con l'aiuto di importanti figure del settore della sicurezza IT e delle tecnologie emergenti, unitamente ai nostri esperti tecnici.

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.

Pasi Siukonen

Pasi guida un team di esperti che supporta diversi dipartimenti interni di Kingston, quali PR, Marketing, Vendite, Supporto tecnico e Servizio clienti dedicato ai prodotti Kingston. Il suo ambito di specializzazione principale consiste nella linea di prodotti SSD e Flash.

La differenza principale tra drive commerciali e drive crittografati

Sebbene i drive commerciali tradizionali non crittografati offrano un semplice accesso ai dati e grande intuitività di utilizzo, le versioni dotate di crittografia hardware garantiscono una maggiore sicurezza sia fisica che digitale, rendendo lo storage USB notevolmente più sicuro. Disponibilità, costi ridotti e la portabilità dei drive commerciali non crittografati, ne fanno dispositivi estremamente pratici per qualunque tipologia di utente. Ma sono anche dispositivi vulnerabili contro gli attacchi perpetrati da attori maligni intenzionati a rubare dati sensibili, inoculare malware o ransomware all'interno delle reti aziendali o perpetrare altre attività illecite. Dato che i driver sono utilizzati con tale frequenza, essi presentano anche molteplici opportunità per condurre attacchi informatici. Esistono due principali rischi associati all'utilizzo dei drive commerciali tradizionali:

- **Attacchi ransomware:** si tratta di attacchi USB che comportano l'inoculazione di malware all'interno delle reti aziendali, o la cattura di informazioni aziendali e il controllo di sistemi aziendali attraverso la crittografia al fine di ottenere un riscatto. Tali tipologie di minacce sono spesso caratterizzate da attacchi BadUSB, e attualmente rappresentano la forma di malware più diffusa.
- **Furto di dati:** è sufficiente che un drive privo di adeguate misure di sicurezza venga lasciato incustodito o vada perso o rubato, affinché gli hacker siano in grado di accedere con facilità ai dati memorizzati all'interno del drive, indipendentemente dal fatto che tali dati contengano informazioni sui clienti, codice sorgente, oppure dati finanziari e prestazionali di natura sensibile.

BadUSB – Questa tipologia di attacco è in grado di sfruttare le vulnerabilità dei drive USB dotati di firmware non protetto consentendone la riprogrammazione mediante software maligno. Questi strumenti di natura maligna sono incredibilmente diffusi e comuni tra i criminali informatici. Tuttavia, la consapevolezza in relazione a questa tipologia di strumenti resta notevolmente bassa, rendendo tali attacchi estremamente semplici da effettuare semplicemente sostituendo il firmware di un drive commerciale standard con un firmware modificato in cui il drive USB può simulare una tastiera ed eseguire script che consentono di effettuare attacchi sul firewall. E dato che così tanti attacchi informatici sono condotti attraverso operatori interni insospettabili con o senza intenti esplicitamente maligni, è estremamente importante per le aziende utilizzare drive crittografati che utilizzano firmware protetti mediante firme digitali, che consentono di prevenire tali attacchi riducendo quindi le possibilità di successo degli hacker.

> **I costi generati dalla necessità di ricostruire un'infrastruttura e la necessità di pagare un riscatto o altre forme di estorsione, sono notevolmente superiori rispetto ai costi sostenuti per l'acquisto di drive USB gestiti.** - David Clarke

Perché utilizzare drive USB crittografati?

I drive crittografati sono specificamente progettati per proteggere i dati contenuti al loro interno nonché qualunque dispositivo ai quali il drive può essere connesso, trasformando tali dispositivi in preziosi strumenti all'interno di qualunque arsenale IT aziendale. Con la crescente diffusione e sofisticazione delle minacce informatiche, i drive crittografati si sono adeguati in termini di funzionalità e sicurezza, consentendo a tali dispositivi di garantire la massima sicurezza contro i tentativi degli hacker di sfruttare le vulnerabilità di tali dispositivi. Come osservato nel caso della gamma di prodotti dotati di crittografia hardware della famiglia Kingston IronKey™, tali prodotti sono dotati crittografia AES a 256-bit con funzionalità XTS, resistenti gusci antimanomissione, firmware firmati digitalmente, tastiere virtuali, modalità di accesso con frasi password o password complesse e tante altre funzionalità aggiunte e integrate nel corso degli anni al fine di garantire che gli utenti siano realmente completamente protetti contro qualunque tipologia di attacco.

Dato che rischi informatici spesso non sono compresi a fondo, molte aziende optano per i tradizionali drive commerciali, nonostante le varie vulnerabilità che caratterizzano tali dispositivi. La facile reperibilità, i costi contenuti e l'uso di software crittografico, giocano un ruolo fondamentale in questi casi, così come l'assenza di procedure di approvazione aziendali per i drive flash. Spesso, le aziende non hanno implementato alcuna best practice o processo organizzativo per garantire la conformità ai vari standard di sicurezza informatica e IT, come lo standard ISO27001, il regolamento GDPR, SOC2 e le best practice governative associate allo standard WISP. Ciò significa che i rischi sono spesso valutati sulla base di opinioni, piuttosto che su prove concrete, esponendo molte organizzazioni al rischio di attacchi.

Benché molti utilizzino drive commerciali con strumenti di crittografia software esistenti, tale operazione spesso si rivela come un falso risparmio, in quanto molti drive dotati di crittografia software possono essere manomessi o violati semplicemente con strumenti gratuiti o a pagamento disponibili per chiunque su Internet. Inoltre, la crittografia software può anche essere rimossa da un drive con una semplice riformattazione dello stesso da parte di un utente, sia per questioni di praticità, oppure per utilizzare il drive su piattaforme con sistemi operativi non supportati. Al contrario, la tecnologia che caratterizza i dispositivi USB con crittografia hardware è attiva in qualunque momento e non può essere disattivata. Ecco perché tali dispositivi sono più adatti per questioni di sicurezza. Inoltre, questi dispositivi sono anche realizzati con funzionalità tieni garantiscono la resistenza alle manomissioni e integrano firmware firmati digitalmente per garantire l'autenticità e l'integrità del Drive. Le funzionalità che limitano i tentativi di inserimento delle password di protezione contro attacchi brute force e le tastiere virtuali (che proteggono contro gli accessi di keylogging e screen logging), sono altre due funzionalità che caratterizzano i drive crittografati come quelli della famiglia IronKey VP50. Ciò significa che tali dispositivi sono conformi alle best practice di settore contro attori maligni i cui obiettivi consistono nell'estrarre le password di utenti inconsapevoli.

> Quando un drive IronKey rileva che il fermo era stato manomesso, l'unità si blocca automaticamente e impedisce l'avvio, innalzando quindi livelli di sicurezza informatica. - Pasi Siukonen

Chi è a rischio?

In realtà qualunque azienda che non abbia un controllo assoluto dei suoi accessi USB è a rischio. Spesso, le aziende non sono consapevoli neppure di quali rischi si corrono. Tuttavia, esistono fattori che possono rendere alcune aziende più inclini e vulnerabili agli attacchi informatici.

Per esempio, i dati delle aziende del settore sanitario e di quello finanziario non sono solamente estremamente attraenti per i criminali informatici; ma la violazione di tali dati ha anche un impatto elevato sulle organizzazioni e sui clienti, con conseguenze molto più gravi. Nel Regno Unito, un attacco informatico condotto nel 2017 contro l'NHS, ha causato la cancellazione di circa 19.000 appuntamenti, con un costo di 92 milioni di sterline in mancati ricavi per l'NHS, a cui si uniscono i costi di ripristino di dati e sistemi. Questo non solo ha impedito ai pazienti colpiti di ricevere assistenza sanitaria, ma l'NHS è stato pesantemente criticato per non aver risposto in modo sufficientemente rapido o sostanziale a precedenti avvisi di minacce informatiche. Nonostante il fatto che in principio tutte le organizzazioni dovrebbero mantenersi aggiornate e informate sul tema della sicurezza informatica, le aziende che utilizzano informazioni sensibili, in particolare dati di categorie speciali, dovrebbero essere doppiamente vigilanti in materia di rischi informatici.

Tanto maggiore è il valore dell'azienda, in termini di fatturato, quanto maggiore è la promessa di guadagni ingenti per i criminali informatici e, pertanto, tanto maggiore sarà l'esposizione di tali aziende ai rischi di minacce informatiche.

Tuttavia, ciò non significa che le organizzazioni più piccole non dovrebbero preoccuparsi delle minacce informatiche. Sebbene le grandi aziende rappresentino bersagli più attraenti per gli attacchi, spesso esse dispongono anche delle risorse e del personale necessari a fronteggiare le minacce informatiche. D'altra parte, molte PMI non dispongono di personale dedicato per fronteggiare le minacce informatiche, e consentono ai dirigenti di fare eccezioni in termini di regole sulla gestione dei dispositivi USB, questi ultimi e le aziende a potenziali attacchi dalle conseguenze devastanti. Alcuni studi indicano che le aziende di piccole e medie dimensioni rappresentano in realtà i principali obiettivi degli attacchi informatici.

Tale rischio cresce ulteriormente per i dirigenti che occupano posizioni chiave in seno a tali aziende. Queste figure possono essere rintracciate facilmente e spesso dispongono di privilegi specifici all'interno delle loro organizzazioni. Ciò significa che per loro natura tali profili sono soggetti a minori restrizioni di sicurezza all'interno delle loro aziende, come nel caso delle procedure di gestione dei dispositivi USB, e ciò ne fa importanti bersagli per i criminali informatici. Ed è proprio in questo caso che i drive dotati di crittografia hardware always-on, unitamente a personale aggiornato e informato in materia di sicurezza informatica nonché l'osservanza di best practice e processi, possono essere di grande aiuto nel ridurre i rischi e garantire un'adeguata protezione in caso di attacchi.

> Molti recenti attacchi informatici sono stati perpetrati da attori maligni specializzati nell'uso di attori interni, consapevoli o meno. - David Clarke

Chi è a rischio?

> Aziende che non fanno abbastanza per fronteggiare le minacce informatiche. - David Clarke

La catena di approvvigionamento rappresenta un altro potenziale punto debole per le aziende. Gli attacchi alle catene di approvvigionamento rappresentano un evento comune. Nel 2013, la catena al dettaglio statunitense Target è stata vittima di una delle più grandi violazioni dei dati nella storia della commercio al dettaglio. L'attacco ha esposto i dati di carte bancomat e carte di credito di oltre 40 milioni di clienti. Sebbene target fosse estremamente già preoccupata è informata sulle minacce informatiche e nonostante l'azienda avesse appena installato un esteso sistema di prevenzione delle minacce informatiche solo sei mesi prima dell'attacco, gli aggressori sono stati in grado di infiltrare uno dei fornitori esterni di Target , accedendo tramite questo alla rete principale del gruppo. In totale, target è stata soggetto di oltre 90 cause legali, e l'azienda ha subito perdite pari a 61 milioni di dollari per risolvere i problemi causati dalla violazione. Sebbene l'azienda non fosse responsabile per l'attacco, questa vulnerabilità alle minacce informatiche all'interno della catena di approvvigionamento e stata sufficiente a causare danni finanziari e di reputazione.

Anche gli escamotage tecnologici utilizzati dai dipendenti per evitare le misure di sicurezza possono essere fonte di vulnerabilità. Sebbene questi accorgimenti consentano ai dipendenti di operare con maggiore efficienza per lo svolgimento delle loro attività quotidiane, spesso le procedure di sicurezza di base le best pratice, come la gestione delle password, vengono ignorate. Nonostante le linee guida elaborate da NCSC e CISA siano piuttosto chiare, spesso è estremamente difficile implementarle in pratica, specialmente da parte di team di membri che non hanno familiarità con l'informatica e con le minacce informatiche. Sebbene l'uso di team di contrasto alle minacce informatiche dedicati sia in grado di contribuire notevolmente alla sicurezza aziendale, resta un fatto che dare ai dipendenti gli strumenti ideali come drive dotati di crittografia hardware può anch'esso contribuire notevolmente nel mitigare i rischi causati da dipendenti che tentano di bypassare o aggirare le misure di sicurezza per questioni di praticità.

> attualmente i driver USB dotati di crittografia hardware sono estremamente facili da utilizzare e integrare nelle procedure e nei regolamenti di sicurezza informatica preesistenti. Tale conformità consente di adattare tali soluzioni a varie interfacce (grafiche, tastierini, touchscreen), con un ampio supporto per differenti sistemi operativi e capacità, al fine di soddisfare le esigenze di qualunque organizzazione. - Pasi Siukonen

In che modo le organizzazioni possono ridurre i rischi di attacchi informatici?

Sotto il profilo organizzativo, è possibile adottare numerose misure per migliorare la sicurezza degli endpoint e proteggere i dati. In assenza di soluzioni di sicurezza informatica GRC (governance, rischio, conformità), le misure di sicurezza contro le minacce informatiche hanno un'elevata probabilità di fallimento. Pertanto, acquisire familiarità con le procedure seguenti riveste una grande importanza per garantire la protezione delle aziende. Disporre di solidi software di sicurezza per gli endpoint consente anche di neutralizzare un elevato numero di minacce informatiche, oltre a garantire la massima reattività quando si tratta di applicare delle patch a qualunque vulnerabilità di sicurezza.

> **Indipendentemente dal fatto che si adottino regole di crittografia o meno, la domanda più importante per la gestione del rischio resta quella associata alla decisione di effettuare o meno il backup dei dati.**
> **- Pasi Siukonen**

Tuttavia, a livello individuale, le soluzioni hardware crittografate possono contribuire a ridurre drasticamente le vulnerabilità associate alle minacce informatiche. Con il graduale incremento e il consolidamento del lavoro ibrido o da remoto, specialmente quando associato a un incremento degli attacchi informatici come quelli verificatisi durante lo scorso anno, garantire la sicurezza del personale a qualunque livello organizzativo, nella gestione trasferimento e preparazione dei dati aziendali, sta assumendo un'importanza sempre maggiore. I dispositivi USB dotati di crittografia hardware consentono agli utenti di continuare a beneficiare dalla portabilità e semplicità dei drive flash, riducendo al contempo notevolmente i rischi associati a tali tipi di utilizzo. Laddove un drive commerciale di tipo tradizionale va perso o viene rubato con tutte le conseguenze che ne derivano in termini di perdita di dati, denaro, reputazione, e altro, i drive con crittografia hardware sono progettati per proteggere i dati sensibili contro un ampio numero di attacchi. E mentre i criminali informatici sviluppano nuovi metodi di attacco, i drive crittografati continuano a evolversi per contrastare queste nuove minacce.

Tutto sommato, i costi associati alle conseguenze di un attacco informatico possono essere enormi. E pertanto, sebbene l'adozione e l'utilizzo di driver crittografati a livello aziendale possa richiedere maggiore complessità in termini di approvazione e configurazione, l'adozione di tali soluzioni può consentire alle aziende di risparmiare notevoli quantità di denaro, sia in termini di costi di estorsione virgola e di perdite di profitti causate dalla danneggiamento di una reputazione nel lungo periodo. I soli costi legali associati a violazioni e attacchi possono facilmente superare i costi aggiuntivi richiesti per l'adozione di drive USB dotati di crittografia hardware.

> **Attraverso l'impegno a lungo termine finalizzato a fornire straordinarie soluzioni USB dotate di crittografia, la gamma di prodotti Kingston consente a qualunque organizzazione di trovare le soluzioni e le configurazioni di contrasto alle minacce informatiche ideali per le loro esigenze, con dispositivi conformi agli standard industriali, dotati di crittografia hardware non disattivabile, design conformi ai regolamenti in materia di endpoint, e funzionalità per la gestione dei dispositivi. - Pasi Siukonen**

Riepilogo

Kingston si mantiene costantemente aggiornata sugli ultimi sviluppi nel settore della sicurezza informatica, assicurandosi che i drive crittografati della gamma IronKey siano sempre aggiornati con i più recenti requisiti e siano conformi alle esigenze di sicurezza informatica delle organizzazioni di qualunque dimensione. Mentre le sfide associate alla sicurezza informatica continuano a crescere su scala globale, siamo fiduciosi del fatto che, attraverso l'utilizzo di strumenti e conoscenze necessarie, consenta alle organizzazioni di dotarsi di soluzioni in grado di affrontare tali sfide, proteggendo se stesse, i loro dipendenti e i clienti.

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.

#KingstonIsWithYou

1. https://www.techtarget.com/searchsecurity/news/252516423/Sophos-66-of-organizations-hit-by-ransomware-in-2021