nexthardware.com

a cura di: **Gian Paolo Collalto - giampa - 09-02-2012 10:14**

La sicurezza in azienda dei drive USB: i consigli di Kingston Technology

LINK (https://www.nexthardware.com/news/ram-memorie-flash/4329/la-sicurezza-in-azienda-dei-drive-usb-i-consigli-di-kingston-technology.htm)

Come migliorare la sicurezza dei dati sensibili al fine di prevenire danni e conseguenze derivanti da perdita o smarrimento dei dispositivi mobili.

↔

Kingston Digital Europe Ltd, affiliata di Kingston Technology Company, Inc., il principale produttore indipendente di memorie del mondo, suggerisce alcune pratica a tutela dei dati contenuti nei drive USB e rivela i rischi associati alla mancanza di adeguate politiche di sicurezza.

↔ â€œ*I dati devono essere considerati il DNA di unâ€™azienda e, come tali, devono essere protetti in qualsiasi momento e gestiti con prudenza e cautela*â€, ha dichiarato Stefania Prando, Business Development Manager di Kingston Technology Italia. â€œ*Le informazioni contenute nei dispositivi USB devono essere preservate con policy che ne regolino la salvaguardia, la conservazione, i download e le condivisioni; in caso contrario, lâ€™azienda viene esposta al rischio di sanzioni, perdite finanziarie e calo di fiducia da parte dei clienti*â€.

↔ Kingston, forte della propria esperienza sul mercato, suggerisce alcune pratiche che le aziende dovrebbero seguire per proteggere i dati sensibili.

In questa difficile situazione economica è ancora più importante per le aziende promuovere allâ€™interno del proprio staff lâ€™importanza della sicurezza dei drive USB e implementare una policy adeguata a tutela dei dati sensibili.

↔

Studiare una strategia che comprenda lâ€™utilizzo di drive USB crittografati

Eâ€™ bene pensare a un piano di questo tipo prima ancora di accorgersi di averne bisogno; la strategia deve includere lâ€™utilizzo di Flash Drive USB sicuri e policy a tutela della sicurezza aziendale.↔

↔

Scegliere i dispositivi USB adatti alle esigenze

La scelta deve considerare lâ€™affidabilità e lâ€™integrità dei dispositivi USB, che devono rispettare gli ↔ standard di sicurezza previsti.

↔

Preparare e formare il proprio staff

Eâ€™ importante che i dipendenti siano preparati sullâ€™utilizzo dei drive USB; è utile quindi organizzare training di formazione che prevedano simulazioni di violazione della sicurezza che possono accadere con lâ€™uso di dispositivi USB non sicuri.

↔

Strutturare una policy aziendale

Senza una regolamentazione precisa, le unità USB possono rappresentare potenzialmente una minaccia per la protezione dei dati sensibili.

Stabilire una policy è il primo passo da affrontare per attuare una strategia di tutela dei dati.

I risultati della ricerca (http://media.kingston.com/europe/mailer/images/201111/Ponemon%20research_EMEA%20summary_UK_1111.pdf) di Ponemon, che sottolineano lâ€™importanza di queste politiche, hanno rivelato che quasi il 50% delle aziende dichiara lo smarrimento di drive contenenti informazioni sensibili o confidenziali negli ultimi 24 mesi.

↔

Utilizzo esclusivo di drive USB approvati dallâ€™azienda

Il sistema di crittografia che utilizza lo standard Advanced Encryption (AES) 256 garantisce portabilità e crittografia superiore rispetto a quella basata su software.↔

↔

Gestione di USB autorizzati e blocco di quelli non approvati

Senza questo accorgimento, i dati sensibili possono essere copiati e condivisi con terzi, esponendo lâ€™azienda al rischio della perdita degli stessi.

↔

Crittografare i dati riservati

Se i dati non vengono criptati prima di essere salvati su drive USB, gli hacker possono oltrepassare lâ€™anti-virus, il firewall o altri controlli, accedendo così alle informazioni.↔

↔

Anti-virus attivo a ogni accesso

Eâ€™ necessario garantire che i sistemi host di ogni computer siano dotati di un software anti-virus aggiornato.

↔

Le violazioni sulla sicurezza dei dati continuano a causare problemi alle aziende, molti dei quali derivano dallo smarrimento di drive o dallâ€™utilizzo di unità USB non sicure.

A novembre, Kingston ha presentato i risultati di uno studio condotto dal Ponemon Institute (http://www.ponemon.org/), intitolato â€œ***Lo stato della sicurezza dei drive USB in Europa***â€ in cui sono stati intervistati 2.942 professionisti nel settore IT o IT security di aziende con sede in Danimarca, Finlandia, Francia, Germania, Olanda, Norvegia, Polonia, Svezia, Svizzera e Regno Unito.

La ricerca ha rivelato che, nonostante sia forte la consapevolezza dei rischi ai quali sono esposti i dati a causa della negligenza dei dipendenti, sono poche le aziende che adottano policy adeguate.

Solo il 48% degli intervistati considera la protezione delle informazioni sensibili su Flash Drive USB una priorità , mentre il 63% ritiene che la violazione dei dati sia causata dallo smarrimento di unità USB.

Le aziende si dimostrano ancora troppo permissive in materia di sicurezza dei drive USB, nonostante si riconoscano i pericoli e le conseguenze derivanti da un uso improprio degli stessi.

Per il 68% dei professionisti intervistati, la società per la quale lavorano adotta una regolamentazione delle chiavette USB accettabile, mentre meno della metà dichiara di non dover rispettare regole particolari come lâ€™uso di password, blocchi, scansione di virus e malware ecc.

â€œ*Le soluzioni di protezione delle unità USB e le relative policy di utilizzo dei drive non devono però diventare macchinose o troppo costose per lâ€™azienda, e non devono in alcun modo ridurre la produttività dei dipendenti*â€, ha continuato Stefania Prando. â€œ*Il nostro obiettivo è aiutare le aziende a risolvere il problema della sicurezza, consigliando lâ€™utilizzo di USB sicuri*â€

↔

La ricerca può essere scaricata al seguente link:

http://media.kingston.com/pdfs/Ponemon/Ponemon_research_EMEA_summary_UK_1111.pdf
(http://media.kingston.com/pdfs/Ponemon/Ponemon_research_EMEA_summary_UK_1111.pdf)

↔

COMUNICATO STAMPA

↔

↔

Questa documento PDF è stato creato dal portale nexthardware.com. Tutti i relativi contenuti sono di esclusiva proprietà di nexthardware.com.
Informazioni legali: https://www.nexthardware.com/info/disclaimer.htm