ADVERTORIAL

Tutelare i dati fin dalla progettazione

Tecnica a dischi rimovibili RDX nel rispetto delle direttive GDPR

Anche se il rispetto del GDPR non è il compito principale dei responsabili IT, il regolamento causa grattacapi soprattutto a piccole e medie imprese. La tutela e la sicurezza dei dati sono in ogni caso un obbligo, anche alla luce di altre prescrizioni regolamentari, di suggerimenti sulla sicurezza dei dati dell'Ufficio Federale per la Sicurezza Informatica oppure per prevenire cyberattacchi. Per una migliore gestione sono stati sviluppati dei sistemi a dischi rimovibili come ad esempio RDX

I 99 articoli del GDPR, suddivisi in undici capitoli, hanno l'obiettivo di contribuire alla tutela della sfera privata e all'elaborazione di dati personali. La buona notizia è che le nuove norme del GDPR non riguardano molti degli aspetti della privacy, ma acquisiscono significato maggiore grazie alle multe salate e al timore di ondate di diffide. Le direttive fanno in modo che le piccole e medie imprese (PMI) possano testare la loro registrazione dei dati: che cosa e dove viene salvato, messo in sicurezza e archiviato? Quanto dura la conservazione dei dati?

Ai sensi dell'art. 25, par. 1 del GDPR, aziende e organizzazioni sono tenute ad avviare procedure tecniche ed organizzative atte a tutelare la sfera privata e a garantire il rispetto dei principi di protezione dei dati. Inoltre, si tratta in questo caso di» Tutelare i dati mediante l'uso della tecnologia «, cosa che, come da GDPR, spetta al dipartimento informatico.

Registrazione dati e scelta tecnologica

In sostanza si tratta di trovare un modo per mettere al sicuro, conservare ed eventualmente cancellare dati. I dati devono sempre essere accessibili, indipendentemente che siano dati online, di backup o di archivio. Visto che questa attività concernente i dati deve essere garantita per dieci anni, è importante selezionare bene la tecnica di memorizzazione...

Rimane comunque necessaria una strategia per la sicurezza dei dati sui supporti rimovibili. Il distaccamento di dati su un supporto sicuro e resistente è fondamentale. I robusti supporti RDX- della Overland-Tandberg sono ideali, in quanto uniscono portabilità e affidabilità del nastro con la velocità di un disco rigido. Nel sistema dei file è possibile accedere velocemente ai dati, i sistemi sono facilmente adoperabili e compatibili con i software di backup, inclusi gli strumenti come Windows Backup oppure Apple Time Machine. I supporti RDX sono estremamente resistenti e sono stai pensati per essere usati più di dieci anni, compatibili sia sul lato anteriore che posteriore. Grazie all'unità RDX è possibile usufruire di un per ogni supporto portatile, garantendo numerose possibilità di tutela dei dati.

Controllo accessi e cifratura

Come da GDPR, i dati personali devono essere tutelati da una» divulgazione non autorizzata «e da un accesso non autorizzato. Ciò riguarda anche la possibilità di sottoporre i titolari di diritti ad un controllo accessi basato su una policy. Il responsabile e l'incaricato intraprendono delle misure, atte a sincerarsi che le persone a loro subordinate, aventi accesso ai dati, ne usufruiscano solo su disposizione del responsabile.

Un ulteriore punto importante riguarda la necessità della » pseudonimizzazione e cifratura «dei dati personali e della» capacità di garantire a lungo termine la riservatezza, l'integrità, l'accessibilità e la portata dei sistemi e servizi legati all'elaborazione dei dati«. Si tratta di un criterio decisivo soprattutto per il trasporto e lo scambio di dati.

La tecnologia RDX indirizza questi aspetti tecnici tramite una serie sviluppi recenti. In primis i sistemi RDX si basano su una tradizionale tecnologia di disco rigido, più familiare del nastro magnetico o delle soluzioni Cloud per i principali utenti, soprattutto in caso di PMI. I dispositivi sono compatibili, un enorme vantaggio in caso di ripristino dei dati archiviati.

Con il software RDX Cartridge Encryptor (RCE) viene messo a disposizione un software libero che consente una comoda cifratura di tutti i dati salvati su RDX. Il software è concepito per un utilizzo semplice ed efficace, si basa sullo standard industriale AES-256-Encryption e allo stesso tempo è Secure Erase secondo gli standard NISP per una eliminazione completa di dati e programmi. In grado anche di cancellare le chiavi (Cryptographic Key Deletion). Il software per cifratura RDX offre alle PMI una soluzione gratuita per salvare dati in tutta sicurezza.

Cifratura hardware secondo i migliori standard

Il PowerEncrypt RDX è una tecnologia a dischi rimovibili che mette a disposizione una cifratura basata su hardware secondo gli standard 256-AES- XTS. La tecnica di cifratura basata su hardware, rispetto a quella software, è più semplice da utilizzare, non grava sulla potenza di elaborazione e non causa conflitti con i sistemi informatici und e altri livelli di software. Il computer più veloce oggi disponibile è teoricamente in grado di produrre 10^{14} chiavi al secondo e necessiterebbe quindi di 3,31 x 10^{56} anni per decifrare la tradizionale cifratura 256-AES. Grazie alla parallelizzazione e in futuro a una maggiore potenza di calcolo offerta dai servizi Cloud sarà possibile decifrare la cifratura 256-AES. Con il PowerEncrypt RDX l'inserimento della chiave sarà limitato ad una chiave al secondoed è così robusto che il software può anche resistere alle tecniche di cracking parallelo hacker utilizzate per ridurre i tempi di cracking. L'amministrazione del PowerEncrypt RDX tramite il portale RDX può essere gestita da un massimo di otto utenti aventi differenti profili di diritto e gerarchie di accesso, gode di un'opzionale identificazione automatica di unità e analizza la sicurezza delle password al momento dell'inserimento.

Da FIPS fino a KPMG – Soluzioni certificate: maggiore sicurezza

Il PowerEncrypt RDX, nella sua prima versione, è compatibile con dispositivi e unità interne RDX-SATA-III su Windows. In questa configurazione nel 2018 sarà validato anche FIPS 140-2. Il FIPS

140-2 (Federal Information Processing Stan- dard) è uno standard del governo americano che descrive la cifratura e le sue pre-scrizioni di sicurezza, che consentano un utilizzo riservato dei prodotti informatici. Questo standard garantisce che un prodotto impieghi delle solide pratiche di sicurezza come ad esempio algoritmi e processi di cifratura complicati. Inoltre stabilisce come singole persone oppure processi produttivi devono essere autorizzati per un corretto uso e come moduli o componenti devono essere sviluppati per un'interazione sicura con altri sistemi. Il livello di validazione FIPS 140-2 è sinonimo di sicurezza e qualità e garantisce a tutti gli acquirenti che i prerequisiti di sicurezza saranno rispettati. La tecnologia WORM (Write Once Read Many) è particolarmente indicata per la archiviazione ai sensi dei requisiti regolatori. Il software rdxLOCK è stato certificato dalla società di revisione contabile KPMG ed è stata quindi sbloccata la funzione WORM per numerosi standard nazionali e internazionali nell'ambito della contabilità e della fiscalità.

Questa funzione WORM è particolarmente indicata per soddisfare tutte le richieste attuali e future delle regole di condizionalità e del Regolamento generale sulla protezione dei dati (EU-GDPR).

Nel dibattito in merito all'attuazione del GDPR rimangono necessarie» misure tecniche e organizzative adeguate «(Art. 25 par. 1), da attuare per hardware, software e i relativi procedimenti. La tecnologia RDX con supporti di memoria rimovibili, unità singole o specifici apparecchi e un software corrispondente può prestarti un grande aiuto: tutelare i dati fin dalla progettazione!