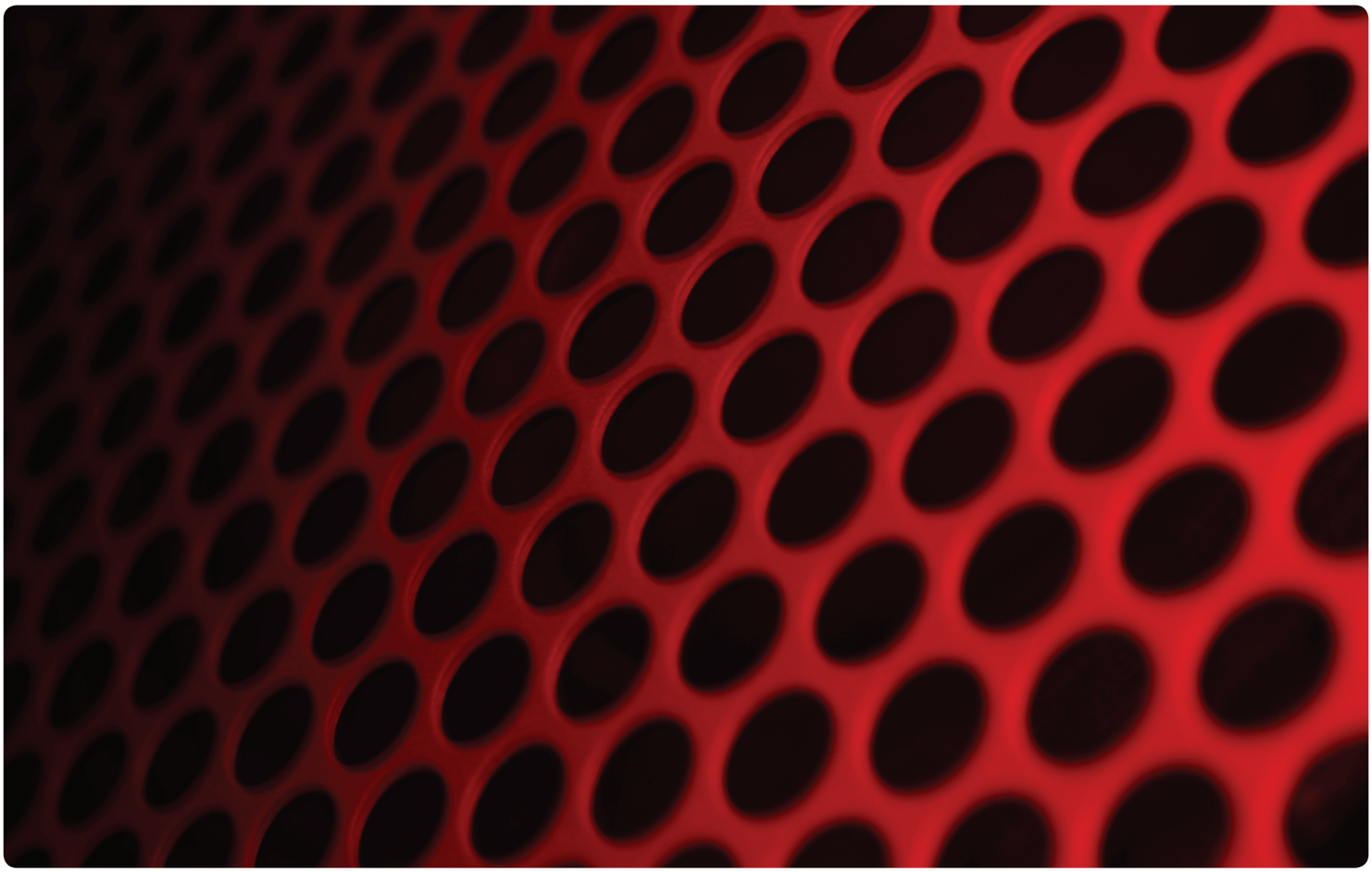
Rischio di violazioni dei dati

Come prevenirle nel rispetto del regolamento GDPR dell'UE



Introduzione

La vita lavorativa quotidiana è cambiata radicalmente, come anche i metodi di lavoro tradizionali. Grazie ai supporti mobili di storage è possibile accedere ai propri dati praticamente in qualsiasi momento da qualsiasi luogo, e si può lavorare da ovunque ci si trovi. La **costante disponibilità** dei dati di lavoro rappresenta un indubbio vantaggio e, grazie alla possibilità di creare **versioni mobili** o copie di backup, si possono ottimizzare gli orari di lavoro e, in definitiva, ridurre i tempi di esecuzione dei processi.

La mobilità dei dati comporta tuttavia anche degli aspetti negativi. La perdita o il furto di drive USB costituisce un grave rischio. Il **72%** delle aziende che hanno partecipato a un sondaggio* ha dichiarato di non riuscire più a trovare singoli drive USB. Ciò è particolarmente grave se si considera che il 25% delle aziende intervistate ha dichiarato che sui drive USB smarriti erano contenuti **dei dati sensibili** . Tali violazioni dei dati minano **la fiducia dei clienti** nelle aziende con le quali interagiscono e sono pertanto accompagnate da danni all'immagine e perdite economiche. Queste cifre non includono i rischi derivanti dalla pubblicazione o dall'utilizzo criminoso dei dati.

Gli organi legislativi hanno reagito a questo aumento del rischio associato alle violazioni dei dati. A partire da maggio 2018, ai sensi del **regolamento generale sulla protezione dei dati dell'Unione Europea** (GDPR) le aziende dovranno assumersi una maggiore responsabilità. Tra le altre misure sono previste pesanti sanzioni in caso di mancata osservanza delle disposizioni obbligatorie.

Questo white paper tratta i seguenti argomenti:

- Cosa è necessario sapere sulla mobilità dei dati e sulle violazioni dei dati
- Cosa stabilisce il GDPR dell'UE e in che modo le aziende si devono comportare in relazione alle nuove disposizioni
- Quali sono le azioni specifiche da intraprendere per evitare la violazione dei dati

CONTENUTO

* Sondaggio condotto da Kingston Technology in Germania nel 2016 (numero di risposte: 200)

Il regolamento GDPR dell'UE stabilisce un approccio basato sulla prevenzione

Il regolamento generale sulla protezione dei dati dell'Unione Europea (GDPR) sostituisce i precedenti regolamenti nazionali in materia di protezione dei dati, ed entrerà in vigore a partire dal 25 maggio 2018, a seguito di un periodo di transizione di due anni. L'obiettivo principale del regolamento GDPR è di accrescere il livello di **protezione dei dati e i diritti fondamentali dei cittadini dell'Unione Europea.**

Il regolamento GDPR dell'UE è applicabile non solo alle aziende europee, ma anche a tutte le organizzazioni che offrono beni e servizi (inclusi quelli in forma gratuita) ai cittadini dell'UE e che nell'ambito di questa attività richiedono la registrazione dei dati personali. Il regolamento GDPR dell'UE non opera una distinzione tra grandi aziende, PMI o piccole start-up. Ecco perché la protezione dei dati deve essere oggetto di disamina in tutte le aziende in cui si effettua l'acquisizione, il trattamento e l'archiviazione di dati personali.

L'obiettivo della protezione dei dati personali viene perseguito attraverso l'applicazione di sanzioni di notevole entità: le violazioni della protezione dei dati, contro le quali non siano state adottate misure adeguate , sono soggette a sanzioni che ammontano fino al **4% del fatturato annuo consolidato dell'azienda, o fino a 20 milioni di euro.**

Inoltre, tutte le violazioni della protezione dei dati devono essere comunicate all'autorità di sorveglianza preposta e alle persone interessate dalla violazione. Oltre alle sanzioni economiche, le conseguenze per un'azienda possono essere ben più gravi in termini di reputazione, fiducia da parte dei clienti e fatturato.

Queste misure sono volte a prevenire quanto più possibile le violazioni dei dati, a ridurre al minimo la diffusione dei dati personali e a incoraggiare le aziende ad adottare misure preventive. L'UE è tuttavia consapevole che la protezione assoluta dei dati non è attuabile. Ciò nonostante, il nuovo regolamento si prepone di **raggiungere il miglior risultato possibile in termini di prevenzione.**

L'analisi predittiva dei rischi rappresenta uno strumento utile

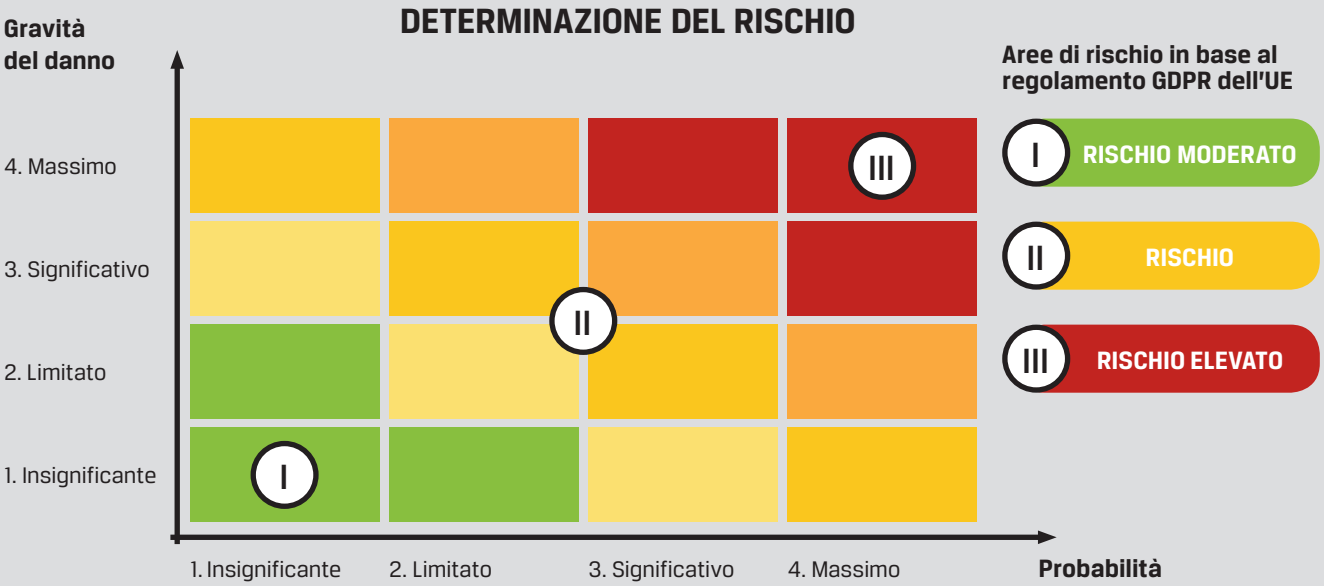
Ai fini della prevenzione, occorre sapere dove possono verificarsi eventuali violazioni dei dati. Pertanto è necessario identificare e analizzare i rischi potenziali. Occorre sottoporre a un'attenta valutazione tutte le aree di un'azienda in cui vengono gestiti dati. Dove vengono acquisiti i dati personali? Come vengono trattati e archiviati?

Il regolamento GDPR dell'UE richiede un'analisi dei rischi di questa tipologia. È inoltre necessario considerare la probabilità che si verifichino tali danni potenziali e la gravità degli stessi. Il responsabile della **protezione dei dat**i può utilizzare queste informazioni per adottare misure adeguate specifiche.

L'articolo 32, comma 1 del regolamento GDPR dell'UE stabilisce che:

"Tenendo conto dello **stato dell'arte** e dei **costi di attuazione**, nonché della **natura**, dell'**oggetto**, del **contesto** e delle **finalità del trattamento**, come anche del rischio di **varia probabilità** e **gravità per i diritti e le libertà delle persone fisiche**, il titolare del trattamento e il responsabile del trattamento mettono in atto misure tecniche e organizzative adeguate per garantire un livello di sicurezza adeguato al rischio[.]"

Una **matrice del rischio** può aiutare a identificare i potenziali rischi relativi all'archiviazione dei dati. Ciò evidenzia dove vi sia la necessità di intervenire. È possibile identificare con precisione ogni rischio potenziale in base alla probabilità che si verifichi e alla gravità dei danni che questo può causare. Tre gruppi di rischio – basso, medio e alto – indicano quindi la necessità di intervento e l'adozione di misure di sicurezza, laddove necessario.



Una **panoramica completa** di tutte le posizioni in cui sono archiviati dati personali semplifica il processo di analisi, indicando con precisione le aree verso cui rivolgere l'attenzione con maggiore urgenza. Le **motivazioni** per la valutazione del rischio possono essere rilevate direttamente dalle colonne relative alle fonti del rischio e da quelle associate alle probabilità e alla portata del danno. In tal modo i rischi possono essere eliminati in maniera efficace, consentendo una preparazione ottimale per la data in cui il regolamento entrerà in vigore, vale a dire il 24 maggio 2018.

Il regolamento GDPR dell'UE propone queste misure di sicurezza

L'obiettivo principale del regolamento GDPR dell'UE in materia di trattamento dei dati personali è "garantire un livello di sicurezza adeguato al rischio" (articolo 32, comma 1). Dopo l'analisi dei rischi, occorre adottare misure protettive che, da una parte, siano adeguate e, dall'altra, siano in grado di garantire la sicurezza.

Il regolamento GDPR dell'UE fornisce anche informazioni specifiche riguardo al livello di precauzioni da adottare per la protezione dei dati sensibili. L'articolo 32, comma 1 stabilisce inoltre che "[Queste] misure includono [...]: [...] la **pseudonimizzazione** e la **cifratura** dei dati personali." Entrambe le procedure possono pertanto essere applicate per garantire la conformità nell'ambito delle misure di sicurezza stabilite dal regolamento GDPR dell'UE.

Per pseudonimizzare le registrazioni dei dati personali, i nomi vengono sostituiti **con codici numerici casuali** e la chiave viene memorizzata in una **tabella master**. Questo processo offre il vantaggio di poter essere interamente automatizzato. Tuttavia, la tabella master deve essere disponibile in qualunque momento e non deve essere smarrita o sovrascritta. Inoltre è estremamente importante che il nome non sia sempre indispensabile per identificare la persona a cui i dati sono associati. L'identità, ad esempio, può essere determinata anche in base al sesso, alla data di nascita e al luogo di residenza. Ne consegue che possa persistere un **rischio residuo** di identificazione. La cifratura è un'altra misura di sicurezza raccomandata nel regolamento GDPR dell'UE. I dati, in qualsiasi condizione e in qualsiasi momento della trasmissione, devono essere crittografati.

Le certificazioni **volontarie dei produttori, quali FIPS 197 o 140 – Level3** sono il marchio che attesta l'alta qualità delle protezioni crittografiche. Queste garantiscono un certo standard di sicurezza e in futuro avranno un ruolo ancora più importante come evidenziato in seno al regolamento GDPR dell'UE.

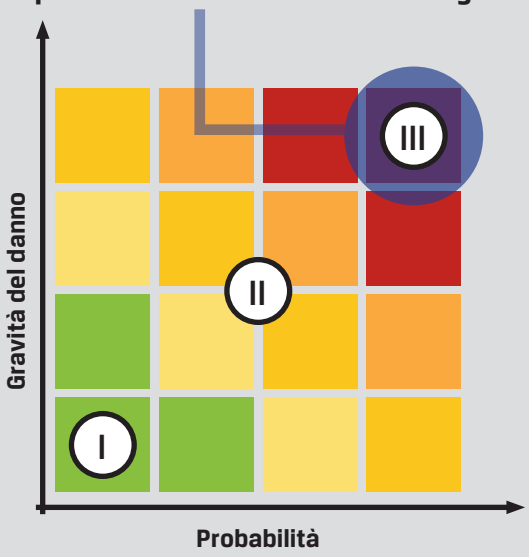
Se i dati personali vengono crittografati in modo sicuro, e in questo contesto la cifratura AES a 256 bit rappresenta la tecnologia più avanzata, i dati non potranno essere utilizzati nemmeno in caso di furto o violazione. In tal caso viene meno l'obbligo di informare le persone interessate o di fare un annuncio pubblico, in quanto non esiste alcun rischio.

Sarà tuttavia necessario informare l'autorità di supervisione responsabile.

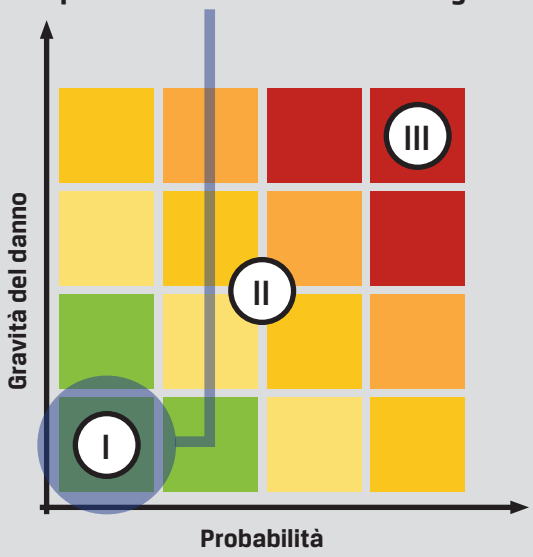
Drive USB crittografati sempre e ovunque: Kingston Technology

Sulla base del sondaggio menzionato in precedenza, le aziende che salvano i dati personali su drive USB non crittografati si espongono a rischi elevati, poiché tali dati spesso vanno persi, rubati oppure non è più possibile individuarli. In tal caso i rischi devono essere considerati complessivamente elevati, in quanto la probabilità e la gravità potenziale dei danni sono a loro volta elevate.

Rischio per i dati senza drive USB crittografato



Rischio per i dati con drive USB crittografato



Con le linee DataTraveler DTVP 3.0 e DT4000G2, e IronKey D300 e S1000, Kingston Technology offre una varietà di drive USB in grado di soddisfare i più elevati standard di sicurezza suindicati. I dati memorizzati sono crittografati al 100% e protetti da una password complessa caratterizzata da requisiti ridotti, che garantisce la massima protezione contro l'accesso non autorizzato. Ad esempio, dopo 10 tentativi di accesso non riusciti, non sarà più possibile accedere ai dati.

I drive USB di Kingston sono crittografati in base allo standard di sicurezza **AES-256** in modalità XTS. L'algoritmo corrisponde agli standard di sicurezza attuali. Le certificazioni conformi agli standard **FIPS 197** e **FIPS 140-2** garantiscono la massima sicurezza dei dati anche quando vengono rubati o smarriti. I drive DataTraveler 4000G2, IronKey D300 e IronKey S1000 offrono inoltre la protezione fisica contro le manomissioni in conformità allo standard FIPS 140-2.

Per alcuni dei suoi drive USB (DTVP3.0, DTVP3.0AV, DT4000G2 con soluzione di gestione e D300), Kingston offre anche un **programma di personalizzazione** con il quale è possibile integrare tali dispositivi in una soluzione di gestione degli endpoint, utilizzando, ad esempio, numeri di serie e ID prodotto oppure con la possibilità di definire il numero di tentativi consentiti di inserimento della password.

Kingston Technology ha collaborato con **DataLocker** per poter offrire anche soluzioni di gestione per i suoi drive USB crittografati. DataLocker integra il software SafeConsole e EMS (Enterprise Management System) per i drive USB crittografati DataTraveler e Ironkey di Kingston, consentendo la gestione dei drive USB da una singola postazione centralizzata all'interno dell'azienda.

I drive DataTraveler Vault Privacy 3.0 e DataTraveler 4000 G2 di Kingston sono disponibili anche in versione gestita (con soluzione di gestione opzionale) ed entrambi supportano la gestione centrale mediante il software SafeConsole di DataLocker. I drive IronKey D300 e S1000 sono disponibili in versione gestita, ed entrambi supportano IronKey EMS di DataLocker.

Queste soluzioni consentono di adeguarsi più facilmente ai **requisiti di conformità** e possono essere fornite con varie forme di **supporto aggiuntivo**, come ad esempio le funzioni di ripristino della password in remoto e di scansione automatica anti-malware. Queste funzionalità semplificano anche la conformità con linee guida di sicurezza globali, poiché consentono agli amministratori di sistema di controllare facilmente tutti i drive dell'azienda.

In tal modo, qualora un drive USB crittografato Kingston dovesse andare perso, tale evento non costituirà necessariamente un incidente connesso a perdita di dati. Le soluzioni di storage crittografate eliminano così una nota e spesso sottovalutata fonte di rischi per la sicurezza delle aziende. L'utilizzo di drive USB crittografati consente di chiudere definitivamente piccole ma pericolose falle per la sicurezza, **evitando le violazioni alla protezione dei dati in conformità all'RGPD UE.**

AVETE ALTRE DOMANDE?

Non esitate a contattarci:

+44 (0) 1932 738888

EncryptedUSB@kingston.eu

www.kingston.com

Questo white paper è stato creato da B2B Media Group GmbH per conto di Kingston Technology Europe Co LLP e Kingston Digital Europe Co LLP.
http://www.b2bmg.de / kontakt@b2bmg.de