MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Proteggi le tue informazioni

Consigli per archiviare in modo sicuro i tuoi dati

Sommario

Cosa troverai in questa brochure

Introduzione

Nell'attuale **contesto digitale**, ogni **interazione online**, come l'invio di **documenti** via e-mail o la trasmissione di **file** tramite **piattaforme di messaggistica**, genera nuove informazioni che vengono condivise e archiviate.

La velocità con cui comunichiamo e produciamo grandi quantità di **dati** rende indispensabili misure mirate per proteggere sia la **riservatezza** delle **informazioni** sia la loro **conservazione sicura**, preservandole da compromissioni e minacce.

Una corretta **conservazione delle informazioni** è fondamentale sia in ambito **lavorativo** che **privato**. È essenziale dunque utilizzare **sistemi di archiviazione** che permettano una **consultazione** rapida dei documenti, che ne assicurino la **protezione dal deterioramento**, dalla **manomissione** e dagli **accessi non autorizzati**, e al tempo stesso ne preservino la **disponibilità** e l'**integrità** nel lungo periodo.

Buone pratiche di gestione documentale

Salvataggio:
puoi salvare temporaneamente i documenti in formato digitale (es. word, ppt, excel, etc.) sul tuo pc per il tempo necessario all'uso.

Archiviazione:
affinché i documenti siano disponibili anche a terzi soggetti, comunque autorizzati ad accedervi, salva i documenti sul sistema di archiviazione selezionato (es. Cloud, hard disk, etc.)

Gestione e backup:
pianifica con cadenza regolare i backup di modo che i documenti archiviati possano essere sempre disponibili anche a fronte di potenziali attacchi informatici.

Statistiche dati esfiltrati

30 TB — Numero di dati esfiltrati in Italia nel 2024 a seguito di attacchi di tipo Ransomware

16 TB — Numero di dati esfiltrati in Italia tra gennaio-agosto 2025 a seguito di attacchi di tipo Ransomware

Fonte: Ransomfeed

Metodi di archiviazione

Principali strumenti

01 USB/Hard Disk

Tra i supporti fisici di archiviazione le **chiavette USB** e gli **Hard Disk** sono strumenti molto diffusi per la gestione e la conservazione dei dati. Essi consentono di archiviare informazioni in maniera semplice e veloce, offrendo maggiore capacità, portabilità e praticità d'uso rispetto ai DVD, ormai considerati meno efficienti per esigenze moderne.

02 Archiviazione Cloud

Tra le più diffuse modalità di archiviazione digitale, rientrano le **soluzioni basate su Cloud**, che consentono di caricare, consultare e condividere dati direttamente tramite Internet. Questo approccio elimina la necessità di supporti fisici, offrendo maggiore flessibilità, accesso da qualsiasi luogo e un livello di praticità oggi considerato fondamentale.

03 Cartelle di rete

Tra le metodologie di archiviazione online, rientrano anche le **cartelle di rete**, che permettono di conservare i dati in maniera centralizzata all'interno di un'infrastruttura condivisa. Questo sistema consente un accesso controllato e sicuro, regolato da specifiche autorizzazioni, garantendo così ordine, tracciabilità e una gestione più efficiente delle informazioni.

Rischi associati

I supporti fisici di archiviazione comportano un **elevato rischio di furto**, **smarrimento** o infezione da malware, con potenziale compromissione dell'integrità, della riservatezza e della disponibilità dei dati archiviati.

In caso di **credenziali deboli** per accedere ai sistemi di archiviazione Cloud, i dati possono essere **accessibili da attori non autorizzati,** potendo compromettere l'integrità, la riservatezza e la disponibilità dei dati.

Se i **permessi di accesso** alle cartelle di rete non sono configurati correttamente, utenti **non autorizzati** possono **consultare o modificare** i file, compromettendone l'integrità, la riservatezza e la disponibilità

Come difendersi?

Archiviazione cifrata

Per proteggere i tuoi dati archiviati, adotta **sistemi di crittografia** avanzata. Tale meccanismo è valido sia per i supporti fisici di archiviazione sia per quelli in Cloud. La cifratura è una misura essenziale per garantire **riservatezza**, conformità normativa e protezione delle informazioni sensibili, riducendo al minimo i rischi di accesso non autorizzato.

Ricorda, inoltre, di conservare correttamente le tue chiavi crittografiche per visualizzare i documenti archiviati.

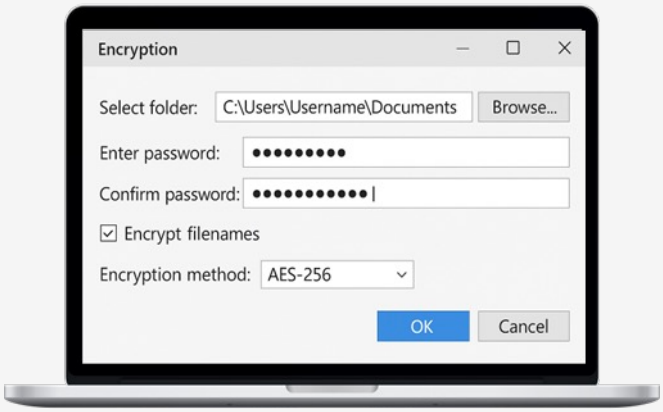
Conservazione sicura

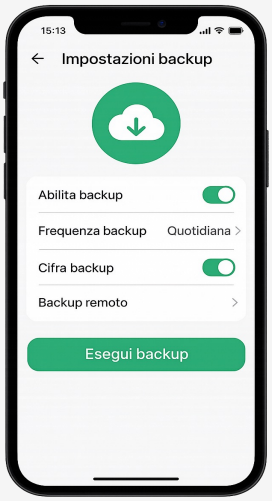
In caso di utilizzo di supporti fisici di archiviazione, ricorda di **conservarli** sempre in **luoghi sicuri e controllati**, evitando di lasciarli incustoditi in ambienti condivisi o facilmente accessibili, e proteggendoli inoltre mediante l'utilizzo di **password** di accesso. In questo modo, anche in caso di potenziale smarrimento o furto, i dati ivi contenuti saranno adeguatamente protetti.

Backup regolari

Per prevenire la perdita dei dati, effettua **backup frequenti e automatizzati, ricordando di proteggerli** tramite **password** robuste.

Effettua, inoltre, **test** periodici volti a verificarne l'integrità dei dati archiviati e la continua leggibilità degli stessi. Questa pratica raf-forza la **continuità operativa** e garantisce resilienza contro guasti e attacchi informatici, rendendo i dati sempre disponibili.





Security Trend

L'attacco che non ti aspetti

Il gruppo criminale denominato FIN7 ha inviato ad una pluralità di aziende statunitensi dei **dispositivi USB compromessi** finalizzati ad infettare i loro sistemi informatici. Nello specifico, tale gruppo criminale, avvalendosi del servizio postale degli Stati Uniti ed impersonificando il Dipartimento della salute USA, ha inviato dei **pacchi regalo** alle **aziende** vittime, spesso accompagnati da note di ringraziamento, e-mail o telefonate che ne preannunciavano l'invio, con la finalità di rendere la truffa maggiormente credibile. Gli utenti delle aziende vittime, una volta collegato al loro computer i dispositivi compromessi, hanno installato dei **software malevoli**, in grado di compromettere i sistemi aziendali ed accedere ad informazioni confidenziali e/o strategiche.

Gli attacchi informatici perpetrati tramite chiavette USB vengono spesso veicolati distribuendo tali dispositivi come **gadget**, oppure **abbandonando** intenzionalmente tali **dispositivi** in **luoghi pubblici**, stimolando la curiosità dei passanti che potrebbero essere indotti a collegarli ai propri dispositivi.

Gennaio 2022

Accesso fraudolento al Cloud

La società americana Snowflake, che offre servizi di **archiviazione** dati in **Cloud**, ha subito un attacco informatico che ha comportato il furto di milioni di dati afferenti ai clienti della società fornitrice del servizio.

Nello specifico, gli attaccanti non hanno sfruttato vulnerabilità di Snowflake, ma hanno ottenuto **accessi** non autorizzati utilizzando **credenziali rubate** agli utenti clienti legittimi della società, con la successiva finalità di **accedere** ai **dati** aziendali **archiviati sul Cloud**.

È stato reso noto che gli account compromessi non avevano abilitato l'autenticazione multifattore (MFA) e/o le **password** per accedere al sistema erano in uso da diversi anni e, pertanto, **obsolete**.

La combinazione di questi fattori, ha comportato la possibilità di accesso fraudolento ai criminali informatici, che, impersonificando utenti legittimi, hanno effettuato numerose **richieste** di **estrazione** dati, esponendoli, poi, al dominio pubblico.

Giugno 2024

MUR
Ministero dell'Università e della Ricerca

CYBER SAPERE

Restate sintonizzati:

nuovi approfondimenti sulla cybersecurity vi aspettano nelle prossime pubblicazioni.