Cancellare in modo sicuro

Cancellare definitivamente i dati è più difficile di quanto si creda: non tutte le cancellazioni cancellano! La soluzione più sicura, ossia la distruzione fisica del supporto dati, il più delle volte non è praticabile. Ma esistono delle alternative.

Cancellate i dati in modo sicuro così:

- Sovrascrivete (più volte) le aree dati liberate sui dischi rigidi o nastri magnetici per mezzo di appositi strumenti.
- Sovrascrivete una volta l'intera area di memorizzazione dei supporti dati elettronici come chiavette USB, schede SD o dischi rigidi SSD per mezzo di appositi strumenti.
- ripristinate le impostazioni di fabbrica dello smartphone o tablet dopo aver attivato la crittografia del dispositivo.
- Distruggete fisicamente i supporti dati ottici come CD-R/RW o DVD-R/RW.
- Crittografate l'intera area di memorizzazione o i contenuti sensibili dei supporti dati di qualsiasi tipo e distruggete la chiave.
- Distruggete fisicamente il supporto dati.

I file che sono stati cancellati senza adottare precauzioni particolari spesso possono essere ripristinati con i programmi giusti. Questo perché è possibile che i dati non vengano cancellati affatto, ma semplicemente sovrascritti con altri dati. La difficoltà sta nel ripulire tutte le aree di archiviazione.

Per cancellare i dati riservati in modo definitivo e irreversibile, sono quindi necessari strumenti specifici e procedure adeguate al tipo di supporto utilizzato.

Supporti dati magnetici come dischi rigidi o nastri

Programmi appositi sovrascrivono l'area del disco rigido o del nastro magnetico in cui si trovavano i dati da cancellare con sequenze di dati (prive di significato) – di solito ripetendo l'operazione più volte. Con questa procedura i dati vengono eliminati in modo irrecuperabile.

Sul mercato si trovano diversi programmi commerciali e anche prodotti gratuiti, come:

Windows

- **Eraser**: Download: eraser.heidi.ie (https://eraser.heidi.ie)
- **Secure Eraser**: una buona introduzione (https://www.computerbild.de/artikel/cb-Downloads-Tuning-System-Secure-Eraser-Tipps-Anleitung-5697825.html) si trova sul sito Internet della rivista «Computerbild». Download: www.secure-eraser.com (http://www.secure-eraser.com)

macOS

- **Permanent Eraser**: Download: www.edenwaith.com (http://www.edenwaith.com)

Supporti dati elettronici come dischi rigidi SSD, chiavette USB e schede SD

Per motivi tecnici i programmi citati non permettono di cancellare in modo affidabile singoli file presenti su supporti dati elettronici come chiavette USB, schede SD o dischi rigidi SSD.

Una possibilità è quella di sovrascrivere completamente il supporto dati, ma ciò comporta la perdita di tutto il contenuto del supporto. In alternativa, i dati possono essere crittografati (vedi sotto).

Smartphone e tablet

Per cancellare definitivamente i supporti dati interni di uno smartphone o tablet, si possono ripristinare le impostazioni di fabbrica dopo aver attivato la crittografia del dispositivo. Attenzione però: tutti i dati utente andranno persi!

Android

1. In **Impostazioni / Sicurezza**, attivate la crittografia del dispositivo e attendete il completamento dell'operazione (potrebbe richiedere parecchio tempo!).
2. Riportate il dispositivo alle impostazioni predefinite di fabbrica in **Impostazioni / Sistema / Opzioni di ripristino**.

iOS

1. Sui dispositivi iOS più recenti la crittografia è abilitata per impostazione predefinita e non si può disattivare.
2. Con l'ID Apple il dispositivo rimane abbinato a voi anche dopo la cancellazione. Pertanto, se desiderate cedere il dispositivo a qualcun altro, dovete (prima di cancellarne il contenuto) eliminare l'abbinamento con l'ID Apple in **Impostazioni / Esci / Disattiva**.
3. Reimpostate il dispositivo in **Impostazioni / Generali / Ripristina / Inizializza contenuto e impostazioni**.

Un altro modo semplice per cancellare in modo sicuro almeno l'area in cui sono memorizzate foto e video è, dopo aver cancellato manualmente i contenuti indesiderati, quello di registrare con l'app della fotocamera un video «vuoto» (inquadrando p. es. il piano del tavolo) fino a quando la memoria non è piena. (Attenzione: questa procedura registra anche l'audio e non cancella/sovrascrive alcune aree di memoria come i messaggi.)

Supporti dati ottici come CD-R/RW e DVD-R/RW

Ai supporti dati ottici come CD-R/RW o DVD-R/RW spesso viene riservata un'attenzione insufficiente quando si trat-

ta di cancellare i dati. Molte volte dopo l'uso finiscono semplicemente nella spazzatura – e con loro i dati sensibili.

Spesso dal punto di vista tecnico (CD-R/DVD-R) i dati non si possono cancellare in modo sicuro, oppure l'operazione appare sproporzionata se si considera il basso valore dei supporti dati (CD-RW/DVD-RW).

In questi casi, la distruzione fisica del supporto dati è un metodo tanto sicuro quanto pratico.

Distruzione fisica del supporto dati

Per i supporti dati di ogni genere la distruzione fisica rappresenta un metodo sicuro. Ad esempio, si può praticare un foro in un disco rigido o colpire una chiavetta USB con un martello per distruggerne il chip di memoria. Procedimenti più professionali e garantiti secondo la norma DIN 66399 vengono offerti da aziende commerciali.

Se si distrugge fisicamente un supporto dati, naturalmente, se ne riduce a zero anche il valore. Soprattutto per i supporti dati più costosi, come i dischi rigidi SSD di capacità elevate o i dispositivi con supporti dati integrati come gli smartphone e i tablet, in generale questa soluzione non è praticabile. In questi casi, la crittografia dei dati rappresenta una buona alternativa.

Protezione tramite crittografia

L'alternativa più sicura e allo stesso tempo la più flessibile a tutte le forme di cancellazione dei dati è la crittografia dei dati sensibili, che rende illeggibili a terzi i contenuti riservati. A differenza della cancellazione dei dati, questa protezione funziona per l'intero ciclo di vita dei dati e anche oltre. Se si cancella la chiave, infatti, i dati vengono persi in modo irreversibile.

Per avere la certezza che in nessun momento vengano memorizzati su un supporto dati contenuti non protetti, l'intero supporto dati andrebbe crittografato già all'atto della sua messa in funzione. Esistono vari programmi anche per questo:

Windows

- **BitLocker** è una funzionalità di crittografia di interi supporti dati disponibile nelle versioni Windows Ultimate/Pro/Enterprise.
- **EFS** è una funzione standard del file system NTFS disponibile in Windows che permette di crittografare singoli file o cartelle del singolo utente.
- **VeraCrypt** è gratuito, potente e facile da usare. Download: www.veracrypt.fr (https://www.veracrypt.fr)

macOS

- **FileVault** è una funzione standard integrata in macOS per la crittografia di file e interi dischi rigidi.
- **VeraCrypt** è gratuito, potente e facile da usare. Download: www.veracrypt.fr (https://www.veracrypt.fr)

La distruzione irreversibile dei dati si ottiene con la distruzione fisica del supporto dati. Un metodo più pratico consiste nel «cancellare tramite sovrascrittura» per mezzo di appositi programmi. Un'alternativa efficace, valida per l'intero ciclo di vita dei dati e oltre, è la protezione mediante crittografia.

Maggiori informazioni

Un'eliminazione dal cestino o la formattazione non bastano

Nei computer, solitamente, un file cancellato viene spostato inizialmente nel cestino. Da lì il file può essere all'occorrenza ripristinato oppure cancellato in modo apparentemente definitivo con lo svuotamento del cestino. Quest'ultima procedura, tuttavia, non «cancella» concretamente i dati, ma solo il riferimento al file nella rispettiva cartella. Ciò rende «invisibile» il file per l'utente, e i settori del disco rigido su cui si trova il file da cancellare vengono messi a disposizione del sistema per la sovrascrittura. Ciò significa che i dati continuano a esistere finché nell'area messa a disposizione non viene scritto un altro file.

Un ragionamento simile vale per la formattazione dei supporti dati. Con la formattazione rapida (Quick Format) vengono cancellati i riferimenti a tutti i file dalla cartella. Tuttavia, il contenuto dei file – per quanto orfano – resta inalterato anche con questa procedura.

La formattazione completa è più efficace. Nei moderni sistemi operativi, infatti, le aree di memorizzazione vengono completamente sovrascritte con degli zeri. Ciò esclude di fatto la possibilità di ripristinare i file con strumenti accessibili.

Per questo motivo è possibile ripristinare i file cancellati che non sono stati ancora sovrascritti. L'operazione può essere molto utile se avete eliminato per sbaglio un file di cui avete ancora bisogno. Per motivi di sicurezza, p. es. quando desiderate eliminare in modo irreversibile un file dal contenuto riservato, la soluzione non è però consigliabile.

Per cancellare in modo irreversibile un singolo file o un intero supporto dati occorrono solitamente programmi specifici. La procedura dipende dal tipo di supporto dati o dal metodo di registrazione utilizzato:

Dischi rigidi magnetici

Sui supporti dati magnetici l'area di archiviazione di un file è ben definita. Programmi appositi sono in grado di individuare e sovrascrivere in modo mirato l'area del disco rigido in questione – solitamente ripetendo l'operazione più volte per sicurezza. Con questa procedura i file vengono eliminati in maniera irrecuperabile.

Se eliminate o vendete il vostro computer vecchio, è consigliabile rimuovere i supporti dati al suo interno oppure eliminare almeno i dati presenti sul disco rigido: è improbabile infatti che vogliate permettere a chi compra il vostro dispositivo di ripristinare i vostri dati sensibili. La soluzione più semplice consiste nell'usare un apposito CD avviabile contenente gli strumenti in grado di sovrascrivere l'intero disco rigido, p. es. DBAN (https://www.dban.org) per Windows.

Chiavette USB e schede SD

Sui cosiddetti supporti di memoria flash, come le chiavette USB o le schede di memoria SD, lo stesso contenuto può essere memorizzato in diversi punti per motivi tecnici. Vengono infatti create delle copie automatiche. In caso di cancellazione tramite sovrascrittura, viene eliminata soltanto la copia che è stata utilizzata per ultima – le altre non vengono toccate.

Bisogna quindi tenere presente che un file su un supporto flash può essere cancellato in modo sicuro solo se si cancella in modo irreversibile l'intero supporto. In generale non è possibile cancellare in modo sicuro singoli file su una chiavetta USB o una scheda SD.

Dischi rigidi SSD

I file sui dischi rigidi SSD installati nei computer più recenti non possono essere cancellati in modo affidabile con i programmi menzionati. I motivi sono di natura tecnica: per consentire un'usura uniforme delle celle di memoria, il contenuto del disco rigido viene automaticamente riorganizzato a cadenza periodica. Ciò si traduce in copie «perse» dei dati, che non è possibile sovrascrivere in modo mirato. Non è quindi possibile una cancellazione affidabile dei dati tramite sovrascrittura.

Alcuni produttori di dischi rigidi SSD offrono funzioni integrate in grado di rintracciare questi dati persi sul supporto e a quanto pare cancellarli definitivamente. La funzionalità e l'affidabilità di queste attività, tuttavia, sono difficilmente verificabili.

Oltre alla distruzione fisica del supporto dati, anche in questo caso si può affermare che la cancellazione sicura di un file si può ottenere soltanto cancellando l'intera area di archiviazione del supporto.

Un'altra alternativa sicura è quella di crittografare i singoli file sensibili o direttamente l'intera area di archiviazione del supporto dati. Senza la chiave i contenuti riservati sono illeggibili per terze persone. Un ulteriore vantaggio di questa soluzione è che i vostri dati sensibili saranno protetti anche nel caso in cui il vostro dispositivo (p. es. il laptop) sia smarrito o rubato – senza chiave, l'accesso è bloccato!

Supporti di memorizzazione ottici

Con i supporti di memorizzazione ottici scrivibili, i dati vengono incisi da un laser su uno strato riflettente come sequenza di forature. A seconda delle caratteristiche dello strato, il processo può essere eseguito solo una volta (R) o ripetutamente (RW).

A causa delle difficoltà tecniche e dello scarso valore dei supporti dati, la distruzione fisica del supporto dati rappresenta la soluzione più pratica per cancellare i dati.

Nastri magnetici

I nastri magnetici vengono utilizzati spesso per il backup di intere raccolte di dati e solitamente sono conservati per lunghi periodi di tempo. Rendono possibile un «tuffo nel passato» – compresa la consultazione di dati che si ritenevano persi da tempo.

I nastri magnetici registrano i contenuti da sottoporre a backup in modo sequenziale, come serie di dati che solitamente costituiscono un'unità immutabile dotata di protezione dell'integrità. I singoli file non si possono rimuovere da queste unità. Piuttosto, per cancellare i dati occorre eliminare l'intero set di dati.