Corso di formazione
Responsabile per la Transizione al Digitale

Modulo 4

Sicurezza, accessibilità e usabilità nell'amministrazione digitale

A cura di
Raffaele Grieco

M. 4.1 Sicurezza informatica: rischi, minacce e soluzioni

Sicurezza informatica ⇨ Sicurezza fisica

(protezione di: server, PdL, accessi, sistemi di comunicazione…)

Obiettivi della sicurezza

Impedire che i dati vengano alterati o distrutti

Impedire che i dati vengano divulgati *(breach)*

Problemi per la sicurezza

- hardware
- software
- umani

vulnerabilità software

- del Sistema Operativo
- degli applicativi
- degli apparati (firmware)

Il fattore umano è il vero problema della cybersecurity

Nuovi studi confermano che il crimine informatico non prende di mira infrastrutture critiche o vulnerabilità dei software informatici, ma le persone e le loro debolezze, per il furto di denaro e dati e per stabilire le basi per attacchi futuri.

il report completo :

www.key4biz.it/wp-content/uploads/2018/04/pfpt-us-wp-human-factor-report-2018-180425.pdf

lettura: come sono entrata…

anche un computer **isolato dalla rete** *("air-gapped")* può essere attaccato in vari modi:

- Supporti esterni (penne USB, HD, CD, DVD…) [esempio: il virus **Stuxnet**]
- Intrusione nel sistema (cattura della password)
- attacchi hardware vari

Un attacco può portare **danni** o **breach**

Provenienza delle minacce

- Siti web
- Email
- Social networks
- Altre fonti (peer-to-peer,…)
- interne

Tipi di minacce

- virus / malware / spyware
  - script malevoli
    - cookies / Flash cookies
      - spam
        - scam
          - port scan
            - intrusioni
              - …

Visita 9.000 siti a luci rosse dall'ufficio e infetta l'intera rete aziendale

www.zeusnews.it/n.php?c=26806

Texas bloccato dai ransomware. I pirati vogliono 2,5 milioni

Ago 22, 2019

I cyber-criminali hanno violato i sistemi dell'azienda che gestisce il settore IT del governo statale e hanno colpito 22 enti pubblici contemporaneamente.

https://www.securityinfo.it/2019/08/22/texas-bloccato-dai-ransomware-i-pirati-vogliono-25-milioni/

DIFESE

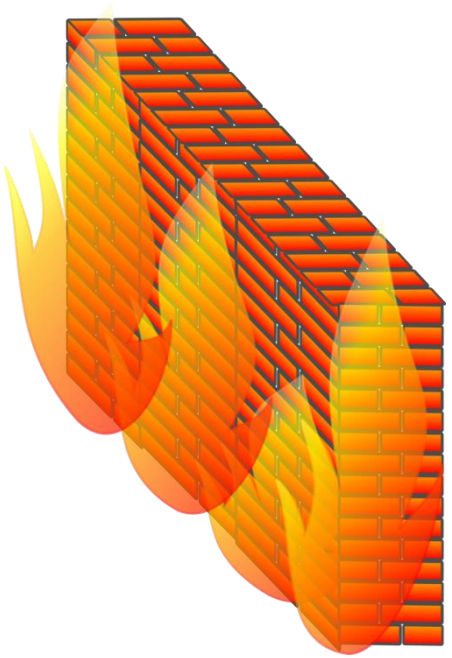
Centralizzazione

Dominio (accessi, policy, account…) *[parte 4.3]*

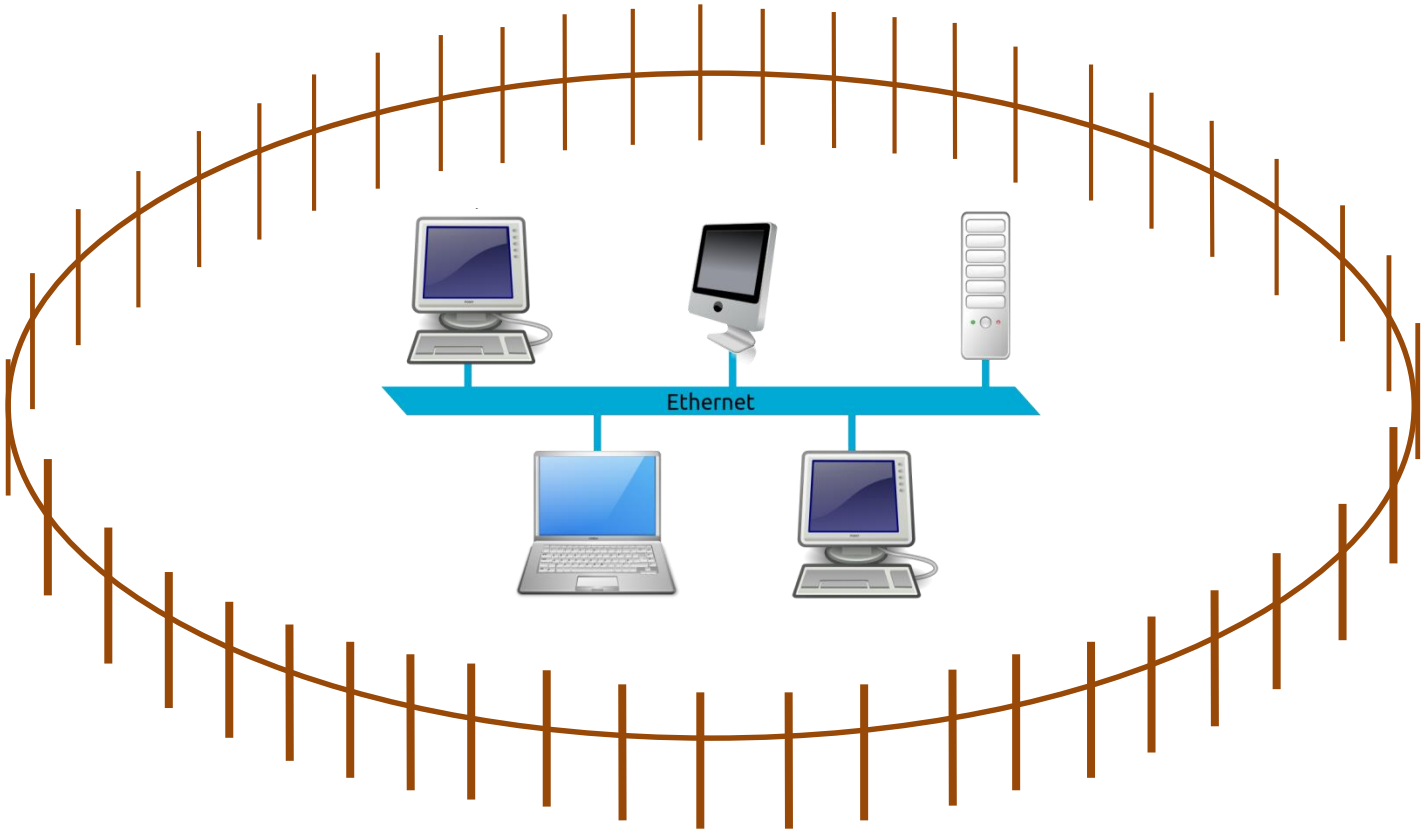
Difese (antivirus, antispam, firewall, web filtering…)

Monitoraggio (traffico, log, problemi H/S, accessi…)

Centralizzazione - **IL FIREWALL**



IL FIREWALL



Funzione principale del **firewall** è limitare (al limite annullare) il traffico potenzialmente pericoloso, applicando:

- Filtraggio delle connessioni
- Blocco di tentativi di accesso dall'esterno
- Suddivisione in sottoreti
- ...

Per impedire ai dipendenti di accedere a siti non pertinenti col lavoro si usano altri sistemi *(web filtering)*

FIREWALL

Home

Enterprise


Mondo esterno
LAN
WAN

I firewall moderni possono avere numerose altre funzioni; alcune proteggono dalle minacce *interne* con varie opzioni:

- Antivirus
- Packet sniffing
- SSL inspection
- VPN
- Data Leak prevention
- …

BACKUP

Protezione essenziale

e

Obbligo normativo

Il backup protegge da:

- Modifiche e cancellazioni accidentali
  (in generale, errori umani)
- aggiornamenti e nuove versioni del software
- Minacce varie (malware, virus, hacker…)

e costituisce il substrato per il **Disaster Recovery**

regola di base

!

non deve mai esistere

una sola copia

di un file

nastri

dischi

…cloud

Crittografia

utilizzi

- cifratura locale (PdL, backup, comunicazioni…)
- cifratura remota (cloud, trasmissioni)
- Firma Digitale
- PEC

Fine

Parte 4.1

M4.2 L'identità digitale

(concetti generali, rischi e minacce, casi di studio)

definizione AGID

L'**identificazione** elettronica è un processo in cui si usano i dati di autenticazione personale in forma elettronica per identificare univocamente: una persona fisica e una persona giuridica.

L'**autenticazione** elettronica è il processo che permette di assicurare il riconoscimento dell'utente elettronico.

www.agid.gov.it/it/piattaforme/eidas/identificazione-autenticazione-elettroniche

L'**autenticazione** è diversa:

dall'**identificazione** (accertare che l'utente sia conosciuto dal sistema)

e dall'**autorizzazione** (dare a un utente il diritto ad usare specifiche risorse, sulla base della sua identità).

usi

- Logon (accesso) locale a una PdL o un server
- accesso remoto (servizi online)
- SPID - Sistema Pubblico di Identità Digitale

(Tentare di) accertarsi dell'identità di qualcuno può basarsi su 3 principi:

- **conoscenza** (password, informazioni)
- **possesso** (token, tool di prossimità)
- **inerenza** (biometria)

I mezzi usati variano per affidabilità, costi, velocità

strumenti biometrici

- Lettore di impronta digitale
- Scanner di impronta retinica
- Lettore di impronta della mano
- Sistema di riconoscimento vocale

Rilevatori biometrici

Rilevatori biometrici

Smartphone

- Lettori di impronta *(Toshiba G500 e G900, Motorola Atrix, Iphone 5S, Galaxy S5...)*
- Face ID (iPhone X)
- Iride (Galaxy S8)

www.news18.com/news/india/motorola-atrix-had-a-fingerprint-scanner-two-years-before-iphone-5s-638036.html

Autenticazione a 2 fattori

- Biometria (impronta digitale, scan retinico, voce…)
- SMS
- Token (chiavetta della banca, app…)

Autenticazione a 2 fattori

(2-factor authentication)

Anche se ci sono altre controindicazioni, protegge dall'immissione della password nel campo *'username'* davanti a terzi (fatto purtroppo frequente), da keylogger e altre minacce

lettura: 2-factor authentication

Facebook Is Using Your Two-Factor Authentication Phone Number to Target Advertising

www.schneier.com/blog/archives/2018/10/facebook_is_usi.html

Autenticazione a 2 fattori

PSD2

(Payment Services Directive 2)

SCA

(Secure Costumer Authentication)

www.zeusnews.it/n.php?c=18795

Google dichiara guerra alle password

Per Google il sistema attuale è troppo insicuro: la soluzione è una chiavetta con tutti i dati per l'identificazione. E assolutamente da non perdere.

Il vantaggio sta nel fatto che la soluzione è multipiattaforma perché non occorre scaricare software aggiuntivo ma è sufficiente il supporto da parte del browser: potenzialmente, dunque, ogni browser potrebbe adottarla.

L’anello digitale che sostituisce le password

L’anello smart Motiv Ring farà felice chiunque non sopporti di dover pescare il telefono dalla tasca per ricevere i codici di accesso ai propri siti preferiti

www.wired.it/gadget/accessori/2018/10/24/anello-password-autenticazione-due-fattori/

FIRMA ELETTRONICA

FIRMA ELETTRONICA

Insieme di dati in forma elettronica usati come sistema di identificazione informatica

Sono allegati oppure associati logicamente ad altri dati elettronici

Firma elettronica

Pin della carta (bancomat)
username / password
Credenziali web

Firma elettronica avanzata

Semplificazione della FEQ

Esempio: la firma grafometrica (su tablet, tavoletta grafica…)

Firma elettronica qualificata

Si firma con un oggetto come token o smart card
Base per la Firma remota e Automatica (*'massiva'*)

Firma digitale

Emessa da una Certification Authority qualificata

Basata su un **sistema crittografico** a chiave pubblica

https://www.diritto.it/articoli/tecnologie/calabrese.html

Falsificazione della firma digitale: un rischio evitabile

PEC

l'email *classica* è assolutamente non sicura

chiunque può comporre un messaggio usando come indirizzo di origine quello di chiunque altro

la PEC offre garanzie di autenticazione, integrità e confidenzialità grazie alla crittografia a chiave pubblica

offre garanzie legali maggiori rispetto alla raccomadata A/R:

si può avere la ricevuta di consegna "completa" che certifica anche il contenuto del messaggio (rendendo inutile la famosa *raccomandata senza busta*)

Un gestore di PEC italiano ha ricevuto un attacco informatico

Sono stati rubati i dati di circa 500mila caselle di posta elettronica certificata, causando gravi disservizi a migliaia di uffici pubblici e tribunali

www.ilpost.it/2018/11/20/pec-attacco-informatico
https://www.wired.it/internet/web/2018/11/20/italia-attacco-hacker-account-mail-pec/

L'attacco informatico è iniziato il 12 novembre scorso e sembra sia provenuto dall'estero. (...)
Repubblica spiega che il problema ha coinvolto almeno 98mila utenti "tra magistrati, militari e funzionari del Cisr, il Comitato Interministeriale per la sicurezza della Repubblica, (...)"

Lo Stato dopo l'attacco hacker ai tribunali: "Cambiate la password della vostra Pec"

Il numero 1 della sicurezza cibernetica italiano, Roberto Baldoni, invita tutti i possessori di un indirizzo di posta certificata a monitorare i propri account dopo l'attacco dei giorni scorsi.

www.repubblica.it/tecnologia/sicurezza/2018/11/19/news/dopo_l_attacco_hacker_ai_tribunali_cambiate_subito_la_password_della_vostra_pec_-212086305

Fine

Parte 4.2

M4.3 La Circolare Agid n. 2/2017 e le misure di sicurezza minime per le Pubbliche Amministrazioni

L'individuazione di misure che rispettano i parametri previsti come minimi **non è sufficiente** a liberare da ogni responsabilità il soggetto che effettua il trattamento.

Le misure *minime* di sicurezza sono tipizzate dal legislatore. Quelle *idonee* no. Devono essere scelte dal Titolare sulla base di:

- natura dei dati
- trattamento
- stato dell'arte della tecnica

In cosa consistono le misure di sicurezza

Le misure consistono in controlli di natura tecnologica, organizzativa e procedurale e utili alle Amministrazioni per valutare il proprio livello di sicurezza informatica.
A seconda della complessità del sistema informativo a cui si riferiscono e della realtà organizzativa dell'Amministrazione, le misure minime possono essere implementate in modo graduale seguendo tre livelli di attuazione.

1) **Minimo:** è quello al quale ogni Pubblica Amministrazione, indipendentemente dalla sua natura e dimensione, deve necessariamente essere o rendersi conforme.
2) **Standard:** è il livello, superiore al livello minimo, che ogni amministrazione deve considerare come base di riferimento in termini di sicurezza e rappresenta la maggior parte delle realtà della PA italiana.
3) **Avanzato:** deve essere adottato dalle organizzazioni maggiormente esposte a rischi (ad esempio per la criticità delle informazioni trattate o dei servizi erogati), ma anche visto come obiettivo di miglioramento da parte di tutte le altre organizzazioni.

https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

Fra le misure minime è previsto inoltre che le PA accedano a servizi di **early warning** per rimanere aggiornate sulle nuove vulnerabilità di sicurezza. A tal proposito il CERT-PA (link) fornisce servizi informativi a tutte le amministrazioni accreditate.

https://www.agid.gov.it/it/sicurezza/misure-minime-sicurezza-ict

Centralizzazione

Dominio (accessi, policy, account…)

Difese (firewall, antivirus, antispam, web filtering…)

Monitoraggio (traffico, log, problemi H/S, accessi…)

DOMINIO

«insieme di computer che condividono un database di risorse di rete e che vengono amministrati come un'unità con regole e procedure comuni»

DOMINIO

Un server centrale (il **Domain Controller**) rilascia i permessi di accesso agli utenti registrati, distribuisce le policy di dominio, gestisce le politiche di sicurezza e le relazioni di fiducia con altri domini

Centralizzazione - **SIEM**

s*ecurity* ***i****nformation and* ***e****vent* ***m****anagement*

SIEM = SIM + SEM (non sono sinonimi)

SIM: *Security Information Management*

SEM: *Security Event Management*

SIM: *Security Information Management*

software utilizzato per automatizzare il processo di raccolta e gestione dei log **non in tempo reale.**

La conservazione di questi dati unita all'analisi degli stessi permette di generare report personalizzati

Più orientato a un punto di vista *storico*

SEM: *Security Event Management*

Fornisce monitor **in tempo reale**, raccolta e aggregazione di dati, una console per il controllo e la gestione degli eventi e sistemi di risposta automatica per problemi di sicurezza

Più orientato a un punto di vista *real-time*

Funzioni di un SIEM

- Raccolta dati (log)
- Normalizzazione dei dati
- Correlazione (con regole built-in o personalizzate)
- Report (per audit o analisi forense)
- Notifiche

un SIEM aiuta a individuare

- Accessi non autorizzati
- Violazioni delle policy di sicurezza
- Tentativi di attacco
- Intrusioni
- ...

esempi di allarme

virus - se un computer qualsiasi della rete individua un malware

attacco esterno - più di x *reject* o *deny* dallo stesso IP in un dato intervallo (p.e. 30 secondi)

intrusione - troppi tentativi di login errati su una postazione in 1 minuto

PEN TESTING

(penetration testing)

Serve a cercare le vulnerabilità del sistema, tra cui:

- Porte inutilmente aperte
- Software con vulnerabilità note
- Software non aggiornato
- Vulnerabilità *Zero-day*
- Problemi hardware (firewall, router...)
- errori di configurazione o impostazione

FINE

Parte 4.3

M4.4 Dati e metadati, il rischio di involontaria divulgazione

definizione

- informazione che descrive un insieme di dati;
- una definizione o una descrizione di dati

esempi

per un libro i metadati possono essere: parole chiave, numero di pagine, numero di parole, abstract, ISBN

per una telefonata: ora, durata, numero chiamante, numero chiamato, posizione…

"I metadati sono dati che 'spiegano' i dati. Cioè descrivono operazioni e attività ad un livello alto. Cyber criminali sofisticati, ma anche quelli meno esperti, possono ricavare grandi vantaggi dallo sfruttamento illecito di questi dati".

Come? Combinando i **metadati** con altri set di **dati**. I metadati non sono pericolosi in sé, tuttavia se associati ad una serie di informazioni che, ad esempio, forniscono indicazioni su chi è la vittima e mettono in evidenza come il potenziale bersaglio agisce, diventando così cruciali in termini di sicurezza.

https://www.dimt.it/index.php/it/notizie/16253-metadati-possono-essere-usati-per-attaccare-le-infrastrutture-critiche-il-report-dell-istituto-per-la-tecnologia-delle-infrastrutture-critiche

Privacy: quello che dicono i metadati (a nostra insaputa)

Due ricerche italiane spiegano che un selfie messo online rivela molto più di quello che vorremmo far sapere

www.wired.it/internet/social-network/2014/09/12/privacy-dicono-i-metadati-nostra-insaputa/

il soldato Alexandr Sotkin pubblicava le proprie foto su Instagram, dimenticando che tra le funzioni della piattaforma c'è Photo Map, ovvero un mappamondo che consente di individuare il luogo in cui è stato immortalato lo scatto. Morale: venne fuori che l'esercito di Putin era sconfinato in Ucraina

«Un altro modo è proporre degli esempi che facciano emergere il valore dei metadati, come fa la Electronic Frontier Foundation. Cito e traduco:»

- *Loro* sanno che hai chiamato una linea erotica alle 2:24 del mattino e hai parlato per 18 minuti. Ma non sanno di cosa hai parlato.
- *Loro* sanno che hai chiamato il numero per la prevenzione dei suicidi mentre eri su un ponte. Ma l'argomento della conversazione resta segreto.
- *Loro* sanno che hai parlato con un servizio che fa test per l'HIV, poi con il tuo medico e poi con il gestore della tua assicurazione sanitaria. Ma non sanno di cosa avete discusso.
- *Loro* sanno che hai chiamato un ginecologo, gli hai parlato per mezz'ora, e poi hai chiamato il consultorio locale. Ma nessuno sa di cosa avete parlato.

https://attivissimo.blogspot.com/2018/02/le-parole-di-internet-metadati-e-cosa.html

«Un primo modo per spiegare meglio l'importanza dei metadati è chiamarli in maniera comprensibile. Come suggerisce Edward Snowden, provate a sostituire *metadati* con *informazioni sulle attività*.»

Are your readers having trouble understanding the term "metadata" *? Replace it with* "activity records." *That's what they are.*

Edward Snowden (@Snowden) 2 novembre 2015

Leak di dati e metadati

Leak di dati e metadati

- PC dismessi
- supporti buttati (CD, DVD, USB, Hard disk…)
- stampanti / fotocopiatrici a noleggio

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1571514

Rifiuti di apparecchiature elettriche ed elettroniche (Raee) e misure di sicurezza dei dati personali - 13 ottobre 2008 [1571514]

G.U. n. 287 del 9 dicembre 2008

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

(...)
VISTI gli atti d'ufficio relativi alla problematica del rinvenimento di dati personali all'interno di apparecchiature elettriche ed elettroniche cedute a un rivenditore per la dismissione o la vendita o a seguito di riparazioni e sostituzioni; viste, altresì, le recenti notizie di stampa in ordine al rinvenimento da parte dell'acquirente di un disco rigido usato, commercializzato attraverso un sito Internet, di dati bancari relativi a oltre un milione di individui contenuti nel disco medesimo;

(...)
CONSIDERATO che rischi di accessi non autorizzati ai dati memorizzati sussistono anche in relazione a rifiuti di apparecchiature elettriche ed elettroniche avviati allo smaltimento (art. 3, comma 1, lett. i), d.lg. n. 151/2005);
(...)

GARANTE
PER LA PROTEZIONE
DEI DATI PERSONALI

(…)

Misure tecniche per la cancellazione sicura dei dati, applicabili a dispositivi elettronici o informatici:

3. Cancellazione sicura delle informazioni, ottenibile con programmi informatici (quali *wiping program o file shredder*) che provvedono (…) a scrivere ripetutamente (…) sequenze casuali di cifre "binarie" (zero e uno) in modo da ridurre al minimo le probabilità di recupero di informazioni (…),

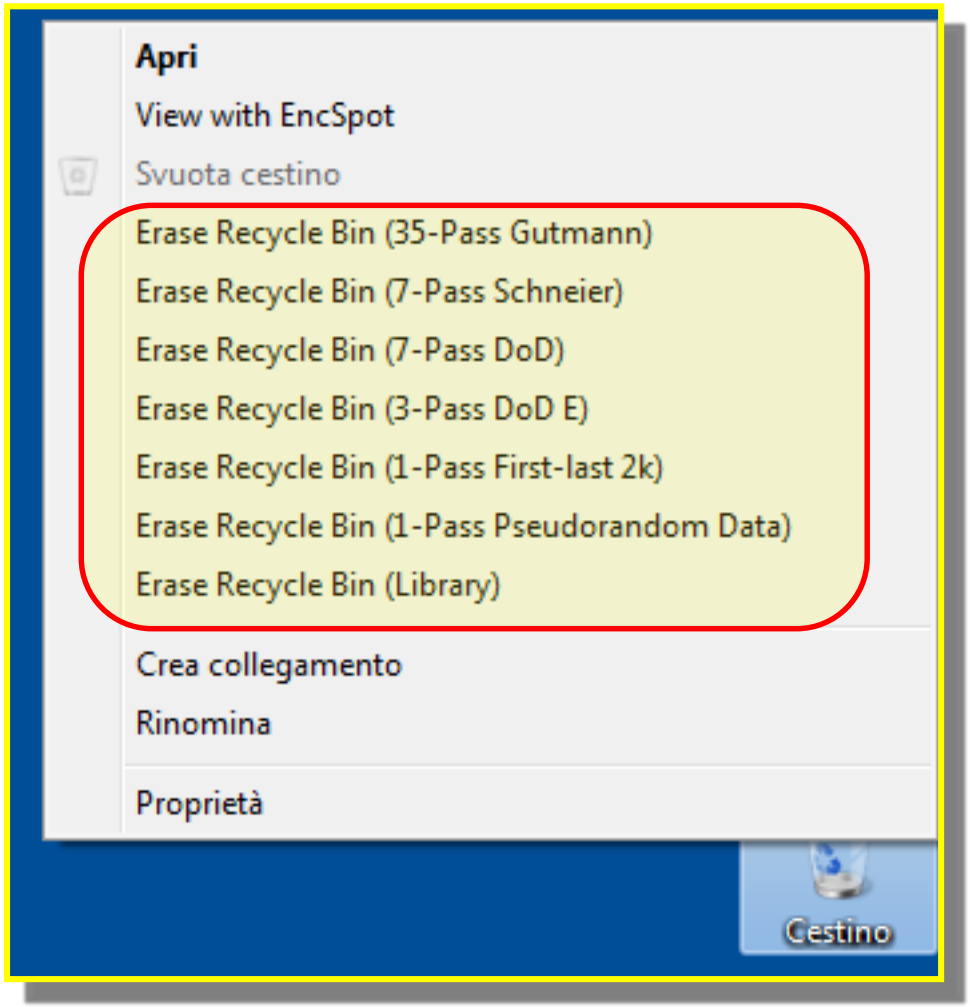
Il numero di ripetizioni del procedimento considerato sufficiente … varia da **sette** a **trentacinque** (…)

(…)

ERASER (free)

ERASER

https://eraser.heidi.ie/



distruzione fisica

trituratore

calore

degausser

DATA LEAKS

Dati (e metadati) possono *uscire* dal PC nei modi più impensati e continuamente in evoluzione:

Dagli altoparlanti
Dal monitor
Con le vibrazioni dell'HD
Dalla presa di corrente
Per colpa dell'utonto *(compresi agenti governativi)*

contromisure

spegnere gli altoparlanti
coprire la telecamera
disattivare il microfono
schermare il monitor e il PC (*Tempest*)
UPS (?)

collegare il cervello e informarsi

Cifratura totale

Cifratura del disco di sistema, dei dischi dati e di tutti i supporti portatili che si usano
(in sintesi: non trattare mai dati in chiaro)

Possibilità offerta da vari programmi di cifratura:

TrueCrypt, VeraCrypt, Scramdisk, LibreCrypt, DiskCryptor, Ciphershed, LUKS (linux)…

FINE

modulo 4