LA SICUREZZA DEI DATI INFORMATICI

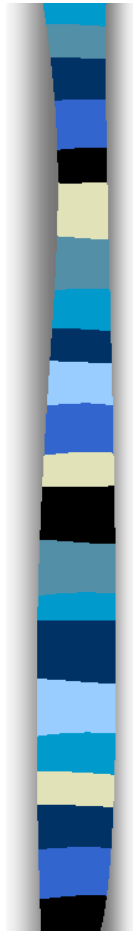
Docente: Marco Fisichella

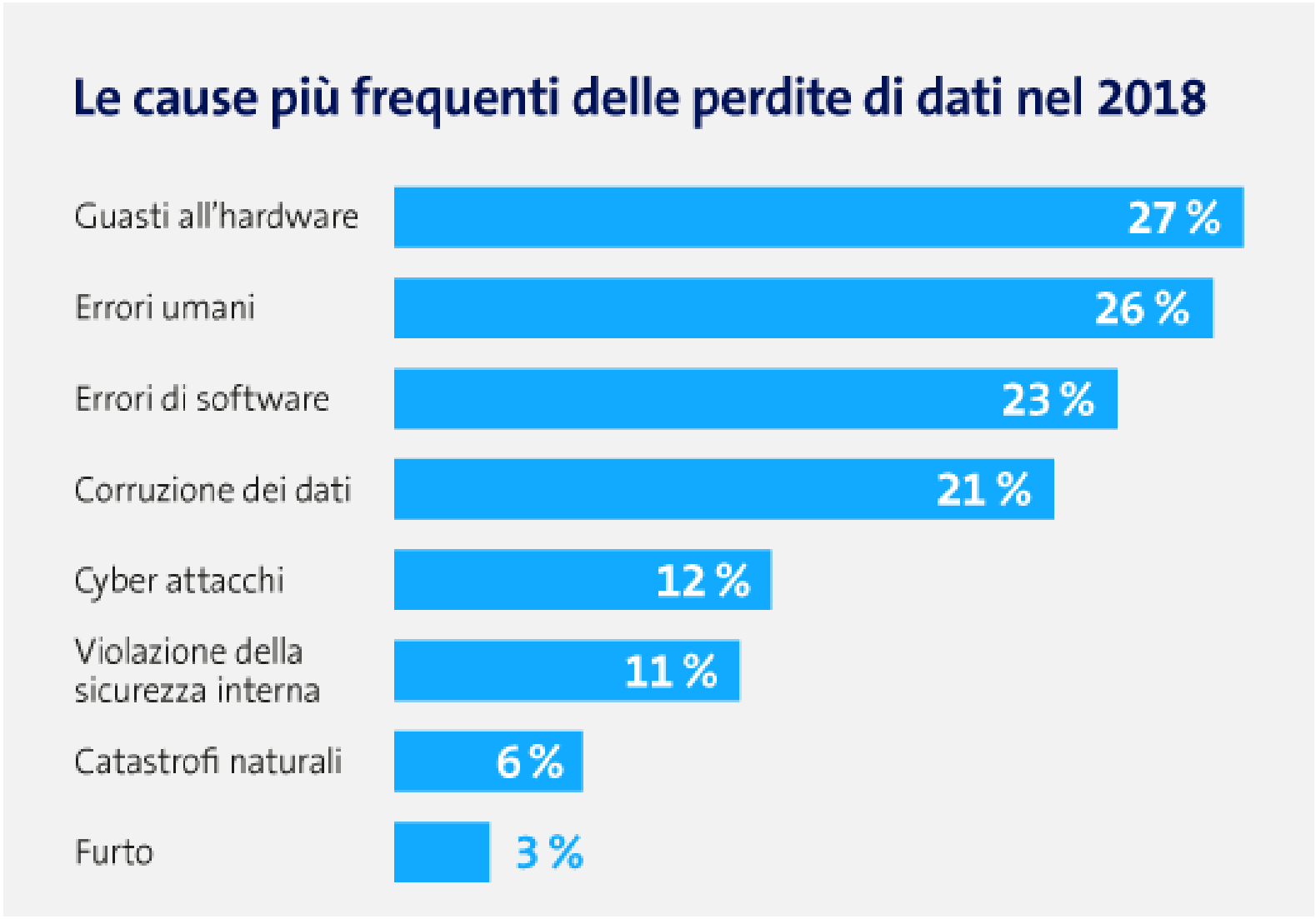
E-mail: marco.fisichella@libero.it

La sicurezza dei dati

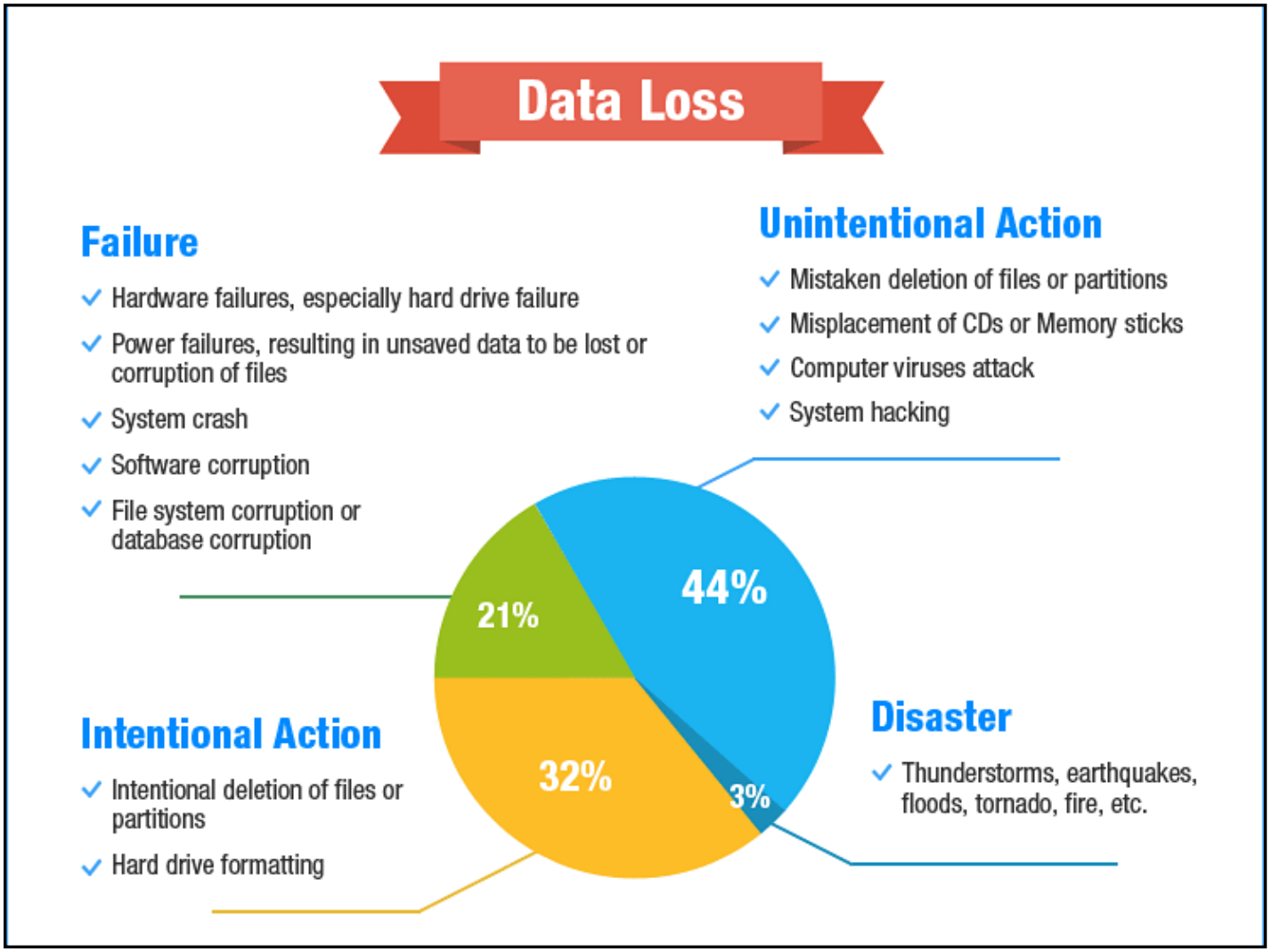
La sicurezza dei dati

La sicurezza dei dati

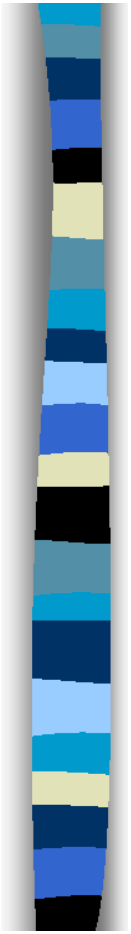


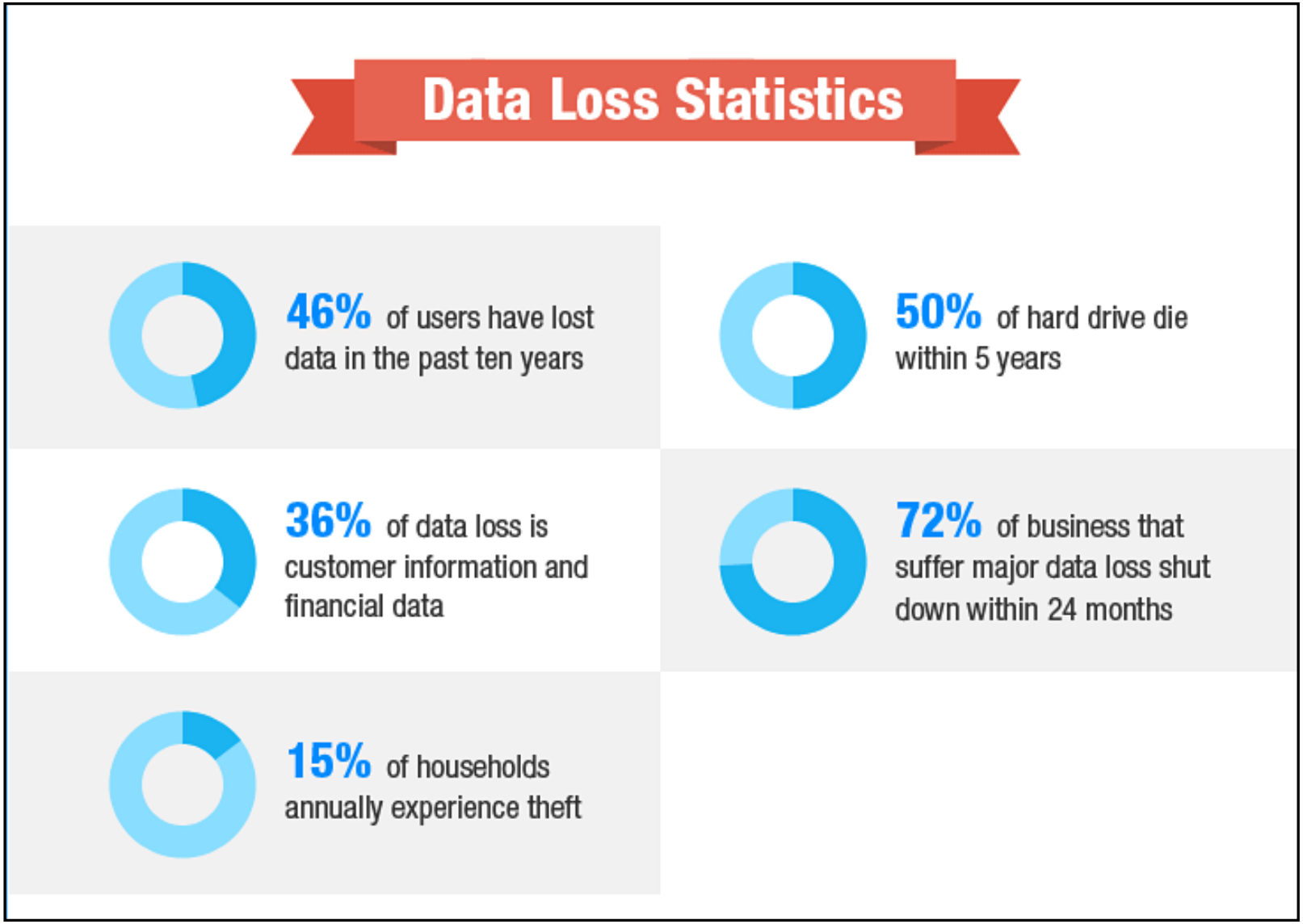


La sicurezza dei dati

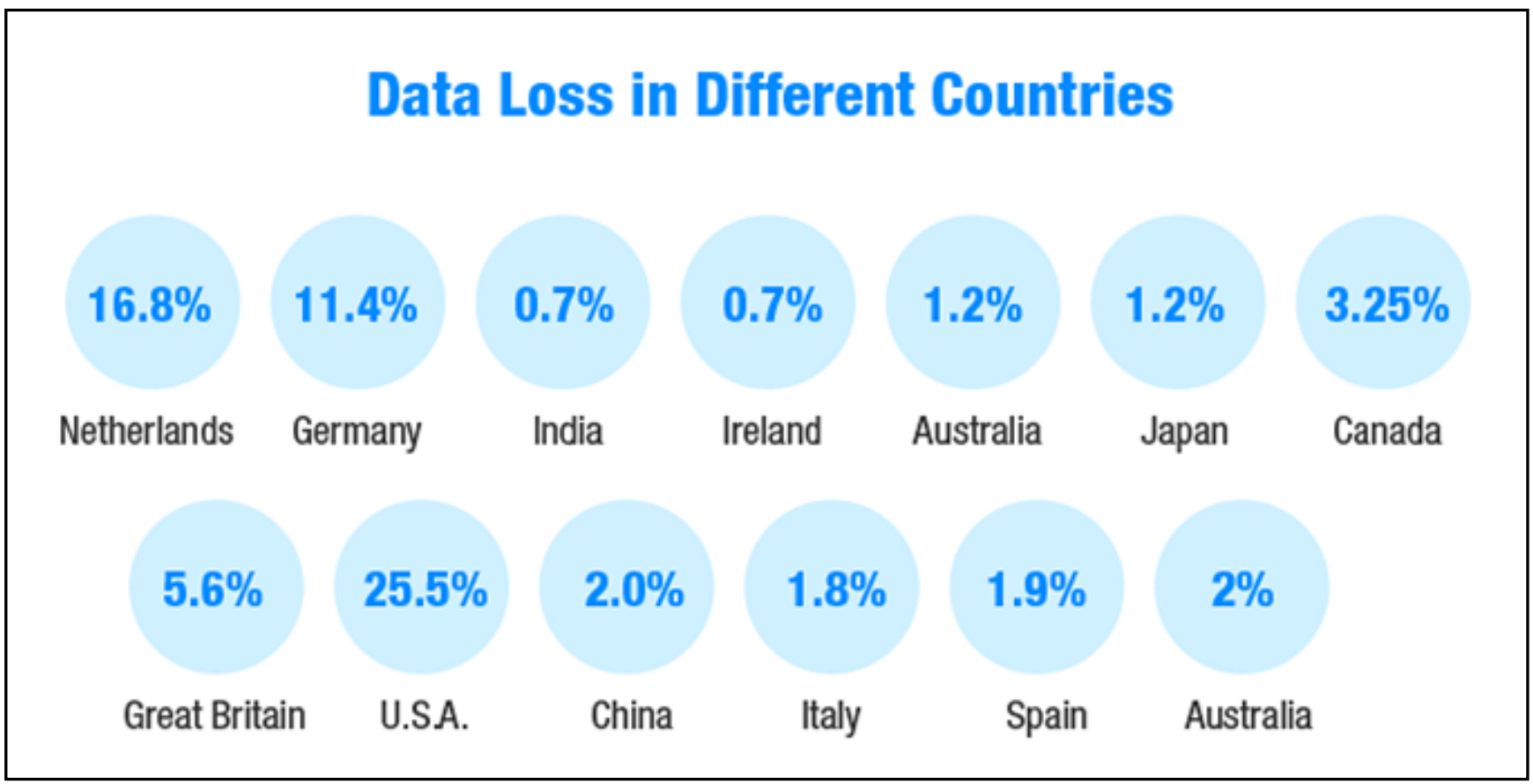


La sicurezza dei dati





La sicurezza dei dati



La sicurezza dei dati

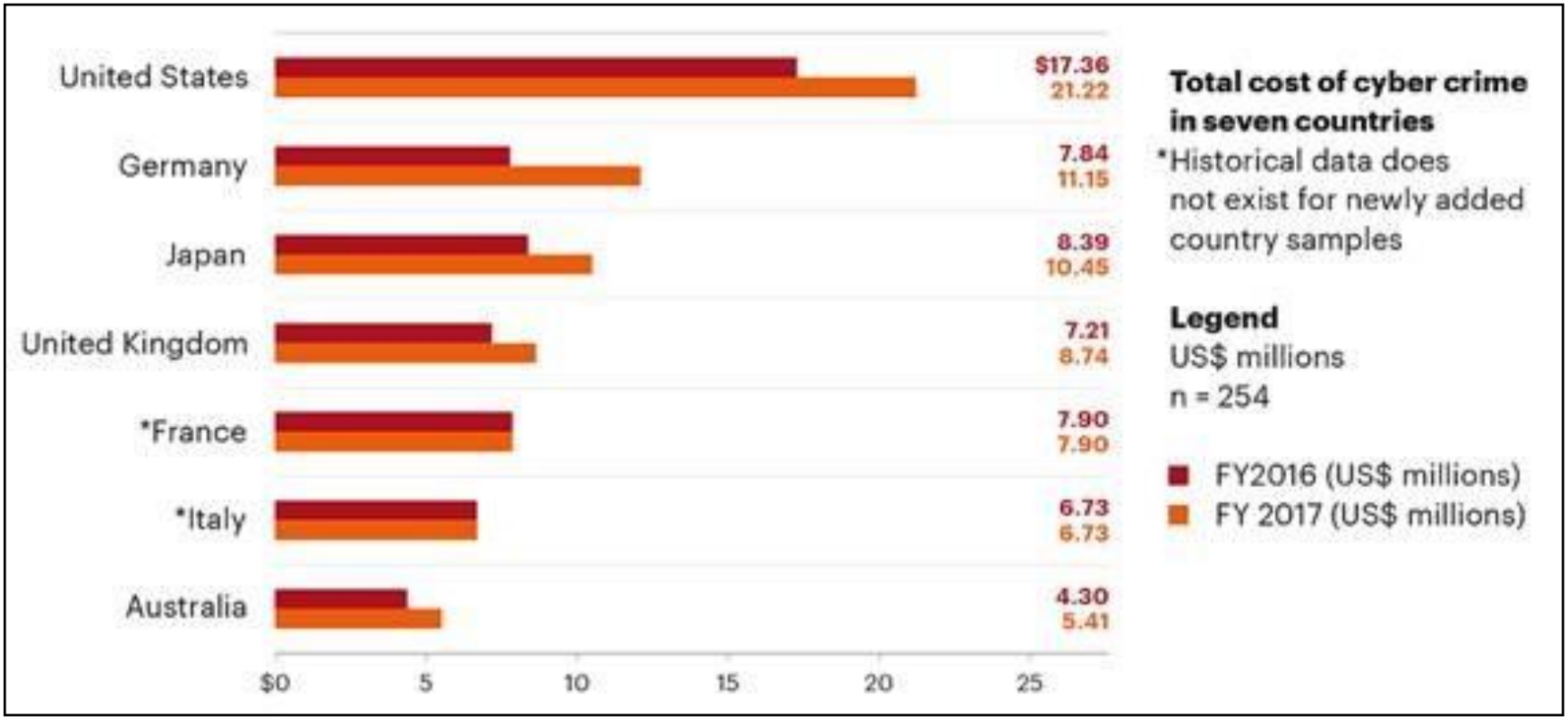
Table 1: Causes and Episodes of Data Loss	
PCs in Use	76.2 million
Causes of Data Loss	**Episodes of Data Loss**
Hardware Failure	1,849,800
Human Error	1,345,300
Software Corruption	588,600
Computer Viruses	294,300
Theft	403,000
Hardware Destruction	126,100
Total	4,607,100

Numero di episodi di perdita dei dati informatici divisi per causa (AA. VV., 2003)

La sicurezza dei dati

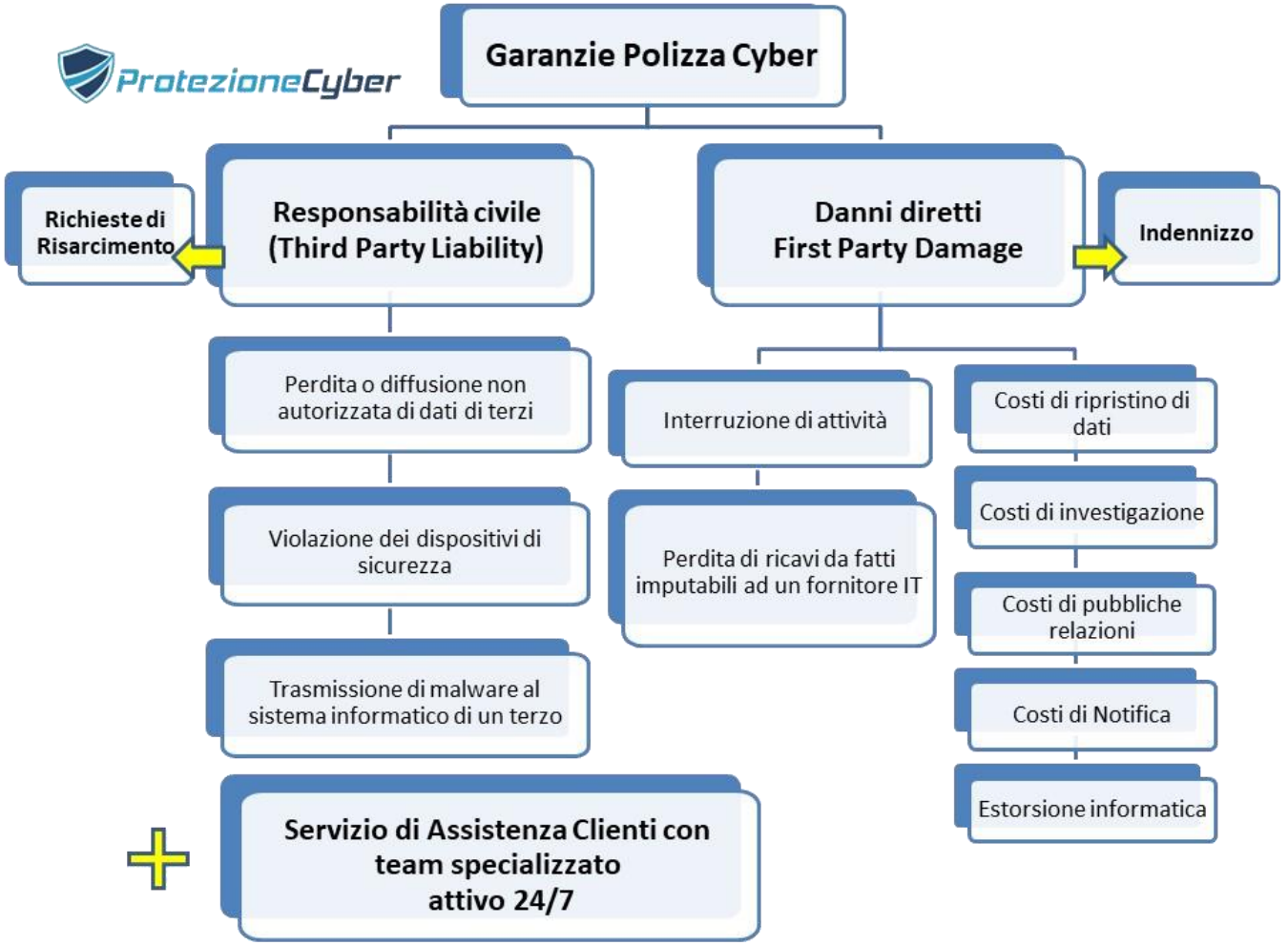
Costo medio di ciascun episodio di perdita di dati informatici (AA. VV., 2003)

La sicurezza dei dati



La sicurezza dei dati

Le polizze assicurative



La sicurezza dei dati

I più comuni incidenti cyber e relativi danni

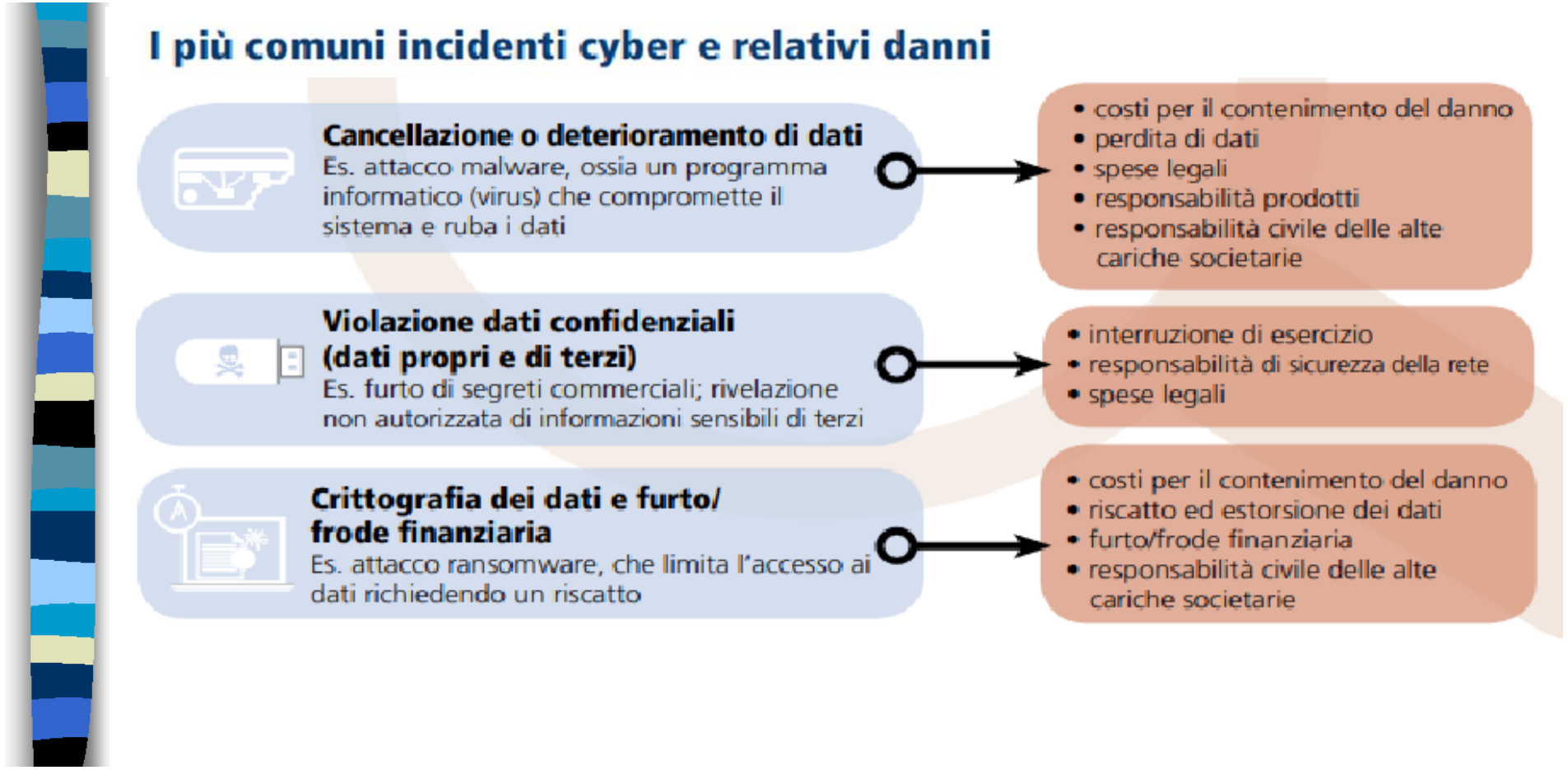
Violazione dati confidenziali (dati propri e di terzi)
Es. furto di segreti commerciali; rivelazione non autorizzata di informazioni sensibili di terzi

- costi per il contenimento del danno
- violazione privacy
- danno reputazionale
- spese legali
- risarcimento danni o multe
- furto di proprietà intellettuale
- responsabilità civile delle alte cariche societarie

Malfunzionamento dei sistemi informatici/rete di comunicazione
Es. manipolazione dei sistemi informatici; attacco al sito web aziendale

- interruzione di esercizio
- risarcimento danni o multe
- danni fisici ai sistemi informatici
- infortunio e morte dei dipendenti
- costi per il contenimento del danno
- danno reputazionale
- responsabilità civile delle alte cariche societarie

La sicurezza dei dati

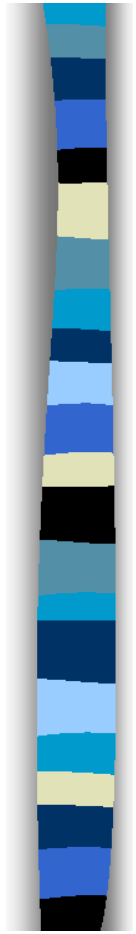


La sicurezza dei dati

Cause di perdita dei dati

- Danni ai supporti che li memorizzano (per smagnetizzazioni, sovratensioni, …)
- Cancellazioni erronee
- Sabotaggio da parte di malintenzionati (hacker, o pirati informatici)
- Virus

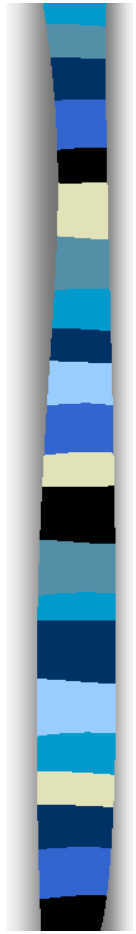
La sicurezza dei dati



Alcuni dati a livello nazionale

- Il 40% delle aziende medie/piccole non fa backup.
- Il 60% dei dati e’ tenuto sui laptop o sui desktop.
- Il 40-50% di tutti i backup non permettono un restore completo e il 60% dei backup fallisce in generale.

La sicurezza dei dati



Alcuni dati a livello nazionale

- Ci vogliono 19 giorni e 17000€ per riscrivere 20 MB di dati di vendita.
- Lo stesso volume di dati costa 19000€ e ci si impiega 21 giorni se i dati sono di contabilità
- Ricreare i dati da zero costa dai 2000€ agli 8000€ per MB.
- Assicurare i dati costa molto e non tutte le compagnie assicurative lo fanno.
- Il 60% delle aziende che hanno perso i loro dati completamente chiudono dopo 6 mesi.
- Il 72% delle aziende che perde i dati sparisce dopo 24 mesi.

La sicurezza dei dati

Alcuni dati a livello nazionale

- 3 persone su 5 perdono files di cui pensano di aver fatto il backup.
- L'82% mantiene una copia cartacea anche se ha una procedura di backup.
- Il 37% ha dichiarato che esegue il backup al massimo una volta al mese.
- Il 9% non esegue mai un backup.
- IL 22% dice di aver preparato un piano di backup ma e' ancora sulla "to do list".

La sicurezza dei dati

Alcuni dati a livello nazionale

- 3 persone su 5 perdono files di cui pensano di aver fatto il backup.
- L'82% mantiene una copia cartacea anche se ha una procedura di backup.
- Il 37% ha dichiarato che esegue il backup al massimo una volta al mese.
- Il 9% non esegue mai un backup.
- IL 22% dice di aver preparato un piano di backup ma e' ancora sulla "to do list".

La sicurezza dei dati

Il General Data Protection Regulation (GDPR) dell'Unione Europea del 2018 impone alle aziende di garantire la sicurezza dei dati personali (sensibili) memorizzati su supporto informatico.

La sicurezza dei dati

Questo obbligo impone alle aziende di dotarsi di:

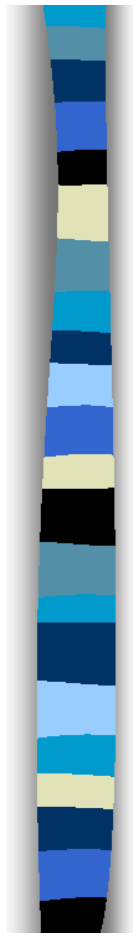
- antivirus a pagamento,
- NAS per backup dati,
- firewall di protezione reti,
- backup protetto su ogni pc,
- autenticazione protetta su ogni computer.

La sicurezza dei dati

Il backup può essere fatto con qualsiasi dispositivo ma perché sia efficiente deve avere queste caratteristiche:

- I file da salvare devono essere copiati nel backup in maniera automatica (senza l'intervento dell'utente) altrimenti quando dovremo recuperare un file ci accorgeremo che ci eravamo dimenticati di salvarlo…
- Ci devono essere più copie degli stessi dati (una al giorno, ogni 2 giorni, una alla settimana).
- Le copie devono essere mantenute per un certo periodo (retention) in modo da poter recuperare da copie vecchie qualora le ultime fossero danneggiate o mi accorgessi della perdita dati dopo un po' di tempo.

La sicurezza dei dati



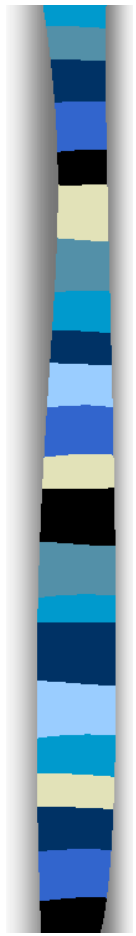
- Le copie devono essere su supporti multipli (non importa di che tipo cassette DVD, Hd, ecc…) questo perché fare più copie sullo stesso supporto renderebbe vano il tutto se il supporto si guasta.
- I supporti non in uso non devono essere accessibili dalla rete o in generale dai pc (questo per evitare che un virus, ad esempio cryptolocker, infetti anche le copie).
- Periodicamente almeno un backup va portato fuori dalla sede aziendale in modo da averlo in caso di disastro grave (questo si può ottenere portandosi a casa o mettendo in banca un supporto del backup ogni tanto o con un servizio di backup remoto).

La sicurezza dei dati

La regola del Backup 3-2-1

La regola prevede **3** copie diverse, **2** differenti tecnologie (NAS, hard disk esterni, memorie flash, tape, DVD , cloud) e 1 copia almeno conservata lontano dall'edificio aziendale o domestico.

La sicurezza dei dati



Backup 3 2 1: perché è efficace?

Avere **3 copie** di backup minimizza statisticamente il rischio di perdita di dati. Immaginate di salvare i dati originali sul disco 1 e il backup sul disco 2. Se la probabilità di malfunzionamento del disco 1 e del disco 2 è di 1/100, la probabilità di un malfunzionamento simultaneo è 1/100 X 1/100 = 1/10000. Con tre differenti copie di backup, la probabilità decresce a una su un milione.

Utilizzare **2 differenti tecnologie** - ad esempio dispositivi diversi – riduce ulteriormente le probabilità di perdita. Accade spesso infatti che due dispositivi della stessa serie abbiano una durata simile (due lampadine che si bruciano nello stesso momento).

Mantenere **1 copia** di backup in un luogo differente è in ogni caso consigliato. Qualora si verificassero problemi di inondazione o fuoco, furto o altri disastri, non tutti i backup saranno persi.

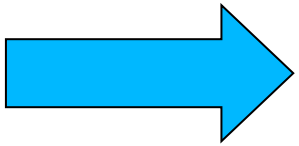
La sicurezza dei dati

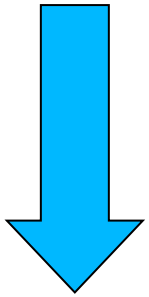
Il back up dei dati

- Copie di sicurezza effettuate su supporti rimovibili.
- Deve essere effettuato periodicamente.
- I supporti devono essere tenuti al sicuro da agenti dannosi (polvere, calore, …), furti (possibilmente in cassaforte) e intrusioni (tramite password d'accesso)
- Il Decreto Legislativo n. 196 del 2003 ha stabilito che è obbligatorio per le aziende fare il back up dei dati.

La sicurezza dei dati

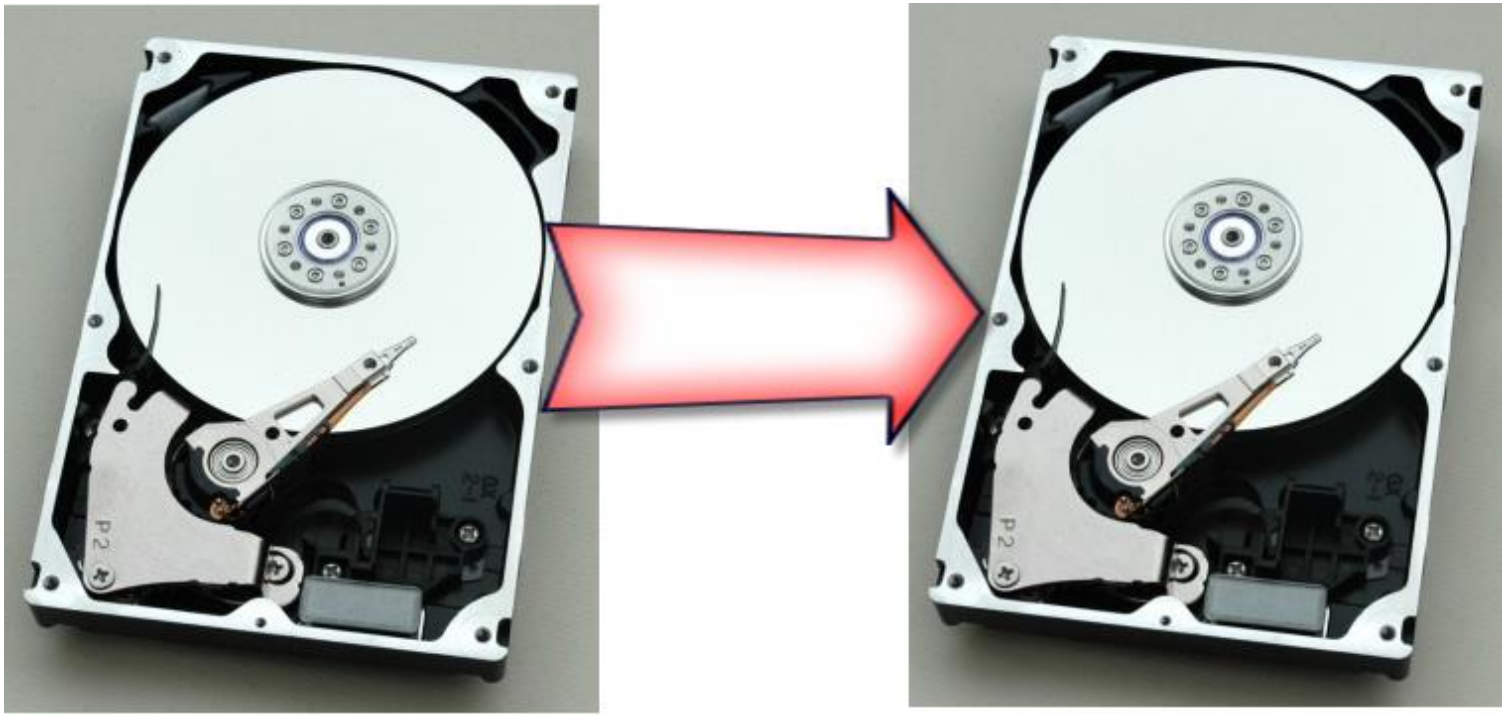
Storage di sicurezza





La sicurezza dei dati

Backup su disco rigido



La sicurezza dei dati

Backup su supporti removibili

La sicurezza dei dati

Backup su disco rigido

Vantaggi

- Poco costoso
- Veloce implementazione
- Compatibilità
- Facilità di restore

Svantaggi

- Non removibile
- Capacità limitata dal disco
- Limitata compatibilità con SW di backup

La sicurezza dei dati

Backup su supporti removibili

Vantaggi

- Capacità illimitata.
- Supporti diversi: tape, USB Keys, DVD.
- Restore possibile su altre macchine.

Svantaggi

- Dipende molto dal SW installato.
- Restore a volte difficoltoso.

La sicurezza dei dati

Nastro
(stream catridge)

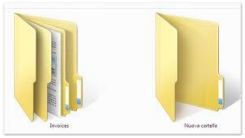
CD o DVD

HDD esterni

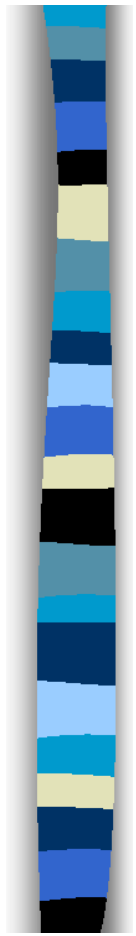
Grande capacità (2TB) **Economico** **Riutilizzo infinito**	**Economico** **Accesso rapido**	**Grande capacità: 10TB** **Rapido accesso**
Lento **Accesso sequenziale**	**Capienza limitata**	**Molto costosi**

La sicurezza dei dati

Cosa deve fare un software di backup?

- Copia di singoli file – cartelle. 
- Copia di un'immagine disco completa. 
- Recupero di file singoli scelti. 
- Backup con compressione. 
- Protezione dati con password e crittografia. 

La sicurezza dei dati



Tipi di back up

Differenziale. = solo dei file modificati

Completo. = di tutti i file

Incrementale. = il primo completo + tutte le modifiche successive.

La sicurezza dei dati

Quando fare i back up

- I backup vanno programmati e fatti ad intervalli di tempo determinati.
- Non devono interferire col normale lavoro per cui è preferibile farli di notte.
- Il piano di backup è la programmazione di quando e come debbano avvenire.

La sicurezza dei dati

I firewall

- Sistemi software, o hardware e software, in grado di controllare le trasmissioni tra una rete aziendale e le reti esterne (o Internet).
- Usati per proteggere computer e reti da accessi non autorizzati da parte di malintenzionati.

La sicurezza dei dati

Gli accessi sicuri

- L'accesso esclusivo ai dati e alle risorse di un sistema informatico è possibile mediante procedure di autenticazione, quali:
  - Codice PIN,
  - Smart card,
  - Biometria (impronte digitali, iride, riconoscimento vocale)
  - Password.

La sicurezza dei dati

I virus

- Frammenti di codice estraneo ai programmi, capace di replicarsi e di infettare altri programmi
- Scritti da programmatori malintenzionati o “in vena di scherzi”
- Spesso contengono istruzioni dannose

La sicurezza dei dati

Danni arrecati dai virus

- Cancellazione di file.
- Danneggiamento di programmi, compreso il sistema operativo.
- Formattazione del disco rigido.
- Effetti grafici indesiderati.
- Rallentamento dell’elaborazione.

La sicurezza dei dati

Gli antivirus

- Programmi in grado di riconoscere ed eliminare un virus (disinfettare).
- Possono essere utilizzati in fase di prevenzione, per evitare l'infezione.
- Devono essere continuamente aggiornati per essere efficaci contro i nuovi virus.

La sicurezza dei dati

I malware

- Virus: infezione di un programma, che infetta gli altri con una copia sullo stesso PC.
- Worm (verme): si duplica attraverso internet.
- Cavallo di troia: software mascherato come “dono” che si annida in programmi apparentemente utili.
- Dialer: deviazione della linea telefonica su di un numero a pagamento (sta scomparendo!)
- Rootkit: un programma nocivo che si nasconde con varie tecniche: è senza protezione nei normali antivirus.
- Spyware: è un tipo di software che raccoglie informazioni riguardanti l'attività online di un utente (siti visitati, acquisti eseguiti in rete etc).
- Keylogger: legge i dati inseriti tramite la tastiera.

La sicurezza dei dati

I malware

Virus

- Sono brevi parti di codice, o frammenti di esso che si diffondono copiandosi all'interno di altri programmi o in alcune sezioni particolari del disco fisso, in modo che essi vengano eseguiti ogni qual volta il file infetto venga lanciato o semplicemente eseguito.
- La loro trasmissione avviene tra differenti Pc, ogni qual volta un file infetto venga spostato su un'altra macchina.
- È una tipologia di malware estremamente dannosa, esistono virus che molto spesso costringono l'utente all'eliminazione totale dei dati presenti sul disco.

La sicurezza dei dati

I malware

Worm

- Al contrario dei virus essi non necessitano dell'apertura del file infettato per diffondersi essi modificano il sistema operativo del PC ospite in modo da essere eseguiti automaticamente e tentare di replicarsi e diffondersi usando come canale privilegiato quello di internet.
- Per indurre gli utenti ad eseguirli usano tecniche di Social Engineering, o sfruttano alcuni difetti (i cosiddetti Bug) di alcuni programmi o di alcuni sistemi operativi non aggiornati o sprovvisti di adeguati aggiornamenti.

La sicurezza dei dati

I malware

Trojan Horse

- Sono software che oltre ad avere delle funzionalità “lecite” e non illegali, utilissime per fare in modo che vengano impiegati o avviati dall’utente, contengono anche istruzioni dannose che vengono eseguite in maniera automatica e all’insaputa dell’utente.
- Non possiedono funzioni di auto-replicazione.

La sicurezza dei dati

I malware

Backdoor:

- Il termine significa letteralmente “porta sul retro”.
- Sono software che consentono un accesso illegittimo e non autorizzato al sistema su cui sono in esecuzione.
- Tipicamente si diffondono in abbinamento a trojan o worms.

La sicurezza dei dati

I malware

Spyware

- Sono software che vengono utilizzati per trasmettere informazioni sul sistema al destinatario interessato.
- Le informazioni possono spaziare dalle attitudini di navigazione dell'utente a password o chiavi crittografiche memorizzate sui Pc.
- Lo spyware registra informazioni presenti sul PC infettato e le invia a terze parti.

La sicurezza dei dati

I malware

Dialer

- Questi programmi si occupano di dirottare la connessione ad internet tramite la normale linea telefonica, quindi attraverso i classici modem da 33/56k.
- Sono malware che hanno lo scopo di redirigere la connessione predefinita verso un numero a tariffazione speciale allo scopo di trarne illecito beneficio a spese delle utenze.

La sicurezza dei dati

I malware

Hijackers

- Come suggerisce il nome si occupano di dirottare la connessione verso pagine web indesiderate.
- Molto spesso si tratta di pagine ad alto contenuto illecito, pubblicitario o pornografico.

Adware

- Molti applicazioni non lecite installano sul pc contenuti pubblicitari non desiderati che appaiono generalmente all'avvio del browser o sul desktop sotto forma di finestre pop-up.

La sicurezza dei dati

I malware

Rootkit

- In genere sono composti da driver o copie modificate di normali programmi inseriti nel sistema.
- Non sono dannosi in sé ma hanno la funzione di nascondere sia all'utente che a programmi tipo antivirus la presenza di particolar file o impostazioni del sistema.
- Possono essere utilizzati per nascondere o mascherare altro software dannoso.

Rabbit

- Sono programmi che esauriscono le risorse del sistema moltiplicandosi ad altissima velocità, possono occupare grandi quantità di memoria sia RAM che fissa in tempi relativamente molto brevi.

La sicurezza dei dati

I malware

Scareware

- Sono così chiamati quei programmi che ingannano l'utente facendogli credere di avere il proprio PC infetto.
- Lo scopo è di convincere l'utente ad installare dei particolari malware, chiamati in gergo rogue antivirus, caratterizzati dal fatto di spacciarsi per degli antivirus veri e propri, talvolta spacciati anche a pagamento.

Adware

- Programmi software che presentano all'utente messaggi pubblicitari durante l'uso, a fronte di un prezzo ridotto o nullo.
- Possono causare danni quali rallentamenti del PC e rischi per la privacy in quanto comunicano le abitudini di navigazione ad un server remoto.

La sicurezza dei dati

I malware

Keylogger

- I Keylogger sono dei programmi in grado di registrare tutto ciò che un utente digita su una tastiera o che copia e incolla rendendo così possibile il furto di password o di dati che potrebbero interessare qualcun altro.
- La differenza con gli Adware sta nel fatto che il computer non si accorge della presenza del keylogger e il programma non causa rallentamento del pc, passando così totalmente inosservato.
- Generalmente i keylogger vengono installati sul computer dai trojan o dai worm.

La sicurezza dei dati

I malware

Batch

- I Batch sono i cosiddetti "virus amatoriali".
- Non sono sempre dei file pericolosi in quanto esistono molti file batch tutt'altro che dannosi, il problema arriva quando un utente decide di crearne uno che esegua il comando di formattare il pc (o altre cose dannose) dell'utente a cui viene mandato il file.
- Non si apre automaticamente, deve essere l'utente ad aprirlo, perciò dato che l'antivirus non rileva i file Batch come pericolosi è sempre utile assicurarsi che la fonte che vi ha mandato il file sia attendibile oppure aprirlo con blocco note per verificare o meno la sua pericolosità.

La sicurezza dei dati

La sicurezza dei dati

I ransomware

Con la parola ransomware viene indicata una classe di malware che rende inaccessibili i dati dei computer infettati e chiede il pagamento di un riscatto, in inglese ransom, per ripristinarli.
Tecnicamente sono Trojan horse crittografici ed hanno come unico scopo l'estorsione di denaro, attraverso un "sequestro di file", attraverso la cifratura che, in pratica, rende il pc inutilizzabile.

La sicurezza dei dati

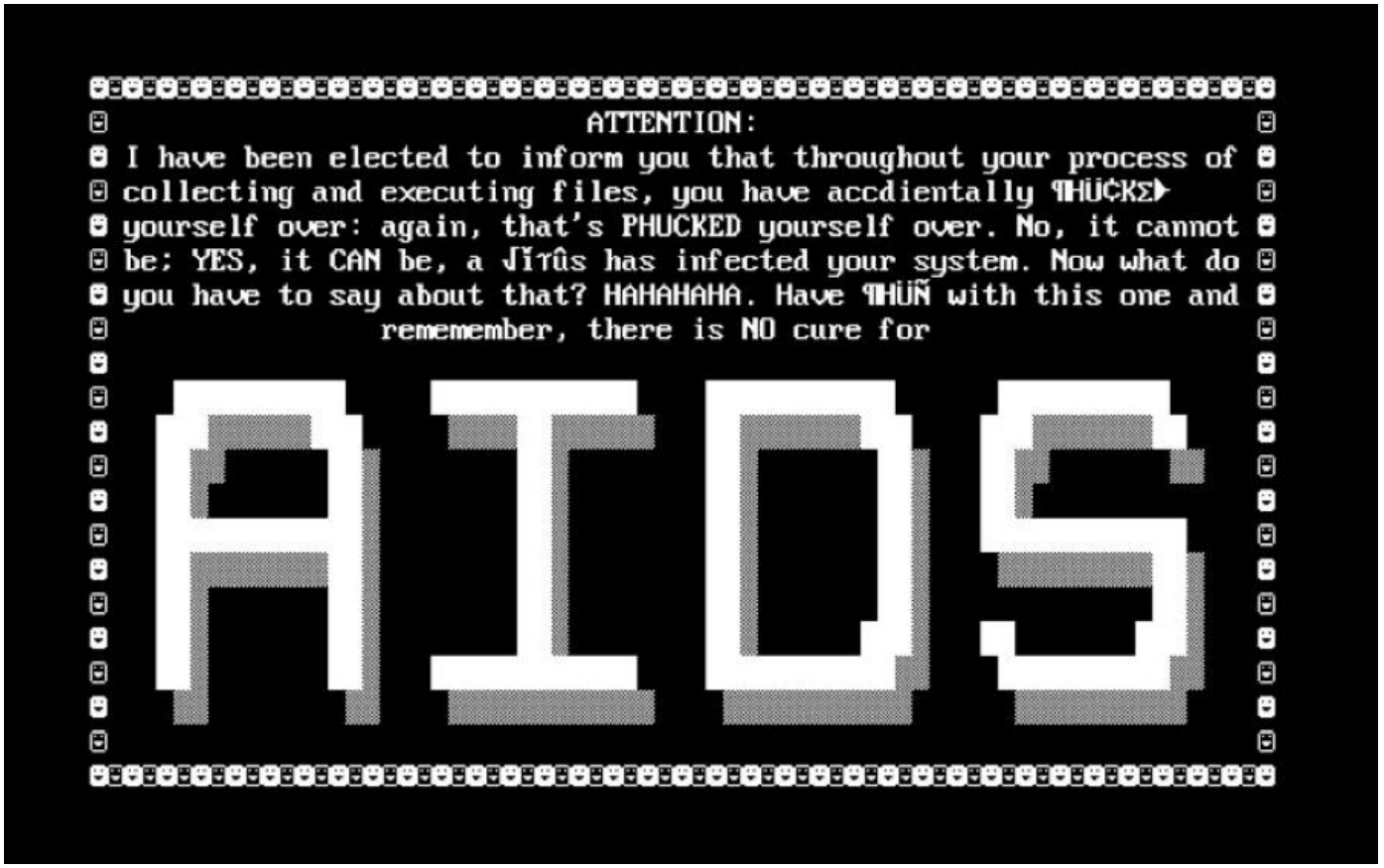
I ransomware

Al posto del classico sfondo vedremo comparire un avviso che sembra provenire dalla polizia o da un'altra organizzazione di sicurezza e propone un'offerta.
In cambio di una password in grado di sbloccare tutti i contenuti, intima di versare una somma di denaro abbastanza elevata (comunque quasi sempre sotto i 1.000 euro): in genere la moneta usata è il bitcoin, la valuta elettronica.

La sicurezza dei dati

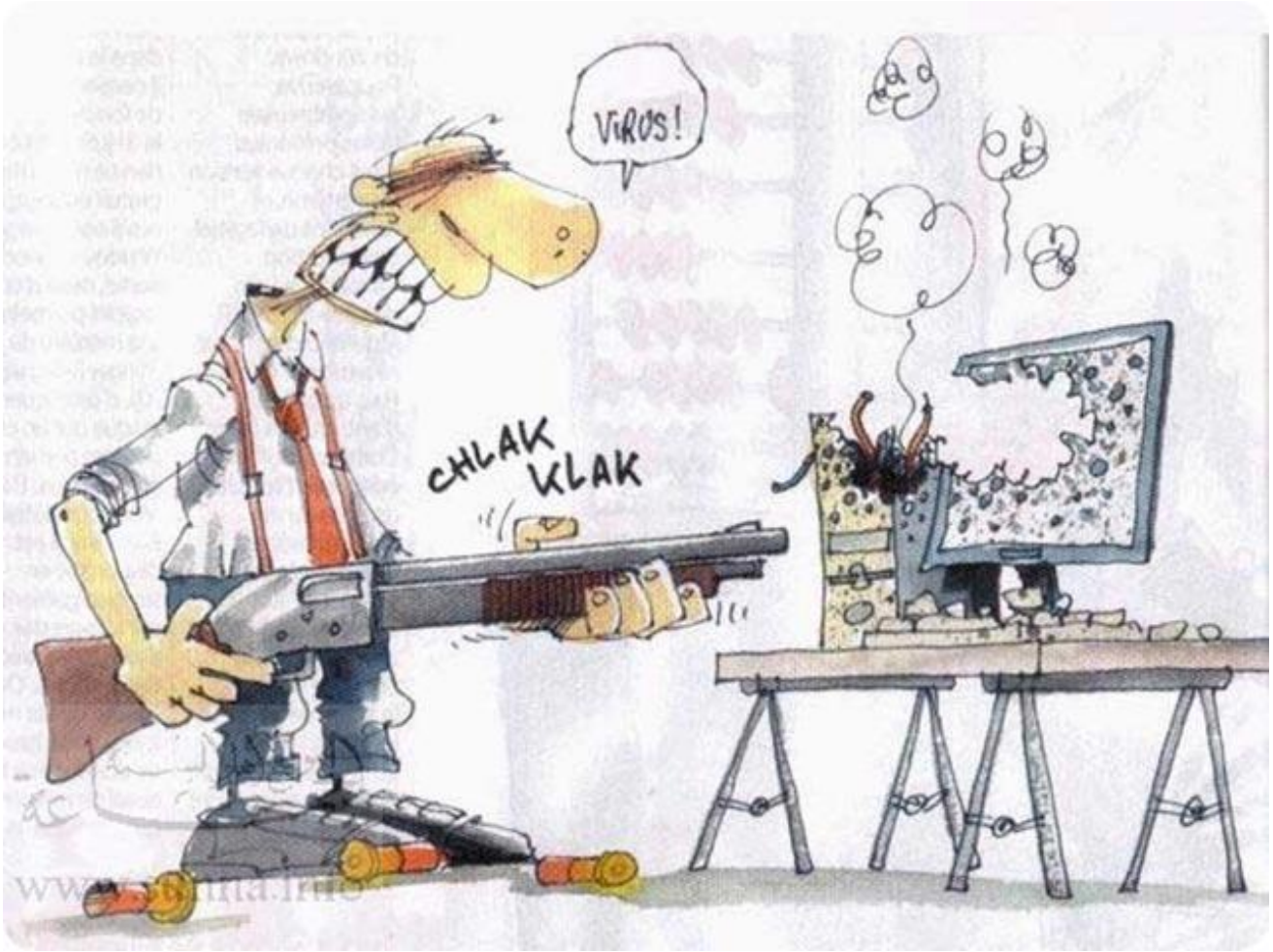
I ransomware

Il primo ransomware della storia: PC Cyborg (1989)



La sicurezza dei dati

Gli antivirus

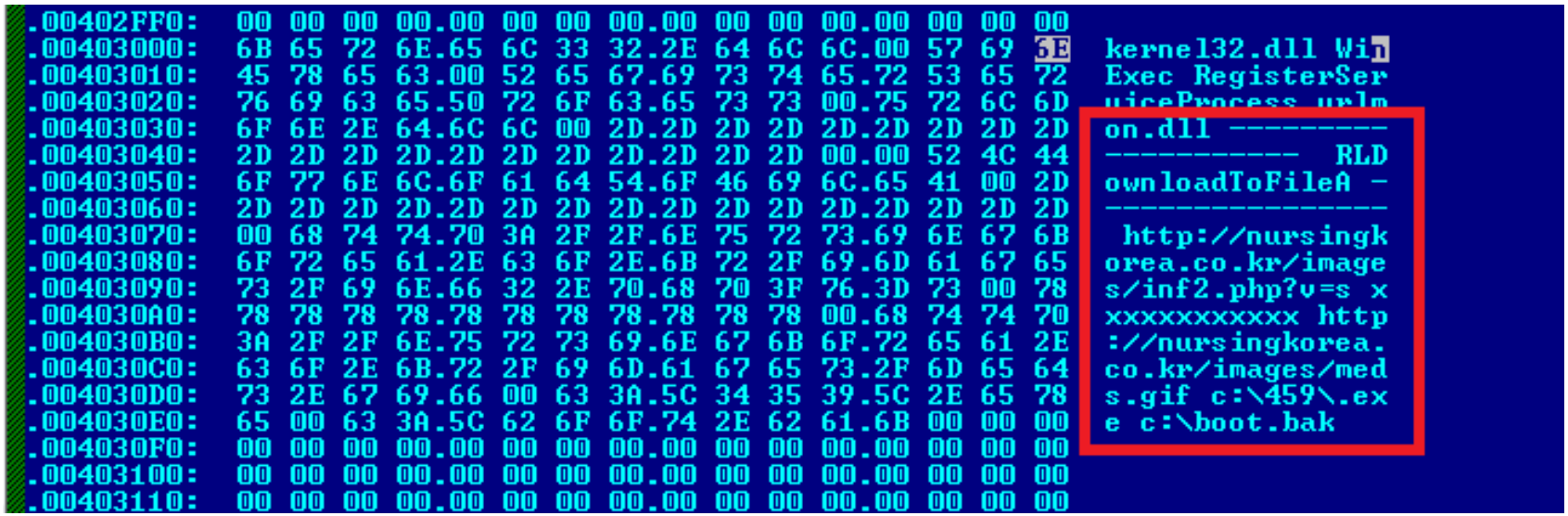


La sicurezza dei dati

Gli antivirus

La sicurezza dei dati

Gli antivirus



La sicurezza dei dati

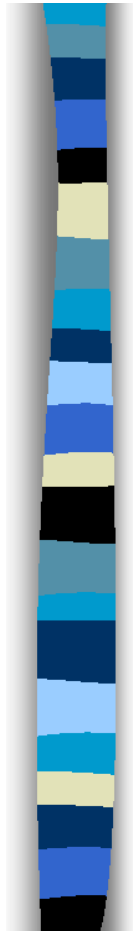
Gli antivirus

Scanner euristici

- Gli scanner euristici individuano i virus con la ricerca di specifici comportamenti nei possibili oggetti infetti.
- Sono di tipo non-identifying e non-preventing.
- La scansione euristica consiste nell'analisi di sequenze di istruzioni di codice: infatti, indipendentemente da tutte le istruzioni accessorie, un virus per replicarsi deve necessariamente compiere un certo tipo di operazioni.

La sicurezza dei dati

I ransomware



Alcuni dei ransomware più famosi:

- Cryptolocker: 2013
- CTB-Locker: metà 2014. Ha migliaia di varianti.
- TorrentLocker: febbraio 2014 (Turkcell).
- Ransom32: fine dicembre 2015.
- Locky: febbraio 2016 (via macro in file Word).
- CryptXXX: inizio 2016 (attraverso pagine Web compromesse)
- Petya: marzo 2016.
- Cerber: marzo 2016.
- PokemonGo: agosto 2016. Nella richiesta di riscatto si presentava con l'immagine di Pokemon, allora molto di moda.
- WannaCry (maggio 2017): il più veloce a propagarsi, grazie ad una vulnerabilità di Windows.
- NotPetya (giugno 2017): probabilmente quello che ha creato i danni maggiori a livello mondiale.
- Bad Rabbit (ottobre 2017)

La sicurezza dei dati

Spoofing

- Atto di introdursi in un sistema informativo senza averne l'autorizzazione.
- L'intruso cambia il proprio numero IP non valido per l'accesso al sistema, in uno autorizzato.

Sniffing

- È l'attività di intercettazione passiva dei dati che transitano in una rete telematica. Tale attività può essere svolta sia per scopi legittimi (ad esempio l'individuazione di problemi di comunicazione o di tentativi di intrusione) sia per scopi illeciti (intercettazione fraudolenta di password o altre informazioni sensibili).
- I prodotti software utilizzati per eseguire queste attività vengono detti sniffer ed oltre ad intercettare e memorizzare il traffico offrono funzionalità di analisi del traffico stesso

La sicurezza dei dati

Phising

- Attività illegale utilizzata per ottenere l'accesso a informazioni personali o riservate con la finalità del furto di identità mediante l'utilizzo delle comunicazioni elettroniche, soprattutto messaggi di posta elettronica fasulli o messaggi istantanei, ma anche contatti telefonici.
- Grazie a questi messaggi, l'utente è ingannato e portato a rivelare dati personali, come numero di conto corrente, numero di carta di credito, codici di identificazione, ecc.