Fondamenti di Informatica

CAP. 7

Accademia di belle Arti di Verona

Università degli Studi di Verona

A.A. 2022-2023

Docente - Vincenzo Giannotti

CAPITOLO 7 – SICUREZZA INFORMATICA

Sicurezza delle informazioni

Il problema di «**come trasmettere informazioni in maniera sicura**» è antico quanto l'Uomo, o almeno, quanto l'Uomo da quando è in grado di comunicare.

Un tempo la «riservatezza» delle informazioni riguardava prettamente il settore militare. Per garantire la riservatezza delle comunicazioni ci si affidava alla «**crittografia**», cioè alla scienza che si occupa di come codificare un messaggio e di come successivamente decodificarlo.

Svetonio, nel suo «la Vita dei Cesari» (intorno all'anno 120 d.C.), racconta che Giulio Cesare, per la sua corrispondenza riservata, utilizzava un suo proprio codice di cifratura molto semplice: ciascuna lettera dell'alfabeto veniva sostituita con un'altra che la seguiva di qualche posizione. In pratica era come se venisse utilizzato un alfabeto che anziché da A -> Z andava, per esempio, da D -> C.

Sicurezza delle informazioni

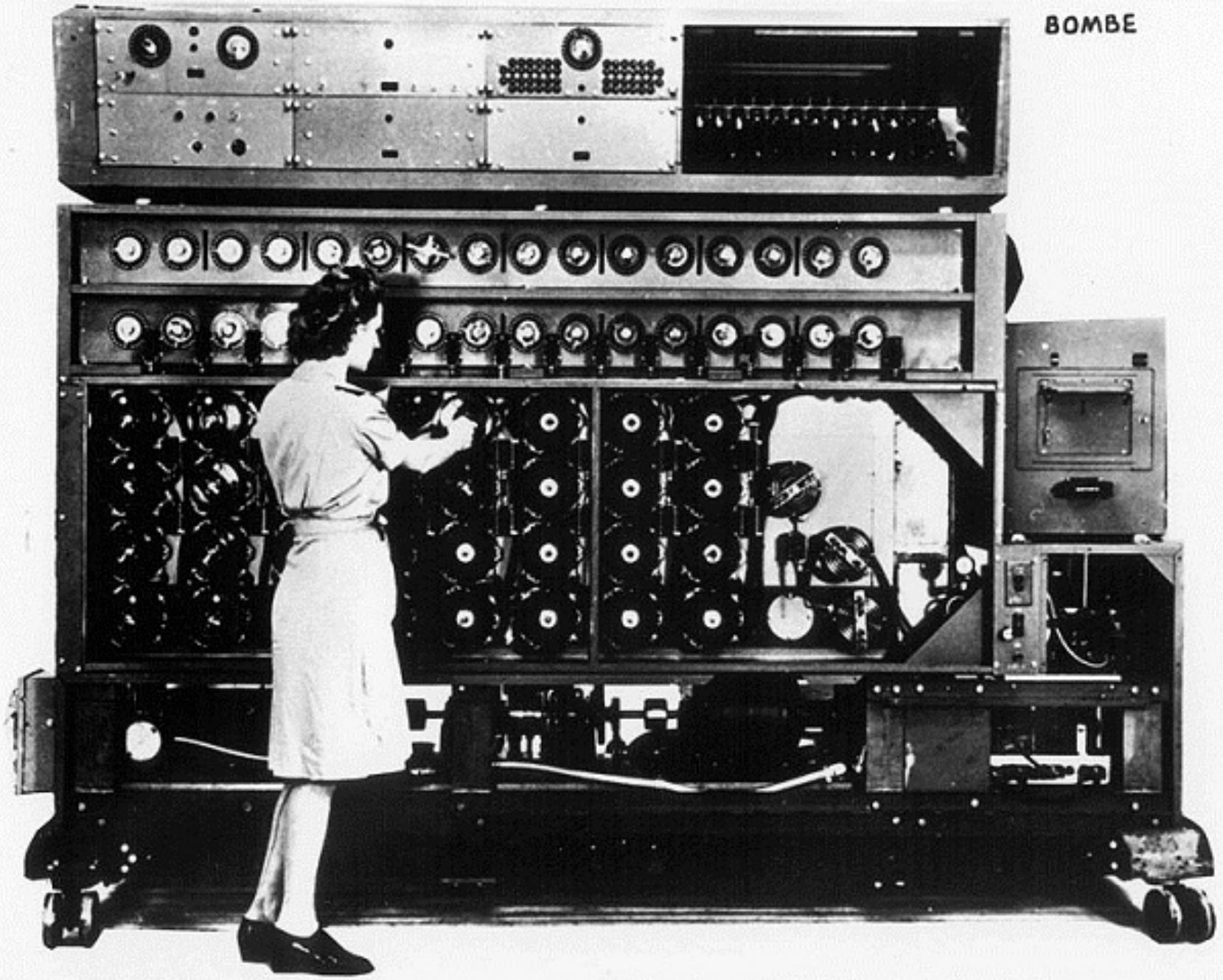
Altri metodi utilizzati nell'antichità utilizzavano le cifre di sostituzione, in cui si sostituiva ciascuna lettera con un simbolo, e la steganografia, l'arte di nascondere messaggi all'interno di altri dati come immagini. Gli egizi e i cinesi usavano inchiostri invisibili e papiri con spazi nascosti.

Nel medioevo la Chiesa cattolica utilizzava cifre e codici per proteggere le sue comunicazioni diplomatiche e finanziarie. Ad esempio, il cifrario papale era un codice segreto usato per crittografare le comunicazioni diplomatiche vaticane.

Alcuni importanti risultati di questa scienza si ebbero nel periodo Rinascimentale (i.e. Tritemio – *Polygrafia* – Francoforte 1550; Giovan Battista della Porta – *De furtivis literarum notis* – Napoli 1563 e molti altri) nei quali si studiavano:

- sistemi a trasposizione - inversione/spostamento di elementi del testo
- sistemi a sostituzione – sostituzione di elementi del testo con segni e simboli
- sistemi misti – entrambe le operazioni precedenti eseguite in sequenza
- La steganografia ha progredito con metodi per nascondere messaggi utilizzando inchiostri speciali, nelle immagini, nella musica, nei libri e altro ancora.

Il maggiore impulso tuttavia si ebbe nel secolo scorso, durante la seconda guerra mondiale, con la costruzione di macchine molto sofisticate per la cifratura dei messaggi (Enigma - Germania) e di macchine altrettanto sofisticate per la loro decifratura (la Bomba - UK).



Sicurezza delle informazioni

- La «**Bomba**» fu una macchina ideata da Alan Turing con lo scopo di individuare giornalmente la configurazione con cui veniva impostata la macchina «Enigma» (di cui gli Inglesi possedevano una copia esatta) utilizzata dai Tedeschi nella II Guerra Mondiale per criptare i loro messaggi.

Sicurezza Informatica

Oggi, viviamo nella società dell'informazione, in cui lo scambio delle informazioni (per lo più digitalizzate) fa parte integrante del nostro modo di vivere e di qualsiasi nostra attività.

La sicurezza informatica è diventata uno degli argomenti più importanti del nostro tempo, soprattutto con la crescente digitalizzazione della nostra vita quotidiana. Le nostre informazioni personali, i nostri conti bancari, le nostre comunicazioni e sempre più aspetti cruciali sono gestiti online o archiviati su dispositivi digitali.

È bene precisare che quando parliamo di «Sicurezza Informatica» ci riferiamo a due aspetti principali:

- La **sicurezza delle informazioni**
- La **protezione dei sistemi informativi**

Questo significa che si deve affrontare il tema sia dal punto di vista dei «sistemi *stand alone*» sia dei «sistemi in rete» per proteggere i dati e i sistemi contro perdite, attacchi virali, intrusioni.

Sicurezza delle informazioni

Proprio per il fatto che la sicurezza (security) è diventata una componente così importante dell'informazione stessa, è fondamentale adottare solide pratiche di sicurezza informatica per provare a sventare le minacce e i rischi che la trasformazione digitale ha introdotto.

Non è più sufficiente limitarsi a garantirne la **riservatezza** – anche se la crittografia è ancora molto importante in moltissimi casi – ma è necessario garantire anche altri aspetti, come la **disponibilità** e l'**integrità** dell'informazione.

«Riservatezza», «Disponibilità» e «Integrità» sono dunque i **tre obiettivi** fondamentali di qualsiasi sistema di sicurezza delle informazioni.

Riservatezza

La Riservatezza si ottiene limitando l'accesso alle informazioni e alle risorse informatiche, solamente alle persone e ai sistemi autorizzati a farlo. Alcuni punti chiave della riservatezza sono:

- Le **informazioni sensibili** devono essere identificate e classificate in base alla loro sensibilità. Ad esempio, informazioni riservate, a uso interno, a uso pubblico etc. Questo aiuta a determinare il livello di protezione appropriato.
- L'accesso alle informazioni deve essere controllato utilizzando dei metodi di **autenticazione**. Gli utenti dovrebbero avere solo i **permessi** necessari per svolgere il proprio lavoro.
- Gli obiettivi di riservatezza si possono realizzare sia nella fase di **archiviazione** dell'informazione, sia durante la **comunicazione**.
- La **crittografia** può essere utilizzata per proteggere le informazioni sensibili durante la trasmissione o l'archiviazione.
- La **segmentazione** di reti migliora la riservatezza limitando l'accesso a parti specifiche della rete e dei sistemi. Ad esempio, le reti interne possono essere segmentate in zone di sicurezza.

Riservatezza

- Può capitare che una informazione sensibile sia data dalla somma di più dati messi in relazione tra di loro – per esempio il mio nome e la mia data di nascita in taluni contesti hanno significato solo se abbinati, poiché consentono di riconoscermi univocamente – ne consegue che la riservatezza può dipendere dal **contesto**.
- La **pseudonimizzazione** e l'**anonimizzazione** possono essere utilizzate per proteggere la privacy dei dati personali rimuovendo le informazioni direttamente identificabili.
- In taluni casi può essere necessario adottare **protezioni fisiche** come pareti, porte, divieti di accesso a locali, con lo scopo di evitare l'esposizione alla vista di informazioni sensibili e dei dispositivi che le memorizzano o le elaborano.
- Le politiche, le **procedure**, la **formazione** e la sensibilizzazione aiutano a garantire che gli utenti proteggano le informazioni in linea con i requisiti di riservatezza. Sviluppare una cultura della sicurezza è fondamentale.

Riservatezza

In relazione all'ultimo punto della slide precedente, se è vero che la riservatezza in gran parte dipende dalle procedure software che adottiamo e dall'hardware che utilizziamo, non dimentichiamo che il fattore umano ha il suo peso. Nella catena della sicurezza l'elemento più debole spesso siamo proprio **noi stessi.** Per fare la nostra parte vi sono alcune semplici regole da seguire:

- Utilizzare **password forti** e uniche per proteggere i nostri account e i dispositivi. Le password devono essere complesse, contenere una combinazione di lettere, numeri e simboli, e non basate su informazioni personali facilmente reperibili.
- Tenere sotto controllo gli accessi al nostro sistema (p.e. con salvaschermo e password di accesso al computer)
- Mantenere segrete le nostre password e cambiarle immediatamente se per qualche motive vengono comunicate ad altri
- Rifiutare di fornire informazioni a persone di cui non siamo assolutamente certi (p.e. via mail a sedicenti tecnici che chiedono i vostri dati) e non cliccare link sospetti
- Cifrare i nostri documenti più riservati (in primis quelli che contengono le password)
- Mantenere aggiornato il sistema operativo e i dispositivi di sicurezza

Disponibilità

Il secondo obiettivo è quello della **Disponibilità**.

Garantire la disponibilità delle informazioni significa far si che queste siano accessibili agli utenti che ne hanno diritto, nel momento in cui essi lo richiedano.

Questo implica che i nostri sistemi, la rete e le applicazioni, debbono fornire le prestazioni richieste e che in caso di malfunzionamento ovvero di eventi catastrofici, esistano delle procedure, degli strumenti e delle persone, in grado di ripristinare i dati e la completa funzionalità dei sistemi in tempi accettabili (**disaster recovery**).

La prima cosa da fare per garantire la disponibilità dei dati e dei sistemi è quella di identificare le risorse IT e i sistemi critici che supportano le operazioni critiche dell'organizzazione. Questi dovranno essere protetti in modo da garantire la continuità operativa.

In linea di massima si deve procedere come segue:

Disponibilità

- preservare la disponibilità delle **condizioni ambientali** (energia, temperatura, umidità etc.), utilizzando idonei sistemi di controllo, sistemi di climatizzazione e gruppi di continuità
- preservare la disponibilità delle **risorse hardware e software** anche a fronte di problemi di varia natura (guasti, errori, disastri etc.), utilizzando sistemi di backup (per gli archivi) e sistemi ridondanti (per l'hardware)
- preservare i sistemi da **attacchi esterni**, per esempio provenienti da Internet, utilizzando sistemi di firewall (per il controllo degli accessi), sistemi antivirus (per la protezione del computer da software dannosi), sistemi antispyware (per la rimozione di software spia)
- educare gli utenti rispetto alle pratiche che influiscono sulla disponibilità dei sistemi. Ad esempio, sulla gestione appropriata degli account, sull'esecuzione delle verifiche di aggiornamento, ecc. La **formazione** degli utenti è sempre un fattore chiave per garantire una migliore disponibilità.

Disponibilità - esempio

- Il **backup** normalmente avviene su due supporti distinti che poi vengono mantenuti in luoghi distinti. Il cosiddetto **piano di backup** (programmato) consiste nella definizione di:
  - cosa salvare (dischi, database, cartelle, utenti, macchine, volumi, ecc.)
  - frequenza di backup (giornalmente, settimanalmente etc.)
  - ora di avvio del backup
  - supporto e percorso di archiviazione
  - tipologia di backup (completo, differenziale, incrementale)
  - modalità di compressione, tipo di log e messaggistica da esporre, tipo di verifica integrità, e molte altre opzioni a seconda della complessità del sistema.

Disponibilità - esempio

- La **ridondanza** in ingegneria consiste nella **duplicazione dei componenti critici** di un sistema con l'intenzione di aumentarne l'affidabilità e la disponibilità, in particolare per le funzioni di vitale importanza che servono a garantire la sicurezza delle persone e degli impianti o la continuità della produzione.
  - RAID (Redundant Array of Independent Disks) è una tecnica molto utilizzata anche in piccoli sistemi, per realizzare un insieme ridondante di dischi indipendenti. Mirroring di memorie e volumi cruciali, come quelli che contengono i database, vengono replicati automaticamente su più unità di archiviazione. Questo protegge dalla perdita di dati in caso di guasto di un supporto di archiviazione
  - talvolta si utilizzano sistemi ridondanti dislocati in aree diverse, con lo scopo di garantire i dati anche nel caso di incidenti o disastri
  - l'implementazione parziale o completa di servizi cloud pubblici o privati fornisce automaticamente una disponibilità estremamente elevata e la ridondanza.

Integrità

L'integrità riguarda il grado di correttezza, coerenza e affidabilità sia delle informazioni, sia delle risorse informatiche.

Quando si parla di **informazioni**, il concetto di integrità riguarda il fatto che queste non possano venire alterate, cancellate o modificate per errore o per dolo. Questo significa, per esempio:

- che all'interno di un database i dati devono essere tra loro coerenti (quando inizia una transazione il database si trova in uno stato coerente e quando la transazione termina si deve trovare in un nuovo stato coerente) e che non debbono verificarsi contraddizioni tra i dati archiviati
- che le informazioni sensibili dovrebbero essere crittografate durante la trasmissione o l'archiviazione. La crittografia previene le modifiche ai dati da parte di entità non autorizzate.
- che è opportuno implementare controlli di accesso basati sui ruoli per limitare le autorizzazioni di modifica solo agli utenti che ne hanno bisogno per svolgere il proprio lavoro. I privilegi eccessivi aumentano il rischio di compromissione dell'integrità
- Che gli utenti debbono essere formati sulle politiche e sulle procedure di integrità delle informazioni, nonché sui segnali da monitorare. La formazione degli utenti riduce il rischio di errori umani che possono compromettere l'integrità.

Integrità

Quando si parla di **hardware**, l'integrità si riferisce, per esempio:

- alla corretta elaborazione dei dati da parte della macchina (che potrebbe avere dei malfunzionamenti)
- alla garanzia di un adeguato livello delle prestazioni (la rete può essere oberata o richiedere una banda maggiore di quella realmente disponibile)
- al corretto instradamento dei dati in rete (nel caso di malfunzionamenti dovuti per esempio ad accessi indesiderati)
- al monitoraggio delle metriche hardware come la temperatura, le frequenze dei processori, l'uso della memoria e dello storage. Le metriche anomale possono indicare un danneggiamento hardware imminente
- alla manutenzione preventiva dei componenti hardware in base alla loro affidabilità. Le attività pianificate come test diagnostici, sostituzioni preventive e pulizia dei componenti garantiscono l'integrità a lungo termine.

Integrità

Infine l’integrità può riguardare il **software**; in tal caso ci si può riferire a:

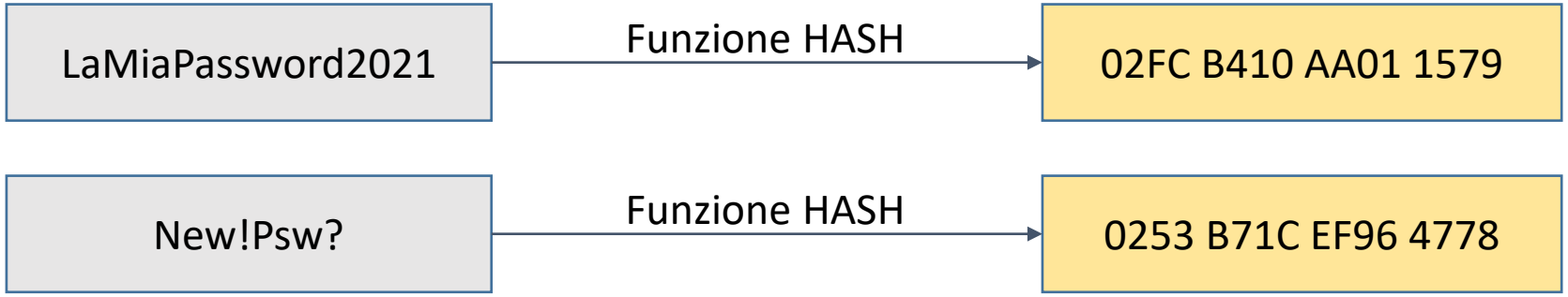
- completezza e correttezza delle applicazioni, dei file di sistema e dei file di configurazione. La verifica del software e dei file critici prima dell'implementazione o distribuzione può rilevare eventuali corruzioni nei file binari
- esecuzione regolare di strumenti di scansione anti-malware. Gli strumenti come gli antivirus e gli antimalware scansionano automaticamente il sistema operativo e tutti i programmi installati per rilevare malware, virus, trojan, worm e altri codici dannosi.
- aggiornamento costante di tutti i software e dei sistemi operativi. Gli aggiornamenti spesso correggono le vulnerabilità che potrebbero essere sfruttate per compromettere l'integrità del software.

Integrità - esempio

- Molti protocolli di comunicazione di rete, assicurano il controllo sull'integrità dei dati scambiati in una comunicazione attraverso un campo cosiddetto «**checksum»** contenuto nell'intestazione di ciascuna unità d'informazione (pacchetto) scambiata tra due peer. Alcuni degli eventuali errori di trasmissione possono essere corretti utilizzando delle opportune tecniche di recupero.
- Vi sono poi altri protocolli, di tipo **crittografico**, utilizzati per proteggere le comunicazioni e le informazioni da accessi non autorizzati o da modifiche non autorizzate. Essi sono fondamentali per garantire la sicurezza e la privacy dei dati sensibili, come quelli che vengono scambiati su internet.
- Alcuni protocolli crittografici, come SSL/TLS e HTTPS, sono molto importanti per la sicurezza delle comunicazioni su internet, specialmente quando si tratta di dati sensibili come quelli utilizzati nelle transazioni finanziarie o nelle comunicazioni tra enti governativi. Tuttavia, è importante notare che, anche se la crittografia protegge i dati durante la trasmissione, non garantisce la sicurezza dei dati sul server o sul dispositivo dell'utente. Per questo motivo, è importante utilizzare anche altre misure di sicurezza, come la crittografia dei dati inattivi e la gestione sicura delle password.

Integrità - esempio

- Tra gli algoritmi crittogafici, ci sono anche le cosiddette tecniche di «**Hashing**», impiegate in varie sitazioni: per verificare l'integrità dei dati (che non vengano alterati per dolo o per errore, anche a causa di errori di trasmissione); nel processo di firma digitale.
- Una **funzione crittografica di hash** è un algoritmo matematico che trasforma un messaggio di lunghezza arbitraria in una stringa di bit di lunghezza fissa chiamata valore di hash o impronta del messaggio.
- La funzione crittografica di hash ideale ha tre proprietà fondamentali:
  - È molto semplice da calcolare;
  - È irreversibile (dal hash non si può risalire al testo che l'ha generato);
  - È deterministica (lo stesso testo genera sempre lo stesso hash).



Integrità - esempio

L'hashing, pur essendo un metodo teoricamente molto sicuro, in realtà non garantisce totalmente la sicurezza dei dati. poiché gli hash possono essere violati attraverso attacchi di forza bruta o di dizionario. Per questo motivo, è importante combinare l'hashing con altre tecniche di sicurezza e con la gestione sicura delle password.

Altri obiettivi di sicurezza

Oltre ai tre principali obiettivi di sicurezza citati, possiamo averne anche altri che oggigiorno sono considerati di rilevante interesse in relazione ad alcune specifiche tipologie di transazione:

- **Autenticità** – per essere certi che un messaggio o un documento sia attribuito al suo **autore** e a nessun altro
- **Non ripudio** – per impedire che un autore possa disconoscere la paternità di un dato documento da lui redatto.

Entrambe queste caratteristiche trovano applicazione nella

FIRMA DIGITALE

in cui vengono utilizzate specifiche tecniche che garantiscono sia l'integrità del documento (hashing) sia la sua provenienza (crittografia).

General Data Protection Regulation (GDPR)

Dal momento che l'informazione è un bene che deve essere tutelato e garantito, ogni organizzazione aziendale deve adottare tutti i provvedimenti necessari affinché ciò avvenga.

Nel contesto attuale, in cui si ha una proliferazione dei rischi informatici ed in particolare di quelli dovuti alla violazione dei sistemi di sicurezza, esistono a carico di Enti e Aziende dei precisi obblighi di legge, soprattutto in materia di tutela della **privacy e di trattamento dei dati personali.**

Il **GDPR** (General Data Protection Regulation) è un regolamento dell'Unione Europea, entrato in vigore il 25 maggio 2018, il cui obiettivo principale è quello di proteggere la privacy e i dati personali dei cittadini europei, garantendo loro maggiori diritti di controllo sui propri dati.

General Data Protection Regulation (GDPR)

Il GDPR si applica a tutte le organizzazioni che trattano dati personali di cittadini europei, indipendentemente dalla loro sede. Ciò significa che anche le organizzazioni non europee che trattano dati personali di cittadini europei devono rispettare il GDPR.

Le organizzazioni che non rispettano il GDPR possono essere soggette a **multe fino al 4% del loro fatturato** globale annuo o a sanzioni amministrative equivalenti.

Il GDPR rappresenta un importante passo avanti nella protezione dei dati personali e della privacy dei cittadini europei, fornendo loro maggiori diritti e controllo sui propri dati. Per le organizzazioni, rappresenta una sfida per garantire la conformità ai requisiti del regolamento e proteggere i dati personali dei propri clienti e utenti.

Quali sono i requisiti fondamentali che GDPR stabilisce, per garantire la protezione dei dati personali?

- **Consenso**: le organizzazioni devono ottenere un consenso chiaro e inequivocabile dalle persone per poter trattare i loro dati personali.
- **Trattamento dei dati**: le organizzazioni devono trattare i dati personali in modo trasparente e lecito, limitando la raccolta e l'utilizzo dei dati solo a scopi specifici e legittimi.
- **Sicurezza dei dati**: le organizzazioni devono adottare misure tecniche e organizzative adeguate per proteggere i dati personali da accessi non autorizzati, perdite o danni.
- **Diritto all'oblio**: le persone hanno il diritto di richiedere la cancellazione dei propri dati personali.
- **Portabilità dei dati**: le persone hanno il diritto di richiedere la trasferibilità dei propri dati personali da un'organizzazione all'altra.
- **Notifica delle violazioni dei dati**: le organizzazioni devono notificare le autorità competenti e le persone interessate in caso di una violazione dei dati personali.

Il controllo degli accessi

I processi di «**Autenticazione**» servono a verificare l'identità di chi sta accedendo ad un dato sistema, attraverso un procedimento che può essere di questo tipo:

- Vengono eseguiti dei **test** sull'identità dell'utente
  - L'utente presenta alcune **credenziali** (password, certificato digitale) come prova della propria identità
- Una volta che l'utente è stato autenticato, gli viene concesso l'accesso alle sole risorse per cui è **autorizzato** (per esempio mediante controlli di accesso, permessi, privilegi).

La «**Autorizzazione»** che è un concetto ben distinto da quello di Autenticazione è il diritto accordato all'utente (che può essere una persona, ma anche un software) di accedere ad un sistema e alle sue risorse, in base ad un dato **profilo**.

Il controllo degli accessi

I metodi di Autenticazione più diffusi sono abbinati alla utilizzazione di:

- Password
- Token
- Dispositivi Biometrici

In generale si considera che tali metodi si basino su:

- qualcosa che **sai** (password, codice etc...);
- qualcosa che **hai** (token, smartcard etc...);
- qualcosa che **sei** (caratteristiche della retina, impronta digitale, voce etc…).

Il controllo degli accessi

- I metodi di Autenticazione da utilizzare possono dipendere da diversi fattori:
  - La tipologia di Utenza da autenticare
  - Il Valore delle Informazioni da proteggere
  - La Distribuzione delle risorse informative.
- In funzione dei fattori suddetti e del grado di sicurezza che intendiamo ottenere, adotteremo uno dei metodi citati ovvero una loro combinazione.
- Vale la pena di sottolineare che, poiché l'autenticazione tramite un dato noto solo al possessore è considerato un metodo vulnerabile (la password si può facilmente dimenticare), normalmente si tende a sostituirla con una combinazione di più metodi (e.g. scheda + PIN).

Il controllo degli accessi – la Password

La richiesta di una **password** (parola d'ordine) è senz'altro uno dei più antichi metodi di autenticazione.

Mentre nei primi computer i metodi di riconoscimento delle password erano piuttosto superficiali e spesso si limitavano a conservate un elenco di codici/stringhe in chiaro su un file (consideriamo però che a quel tempo non si parlava certo di attacchi informatici), con l'andar del tempo i metodi di confronto divennero sempre più sofisticati. Nel 1967 fu introdotto l'**hashing** delle password che come abbiamo visto è il metodo tuttora più utilizzato.

Nel caso del hashing il sistema conserva in un file i nomi degli utenti e l'hash delle relative password; durante l'autenticazione, l'hash viene ricalcolato in base alla password digitata e viene confrontato con quello registrato.

Il controllo degli accessi – la Password

Alcuni parametri da utilizzare per la creazione e il mantenimento di una buona password possono essere:

- **Lunghezza -** più la password è lunga, più sarà difficile da decifrare
- **Tipologia dei Caratteri –** possibilmente una password dovrebbe contenere minuscole, maiuscole, cifre ed altri segni (quando concessi)
- **Contenuto -** dovrebbero essere evitati nomi di persone, luoghi, date, parole del dizionario e soprattutto nomi riconducibili all'utente
- **Durata –** è consigliabile modificare la password con una certa frequenza, ovviamente scegliendo una nuova password diversa
- **Conservazione** – se si intende memorizzare la password da qualche parte, conviene utilizzare un file crittato.

Il controllo degli accessi – il Token

Il **token** è un dispositivo elettronico portatile in grado di generare un codice di sicurezza in base ad un algoritmo che talvolta tiene conto del «momento» in cui viene utilizzato.

L'utente normalmente possiede un suo proprio codice che combinato con quello generato dal token fornisce una password che viene riconosciuta dal server di autenticazione.

Questo metodo, di tipo misto, è uno dei più difficili da violare, poiché l'oggetto fisico deve essere posseduto al momento della autenticazione e il possessore sa se questo è stato smarrito o gli è stato rubato.

Per contro il token ha un certo costo, si può rompere e può essere smarrito.

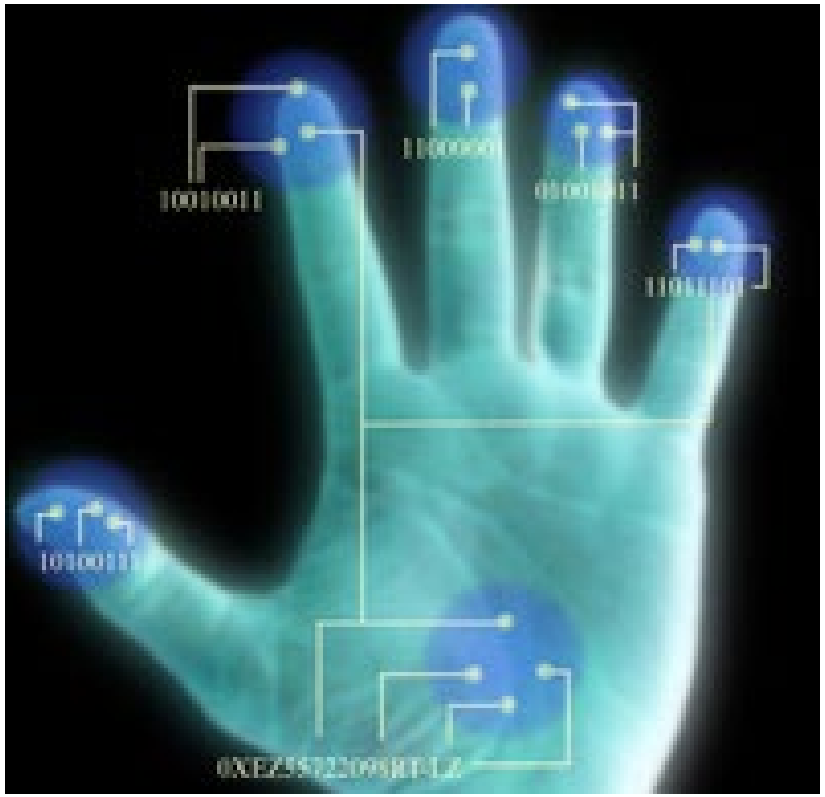
I Token possono essere di tipo «**passivo**» (il bancomat o un dispositivo RFID) o di tipo «**attivo**» (una smartcard dotata di processore crittografico).

Il controllo degli accessi – la Biometria

I **Sistemi Biometrici** utilizzano le caratteristiche fisiche o comportamentali di una persona per verificarne l'identità.

Le caratteristiche fisiche più utilizzate per l'autenticazione biometrica sono:

- **Impronte digitali** - gli scanner per impronte digitali sono molto diffusi ed hanno un costo ridotto
- **Geometria delle mani** – è un metodo più solido del precedente che però richiede che le mani siano pulite
- **Scansione della Retina o dell'Iride** – utilizzata per lo più in installazioni militari o governative che richiedono elevati standard di sicurezza. Quest'ultimo metodo richiede un'esposizione prolungata a bassa intensità luminosa ed è considerato «intrusivo» sebbene non rechi alcun danno agli occhi.



Il controllo degli accessi – la Biometria

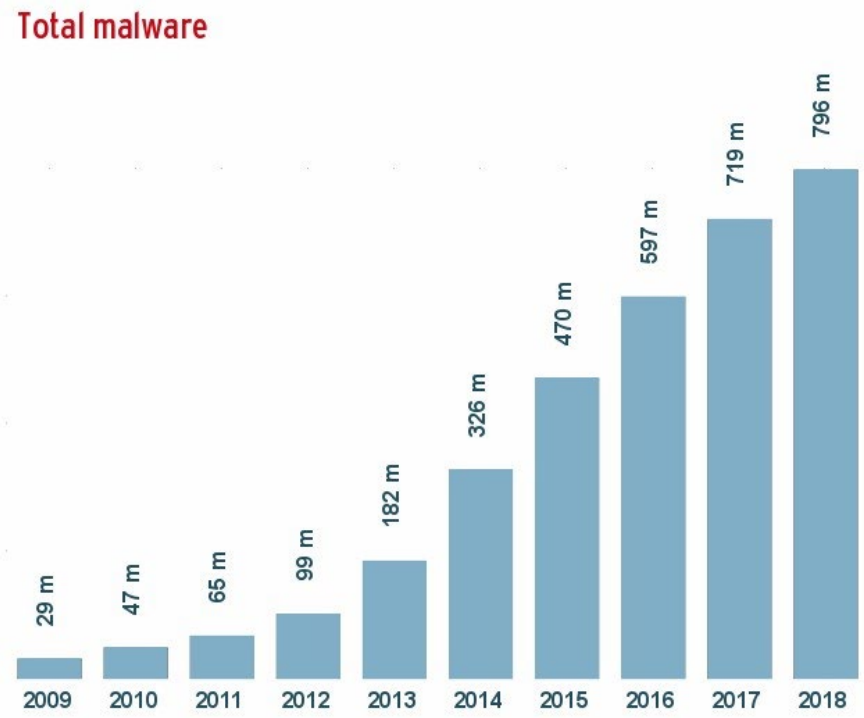
- **Riconoscimento del Volto** – può essere utilizzato all'insaputa del soggetto e in taluni casi anche tra la folla (sistemi antiterrorismo)
- **Voce** – è un metodo che analizza l'impronta vocale del soggetto e rientra tra i metodi di analisi comportamentale
- **Firma** – anche questo rientra tra i metodi di riconoscimento basati sul comportamento
- **Digitazione della Tastiera** – si tratta di un metodo che riconosce il comportamento dell'utente di fronte alla tastiera: pressione di battitura, ritardo tra le battute etc…

Attacchi informatici

Quando si parla di sicurezza informatica il termine **malware** indica un software creato per causare danni a un computer o ai dati degli utenti di un computer, oppure danno ad un intero sistema informatico.

Il termine deriva dalla contrazione delle parole inglesi «**mal**icious» e «soft**ware»** e significa «codice maligno».

In circolazione esistono diversi tipi di malware molti dei quali sono illegali e pericolosi. Il fenomeno della diffusione di malware è in continua evoluzione tanto che il 2017 ha fatto segnare un +20% di minacce a livello globale rispetto al 2016 e un +10% nel 2018 rispetto al 2017 (l'Italia è uno dei paesi più colpiti in Europa).



*Fonte: Cyber Security 360

Attacchi Informatici

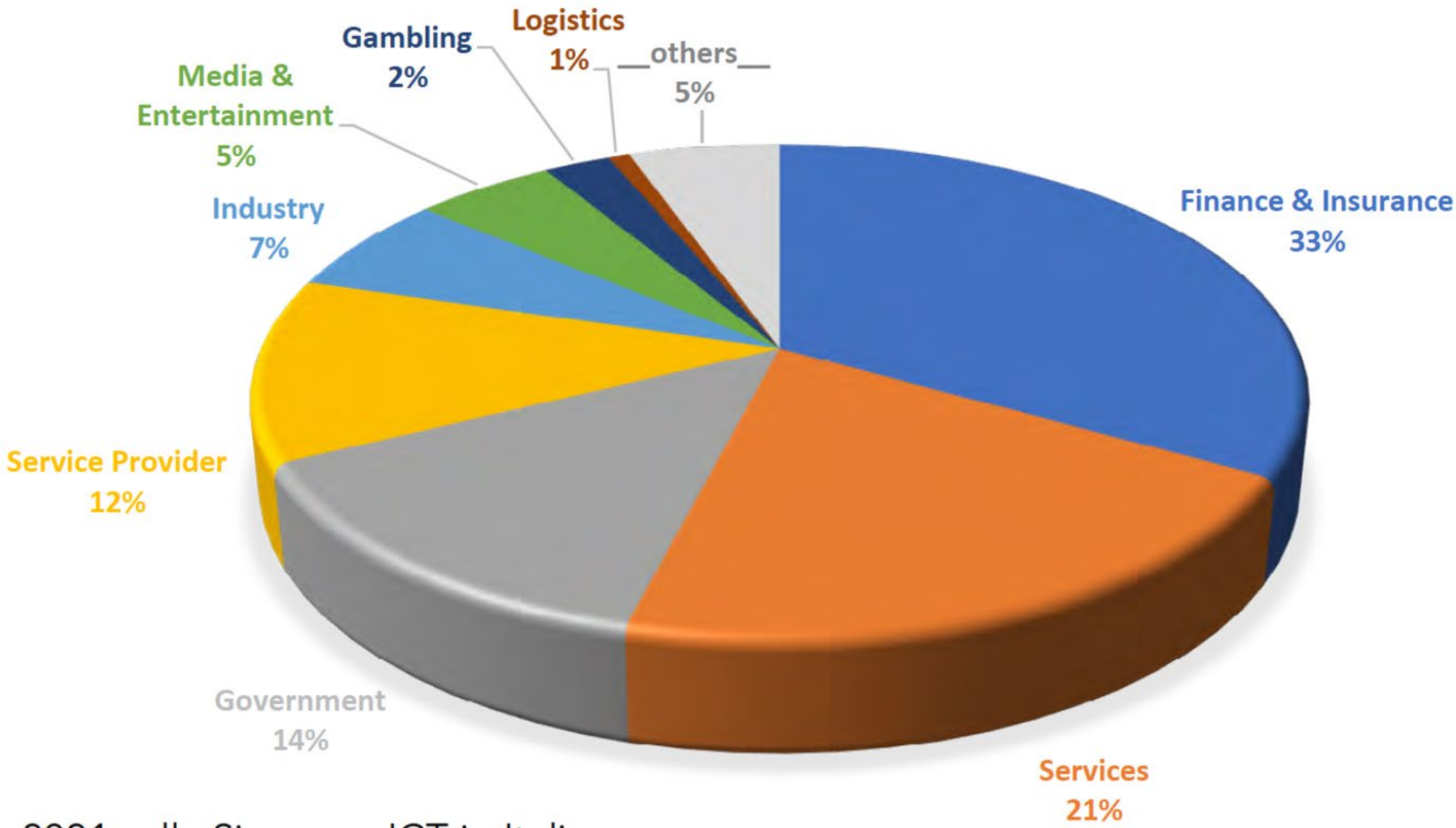
Tutte le minacce *«… possono creare notevoli danni. Il più diffuso e comune è l'encryption dei dati locali e di rete della macchina infetta, che costringe l'utente al pagamento di un riscatto per poter ottenere i mezzi per recuperare i propri dati. Gli utenti e le aziende più sprovveduti, ovvero coloro che non si sono premuniti di avere un backup verificato, sono costretti a pagare. Spesso, purtroppo, succede che nonostante il pagamento i criminali svaniscano lasciando in seri guai i malcapitati»*.*

Col termine "**ransomware**" ci si riferisce proprio a questo: un attacco informatico teso alla richiesta di un riscatto.

L'attacco portato da **WannaCry**, nel maggio 2017, fu capace di infettare centinaia di migliaia di computer nel giro di poche ore. Molti esperti del settore l'hanno considerato come il peggior attacco informatico degli ultimi anni, sia per velocità di contaminazione, sia per portata dell'attacco. WannaCry mise in pericolo il funzionamento di molti uffici pubblici, ospedali, catene di montaggio e fabbriche.

*__David Gubiani__, security engineering manager di Check Point Italia.

I settori più colpiti dai cyber attacchi



Rapporto 2021 sulla Sicurezza ICT in Italia

I primi malware

Nel 1949 **John von Neumann** dimostrò matematicamente la possibilità di costruire un programma per computer in grado di replicarsi autonomamente.

Nei primi anni ‘60 un gioco ideato da un gruppo di programmatori dei **Bell Laboratories,** nel quale più programmi si dovevano sconfiggere sovrascrivendosi a vicenda, dava l'inizio alla storia dei virus informatici.

Jerusalem fu uno dei più vecchi (1987) e noti virus informatici comparsi per i sistemi MS-DOS e fu il virus con il più alto numero di file infettati a quell tempo.

- Il nome trae origini dal fatto che all'epoca si riteneva che il virus avesse fatto la sua prima comparsa in un computer di una università di Gerusalemme. Analisi successive (1991) hanno invece dimostrato che il virus ha fatto la sua prima comparsa in **Italia.**
- Il virus si agganciava poi ai processi di **interrupt** del sistema (gli interrupt 8 e 21) e dopo 30 minuti di esecuzione rallentava le attività del computer di un fattore 10. Il virus aveva poi una bomba logica: se si accorgeva che la data del sistema era un «venerdì 13» iniziava a cancellare ogni file che l'utente cercava di aprire.

Esistono diversi tipi di malware, ognuno con caratteristiche, metodi di diffusione e pericolosità differenti:

Virus: i virus sono programmi che infettano i file eseguibili e si replicano all'interno del sistema. Possono essere diffusi attraverso allegati di posta elettronica, download di software da siti non sicuri o dispositivi di archiviazione infetti. I virus possono causare danni al sistema, come la cancellazione di file, la corruzione dei dati o il rallentamento del sistema.

Worm: i worm sono programmi che si replicano senza bisogno di un file eseguibile e si diffondono attraverso la rete. Per indurre gli utenti ad eseguirli utilizzano tecniche di **ingegneria sociale** (studio del comportamento individuale di una persona al fine di carpire informazioni utili) oppure sfruttano dei difetti (Bug) di alcuni programmi per diffondersi automaticamente. Possono causare danni al sistema, come la saturazione della banda di rete, la cancellazione di file o la compromissione dei dati.

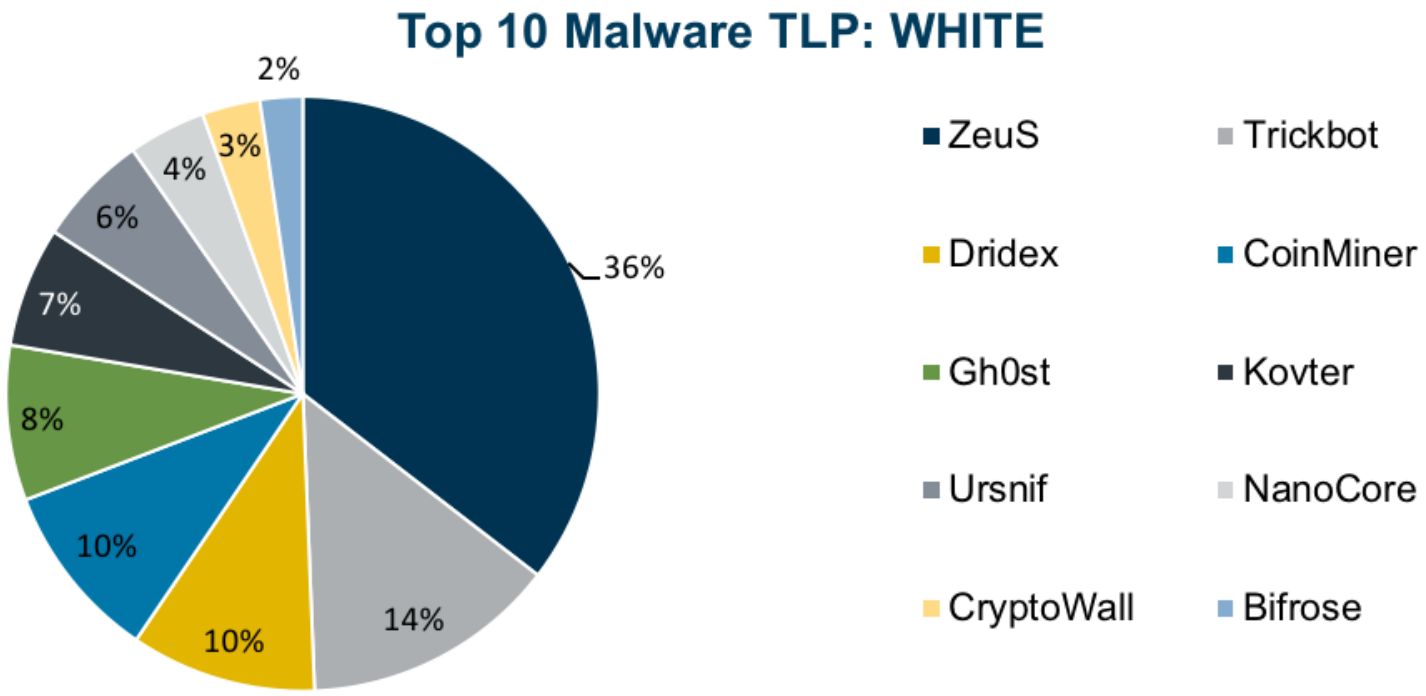
Trojan: i trojan sono programmi che si presentano come software legittimo, ma in realtà contengono funzionalità malevole. Possono essere diffusi attraverso download di software da siti non sicuri o allegati di posta elettronica. I trojan possono essere utilizzati per rubare informazioni, installare software dannoso o controllare il sistema infetto.

Spesso i Trojan (come pure virus e worm) hanno lo scopo di installare dei **Keylogger**, ossia degli strumenti di sniffing, hardware o software, in grado di intercettare tutto ciò che un utente digita sulla tastiera del proprio o di un altro computer. Altre volte installano delle **Backdoor**, ossia delle porte che consentono di superare in parte o in tutto le procedure di sicurezza attivate in un sistema informatico consentendo ad un Hacker di accedere illegittimamente al sistema.

Ransomware: il ransomware è un tipo di malware che crittografa i dati del sistema e richiede un riscatto per ripristinarli. Può essere diffuso attraverso allegati di posta elettronica, download di software da siti non sicuri o exploit di sicurezza. Il ransomware può causare danni finanziari e la perdita di dati importanti.

Adware: l'adware è un tipo di malware progettato per visualizzare pubblicità indesiderate sul sistema infetto. Può essere diffuso attraverso download di software da siti non sicuri o exploit di sicurezza. L'adware può causare fastidi e rallentamenti del sistema.

Spyware: lo spyware è un tipo di malware progettato per raccogliere informazioni sulle attività degli utenti e inviarle a terzi. Può essere diffuso attraverso download di software da siti non sicuri o exploit di sicurezza. Lo spyware può compromettere la privacy degli utenti e causare danni finanziari.



ZeuS è un Trojan che attacca Microsoft Windows e altri SO come Android. Zeus agisce come un Trojan di servizi finanziari. Il malware riconosce che l'utente si trova su un sito di una banca e registra i tasti digitati. Il creatore del malware ha reso pubblico il codice sorgente di Zeus nel 2011, dando il via alla creazione di versioni nuove e aggiornate tuttora circolanti.

NanoCore è distribuito principalmente con attacchi di phishing via e-mail: molte delle campagne in corso che distribuiscono il malware sono progettate per apparire come fatture o ordini di acquisto con nomi di allegati progettati per invogliare ad aprire gli allegati. Il creatore di questo malware è stato condannato per questa sua attività criminosa e tuttavia durante la sua permanenza in carcere il suo malware ha continuato a circolare. L'autore infatti ne ha distribuito il codice nel **dark web**.

NanoCore consente di compiere diverse azioni da remoto tra cui:

- Spegnimento e riavvio del PC
- Esplorazione dei file salvati
- Accesso e controllo del Task manager (Gestione attività)
- Modifica dell'editor di registro di sistema
- Controllo del mouse
- Apertura di pagine web
- Disattivazione del LED che indica l'uso della webcam
- Cattura di audio e video
- Rilevamento di password e credenziali di login

Deep-Web e Dark-Web

Il **Deep Web** è l'insieme delle risorse informative del World Wide Web (www) non indicizzate dai normali motori di ricerca. Per dare l'idea dell'estensione del Deep Web si stima che dell'insieme delle informazioni di cui è costituito il web, solamente qualche frazione percentuale (0,2% ?) sia effettivamente indirizzata dai maggiori motori di ricerca. Di questa categoria fanno quindi parte nuovi siti non ancora indicizzati, pagine web a contenuto dinamico, software, siti privati, pagine scritte in linguaggi diversi dal html, contenuti banditi dai normali motori di ricerca reti di file-sharing e alter risorse web che richiedono un'autenticazione per l'accesso.

Il Deep Web non è necessariamente illegale o pericoloso e molte organizzazioni lo utilizzano per proteggere informazioni sensibili e garantire la sicurezza dei dati. Tuttavia, il Deep Web può essere utilizzato anche per attività illegali, come la vendita di droghe, armi, informazioni rubate e servizi illegali.

Per navigare in sicurezza nel Deep Web, è importante utilizzare un browser sicuro (i.e. **Tor)** che garantisca l'anonimato e la privacy. All'interno del Deep Web, si può notare che i siti web possono avere URL diverse dalle usuali che terminano con ".com" o ".org". Inoltre, i siti web del Deep Web spesso richiedono un'autenticazione per l'accesso e potrebbero essere inaccessibili attraverso i motori di ricerca tradizionali come Google o Bing.

Tuttavia, è importante ricordare che l'accesso al Deep Web può essere pericoloso e che l'utilizzo di servizi illegali o di siti web illegali può comportare conseguenze legali e penali.

Deep-Web e Dark-Web

Il **Dark Web** invece è un sottoinsieme del Deep Web. Anche in questo caso è necessario utilizzare dei browser che garantiscano un elevato livello di anonimato e talvolta questa parte del web non è raggiungibile attraverso una normale connessione Internet in quanto si compone anche di parti di reti private sovrapposte alla rete Internet (le cosiddette darknet). In tal caso per l'accesso è necessario utilizzare dei software specifici che consentano l'utilizzazione di tali reti.

Il Dark Web viene sovente impiegato per occultare materiale illegali o svolgere attività illegali. All'interno vi si può trovare un po' di tutto:

- condivisione di file illegali o contraffatti
- protezione della privacy di cittadini sotto sorveglianza
- compravendita di beni o servizi illegali
- aggiramento della censura propria di internet e dei sistemi di filtraggio

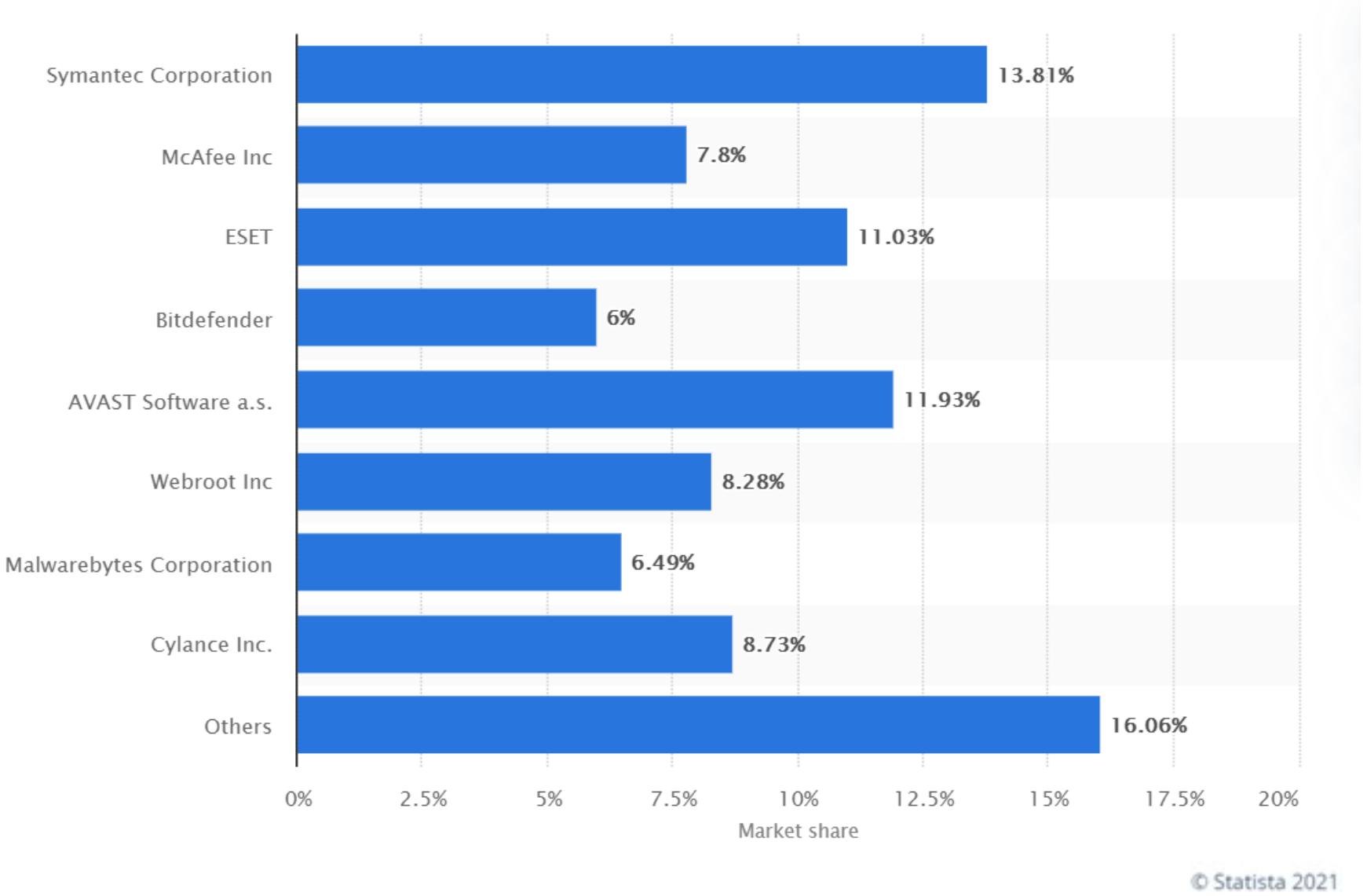
È importante notare che l'utilizzo di browser del Dark Web potrebbe attirare l'attenzione delle autorità competenti, poiché questi browser sono spesso utilizzati per accedere a siti web illegali e pericolosi. Pertanto, è necessario essere consapevoli dei rischi che può comportare la navigazione in queste parti del web.

Anti-Malware

Gli Anti-malware (o più comunemente Anti-virus) sono dei software che hanno lo scopo di prevenire, rilevare ed eventualmente rendere inoffensivi i codici malware.

Gli **Anti-virus** propriamente detti, non sono in grado normalmente di proteggere in maniera completa un sistema informatico, ma necessitano di essere abbinati ad altri software come gli **Anti-spam**, i **Firewall** etc..

Mercato dei principali produttori di anti-malware per sistemi windows



Anti-virus e Anti-spyware

I classici **Anti-virus** sono normalmente composti da più parti:

- Un **file di firme** - è un archivio che contiene tutte le firme dei virus conosciuti.
- Un **programma anti-virus** - permette di eseguire su richiesta una serie di operazioni, la scansione completa del sistema o di singoli files, l'eliminazione dei file sospetti etc..
- Un **programma di ascolto** – caricato in memoria all'avvio richiama l'anti-virus ogni volta che viene creato o modificato un nuovo file o una zona di memoria.
- Un **programma** che provvede su richiesta, all'aggiornamento del file delle firme

Gli **anti-spyware** sono programmi utilizzati per eliminare dal sistema diverse tipologie di malware e in particolare spyware, adware. Le funzioni di questi programmi sono simili a quelle degli antivirus, ma non sono la stessa cosa poiché gli anti-virus propriamente detti proteggono il computer solamente da una tipologia di malware: i virus appunto.

È vero però che spesso gli «anti-virus» sono distribuiti come **suite complete** che includono anche funzioni anti-malware e firewall.

Anti-spam

Lo **spamming** è l'invio di messaggi indesiderati (generalmente di tipo commerciale e pubblicitario) ed è noto anche col nome di «posta spazzatura».

Poiché lo spam viene inviato senza il permesso del destinatario è considerato altamente dannoso anche dagli Internet Service Provider.

Questi ultimi vi si oppongono non solo per i costi generati dal traffico indesiderato ma anche perché può verificarsi una violazione contrattuale della «Acceptable Use Policy» che può essere causa di interruzione dell'abbonamento da parte dell'utilizzatore.

Gli **antispam** sono software che analizzano la provenienza e/o il contenuto dei messaggi, effettuando una azione di filtraggio preventiva.

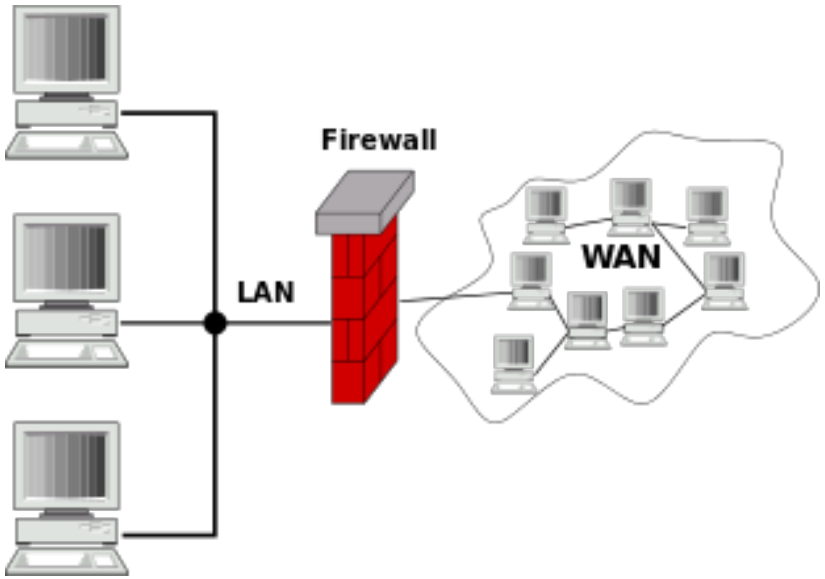
Prodotti Anti-malware

- **Nod32** (ESET azienda slovacca) molto discreto, controlla, scansiona e si aggiorna in modo del tutto automatico e continuo.
  Più volte premiato in passato come miglior antivirus, viene venduto oggi in una suite che comprende anche la funzione di firewall, antispyware e di antispam. Offre anche funzionalità di sicurezza per la navigazione web e per l'identità digitale.
- **Kaspersky** è prodotto da un’azienda Russa e si presentava come una suite completa già da tempo. per la sua completezza, è considerato un prodotto di punta dotato di firewall, antispyware e antivirus. Nel 2022, tuttavia, a seguito della crisi in Ucraina, è stato emesso il cosiddetto «Decreto Ucraina» che ne vieta l’utilizzazione nelle pubbliche amministrazioni.
- **Norton** è uno dei più noti software antivirus disponibili sul mercato. È stato sviluppato da NortonLifeLock, una società specializzata nella sicurezza informatica. Norton Antivirus offre un'ampia gamma di funzionalità, tra cui la protezione da virus, spyware, malware, phishing e altre minacce informatiche. Inoltre, Norton Antivirus offre anche funzionalità di backup e ripristino dei dati.

Prodotti Anti-malware

Tra gli antivirus open-source vale la pena di citare:

- **AVG Antivirus:** AVG Antivirus è un software antivirus open source disponibile per Linux. Offre una vasta gamma di funzionalità di sicurezza informatica, tra cui la protezione da virus, spyware, malware e altre minacce informatiche.
- **ClamAV**: ClamAV è un software antivirus open source ampiamente utilizzato per la sicurezza informatica. È disponibile per molte piattaforme, tra cui Linux, Windows e macOS.
- **Avast** è l'antivirus free in italiano salito alla ribalta perché è stato scelto da Google. Non è open-source ma ne esiste una versione gratuita.
- **Comodo Internet Security** Comodo Antivirus è un software antivirus open source disponibile per Windows. Offre una vasta gamma di funzionalità di sicurezza informatica, tra cui la protezione da virus, spyware, malware e altre minacce informatiche..



Firewall

Il **firewall** (muro tagliafuoco) è un componente passivo (hardware o software) di difesa perimetrale di una rete informatica, che può anche svolgere funzioni di collegamento tra due o più parti di rete.

Normalmente la rete viene divisa in due sottoreti: una esterna che comprende Internet, l'altra interna che comprende i computer utilizzati nella nostra rete locale (LAN).

Il funzionamento del firewall

1. **Monitoraggio**: il firewall monitora il traffico di rete in entrata e in uscita, analizzando i pacchetti di dati e verificando se rispettano le regole di sicurezza impostate.

2. **Decisione**: in base alla configurazione del firewall, viene presa una decisione su come gestire il traffico di rete. Ad esempio, il firewall può bloccare il traffico proveniente da un indirizzo IP sospetto o consentire l'accesso solo a determinati servizi o protocolli di rete.

3. **Azione**: in base alla decisione presa, il firewall gestisce il traffico di rete in modo appropriato. Ad esempio, il firewall può bloccare il pacchetto di dati sospetto o consentire l'accesso solo a determinati servizi o protocolli di rete.

I firewall possono essere configurati in diversi modi a seconda delle esigenze di sicurezza della rete. Ad esempio, possono essere configurati per bloccare l'accesso a siti web specifici o per impedire l'accesso a determinati servizi di rete come la posta elettronica o il file-sharing. Inoltre, i firewall possono essere configurati per rilevare e prevenire gli attacchi informatici, come i tentativi di intrusioni e le vulnerabilità dei sistemi.

Honeypot

Il **honeypot** (barattolo del miele) è un sistema o componente hardware o software usato come «trappola» ovvero «esca» a fini della protezione contro gli attacchi di pirati informatici.

Normalmente è utilizzato per proteggere reti locali.

Solitamente consiste in un computer dedicato o un sito web che «sembra» contenere informazioni importanti e preziose ma che in realtà non contiene alcuna informazione sensibile.

FINE DELLE LEZIONI TEORICHE