SICUREZZA INFORMATICA

Cos'è la sicurezza informatica?
La **sicurezza informatica** è l'insieme di **tecnologie, regole e comportamenti** che servono a proteggere **dati, sistemi e reti** da:

- accessi non autorizzati
- modifiche non volute
- interruzioni del servizio

accesso non aut. =

- una persona entra in un account email senza conoscere la password
- qualcuno accede al registro elettronico senza essere un docente
- accesso a un computer o a una rete aziendale senza permesso

modifiche non volute:

- voti scolastici modificati senza autorizzazione
- file importanti cambiati o cancellati accidentalmente
- dati di un documento alterati da un virus o da un attacco informatico

interruzioni di servizio :

- un sito web che non è raggiungibile
- il registro elettronico che non funziona durante l'orario scolastico
- un server bloccato da un attacco che ne impedisce l'utilizzo

Non riguarda solo i computer , ma qualsiasi si stema che gestisce informazioni digitali.

La sicurezza informatica riguarda:

- i **dati personali** (password, messaggi, foto, documenti)
- le **aziende** (clienti, contabilità, progetti)
- i **servizi online** che usiamo ogni giorno (scuola, banche, social network)

Un sistema informatico si può definire **sicuro** quando:

- i dati **non vengono letti** da persone non autorizzate
- i dati **non vengono modificati** senza permesso
- i servizi **rimangono disponibili** e funzionanti

MODELLO CIA : Confidenzialità, Integrità, Disponibilità

La sicurezza informatica si basa su **tre principi fondamentali**, chiamati **modello CIA**:

- Confidenzialità
- Integrità
- Disponibilità

Ogni misura di sicurezza serve a proteggere **uno o più** di questi tre aspetti.

Confidenzialità

La **confidenzialità** garantisce che **solo gli utenti autorizzati** possano accedere ai dati.

In pratica:
chi **non ha il permesso**, **non deve vedere** le informazioni.

Esempi di strumenti per la confidenzialità

- **Password**: una chiave segreta per accedere a un sistema
- **PIN**: codice numerico usato per autenticarsi (es. bancomat) , autenticazione a due fattori
- **Crittografia**: trasformazione dei dati in una forma illeggibile per chi non ha la chiave
- **Username e password**: identificano l'utente e verificano che sia autorizzato

Violazioni della confidenzialità

- qualcuno legge email private
- furto di password
- accesso abusivo a un account social o bancario

Integrità

L'**integrità** garantisce che i dati **rimangano corretti e completi** e che **non vengano modificati** senza autorizzazione.

In pratica:
i dati devono essere **affidabili** e **non alterati**.

Esempi di violazione dell'integrità

- voti scolastici modificati
- dati di un file cambiati senza permesso
- software manomesso o alterato

Strumenti per garantire l'integrità:

- **Backup**: copie dei dati che permettono di ripristinare la versione corretta
- **Controlli di modifica**: sistemi che registrano chi ha modificato un file e quando
- **Firme digitali**: sistemi che permettono di verificare che un file o un documento non sia stato alterato

Disponibilità

La **disponibilità** garantisce che **dati e servizi siano accessibili quando servono**.

In pratica:
il sistema deve **funzionare** e non essere bloccato.

Esempi di disponibilità

- un sito web sempre raggiungibile
- un registro elettronico funzionante
- un server che non va offline

Violazioni della disponibilità

- blocco di un sito web
- sistemi non accessibili
- attacchi che mandano in crash i server

ATTACCHI E MINACCE INFORMATICHE

Una minaccia è un possibile pericolo per un sistema informatico.
Un attacco è quando la minaccia si realizza davvero.

Principali attacchi informatici:

Malware: software dannoso progettato per danneggiare o rubare dati

- virus
- trojan
- ransomware

Phishing: messaggi o email false che imitano enti reali per rubare dati personali

Attacco DDoS: sovraccarico di un sito o server con troppe richieste per renderlo inutilizzabile , esempio: ticketone

Accesso non autorizzato: entrare in un sistema senza permesso

Furto di dati: copia o vendita di informazioni sensibili

Molti attacchi sfruttano:

- password deboli
- disattenzione degli utenti
- software non aggiornato

Meccanismi di sicurezza

I **meccanismi di sicurezza** sono **strumenti tecnici** che **applicano concretamente** le politiche di sicurezza.

In pratica: fanno rispettare le regole.

Esempi di meccanismi di sicurezza (spiegati)

- **Antivirus**: programma che individua, blocca ed elimina software dannoso
- **Firewall**: sistema che controlla il traffico di rete e blocca accessi non autorizzati
- **Backup**: copie dei dati salvate per poterle recuperare in caso di perdita
- **Crittografia**: protezione dei dati rendendoli illeggibili senza una chiave
- **Autenticazione a due fattori**: accesso che richiede due verifiche (es. password + codice sul telefono)

Politiche = regole
Meccanismi = strumenti che fanno rispettare le regole

le regole senza strumenti non funzionano,
gli strumenti senza regole vengono usati male.

Esercizio 1 – Vero o Falso

Indica se l'affermazione è vera (V) o falsa (F).

1. La sicurezza informatica serve solo alle aziende. F
2. La confidenzialità protegge i dati da accessi non autorizzati. V
3. L'integrità riguarda la disponibilità dei servizi. F
4. Il phishing è un tipo di attacco informatico. V
5. Un attacco DDoS colpisce la disponibilità. V
6. Le politiche di sicurezza sono strumenti tecnici. F

Esercizio 2 – Completa le frasi

Completa con le parole corrette:
(confidenzialità – integrità – disponibilità – attacco – minaccia – malware – firewall)

1. Un software dannoso si chiama malware.

2. L’ integrità garantisce che i dati non vengano modificati.
3. Un attacco è un evento che causa un danno reale.
4. Il firewall protegge una rete da accessi esterni.
5. La disponibilità assicura che i servizi siano sempre accessibili.
6. Una minaccia è un possibile pericolo per un sistema.

COMPITO PER MARTEDÌ 10 FEBBRAIO: allegare prima dell'inizio della lezione.

COMPITO DI RICERCA – SICUREZZA INFORMATICA E CALCIO

In questo lavoro analizzeremo alcuni **casi reali di problemi di sicurezza informatica** che hanno coinvolto **grandi squadre di calcio internazionali**.
L'obiettivo non è scrivere tanto, ma **capire cosa è successo e collegarlo ai concetti studiati in classe**.

Casi da analizzare (tutti obbligatori)

Nel tuo lavoro dovrai analizzare **tutti e tre** i seguenti casi:

- **Manchester United – Attacco ransomware (2022)**
- **FC Barcelona – Furto e diffusione di dati (2020)**
- **Paris Saint-Germain – Attacchi ai profili digitali (2021)**

Non è possibile sceglierne solo uno: **vanno fatti tutti e tre**.

Cosa devi fare

Per **ognuno dei tre casi** devi seguire la stessa struttura.

1. Informazioni di base

Indica:

- il nome della squadra
- l'anno in cui è avvenuto l'episodio
- una breve spiegazione di cosa è successo

In questa parte devi solo raccontare i fatti, in modo chiaro e semplice.

2. Analisi del problema (modello CIA)

Dopo la descrizione, devi spiegare **quali aspetti della sicurezza informatica sono stati coinvolti**, usando il **modello CIA**.

Per ogni caso indica se sono stati colpiti:

- **Confidenzialità** (dati rubati o accessi non autorizzati)
- **Integrità** (dati modificati o alterati)
- **Disponibilità** (servizi o sistemi bloccati o non funzionanti)

Può essere coinvolto **più di un principio**, ma devi spiegare **perché**.

Come deve essere il lavoro:

- Usa fonti online affidabili
- Scrivi con parole tue
- Linguaggio semplice ma corretto
- Lunghezza totale: circa **una pagina / una pagina e mezza**

Scopo del lavoro:

Questo compito serve a capire che la **sicurezza informatica è importante anche nel calcio professionistico** e che problemi di questo tipo possono colpire **chiunque**, anche le squadre più famose.

link fonti attendibili Manchester (copia e incolla per visitarli) :

- https://www.manutd.com/en/news/detail/official-manchester-united-club-statement-20-november-2020?utm_source=chatgpt.com
- https://www.wired.it/internet/web/2020/11/23/manchester-united-attacco-cyber/?utm_source=chatgpt.com
- https://dataprotectionpeople.com/resource-centre/manchester-united-are-being-held-to-ransom-for-millions-of-pounds-after-cyber-attack/?utm_source=chatgpt.com