principi della cybersecurity

Le normative di riferimento sono due regolamenti europei, Gdpr ed Gdpr, e due direttive, Nis e 680 CIE

La cybersecurity o sicurezza informatica, o IT SECURITY nasce dall'obiettivo di tutelare le informazioni e le tecnologie dall'azione di terzi per l'appunto gli Hacker o da rischi di qualunque altra natura,infatti la cybersecurity serve proprio ad evitare danni al sistema ad attrezzare i rischi o quantomeno o diminuirli quindi può essere definità come la sintesi di tutte le operazioni che si mettono in pratica per la difesa dei sistemi digitali e non.

La cybersecurity si appoggia su tre principi che possono essere racchiusi nell'acronimo CIA o CID ovvero confidenzialità con il mondo cyber garantire una integrità ed una disponibilità;

ciò significa che la combinazione delle misure prese a partire da ognuna di questa triade coincide con la modalità dei gestori di rischio ovvero il sunto dei tre principi dell'ITsecurity che porta a configurare un system efficace.

vediamo allora le tre leggi che governano il IT security: "CID"

- **confidenzialità**

Per confidenzialità dei dati informatici si vuole intendere per protezione dei dati durante il loro ciclo di vita ovvero durante la creazione di questi ultimi,il loro immagazzinamento la loro transizione ,diffusione e utilizza da parte di soggetti terzi non autorizzati;

quindi la confidenzialità ha lo scopo di proteggere la riservatezza dei dati dell'utente da intenzioni malevoli,le tecniche che mirano alla garanzia di confidenzialitàdei dati sfruttano di norma gli attachi informatici come i social-engineering.

il centro di questo corpo è l'autorizzazione all'accesso dei dati personali,per eliminare questa problematica l'ITsecurity adopera la cifratura a due fattori 2FA.

- **Garanzia dell'integrità**

per integrità dei dati si vuole intendereil mantenimento all'incolumità dei dati del cliente e alla

loro salvaguardia,ovvero alla protezione da ogni tipo di manomissione come la stessa modifica del testo o perduta di perte di esso letteralmente si fa riferimento alla capacità di antenere originali i propri dati e le risorse che offre quel sito affichè non vengano cancellate o modificate per gagantire questa integrità del dato come ad esempio evitare la modifica di un dato raster "dato che occorre al SIT di leggere la descrizione e garatire l'integrità dell'immagine e descrizione al livello paleontologico/vulcanologico/sedimentario di quel luogo".

E' necessario attivare delle policy authenticator che siano in grado di monitorare gli accessi al dato raster e gli stessi tentativi di accesso. Ma non solo altre soluzioni sono volte a garantire questo principio sono:

I. i sistemi di intrusion detection (kali linux : password attacks Hydra)

II. e la stessa restrizione di accesso (captcha)

III. e il livello di formazione degli utenti

- # disponibilità

L'indice di disponibilità è un indice del diritto all'accesso alle risorse agli utenti in merito ad una richiesta.

in sostanza!!!

impedire che durante un intervallo di tempo definito avvenga interruzioni di servizio

garantire che le risorse infrastrutturali sono pronte per la coretta erogazione di quanto richiesto e al tel proposito deve essere gantita oltre alla protezione dello stesso sftware o della stessa paggina anche la continuità del servizio per un tempo predeterminato. Possiamo citare alcune minacce che minano la disponibilità delle informazioni;

1. attacchi DOS
2. DDos attacck
3. attacchi ransomware(attacchi virali che prendono il controllo del PC in primis e impediscono di accdere al file o alla pagina web)

per le contromisure possiamo citare o meglio adottare:

I. backup dati

II. piani disaster recovery

III. soluzioni firewall

I tre principi dell'IT security in poche parole possono dimostrare che adoperando mezzi semplici ma efficaci che è l'utente stesso a dover proteggere in primis i propri dispositivi e la tutela della privacy disponendo di app e software "malwarebite" deputati a garantire l'incolumità dei dati e mantenere alto il livello di sicurezza.