CYBERSECURITY

Cosa è la Cybersec, dove opera
cosa bisogna sapere.

La definizione di Cybersec

La Cyberserc è quella branca dell’informatica che si occupa di proteggere dati e sistemi da attacchi digitali.

La triade della SEC, ovvero, cosa deve assicurare la Security agli utenti

Confidenzialità

E’ la possibilità di accedere al dato in modo autorizzato tagliando fuori nello stesso tempo, chi non lo è.

Integrità

Assicura che il dato sia esattamente quello richiesto, che non sia stato modificato e che sia completo.

Disponibilità

è la possibilità di accedere al dato ogni volta che ve ne è necessità

ENISA

- L'European Union Agency for Cybersecurity è un punto di riferimento per tutti i professionisti del settore.

https://www.enisa.europa.eu/

La Triade in pratica

Confidenzialità

Informazioni Personali ed informazioni sanitarie sono la parte più sensibile da progeggere.

Integrità

bisogna evitare che un dato, possa essere modificato, ad esempio una cartella clinica

Disponibilità

introduce il concetto di “Criticità” nella necessità di accesso al dato.

Autenticazione

MFA

Ciò che conosci

Password o gesto

Ciò sei

retina, impronta digitale, viso

Ciò possiedi

token, smart card

Powershell per i metadati di un file

```
$file = "C:\percorso\del\file\nomefile.txt"
$hashProvider =
[System.Security.Cryptography.HashAlgorithm]::Create("SHA256")

Write-Host "Data di creazione: " (Get-Item $file).CreationTime
Write-Host "Data di modifica: " (Get-Item $file).LastWriteTime
Write-Host "Hash: "
([System.BitConverter]::ToString($hashProvider.ComputeHash([System.IO.
File]::ReadAllBytes($file))).Replace("-",""))
```

```
$file = "c:\users\virtual\desktop\prova.txt"
$outputFile =
"c:\users\virtual\desktop\prova_metadata.txt"

$shell = New-Object -ComObject Shell.Application
$folder = $shell.Namespace((Get-Item
$file).DirectoryName)
$fileItem = $folder.ParseName((Get-Item $file).Name)

$output = @()
for ($i = 0; $i -le 266; $i++) {
    $name = $folder.GetDetailsOf($null, $i)
    $value = $folder.GetDetailsOf($fileItem, $i)

    if ($value) {
        $output += "$name=$value"
    }
}

$output | Out-File $outputFile
```

Disponibilità del dato

1. Backup: la creazione di una copia dei dati e la conservazione di tale copia in un luogo sicuro.
2. Replica dei dati: la copia di dati su più dispositivi o server in modo che se uno diventa inaccessibile, ci sono altre copie disponibili.
3. Failover: il passaggio automatico ad una replica dei dati o ad un altro sistema in caso di malfunzionamento del sistema primario.
4. Ridondanza: l'uso di hardware e software di backup, che permettono di continuare ad accedere ai dati anche in caso di guasti.
5. Bilanciamento del carico: la distribuzione del traffico dei dati su più server o dispositivi in modo che nessuno di essi venga sovraccaricato.
6. Monitoraggio continuo: il monitoraggio costante delle prestazioni del sistema per identificare eventuali problemi e risolverli prima che causino interruzioni.
7. Protezione contro le minacce esterne: l'utilizzo di misure di sicurezza, come firewall, antivirus e sicurezza dei dati, per impedire attacchi esterni e prevenire la perdita di dati.
8. Aggiornamenti regolari: l'aggiornamento regolare del software e dell'hardware utilizzati per assicurare che siano in grado di proteggere i dati in modo adeguato.
9. Disaster Recovery: la preparazione di un piano di recupero di emergenza per affrontare situazioni come incendi, alluvioni o altri disastri naturali che potrebbero mettere a rischio i dati.

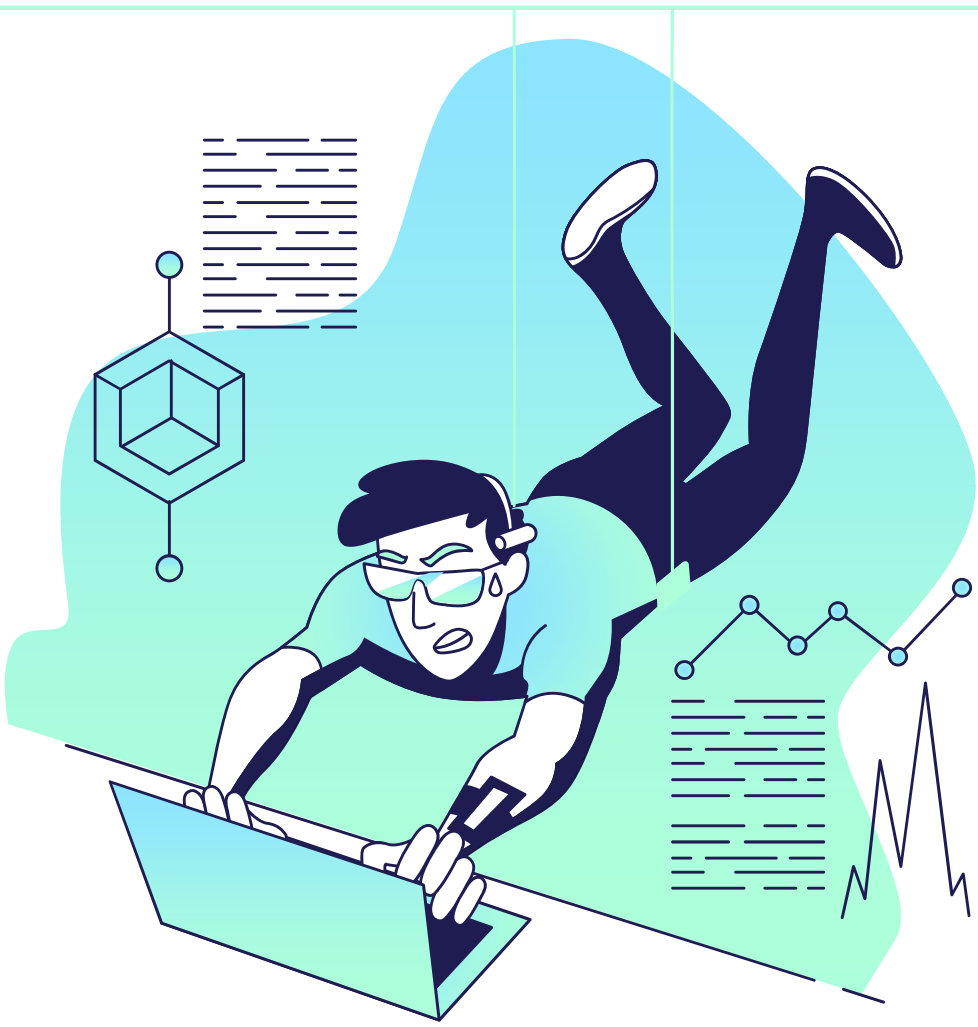
NB: Queste sono solo le principali modalità!

Privacy e GDPR

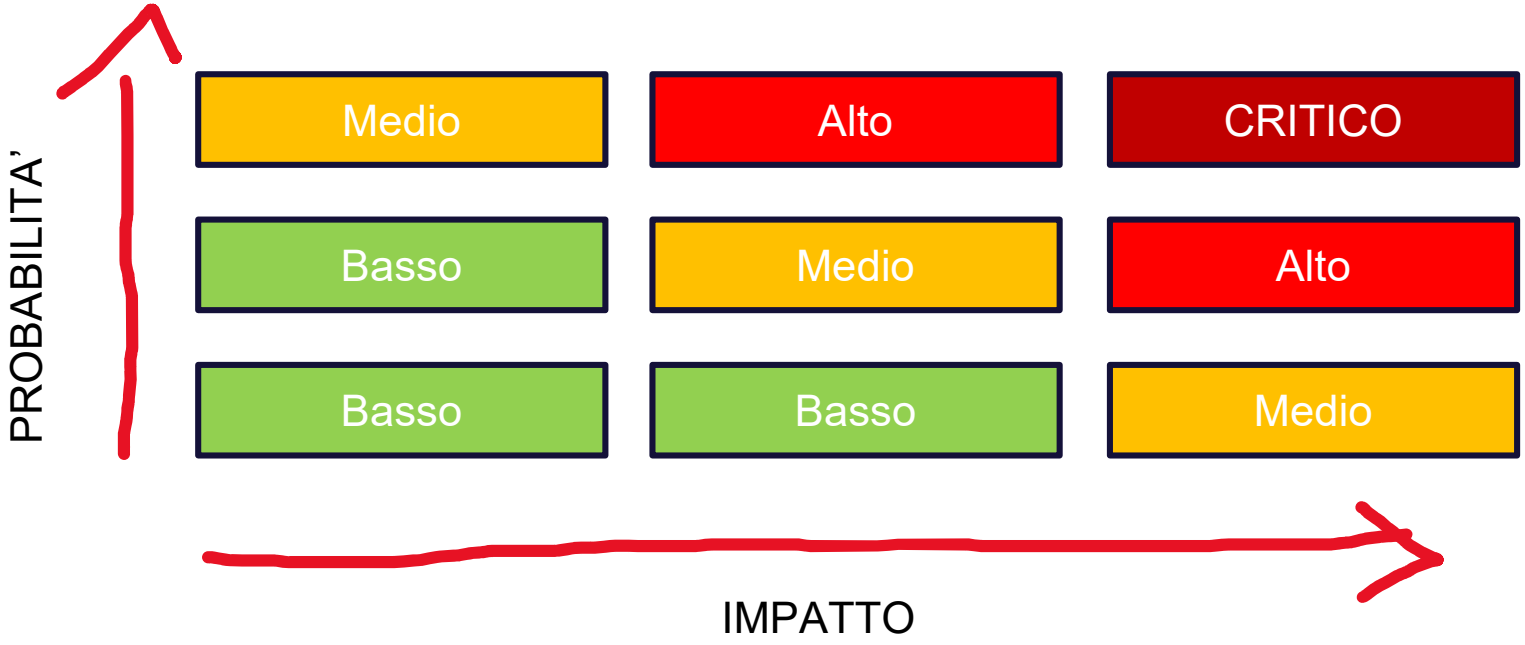
https://gdpr.eu/

Analisi e gestione dei rischi

L’analisi dei rischi è una componente importantissima del mondo della Cybersec perchè ci guida nelle scelte che dovremo fare per proteggere gli asset. Dovremmo quindi vagliare ogni possibile vulnerabilità che può essere sfruttata da eventuali threat.



La matrice del rischio



Siete diventati un target

siete quindi a rischio di minaccia (threat)

01

I vostri dati sono esposti perchè non avete le protezioni adeguate

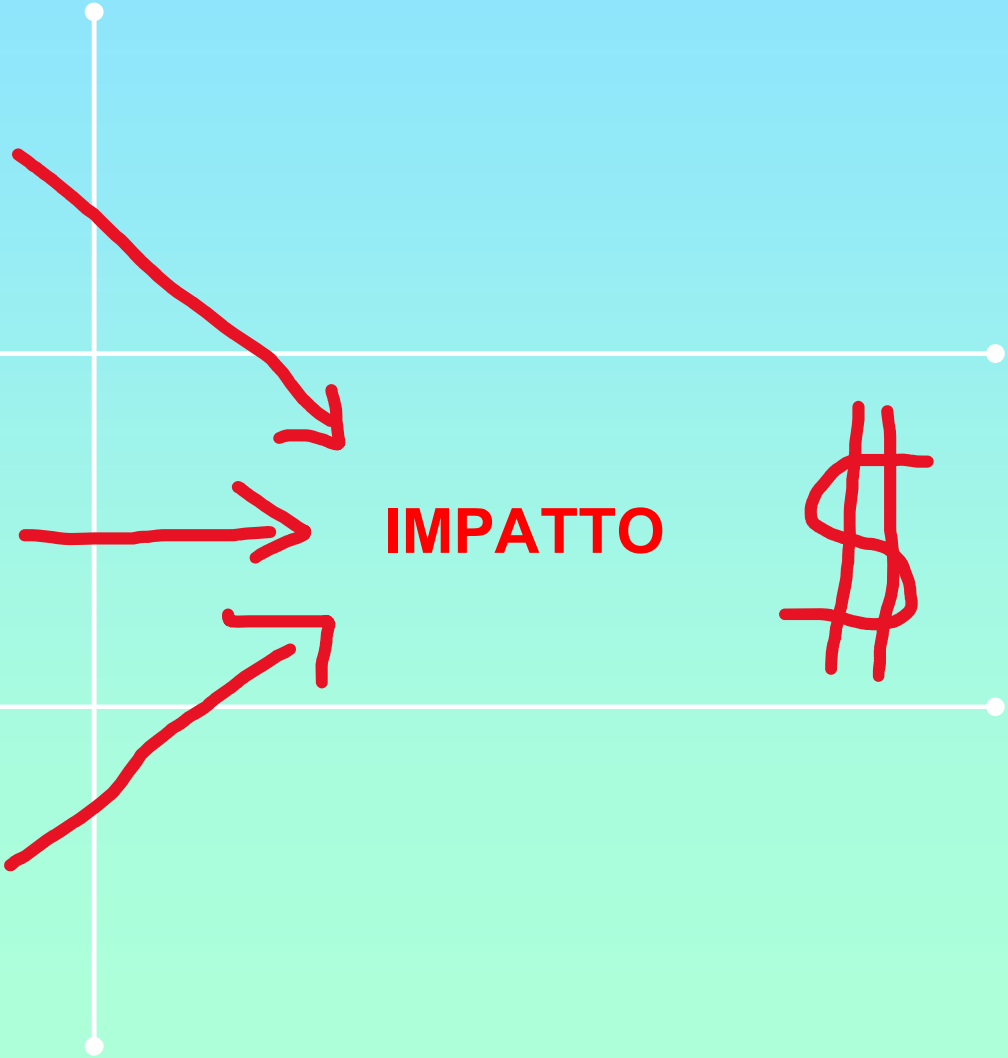
avete delle vulnerabilità

02

La vostra esposizione è molto elevata

la probabilità che l'evento accada è molto maggiore

03



Le 4 modalità di gestione del rischio

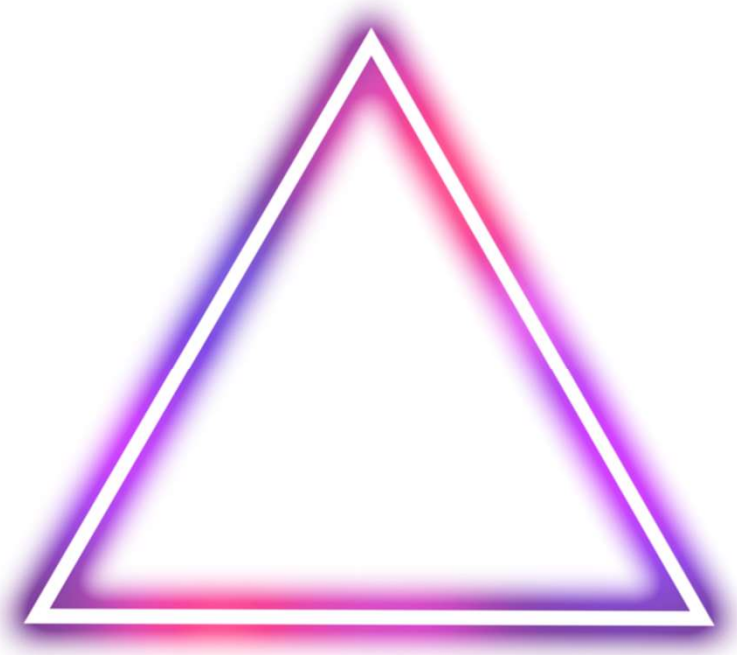
Eliminazione: quando si pongono i campo fattori per eliminare totalmente un rischio associato.

Accettazione: il rischio viene accettato per interno e non si attua nessuna misura per mitigarlo.

Mitigazione: è la più comune delle modalità. Si cerca di fare il possibile per ridurre eventuali rischi.

Trasferimento: il rischio viene interamente trasferito a terzi in modo da non avere più responsabilità.

I Controlli di Sicurezza



I controlli di sicurezza sono quei meccanismi che messi in atto per proteggere un asset, assicurano confidenzialità, disponibilità ed integrità ed abbassano il rischio al giusto livello di accettabilità a seconda della modalità sceltà.

I controlli di sicurezza in minutes

Fisici

- sono quei controlli che proteggono fisicamente l'accesso al dato. Badge, cancelli, armadi rack ecc.

Tecnici

- o «logici» sono quei controlli che vengono implementati a livello rete, sistemi e che allertano in caso di violazioni.

Amministrativi

- policy aziendali, autorizzazioni del personale, privilegi di accesso al dato (least privileges) ecc.

La GOVERNANCE

Policy

una gestione che comprende procedure e regole ed è il documento che sancisce come operare all'iterno di una organizzazione

Regolamenti

dettati da leggi che spesso portano a multe se non rispettati (GDPR)

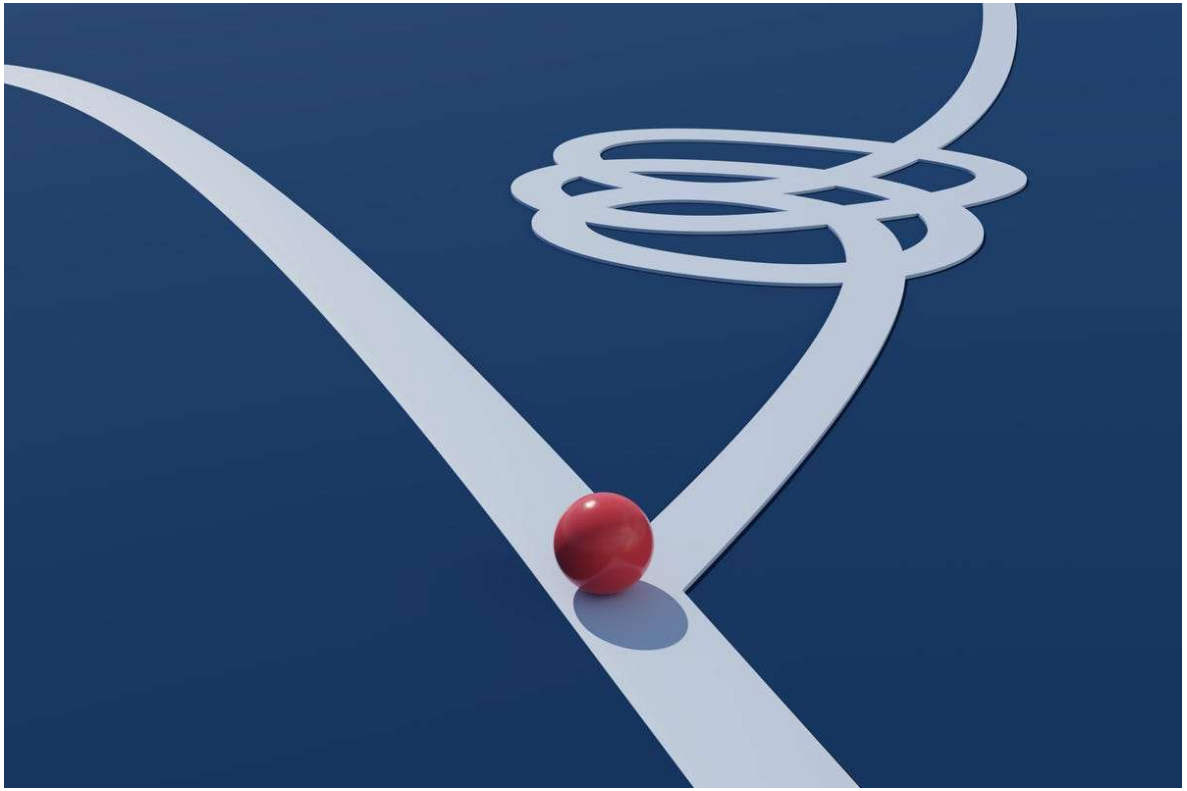
Procedura

un insieme di processi per eseguire un determinato task

Standard

un insieme di policies e procedure universalmente riconosciuto (ISO)

ETICA



- PROTEZIONE
- RISPETTO
- DIVULGAZIONE
- FORMAZIONE CONTINUA
- ONESTA’
- PRINCIPI
- INTEGRITA’
- OBIETTIVITA’
- NON CONDIZIONABILITA’

Assicurare la continuità del dato

Disaster Recovery

E’ la possibilità di recuperare i dati dopo un evento disastroso. Incendio, Allagamento, Terremoto.

Business Continuity

E’ la capacità di assicurare che il dato sia sempre disponibile (HA, Fault Tolerance, Delocalizzazione).

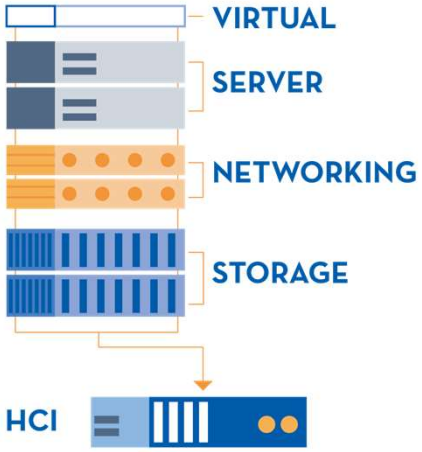
Incident Response

E’ quel piano di difesa permette di reagire ad un «incident» mantenendo la disponibilità del dato.

Disaster Recovery

Il DR è l'ultima spiaggia di recupero del dato. Serve in caso un disastro naturale od umano intervenga a distruggere i nostri dati. Il backup del DR dovrebbe essere almeno a 300KM di distanza dal dato principale, dovrebbe essere immutabile e seguire la filosofia del 3-2-1.
Molte volte il DR viene eseguito con dischi o nas esterni che vengono portati fuori dalla struttura.
Il tempo di ripristino è sempre molto elevato.

Business Continuity



La BC di base ha almeno 2 nodi in replica sincrona. Possiamo anche parlare di nodi a replica asincrona volendo. La ridondanza è la chiave della BC in modo che nulla possa essere un singolo punto di fallimento.

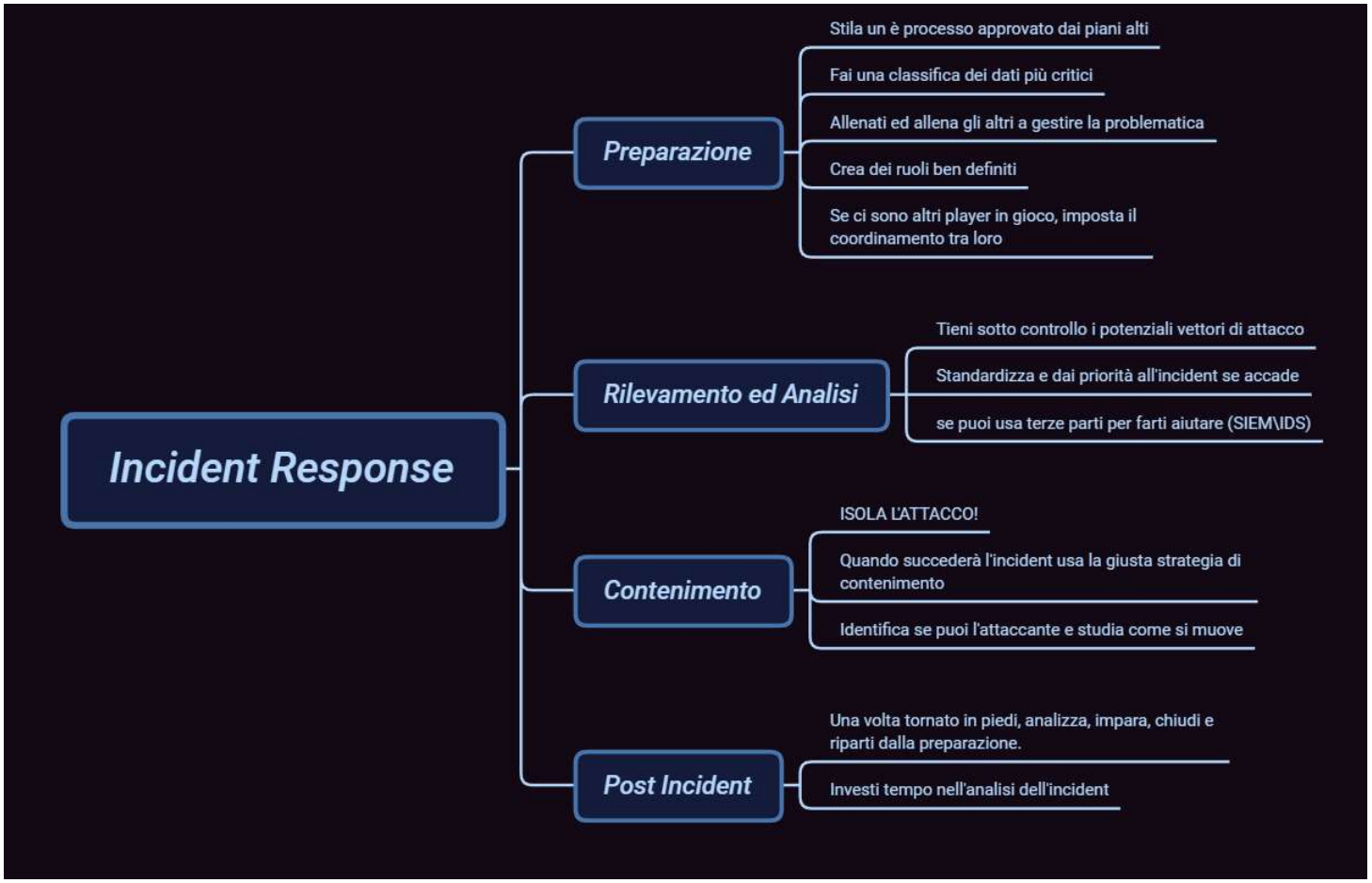
La BC è un insieme di step che assicura che il dato sia sempre disponibile e che quindi il business possa continuare. L'ultima frontiera della BC è l'HyperConvergenza che ha accorpato tutti i fattori precedenti in un un'unica appliance ridondata. Nutanix,Sangfor,Syneto,Simplivity ecc sono esempi di HCI.

Incident Response

Può succedere che nonostante tutti i nostri sforzi, si verifichi un «incident». Un Incident viene identificato con un attacco dall'esterno, una cancellazione del dato, uno zeroday, insomma qualsiasi fattore che comprometta la triade degli assett.

Tutti i team e chi opera nel campo della Cybersec, dovrebbero essere in grado almeno di essere preparati alla gestione di un incident. In realtà, lo stress, le conoscenze necessarie ed i costi da mettere in campo prima che questo accada, fanno sì che molti incident peggiorino poi nel corso del tempo.
Un attacco ransomware è il classico tipo di incident che metterà a dura prova le capacità degli IT che dovranno gestirlo.
La regola più importante è «Sii sempre pronto!» come i boyscouts.

Le fasi di gestione dell'incident in minutes



I controlli di Accesso

I controlli di accesso, assicurano una protezione dell'asset in modo che solo chi è preposto ad utilizzarlo, possa farlo.

I controlli di Accesso sono di tre tipi:

- Fisici
- Logici
- Amministrativi

Least Privileges e le BP di gestione

La segregazione dei ruoli (least privileges) serve per gestire i vari compiti e permessi di accesso ai dati.
Gli utenti possono essere divisi in “amministratori” e semplici “users”
Per tutti gli utenti adrebbe attivato un LOG (non è automatico) sia sul login che sulle modifiche ai vari files.

Gli utenti dei Sysadmin e degli IT interni NON DEVONO essere utenti con accesso a qualsiasi cosa. Quello deve essere gestito da super accounts in maniera indipendente.

Password Length	Numerical 0-9	Upper & Lower case a-Z	Numerical Upper & Lower case 0-9 a-Z	Numerical Upper & Lower case Special characters 0-9 a-Z %$
1	instantly	instantly	instantly	instantly
2	instantly	instantly	instantly	instantly
3	instantly	instantly	instantly	instantly
4	instantly	instantly	instantly	instantly
5	instantly	instantly	instantly	instantly
6	instantly	instantly	instantly	20 sec
7	instantly	2 sec	6 sec	49 min
8	instantly	1 min	6 min	5 days
9	instantly	1 hr	6 hr	2 years
10	instantly	3 days	15 days	330 years
11	instantly	138 days	3 years	50k years
12	2 sec	20 years	162 years	8m years
13	16 sec	1k years	10k years	1bn years
14	3 min	53k years	622k years	176bn years
15	26 min	3m years	39m years	27tn years
16	4 hr	143m years	2bn years	4qdn years
17	2 days	7bn years	148bn years	619qdn years
18	18 days	388bn years	9tn years	94qtn years
19	183 days	20tn years	570tn years	14sxn years
20	5 years	1qdn years	35qdn years	2sptn years

I «tempi della password»

Per craccare una password servono ad oggi, 5 giorni con la classica 8 caratteri.

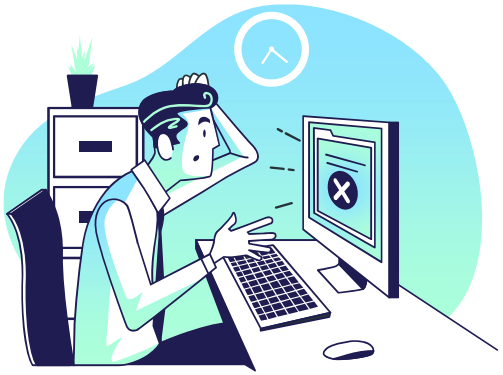
La Sicurezza Fisica

Telecamere\DVR

Sensori di accesso

Sensori Fumo\Allagamento

Le Autorizzazioni



Copia dei Profili

Spesso si tende a copiare un profilo di una persona che ha lasciato l'azienda o che è presente perchè dobbiamo dare le stesse policy del collega. La procedura è molto rischiosa.

L'accesso Logico

L'accesso logico ed i permessi che vengono dai ai files sono di due tipi.

Discrezionari sono prerogativa del proprietario

Obbligatori sono prerogativa dell'amministratore

LE Minacce (Threads) e la difesa dalle stesse

Ransomware

Dati in ostaggio e pericolo di esfiltrazione sono il loro pane.

Malware

Un precursore del ransomware o tante volte un collector di informazioni

Basista (insider threath)

Se pagato abbastanza, chiunque può diventare una minaccia..

Man in the Middle

“Stare in Mezzo” è il suo comportamento preferito

Dos/DDOS

Quando non si può fare di meglio, si affossa il servizio

Spoofing\Phishing

Impersonare qualcosa o qualcuno è spesso il modo principe per entrargli in casa

Best Practise di protezione di un dato

Updates

I sistemi devono essere aggiornati sempre e così i firmware degli apparati di rete

Firewall\UTM

Sono pressochè obbligatori su una rete, vanno acquistati coi servizi attivi

Porte e Protocolli chiusi

la regola è: se non serve non deve esserci

IDS

I sistemi IDS sono spesso costosi ma utilissimi se la rete è molto distribuita

EDR\XDR

L'erede dell'Antivirus deve essere presente e gestito

Inventario Aggiornato

Last but not least, sapere sempre cosa avete in casa vostra

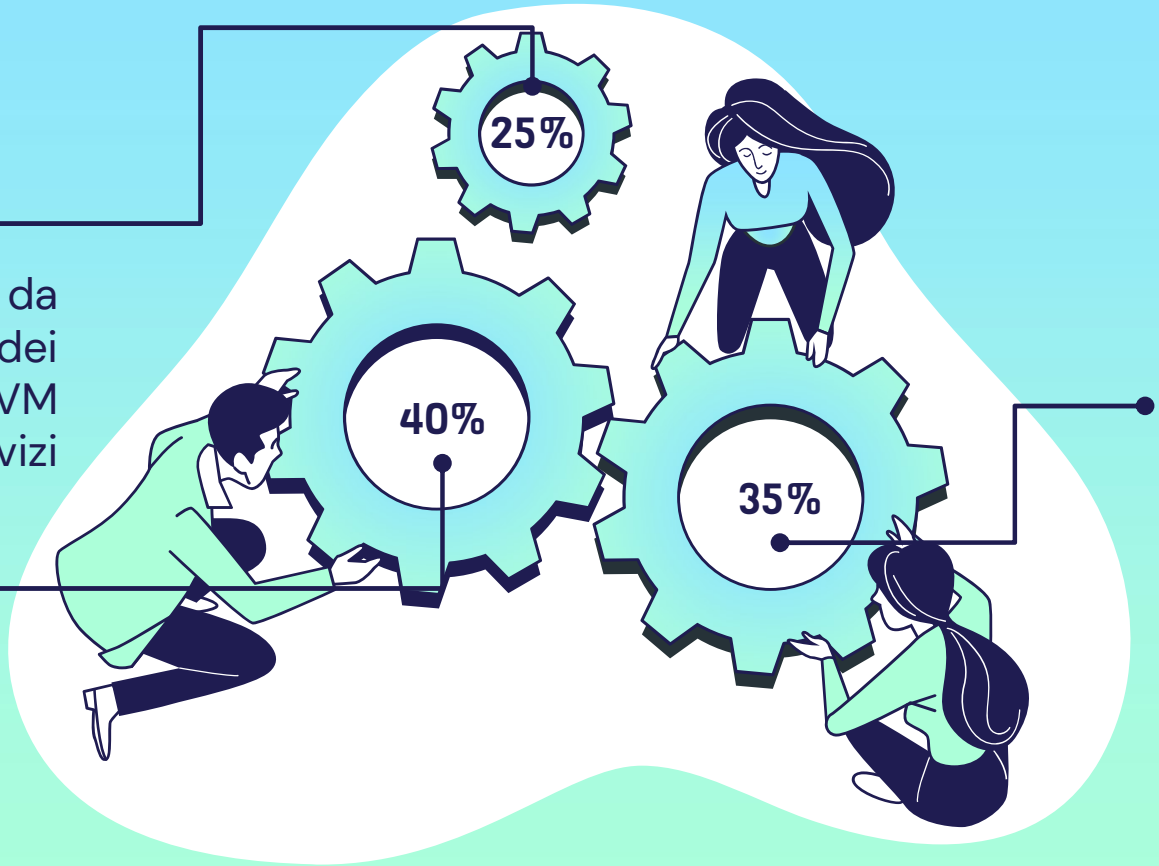
I tipi di reti da proteggere

Cloud

La rete è ospitata da altri, voi fruite dei server o delle VM oppure dei servizi

On Premise

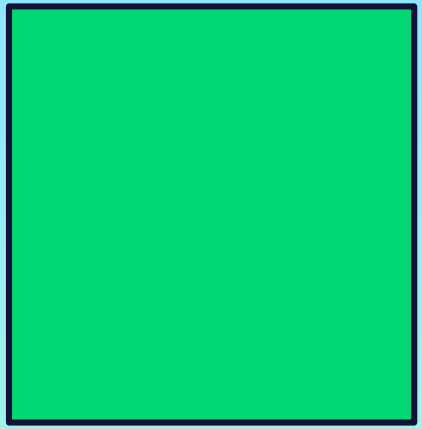
Reti gestite totalmente di proprietà



Hybrid

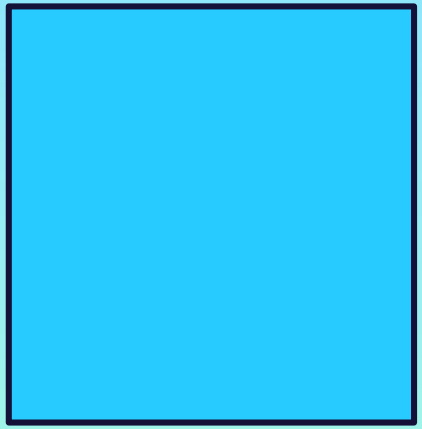
Insieme tra le reti in cloud ed onpremise (il futuro a mio avviso).

I tipi di piattaforme che può darvi il cloud



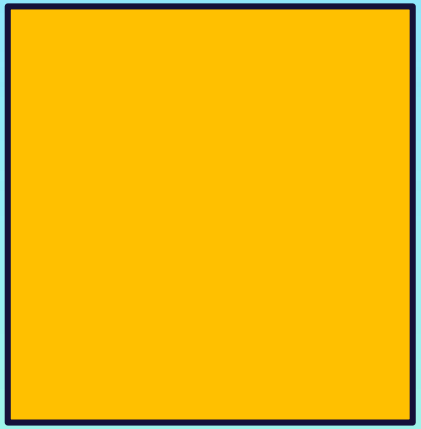
SaaS

Software as a service in pratica significa che vi viene dato un software da usare di cui non siete proprietari, esempio: Office 365\Gapps



PaaS

Platform as a service ti mette a disposizione macchine per calcolo, sviluppo, crm ecc

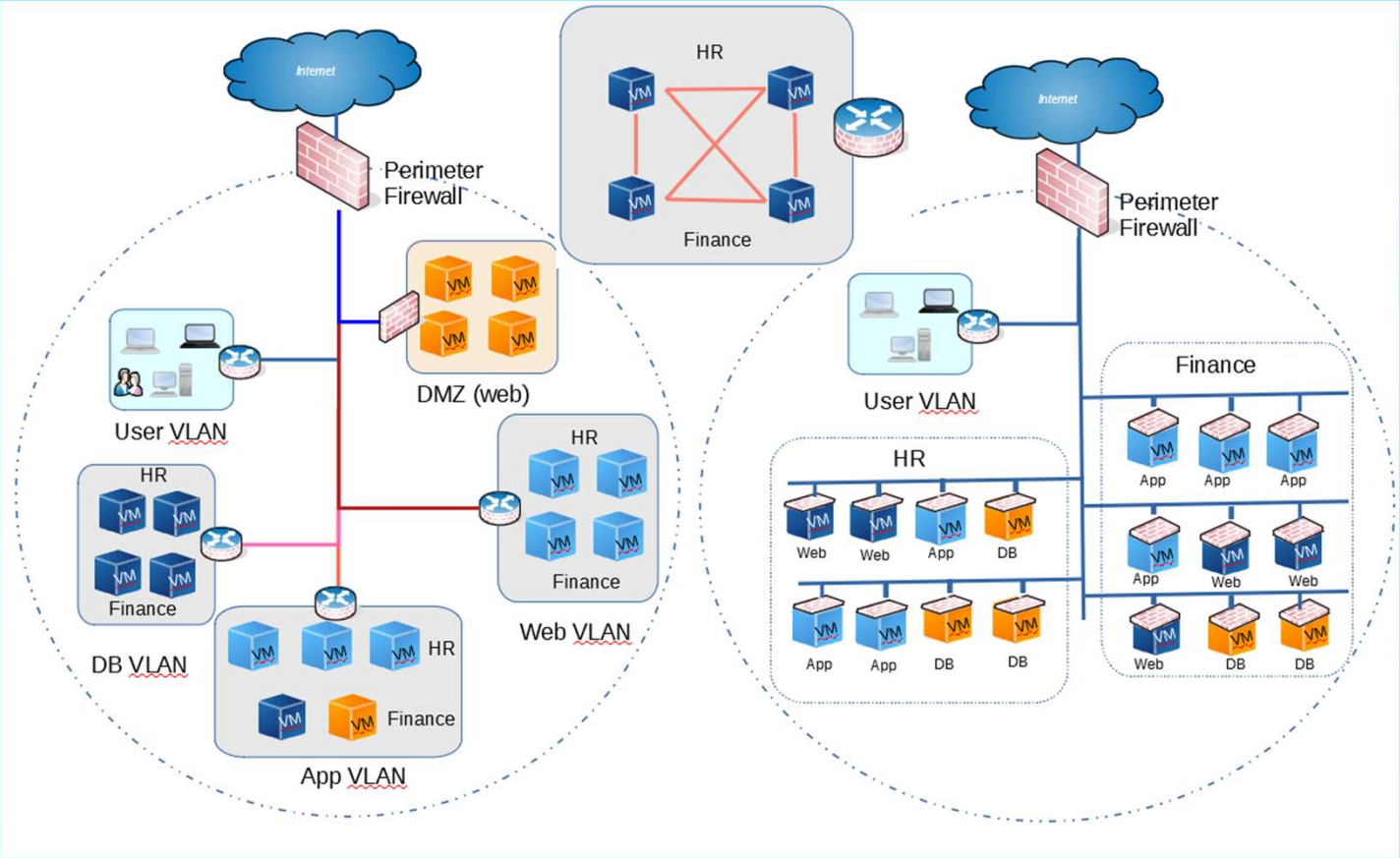


IaaS

Infrastructure As a Service
Ti vengono dati server e reti in cloud da gestire come preferisci.

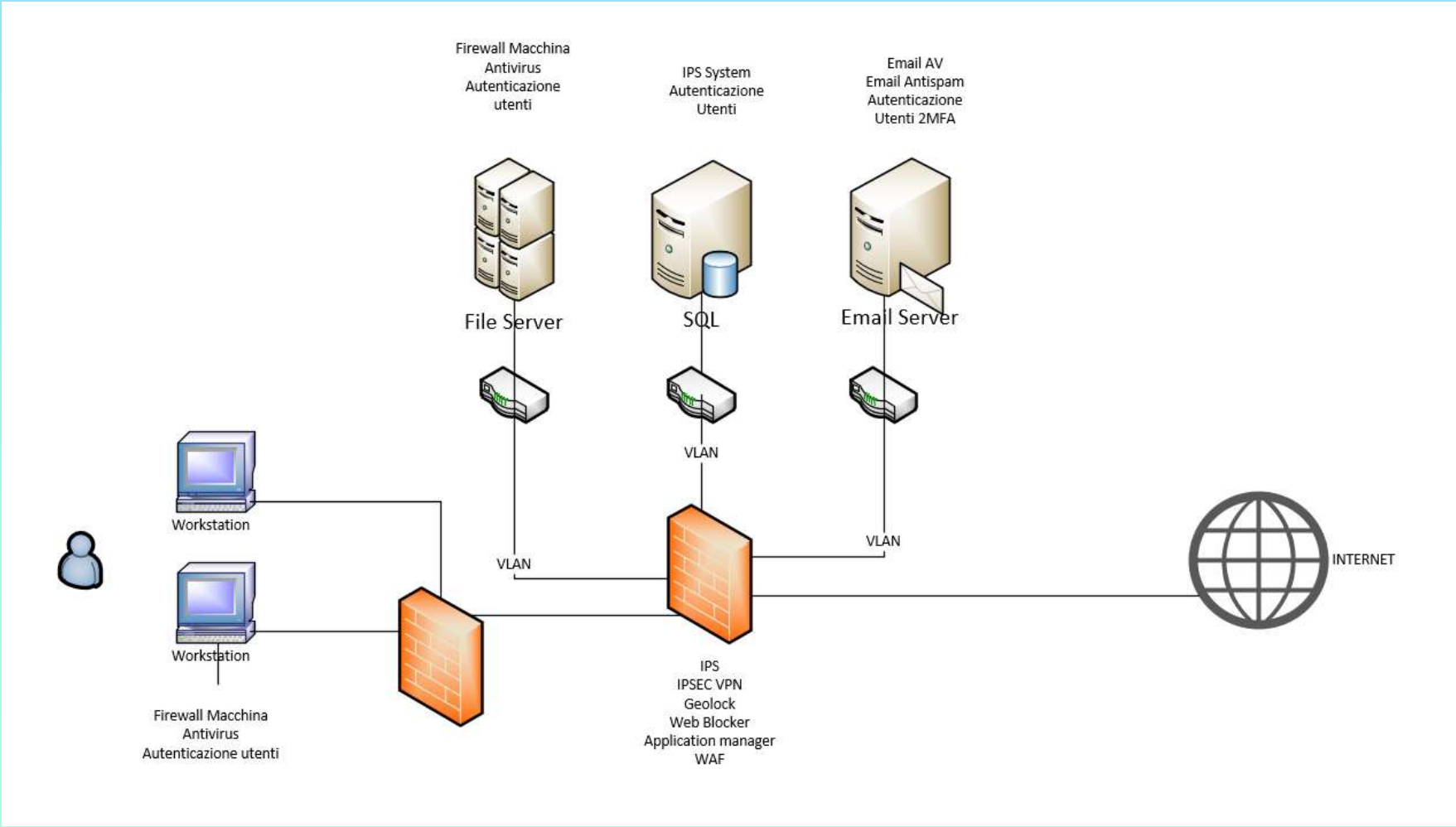
NB:
In qualunque scelta, ci sarà uno SLA (service level agreement)

ZERO TRUST e la Microsegmentazione

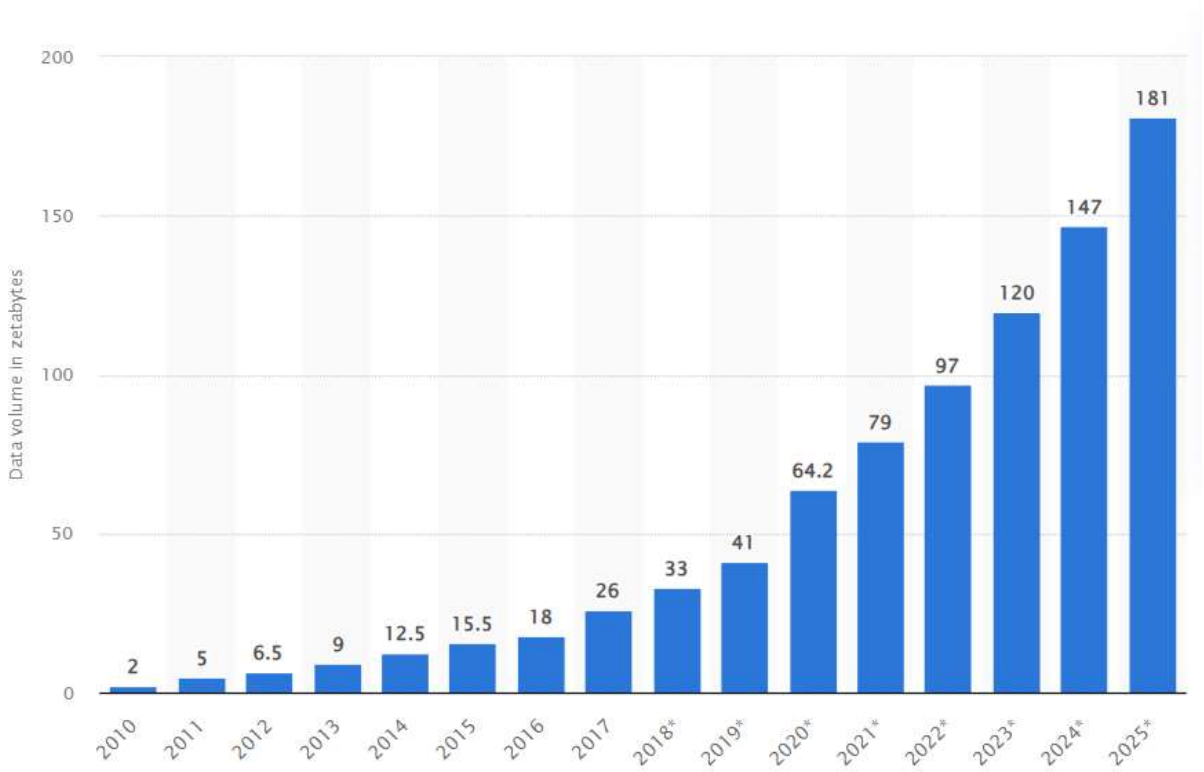


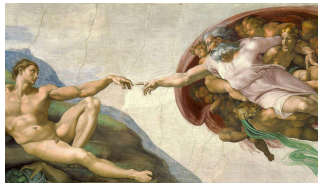
Da qualche anno è entrata in uso la modalità «Zero Trust» significa ammettere che ogni punto ha potenziale fallimento e quindi gestire ogni nodo in autonomia.
Microsegmentare la rete in modo da avere più facilità nella soluzione delle problematiche.

Implementazioni Protezioni Microsegmentazione



I dati e la loro vita





CREAZIONE

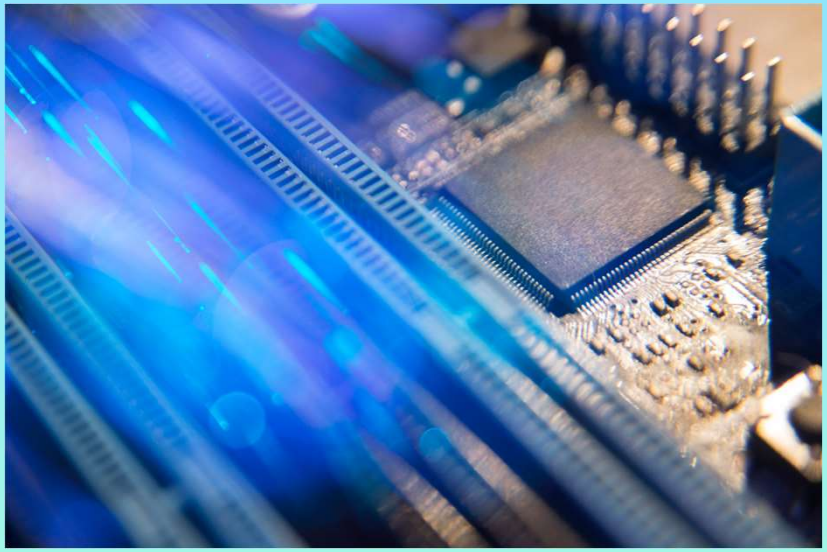
STORAGE

USO

ARCHIVIAZIONE

DISTRUZIONE

La crittografia



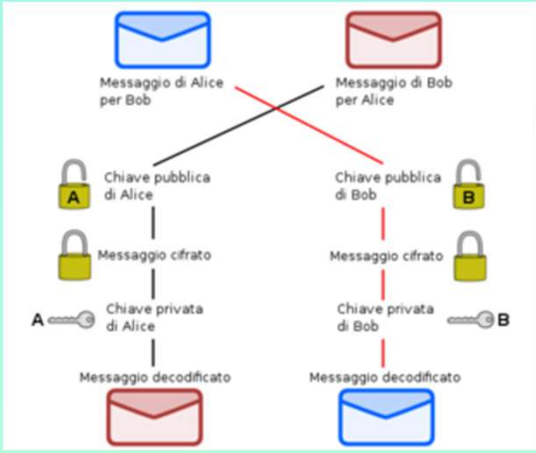
CRITTOGRAFIA SIMMETRICA

è un tipo di crittografia in cui la chiave di crittazione e decrittazione è la stessa.

Il tutto è gestito da un algortimo.

AES è ad oggi il “portavoce” della crittografia simmetrica.

CRITTOGRAFIA ASIMMETRICA



è un tipo di crittografia in cui c’è una chiave distribuita (Pubblica) ed una Privata.

Il messaggio può essere decriptato solo con la chiave privata.

RSA è l’esempio più conosciuto

Formazione, Training ed Awareness

Formazione

Voi potrete coprire tutto, ma non la sicurezza delle persone.

Training

Per tutta la vostra vita, dovrete studiare ed aggiornarvi

Awareness

La consapevolezza della sicurezza e del potenziale dovrà essere sempre presente

Percorso di studi

Studia da solo

se puoi e se ce la fai, formati in autonomia.

Se non ce la fai, scegli bene i tuoi tutor.

Certificati

Mira a 2 o 3 certificazioni standard e portale a casa. Compra gli esami e dalli in autonomia.

Evolvi

Sali di livello, non mollare e continua ad investire in te stesso.