

1 Cyber Kill Chain / Attacchi e Malware	1 - 13
2 Autenticazione e gestione degli accessi	13 - 26
3 Gestione e Modelli di rischio	26 - 39
4 Privacy	39 - 40

1 Cybersecurity

Introduzione

La funzione principale della cybersecurity è quella di proteggere i dispositivi che utilizziamo e i servizi a cui accediamo da accessi non autorizzati, danni o abusi. Inoltre si usa anche per prevenire accessi non autorizzati a grandi quantità di dati che salviamo nei dispositivi e online.

Gli elementi fondamentali della cybersecurity sono:

- **Confidenzialità**
- **Autenticità**
- **Integrità**
- **Accountability**
- **Disponibilità**
- **Safety** → sistemi progettati e funzionanti in modo sicuro

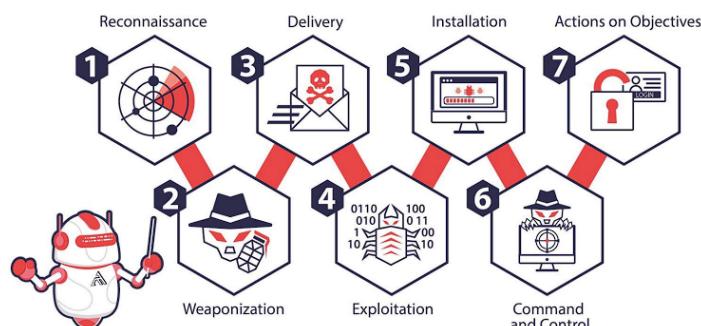
Gli **assets** invece sono qualsiasi cosa che ha valore per un'organizzazione, tra cui persone, dispositivi, sistemi IT, network, software, e tanti altri elementi a cui si può attribuire valore.

Tra i concetti chiave della cybersecurity troviamo:

- **Vulnerabilità:** un bug/difetto/debolezza di un'applicazione/sistema/servizio che potrebbe portare a un fallimento delle proprietà.
- **Cyber Threat:** qualsiasi minaccia o evento che possa impattare avversamente sulle operazioni di un'organizzazione.
- **Attacco:** la realizzazione di un threat che impatta su confidenzialità/integrità/accountability/disponibilità di una risorsa.
- **Threat Actor:** la persona o gruppo che cerca di sfruttare vulnerabilità di un sistema.
- **Rischio:** il livello di impatto sulle operazioni, gli asset dell'organizzazione, sugli individui, su altre organizzazioni o sulla reputazione, derivante dal funzionamento di un sistema informativo, dato l'impatto potenziale di una minaccia e la probabilità che questa si verifichi.
- **Security Controls:** gestione e controlli tecnici prescritti affinché un sistema protegga confidenzialità, integrità, disponibilità, i suoi componenti, processi e dati.

Cyber Kill Chain

È la sequenza di fasi che si attraversa quando si vuole eseguire un attacco informatico.



- **reconnaissance:** fase in cui si selezionano e raccolgono da fonti pubbliche le informazioni riguardanti il target(es email) può essere:
 - **attiva:** si raccolgono informazioni interagendo con il target(nmap, port scanning).
 - **passivo:** si raccolgono informazioni senza interagire con il target(whois, social media).
- **weaponization:** cerca o crea l'attacco per sfruttare le debolezze(metasploit, aircrack, s.e toolkit).
- **delivery:** si seleziona in che modo trasportare l'exploit(usb, mail, social media).
- **exploitation:** sfruttamento effettivo della debolezza(sql injection, malware, buff overflow).
- **installation:** fase in cui si mantiene la persistenza nell'ambiente(remote access trojan, powershell commands, dll hijacking). Si cerca anche di fare movimento laterale e spostarsi su altre macchine.
- **command & control:** stabilire un canale di comando/controllo(c2) in maniera da poter manipolare la vittima, si apre un two way communication channel
- **actions on objectives:** effettuare azioni per raggiungere l'obiettivo prefissato(furto di credenziali, sovrascrivere o eliminare dati ecc).

TrickBot

TrickBot è un trojan avanzato che si distribuisce principalmente tramite phishing, una volta scaricato inconsciamente aprendo un'immagine per mail, veniva instaurato un canale C2 con cui l'attaccante può mandare trickbot e altri malware che si distribuiscono anche nella rete.

MITRE PREATT\$CK E ATT\$CK MODELS

Sono due modelli forniti da mitre che raccolgono un insieme di tattiche e tecniche che gli attaccanti utilizzano prima e nel mentre di un attacco, ossia nella cyber kill chain.

Possiamo mappare nella cyber kill chain il **pre-attack** nelle fasi di recon e weaponize, mentre **attack** dalla fase di deliver in poi

MITRE PREATT\$CK

Troviamo la pre-att\$ck matrix, dove sono raccolte tutte le tattiche e relative tecniche utilizzate in questa fase, è costruita con colonne di tattiche dove le righe formano le varie tecniche

Ad esempio la tattica **technical information gathering** è il processo con cui si identificano elementi critici che l'attaccante deve conoscere del target per compiere al meglio l'attacco.

Tra le tecniche di questa tattica troviamo **discover target logon/email address format** dove si va a conoscere come sono strutturati i domini di mail di una certa organizzazione

MITRE ATT\$CK

In questo modello invece troviamo tutte le tattiche e tecniche adottata quando si compie l'attacco vero e proprio, quindi troviamo tecniche ad esempio per l'initial access, per la persistenza, per il C2 e l'esfiltrazione.

Mitre Att\$ck matrix

Anche qui le colonne sono le tattiche e le righe sono le tecniche relative a quelle tattiche, dove effettivamente le tattiche non sono altro che quello che l'attaccante spera di ottenere.

Ad esempio nell'ambito della tattica **Initial Access** troviamo la tecnica di **phishing**, ossia si cerca di recuperare informazioni sensibili o prendere controllo di un sistema tramite dei messaggi che ingannano l'attaccato, se questo è mirato viene chiamato **spearphishing**, questo a sua volta ha una sottotecnica, che è lo **spearphishing attachment** dove ad esempio si manda una mail con un allegato malevolo che cerca di recuperare informazioni sensibili o ottenere accesso al sistema, si possono usare eseguibili, pdf, documenti office.

Se si utilizzano network intrusion detection system, email gateways e antivirus, generalmente si riesce a rilevare l'allegato malevolo.

Tattiche e tecniche che usa TrickBot

Vediamo ora le varie tecniche di ATT\$CK e come trickbot le usa nelle varie fasi della cyber killchain:

- **reconnaissance**: usando ad esempio spearphishing attachment o spearphishing link
- **execution**: scheduled task, malicious js file.
- **persistence**: si cerca di mantenere l'accesso, trickbot ad esempio crea un servizio che parte quando la macchina si accende
- **privilege-escalation**: cerca di ottenere privilegi maggiori
- **defense-evasion**: si cerca di raggirare le difese, tra le tecniche ci sono l'offuscamento, cifratura codice malware, disattivare windows defender, ecc
- **credential-access**:
- **discovery**
- **lateral movement**
- **collection**:
- **command and control**
- **exfiltration**
- **impact**

Chi c'è dietro gli ultimi attacchi?

Troviamo attaccanti cybercriminali, ma anche finanziati dallo stato e hactivisti.

Le origini principali di quest'ultimi sono **Russia e Cina**, mentre gli obiettivi principali sono gli stati uniti seguiti dal regno unito, tra le industrie invece più colpite troviamo il governo, servizi finanziari e tecnologia.

I **cyber criminali** sono interessati in profitti illegali e gli attacchi tipici compiuti sono: **ransomware**, **infostealers(raccoon stealer)** e **proxyjacking(avrecon)**, riguardante quest'ultimo sappiamo che è una tipologia di attacco che sfrutta l'utilizzo di servizi proxyware che consentono agli utenti di guadagnare condividendo la propria connessione Internet con altri. Gli attaccanti sfruttano queste piattaforme per monetizzare la larghezza di banda Internet delle vittime

Ci sono poi i **nation states hacker**, i quali interessi principali sono l'intelligence, sabotaggio e spionaggio. Tra gli attacchi tipici che eseguono troviamo: attacchi a infrastrutture critiche, wipers e DDoS.

Ci sono infine gli **hacktivisti** motivati da visioni politiche, credo religiosi/sociali o ideologie terroristiche, tra i tipici attacchi che eseguono troviamo: DDos, data breach o leaks, data wipers. Tra i gruppi più famosi troviamo Anonymous, GhostSec, KillNet

Come operano gli attori?

Una tecnica diffusa è quella di utilizzare l'**attack as a service**, ossia in cambio di una fee affittano l'attacco come se fosse un qualsiasi servizio.

Si compromettono anche i device di rete per l'accesso iniziale, ad esempio, Shodan, Censys, Kamerka, sono utilizzati per trovare dispositivi esposti all'internet, moltissimi router o ip camera sono spesso compromesse usando le credenziali di default o debolissime.

Si utilizzano ovviamente offensive security tools come può essere metasploit.

C'è anche l'utilizzo dei **living off the land binaries**, ossia l'utilizzo di elementi proprietari, come ad esempio processi windows per nascondere malware

↳ macro di word malevole

Tipologie di Malware

Il **malware** (malicious software) è un software o firmware che esegue un processo non autorizzato che porta ad avere un impatto su **confidenzialità, integrità o disponibilità di un sistema**.

I sistemi vengono infettati da questi in varie maniere come possono essere:

- **accesso diretto al sistema** → disco infetto/usb infetta.
- **Ingegneria Sociale**
- **Phishing** → spearphishing o whalephishing
- **visitare un sito malevolo**

Il **virus** è in grado di replicare se stesso e ha bisogno di un'azione umana per poter eseguire. Può infastidire gli utenti infettati con modifiche alle loro macchine e può ovviamente essere trovato dagli antivirus.

Virus

Ci sono diverse categorie di virus: **Macro** (sfruttano macro nei documenti), **Polymorphic** (modificano la loro firma ogni volta che si diffondono), **Companion**. (si maschera da file legittimo presente sul pc)
esempio explorer.exe

Worms

Sono simili ai virus, ma non infettano e non richiedono azioni da parte dell'utente, si spargono per la rete con movimento laterale, sono solitamente più pericolosi di un virus e spesso attaccano i server sfruttando difetti di configurazione.

Key Loggers

Dal nome si può intuire che sono un malware che registra ciò che viene battuto in tastiera, è quasi sempre presente un'operazione di data exfiltration (upload ftp, emailing logs), anche se comunque spesso i dati vengono salvati localmente. Vengono tipicamente utilizzati per **password stealing**.

Trojans

Spesso rappresentano se stessi come un software utile, creano una backdoor da dove gli hacker controllano la macchina, spesso scaricati da siti non ufficiali, usati per rubare informazioni personali, files e trasformare la macchina in uno zombie.

RATs(Remote Access Trojan)

Sottocategoria dei trojans, sono progettati per permettere a un attaccante di controllare da remoto la macchina infetta, essenzialmente imposta un C2(command and control channel) con il server dell'attaccante da dove vengono mandati i comandi al RAT e dove i dati che vengono generati da quel comando sono spediti. Spesso hanno dei built-in commands e metodi per nascondere il traffico del C2.

Rootkits

Si installano tra il sistema operativo e l'hardware del computer, usati per assicurare agli hacker il controllo di una macchina infetta e per mascherare la presenza di altri malware nel sistema, alcuni sono impossibili da rimuovere a tale livello che il drive deve essere distrutto.

Droppers/Downloaders

Dal nome i droppers "droppano" un file embedded spesso contenuto in word o excel document per esempio, da soli non sono pericolosi, ma lo è ciò che scancano

Bots

Una volta infettato il sistema, quest'ultimo diventa parte di una botnet controllata dal botmaster, spesso usata per DDoS attack o per distribuire malicious spam, botnet note sono Mirai e Satori.

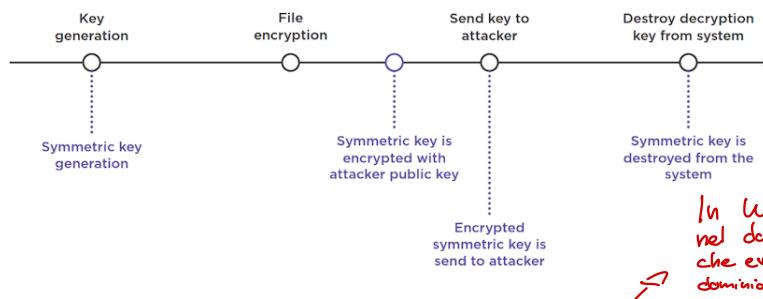
Cripto Miners

Minano criptovalute con la macchina della vittima che vengono poi spedite al wallet dell'attaccante

Ransomware

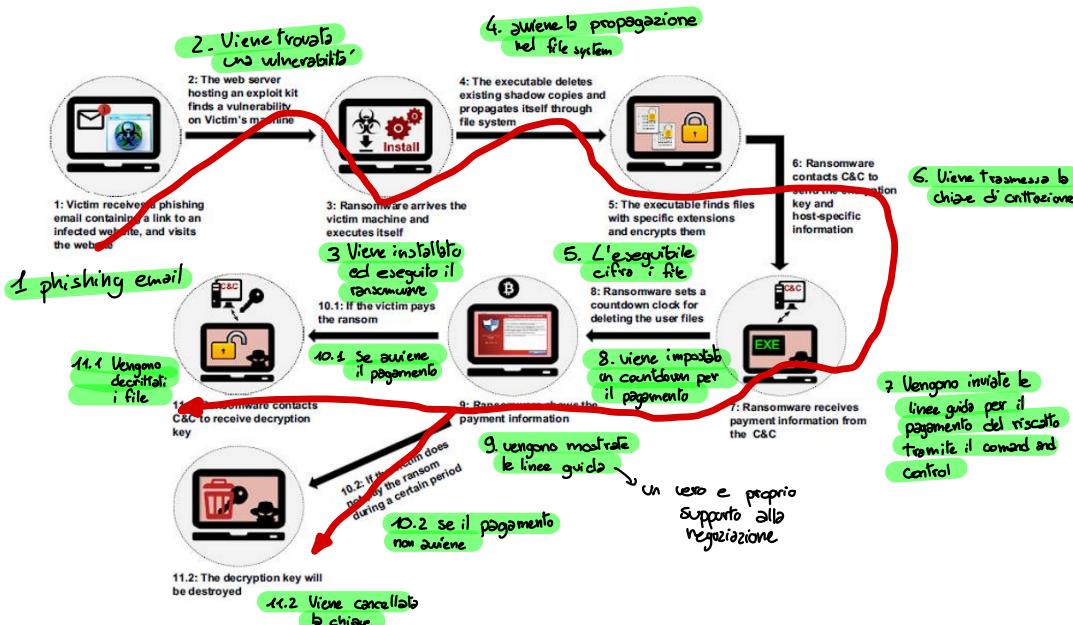
Cifra tutti i file sul sistema quando viene eseguito, mostra un messaggio dove dice alla vittima di pagare per riavere i file decifrati, tipicamente accetta pagamenti in bitcoin.

La chiave usata per cifrare i file è simmetrica ed è a sua volta criptata in chiave asimmetrica in maniera da rendere l'attaccante l'unica persona ad avere la chiave privata



Altro elemento importante quando si parla di ransomware sono i **kill switches**, implementati dagli autori dell'attacco permettono a questi ultimi di evitare di infettare la propria infrastruttura, a volte per errore vengono lasciati nel codice e di conseguenza riconosciuti dai ricercatori che li utilizzano per stoppare il malware.

Cyber Kill Chain di un ransomware:



Si può inoltre parlare di **doppia, tripla o quadrupla estorsione** in base a quanto profitto cerca di fare l'attaccante, ad esempio con la doppia estorsione l'attaccante oltre a cifrare i file, prima li esfiltrano da mettere ancora più pressione della vittima e quindi anche un maggiore costo di riscatto che sicuramente pagherà.

Nuovi target dei ransomware sono anche i cloud, ai quali si recupera accesso iniziale tramite phishing.

Vediamo ora come utilizza le varie tattiche modellate da mitre in PREATT\$CK e ATT\$CK matrix un ransomware:

- **initial access**
 - Phishing: viene mandata una mail malevola con allegati o link malevoli
- **execution**
 - command and scripting interpreter: si sfruttano le cmd interfaces per eseguire comandi o script sul sistema target.
 - user execution: gli attaccanti ingannano l'utente portandolo a eseguire file con codice malevolo.
- **persistence**
 - account manipulation: tecnica che include la modifica di credenziali o permessi
 - scheduled task: si schedula l'esecuzione del malware
 - boot or logon autostart: si fa runnare il programma durante il boot o logon per mantenere persistenza.
- **privilege escalation**
 - exploitation per privilege escalation: gli attaccanti usano vulnerabilità del sw per ottenere più privilegi.
- **defense evasion**
 - system binary proxy execution: usata per eseguire utilities di sistema tramite un proxy malevolo e modificare le chiamate ai binari di sistema legittimi
 - mascheramento
- **credential access**

- brute force
- Os credential dumping: si recuperano le password che vengono salvate dai sistemi operativi in database o file locali per agevolare l'utente.

- **discovery**

- Account discovery: usato per identificare account e credenziali che potrebbero essere usate per exploitation future, può essere fatto interrogando gli OS su informazioni di account locali o di dominio o intercettando e analizzando il traffico di rete.

- **lateral movement**

- pass the hash: si affida agli hash delle password rubate per accedere a sistemi remoti
- remote services: l'attaccante usa servizi remoti come RDP o SMB per runnare comandi sul sistema remoto

- **collection**

- l'avversario cerca di ottenere file di interesse cercando nelle reti condivise o sistema locale

- **command and control**

- exfiltration over C2 channel:
- exfiltration over web service: esfiltrazione dei dati su cloud storage

- **impact**

- data encrypted for impact: gli attaccanti distruggono la disponibilità e integrità del sistema e rete criptando i dati nei sistemi target rendendoli inaccessibili.
- inhibit system recovery: gli attaccanti possono rimuovere o eliminare dati essenziali del sistema operativo e disabilitare i servizi di recovery.

• crittografia a intermittenza: crittata solo una porzione del file, risulta più difficile da rilevare

Come ci si può proteggere dai ransomware?

Non cliccare su link non verificati o scaricare sw da siti untrusted, mantenersi aggiornati e eseguire backup per il recovery.

Come invece rispondiamo a un ransomware?

Disconnettersi dalla rete per evitare movimenti laterali, ransomware decription tool, restore file from backup.

Tra i malware più gettonati su windows troviamo botnet, infostealer, RATs, ransomware.

Tra quelli di linux invece Miner, DDos, Tsunami. → botnet

Per MacOs invece Nukesped(trojan), VSearch(browser hijacking)

Malware Prevention, Detention, Eradication

Per prevenire che il malware venga consegnato: si può adottare mail filtering(blocca e pulisce allegati malevoli), intercettare proxies, internet security gateways, lista di safe browsing.

Per prevenire che il malware venga eseguito: gestione centralizzata dei device così che solo le app trusted dall'azienda possano eseguire, antivirus/antimalware, disattivare autorun di mounted media, limitare o disabilitare macro e ambienti come powershell, usare ultima versione dell'Os, network firewalls.

Per far sì di fermare l'espansione del malware: uso di MFA aut, così che se il virus usa credenziali rubate non riesce a riutilizzarle, isolare piattaforme obsolete, rimuove permessi non necessari.

Sempre per prevenire ciò che può fare il malware è utile anche procedere con backup e mantenerli in posti diversi, se mantenuti in un dispositivo assicurarsi che non sia permanentemente connesso alla rete, scan dei backup da malware prima di fare il restore.

Se invece il malware ha già infettato un'organizzazione: disconnetere subito i device infetti, disattivare wifi e qualsiasi canale della rete, wipe dei dispositivi infetti, connetterli a una rete pulita per installare varie cose, monitorare il traffico di rete e usare antivirus per trovare residui.

Sono un tipo di attacco che è sempre più diffuso.

Social Engineering

Il social Engineering è il processo con il quale si manipolano psicologicamente le persone per fargli compiere delle azioni che divulgano informazioni personali.

Com'è possibile immaginare un punto chiave della cybersecurity sono firewalls, access control e antivirus che servono a proteggere i sistemi dagli attacchi, c'è però un altro elemento non ancora considerato che è in realtà il più debole, l'essere umano, difatti un'azienda può anche spendere milioni di dollari in tali sistemi di prevenzione, ma se un attaccante riesce anche solo a corrompere una persona all'interno dell'organizzazione tutti quei milioni risultano sprecati.

Soltanente dietro agli attacchi di social engineering ci sono cybercriminali, ladri d'identità e artisti dello scam.

Com'è facile immaginare il ciclo di vita di un attacco di questo tipo è:

raccolta di informazioni → stabilire la relazione → exploitation → execution

Tipi di Social Engineering Attacks

Phishing

Si cerca di ottenere informazioni sensibili come credenziali o dettagli della carta di credito mascherandosi come un'entità di fiducia in una comunicazione elettronica.

Speарphishing

È un attacco di phishing ma specificamente indirizzato a un'organizzazione o user, solitamente costruito in maniera da fare arrivare qualche informazione a loro nota o familiare.

Vishing

Attacco dove l'attaccante camuffato da ente apparentemente rispettabile utilizza chiamate telefoniche o servizi di messaggistica vocale per indurre le vittime a rivelare informazioni personali

Whaling

È un attacco di spear phishing rivolto esclusivamente a un dirigente o funzionario di alto livello mascherandosi anche dall'altro lato da altri funzionari o dirigenti.

SMiShing

Conosciuto anche come sms phishing è una forma di phishing che utilizza i telefoni cellulari come piattaforma di attacco per richiedere dati personali come codice fiscale o numero di carta ecc...

Dumpster Diving

Shoulder Surfing

È un attacco dove l'attaccante non utilizza la tecnologia, bensì ricerca informazioni sensibili e dati di interesse direttamente dalla spazzatura, per esempio dati sulle bollette buttate via o simili.

L'attaccante spia da dietro le spalle ciò che fa la persona cercando magari di reperire credenziali o info utili, può anche essere che l'attaccante si mascheri da persona delle pulizie per entrare negli uffici e sbirciare desktop, carte, archivi, ecc...

Tailgating

L'attacco è della forma che enfatizza gli elementi fisici rispetto a quelli virtuali. Il tailgating è essenzialmente un attacco di ingegneria sociale in cui l'aggressore segue un individuo legittimo in un'area proibita in cui non è autorizzato a stare

Phishing Attacks

Concentriamoci meglio sugli attacchi di phishing che sono tra i più diffusi al mondo, basta pensare che nel 2019 l'88% delle aziene ha avuto esperienze con un attacco di spearphishing, più generalmente parlando invece il 95% degli attacchi alle aziene ha avuto esito positivo e il 97% degli utenti non riesce a identificare le email di phishing sofisticate da email invece non malevole.

Sempre da degli studi emerge che il 30% delle mail sono aperte dai target, il 12% clicca sui link nelle email o apre gli allegati e il 15% è vittima almeno una volta all'anno di phishing.

Per quanto riguarda l'influenzare la vittima, per far sì che si fidi dell'attaccante, troviamo diverse tattiche tra cui sfruttar la figura di un'autorità per influenzare una persona fingendosi un ente autorevole, o ancora il principio di scarsità ci viene detto di sbrigarsi perché ci sono ancora pochi posti disponibili o per fare il liking sui social.

Una domanda che ci si è posti in uno studio è: "autorità e urgenza incrementano la suscettibilità al phishing degli impiegati?".

Per rispondere a ciò sono stati mandati 3 tipi di mail:

principio del dovere → usato per capire fino a che punto una vittima può spingersi.

1. una normale mail senza persuasione
2. una mail che arriva da qualcuno con più autorità
3. mail che arriva da un altro impiegato sotto pressione di tempo

Fin da subito si è notato che il 31% clicca il link, il 25% fa il login e il 69% di chi ha cliccato ha rilasciato le credenziali al sito.

Se parliamo di persuasione o meno il 33% era più suscettibile all'urgenza, il 21% all'autorità e il 15% era suscettibile addirittura senza persuasione.

Altro elemento ricorrente nel phishing sono i phishing websites, riconoscibili dai domini e sottodomini irregolari o per la mancanza di https in primis

È anche possibile come per altri attacchi utilizzare il phishing come un servizio per cui pago e ne ottengo i risultati senza dover fare niente.

Riconoscimento e exploitation technique

Tra le fasi di un attacco c'è la raccolta di informazioni, tra le analisi che si possono compiere troviamo:

Dns Analysis

Si controlla il traffico dns per trovare informazioni come nomi di dominio, server mail o servizi di 3 parti.

Tra altre informazioni che troviamo ci sono i **dns records**:

- **soa: state of authority**
- **ns: nameserver**
- **a: ipv4 addr**
- **mx: mail exchange**
- **cname: canonical name**
- **txt: text**

Per fare analisi si può usare **dns recon**:

- `dnsrecon -d <domain>` allows to retrieve dns records for the specified domain
- `dnsrecon -D <dictionary of domain names> -d <domain>` looks for possible subdomains
- `dnsrecon -v -d <domain>` allows to retrieve dns records for the specified domain
- `dnsrecon -w -d` allows to run the whois command
- `sudo dnsrecon -j <name of json file> -d <domain>` allows to save the output in a json file

DnsEnum main commands

- `dnsenum <domain>`

Osint Analysis

si cercano informazioni su dipendenti e l'organizzazione in generale, il tutto da fonti pubbliche quindi nella totale legalità.

Degli impiegati ad esempio si cercano:

- **username**
- **email address**
- **phone number**
- **social network**

Mentre delle organizzazioni è solito cercare:

- **posizione**
- **business records**
- **website**
- **ip pubblici**
- **sottodomini**
- **credenziali**

Tra i tool per compiere questo tipo di analisi troviamo:

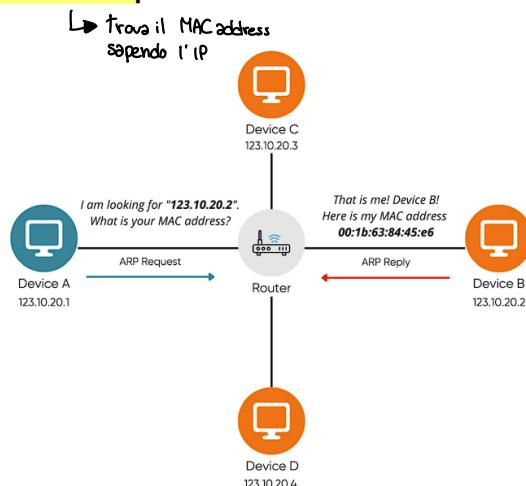
- **spiderfoot**: serve per automatizzare il processo di raccolta di informazioni su un certo target
- **theHarvester**: `theHarvester -d <domain> -b <source> -l <num of results>`
 - **d**: specifica il dominio
 - **b**: specifica il source dove vogliamo pullare i dati
 - **l**: permette di specificare il numero di risultati da tornare
- **Shodan**: striscia su internet 24/7 e recupera informazioni riguardo ip pubblici, i dispositivi runnano dei servizi descritti dal loro service banner, shodan recupera questi service banner. Documentazione slide 15-17.

Active Scanning

Si cercano nomi di sistema, sistemi operativi, porte aperte e servizi TCP/UDP, l'attaccante fa tutto ciò sondando l'infrastruttura con il traffico di rete.

- Scanning Ip blocks: gli ip pubblici potrebbero essere allocati a blocchi dalle organizzazioni, l'attaccante può scannerizzare questi blocchi per trovare informazioni come quali ip sono in uso o che host sono assegnati a tali address
- Vulnerability scanning: si controlla se la configurazione di un host/application target si allinea con il target di uno specifico exploit che l'attaccante potrebbe usare.

Si può usare ad esempio il protocollo arp



Tool per host identification:

- netdiscover
- arp-scan
- nmap
- metasploit
- ...

Attacchi ad infrastrutture critiche, sistemi di controllo industriale, attacchi di cyberwar

Le strutture critiche sono strutture, informazioni, sistemi nazionali necessari per una nazione per funzionare e dalle quali la vita quotidiana dipende, include anche funzioni siti e organizzazioni che non sono essenziali al mantenimento di servizi essenziali ma che necessitano di protezione per danni che potrebbero arrecare ai cittadini.

Alcuni esempi ne sono le dighe, energia, healthcare servizi finanziari e via così.

La compromissione degli elementi critici di queste infrastrutture può portare a:

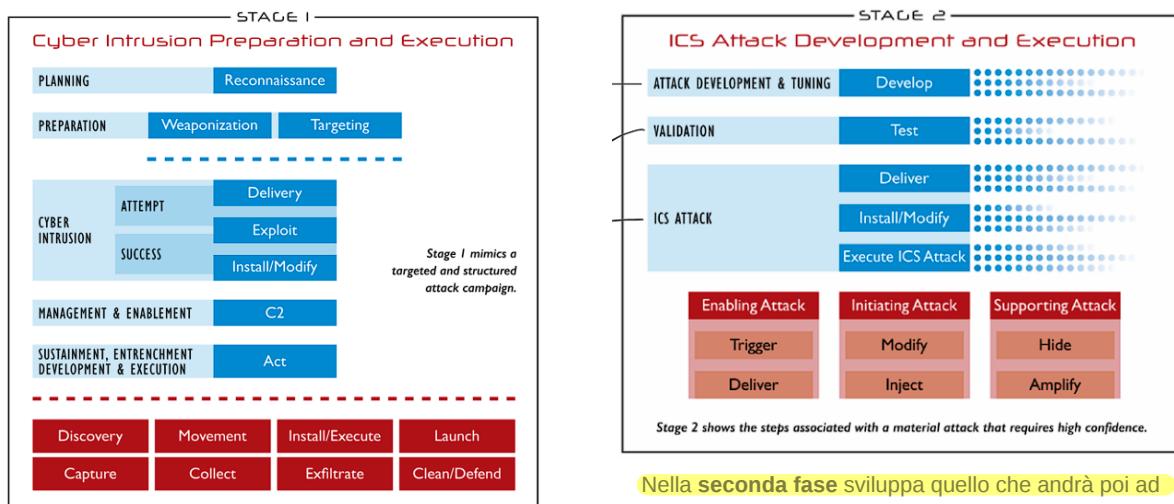
- forte impatto negativo su disponibilità, integrità o consegna di servizi essenziali
- impatto significativo sulla sicurezza, difesa nazionale e il funzionamento dello stato

Molte di queste sono controllate e monitorate dagli **ICS(Industrial Control Systems)**, che verificano ad esempio se i processi di produzione presentano irregolarità, sono sistemi vulnerabili.

Tra i dispositivi più vulnerabili troviamo nas, ip camera, plc, ups, patient monitor.

ICS Cyber Kill Chain

↳ Industrial Control System



Nella **prima fase** si scoprono informazioni legate all'infrastruttura da attaccare

Nella **seconda fase** sviluppa quello che andrà poi ad essere l'attacco all'ics, solitamente questi attacchi sono multi-stage

Cyber War

Nascono nel momento in cui una nazione attacca le infrastrutture critiche di un'altra nazione, attacchi in questo tipo di guerra possono essere: spionaggio, sabotaggio, attacchi a fornitori di energia.

Stuxnet

È la prima cyber weapon, targetizzata ai PLC di centrifughe utilizzate in una centrale iraniana per l'arricchimento dell'urano è stata usata per rallentare lo sviluppo del programma nucleare iraniano, sviluppata probabilmente da U.S NSA, CIA, e Israeli intelligence.

Funzionamento

Per la fase di **reconnaissance** sono stati utilizzati dei video propagandistici iraniani che avevano nello sfondo monitor per il controllo del sistema delle centrifughe, da questi si è riusciti a estrarre molte informazioni utili, per il **delivery** il sistema è stato poi infettato via USB, per la **propagazione** ha usato varie tecniche tra cui tecniche di propagazione di rete ad esempio usando un database di password hardcoded o con drive rimovibile ad esempio usando la vulnerabilità LNK(gli LNK sono shortcut file in windows, se la shortcut la riporto a un binario malevolo questo viene eseguito pensando si esegua altro) o con autorun.inf, ha poi evaso gli automated detection system di tutte le macchine windows mostrando un certificato veritiero.

A questo punto stuxnet controllava di essere in una macchina target(quelle su cui girava il control software dei PLC di siemen) e dopo l'installazione cerca di accedere a internet per instaurare un C2 con il quale recuperare una versione più recente o ricevere comandi da server che si è scoperto essere poi fake di siti di streaming(todaysfutbol.com).

A questo punto il worm compromette controller logici del sistema usando zero-day vulnerabilities, spia le operazioni dei sistemi target, avendo poi queste informazioni prende controllo delle centrifughe per farle rompere, una volta fatto il danno da false informazioni su cosa stia succedendo fino a quando non è troppo tardi per recuperare i danni.

Sandworm's Attacks(gruppo di hacker)

Ce ne sono stati diversi, alcuni tra i famosi sono quelli fatti al governo e infrastrutture ucraine nel 2015 e 2016.

Nel 2015 sono state attaccate 3 società di distribuzione della corrente elettrica che hanno portato a interruzioni di quest'ultima ovviamente.

Metodologia dell'attacco

Sono state mandate delle email al personale amministrativo o IT delle rispettive società, a quel punto una volta aperti gli allegati chiedeva di abilitare le macro (sequenze che automatizzano task nel file) così facendo si installava in realtà il malware **BlackEnergy 3**, quest'ultimo era ovviamente connesso a un server C2 e ha operato come un **killdisk** ossia ha cancellato dati dal disco rendendo inutilizzabili i sistemi (penso?????), si è inoltre fatto un attacco Dos telefonico così che gli operatori non potessero fare segnalazioni di errori.

Nel 2016 c'è stato il secondo attacco, in questo caso solo una sottostazione di trasmissione ha perso corrente, il tutto è cominciato con una campagna di spearphishing, dopodiché i sandworm sono riusciti ad automatizzare il controllo degli interruttori senza compromettere le postazioni di lavoro degli operatori, il malware usato era più avanzato e indirizzato per gli ICS.

Si parla questa volta di **industroyer**, usato per disturbare il lavoro degli ics, più precisamente quelli nelle substation elettriche, implementava vari protocolli di comunicazione utilizzati negli ics e anche un ddos contro relè di protezione di Siemens e Siprotec.

Altro ransomware che troviamo è **notpetya** che colpisce diverse organizzazioni tra cui: banca centrale ucraina, shipping comp Maersk, e altre organizzazioni.

Consegnato come aggiornamento di un software per l'acconto di tasse, reindirizzava il pc a un server in Francia dal quale scaricava il malware al posto del server di update, una volta installato nella macchina cerca altri host in rete da infettare usando exploit come EternalBlue o EternalRomance.

Cifra i file e dischi con AES128 e chiede 300\$ in bitcoin

2 User Authentication

Il processo di autenticazione è quel processo che determina l'identità di una persona solitamente con una combinazione di ciò che la persona:

- conosce
- ha
- è

Autenticazione con password

È la tecnica più utilizzata, si forniscono username e password, il sistema li compara con quelli salvati sul server e se coincidono l'identità è autenticata.

Questo sistema di autenticazione però non è sicuro difatti incontriamo vari problemi, tra cui:

- **password overload:** ad oggi le persone devono tenere a mente sempre più password e username legati a molti account, questo comporta che le password diventino più prevedibili e comuni tra le persone
- **password reuse:** c'è inoltre da parte delle persone un ampio riutilizzo delle password, quindi una certa password utilizzata per più servizi a cui si è iscritti.

Ci sono vari tipi di attacco alle password tra cui:

- **offline attacks:** attacco senza accesso al sistema di autenticazione
- **active online attacks:** si ha accesso al sistema di autenticazione
- **non technical attacks:** attacchi di ingegneria sociale
- **passive online attacks:** la password viene intercettata

Tra gli attacchi comuni invece che troviamo alle password abbiamo **brute force, social engineering, key logging, shoulder surfing**

Nei sistemi operativi le password sono contenute in locazioni diverse:

- **windows:** nel database SAM che si trova in System32\config
- **linux:** etc/passwd e etc/shadow

Regolarmente le password in qualsiasi ambito non sono salvate in chiaro, bensì viene salvato il loro **hash** che è irreversibile. Per quanto riguarda windows, con quest'ultimo abbiamo due possibili hash:

- LM Manager* *New Technologies Lan Manager*
- **LM:** salva password lunghe max 14 caratteri, lettere convertite in maiuscolo e in caso fossero minori di 14 caratteri viene fatto padding, spartite in due parole da 7 caratteri, hashate separatamente e riunite.
 - **NTML:** lunghezza massima psw in input di 256 char, hash calcolato su tutta la stringa

Tra gli attacchi alle password abbiamo detto che troviamo varie possibilità tra cui:

- **brute force:** si provano tutte le possibili combinazioni fino a quanto non si indovina la password, la dimensione dello spazio delle password è $|A|^n$, con n # caratteri e A alfabeto, consideriamo 8 caratteri con tutti i caratteri alfanumerici, avremmo $96^8 = 7.2$ quadrillioni di password combinations
- **dictionary attack:** è una sorta di bruteforce, con la differenza che prova le password basandosi su un dizionario che gli forniamo, spesso contenente le password più utilizzate dalla gente, ovviamente la password viene trovata solo se è nel dizionario.
- **hybrid attack:** si utilizza un dizionario ma si provano anche tutte le possibili variazioni includendo caratteri speciali e numeri
- **rainbow tables:** si ha un insieme di password e hash corrispondenti precalcolate, per mitigare questo attacco è consigliato usare il "salt", sono più potenti di bruteforce, dictionary e hybrid ma richiedono ancora più memoria di questi ultimi.
- **pass-the-hash:** l'attaccante manda una richiesta per autenticarsi al server e fornisce l'hash della password della vittima (precedentemente recuperata) autenticandosi così senza aver avuto bisogno di decifrare la password.

- **online dictionary attack:** prova password associate all'utente, prova password in un dizionario e prova password popolari, non garantisce di trovare la password corretta.
- **credential stuffing:** l'attaccante ha una collection di credenziali rubate che gli utenti utilizzano per un certo servizio, usa queste in altri servizi per accedere anche a questi nel caso l'utente abbia fatto password reuse.
- **password spraying:** si prova ad utilizzare la stessa password per più persone.
- **keylogger:** piccolo programma che registra tutti i keystroke che lo user batte sulla tastiera, solitamente installato tramite un file inserito in un immagine/file mandato via mail.
- **social engineering:** tra gli attacchi di social engineering troviamo: **phishing, shoulder surfing, dumpster-diving**, tra le uniche contromisure possibili troviamo attenzione da parte dello user e training.

Se parliamo di **password strength** parliamo della proprietà della password di resistere agli attacchi bruteforce, è solitamente calcolata con $\log_2(|A|^n)$, solitamente a una password strong corrisponde un valore calcolato dalla funzione precedente di almeno 60.

↳ Entropia

Zxcvbn

Libreria che fornisce uno strumento per valutare la password strength, per la stima usa fattori come lunghezza, caratteri maiuscoli, minuscolo, alfanumerici e speciali, presenza di parole in dizionari e sequenze comuni

Possibili e Effettive contromisure agli attacchi

Tra le misure effettive a tutti questi attacchi che si possono adottare ci sono:

- **salting:** aggiungere del sale alla password prima di hasharla → aumentano le combinazioni per la stessa pwd.
- **controllo degli accessi ai file delle password:** solo gli autorizzati possono accedervi, e le password vengono mantenute in posti separati rispetto agli id.
- **lockout mechanism:** bloccare l'account dello user dopo molti tentativi di login falliti
- **throttling:** time delays tra un attempt di login e il prossimo
- **security monitoring:** monitorare login per trovare utilizzi insoliti e avvisare l'utente di tentativi di login
- **password blacklisting:** controllare se una password è in una lista di parole comuni

Consideriamo anche un contesto in cui c'è l'attaccante che intercetta la comunicazione tra un user e il servizio, se la password è in chiaro è logico che l'attaccante otterrà l'informazione, la soluzione è cifrare la comunicazione con ssl/tls.

Summary

I sistemi di autenticazioni basati su password non sono sicuri, gli utenti tendono a usare password facili per ricordarle meglio tra i vari servizi e/o riutilizzano la stessa password per più servizi, come abbiamo visto sono vulnerabili a numerosi attacchi di vario tipo e le contromisure più efficaci sono account lockout e throttling, predictive monitoring e password blacklisting.

Multi-factor authentication

Se all'autenticazione con password aggiungiamo un altro fattore, otteniamo la multifactor authentication, consiste nell'utilizzare un secondo fattore che solo l'utente può ottenere:

- **pin**: codice o stringa spesso mandata per mail o sms
- **biometric details**: fingerprint
- **security token**: va fisicamente connesso al device(usb)
- **app**: installata su un dispositivo fidato

Per ottenere appunto queste **one-time password** ci sono vari metodi tra cui:

- **sms-based**: ogni volta che l'utente logga, riceve un sms al numero di telefono registrato che contiene la otp.
- **totp-based**: all'utente è richiesto di scannerizzare un QR in una data applicazione, è proprio da questa app che riceverà ogni volta la otp.

HMAC-based OTP algorithm(HOTP)

1. L'utente abilita la MFA.
2. Il server backend crea una chiave segreta per lo user
3. Il server condivide la chiave segreta K con l'applicazione nel telefono dello user
4. L'applicazione inizializza un counter C.
5. L'applicazione prima incrementa C e poi genera una otp usando la chiave segreta e C:
 - a. $\text{HOTP}(K,C) = \text{Truncate}(\text{HMAC-SHA1}(K,C))$
6. A questo punto viene mandato il valore al server che lo confronta con quello che lui ha generato, se gli hash corrispondono allora l'utente è autenticato e il server incrementa C.

Lo così è già pronto a generare il nuovo codice

Time-based OTP

L'unica differenza dal metodo precedente è che usa il tempo al posto del contatore, entrambi applicazione e server non inizializzano il counter, è solamente necessario che entrambe conoscano o siano in grado di ottenere il currentUnix time(numero di secondi passati dal 01/01/1970).

$$\text{TOTP}(K, C) = \text{HMAC-SHA256}(K, T)$$

$T = (\text{Current Unix time} - T_0)/X \Rightarrow \text{N}^{\circ} \text{ di secondi passati dall'UNIX TIME}$

X represents the time steps in seconds

T_0 is the Unix time to start counting time steps

Biometrics

Si riferisce a qualsiasi misura usata per identificare univocamente una persona basandosi su tratti biologici o fisiologici, generalmente i sistemi biometrici integrano qualche sensore come scanner per leggere le informazioni biometriche e confrontarle con quelle che sono salvate.

Affinchè si possa utilizzare un'autenticazione biometrica bisogna che siano rispettate:

- **universalità**: quasi tutte le persone dovrebbero avere questa caratteristica
- **distintività**: ogni persona deve avere differenze distinguibili in questa caratteristica
- **permanenza**: la caratteristica non deve cambiare nel tempo

- **collezioneabilità:** la caratteristica deve poter essere determinata e quantificata.

Tra le caratteristiche più utilizzate troviamo: fingerprint, firme, voice recognition, dna.

Tra le limitazioni di questa categoria troviamo l'accuratezza degli algoritmi che fanno il matching, ci possono essere falsi positivi che quindi fanno accedere utenti non autorizzati o falsi negativi che non lasciano accedere user legittimi, è inoltre facile ricostruire alcuni tratti biometrici come le fingerprint e non tutti gli user potrebbero accettare di farsi scannerizzare.

Digital Identity Management

FIDO2 Protocols

Basati su crittografia a chiave pubblica per autenticare utenti a servizi online, supportano autenticazione passwordless, mfa con authenticatori embedded o esterni.

Il protocollo garantisce resistenza a phishing e replay attacks e user privacy.

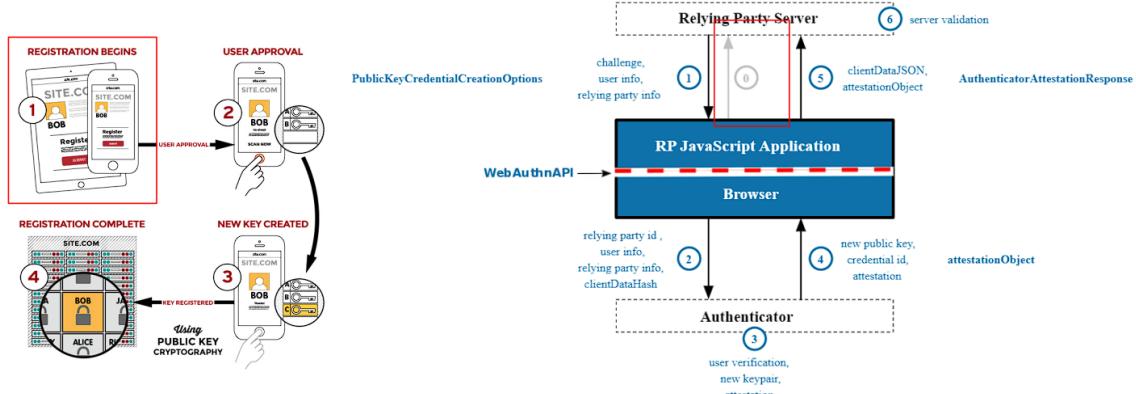
Gli attori principali sono:

- **user:** che si deve autenticare al servizio
- **relying party:** l'organizzazione responsabile di registrare e autenticare l'utente
- **client platform:** il client e il dispositivo del client
- **authenticator:** fornisce gestione di chiavi e firme crittografiche

Specifiche principali:

- **WebAuth:** standard web nei browser che consente il supporto per la FIDO auth
- **CTAP2:** protocollo per interagire con authenticator esterni(usb,nfc, ble per auth passwordless o mfa) per l'autenticazione su browser e sistemi operativi abilitati a FIDO2

Cerimonia di registrazione



1. **Richiesta di registrazione:** l'utente comunica al relying party che vuole registrare un dispositivo autenticatore, il party genera una richiesta di registrazione contenente una challenge, info sull'utente e sul relying party.

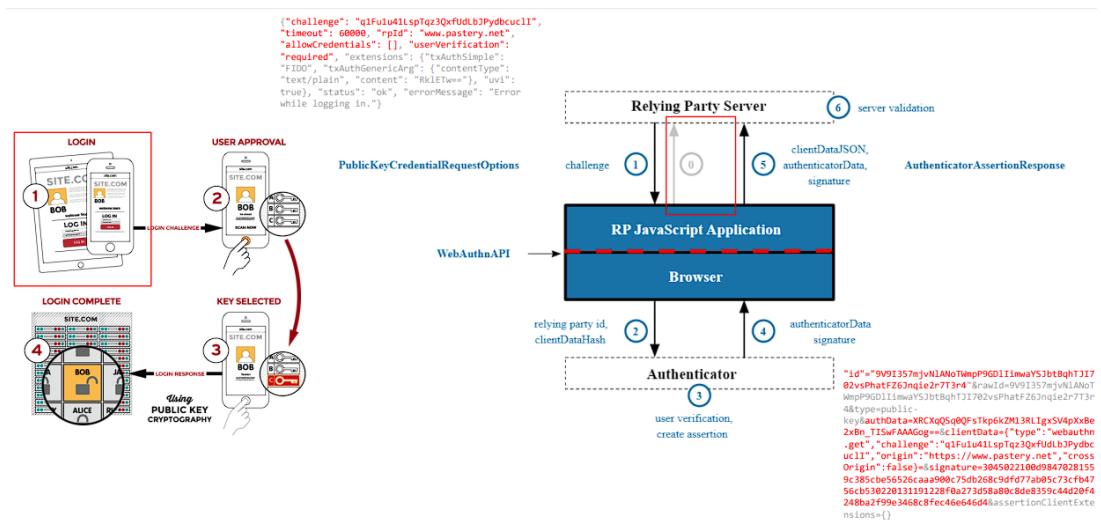
2. **Trasmissione della richiesta all'utente:** viene inviata la richiesta contenente l'id del party, le info sull'utente e sul party e un hash dei dati del client.
3. **interazione dell'utente:** l'utente interagisce con il dispositivo autenticatore per confermare l'intenzione di registrarlo, solitamente con un pin o conferma biometrica.
4. **generazione chiavi:** a questo punto il dispositivo genera una coppia di chiavi, la chiave pubblica viene mandata insieme all'id e un'attestazione al relying party.
↳ firma con chiave privata
5. **registrazione utente presso il relying party:** il party verifica quindi la firma della public key e memorizza le informazioni relative all'utente(chiave pubblica compresa) associandole a un id unico
6. **conferma registrazione:** per finire si manda una conferma di avvenuta registrazione.

Attestation Object

È una parte dei dati restituiti dal dispositivo autenticatore durante il processo di registrazione, contiene diverse informazioni e metadati che il relying party può usare per verificare l'autenticità del dispositivo e la validità della chiave pubblica associata, tra i campi principali troviamo:

- **fmt:** formato attestazione
- **attSmt:** contiene la dichiarazione di attestazione, ossia una firma o prova di integrità per la chiave pubblica del dispositivo
- **authData:** dati relativi all'autenticazione, tra cui chiave pubblica, id utente, challenge iniziale e il serial number.

Processo di autenticazione



1. **richiesta di autenticazione:** l'utente chiede di accedere al servizio e il party genera la richiesta di auth con una challenge.
2. **invio della richiesta all'utente:** la richiesta viene mandata all'utente includendo l'id del relying party.
3. **interazione con l'utente:** l'utente interagisce con il dispositivo per confermare l'intenzione di autenticarsi
4. **generazione risposta:** il dispositivo usa la chiave privata associata all'utente per firmare la challenge richiesta dall'autenticazione, la risposta viene mandata includendo la challenge firmata

5. **invio risposta al party e verifica risposta:** il party verifica la firma usando la chiave pubblica e successivamente la validità della challenge

6. concessione accesso

Questo processo quindi permette all'utente di autenticarsi senza però l'utilizzo della tradizionale password.

Single Sign On Protocols

Tradizionalmente siamo abituati ad avere più servizi sui quali creiamo account e per ognuno di questi usiamo le credenziali create, ciò può diventare pesante e un'alternativa più comoda è quella che utilizza l'idea di mettere nel mezzo di ciò una **identity management platform**.

Una **identità digitale** è una rappresentazione digitale delle informazioni conosciute di un individuo(nome,cognome, userid e password, national insurance number, eccc...).

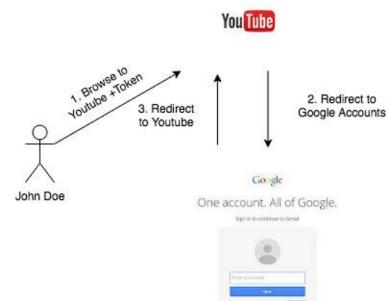
Un **sistema di gestione di identità digitale** fornisce una soluzione centralizzata che gestisce le informazioni digitali degli utenti e l'accesso a risorse/servizi, quindi mantiene l'identità dell'utente e gli associa degli attributi, inoltra verifica l'identità di quest'ultimo basandosi appunto sugli attributi dell'identità.

Gli attori principali sono:

- **User:** entità di cui si può affermare qualcosa
- **Identity provider(asserting party):** verifica l'autenticità dell'utente e crea asserzioni su di esso.
- **Service provider(relying party):** delega la verifica dell'utente all'identity provider e consuma le asserzioni che questo genera.

Con il **single sign on** l'utente si autentica una volta e poi accede alle risorse a cui è autorizzato, l'autenticazione alle risorse è gestita dall'identity provider in maniera trasparente all'utente.

Shibboleth, progetto che permette alle università di condividere le risorse.



Se parliamo di **federated identity**, ci riferiamo al fatto che spesso organizzazioni diverse stabiliscono uno **shared identifier** comune per riferirsi ad un soggetto, così facendo si facilita la condivisione dell'identità tra varie organizzazioni e si facilita di conseguenza l'sso, perchè uno user che si autentica in uno dei membri della federazione si sta loggando in realtà a tutti i membri, inoltre si riducono i costi di manutenzione e di gestione delle identità

SAML

Saml è uno standard che abilita l'SSO e l'identity federation fornendo una rappresentazione standard per le attribute assertion e authentication assertion.

Saml identity provider(asserting party) verifica l'identità dello user e emette un'authentication assertion.

Così facendo lo user può presentare a un service provider l'authentication assertion senza doversi autenticare di nuovo.

Essenzialmente quello che succede è che un user vuole accedere a un service provider, quest'ultimo manda una richiesta di auth assertion all'identity provider che risponde con l'auth assertion, niente di meno che una prova della sua autenticità firmata con la sua chiave privata, a questo punto il processo è terminato.

Le **asserzioni saml** sono dichiarazioni di fatti riguardo un soggetto che un asserting party dice siano vere, ci sono 3 tipi di asserzioni:

- **asserzioni di autenticazione**: descrive i mezzi utilizzati per autenticare un soggetto
- **asserzioni di attributi**: lista di attributi di un soggetto
- **asserzioni di autorizzazione**: definiscono i permessi di un soggetto

Authentication request

• Id	• version	• IssueInstant : istante temporale della generazione della richiesta	• AssertionConsumerService URL : url dell'interfaccia del service provider al quale l'identity provider manda il token di autenticazione
• Subject : il soggetto da autenticare	• Issuer : uid del service provider	• NameIDPolicy : livello di security richiesto per l'autenticazione	

Response

• Id	• Version	• IssueInstant	• InResponseTo : id auth request
• Destination : url service provider	• Status : req success or fail	• Issuer	• Assertion :
• Signature : firma digitale dell'identity provider			

Assertion

• Id	• Version	• IssueInstant	• Subject
• Issuer	• Conditions : specifica l'intervallo temporale in cui la req è valida	• AudienceRestriction : dice quale service provider deve consumare l'asserzione	• AuthStatement : specifica il contesto di auth
• AttributeStatement : lista degli identity attributes certificati dall'identity prov		• Signature	

Spid

Gli attori del sistema di identità digitale italiano sono:

- **AgID**: entità che monitora e autorizza le entità ~~che~~ ad emettere lo spid
- **Identity Provider**: entità pubbliche e private certificare da AgID che verificano l'identità dello user ed emettono spid.
- **Service Provider**: entità che chiedono agli utenti gli attributi che li qualificano
- **User**: proprietario dello spid.

Spid presenta vari livelli di autenticazione sicura:

1. accesso con username e password
2. accesso con le credenziali e otp message
3. accesso con credenziali e dispositivi fisici

OpenID Connect

È un protocollo di autenticazione che profila e estende OAuth2.0 per aggiungere un layer di identità, permette ai client di confermare l'identità di un end user usando l'autenticazione tramite un server di autorizzazione.

Implementare oidc su oauth2.0 crea un framework che protegge le api, le applicazioni native e le applicazioni web in un'architettura unificata.

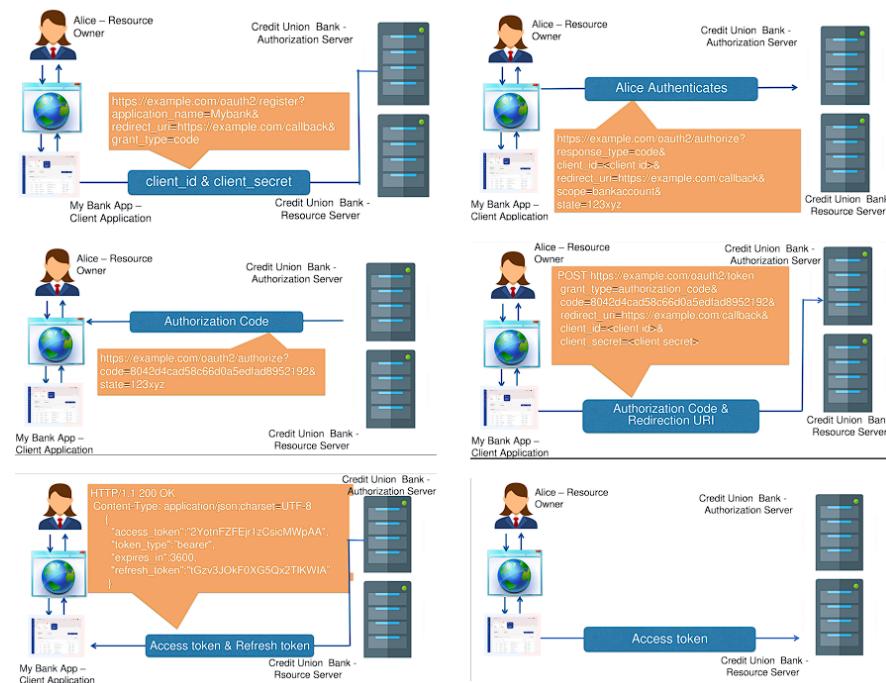
OAuth è un protocollo standard di autorizzazione che consente a un'applicazione di terze parti ad accedere a risorse protette su un server http, richiede un token di accesso dal server di autorizzazione, a questo punto l'applicazione usa l'access token per accedere alle risorse protette.

Ci sono quattro attori:

- **Resource Owner**: entità capace di garantire l'accesso alle risorse protette
- **Resource Server**: server che contiene le risorse
- **Authorization Server**: il server che emette l'access token al client dopo aver autenticato il proprietario della risorsa e ottenuto l'autorizzazione da quest'ultimo.
- **Client**: applicazione che richiede l'accesso alle risorse protette a nome del possessore e con la sua approvazione

Essenzialmente il flow dell'autorizzazione è il seguente:

Alice che è la proprietaria delle risorse si autentica e ottiene dal server di autorizzazione un token, a questo punto richiede dal resource server dall'applicazione in cui si è autenticata le risorse, per fare questo inoltra una richiesta al server con il token ottenuto e il server risponde con le risorse richieste.



Access Control

È un elemento centrale della cyber security e serve per prevenire che entità non usino risorse a cui non sono autorizzati ad accedere o che utilizzino risorse in maniera non autorizzata.

I 3 principi dell'access control sono:

- **Authentication:** verificare l'identità di un entità
- **Authorization:** dare diritti o permessi rispetto a una risorsa a un'entità
- **Accountability:** monitoraggio e processamento degli accessi alle risorse.

Gli elementi delle policy di access control sono quindi 3:

- **soggetto:** entità che accede agli oggetti
- **oggetto:** risorsa il cui accesso è controllato
- **permessi:** maniere in cui il soggetto può accedere al soggetto

Modelli di Access Control

Discretionary Access Control(DAC)

Accesso basato sull'identità del soggetto.

Ci sono delle regole di accesso che esplicitano chi può eseguire determinate azioni su quali risorse, **discretionary** perché l'utente può dare i suoi permessi anche ad altri utenti, ciò è regolamentato da una policy amministrativa, per capire che permessi ha un soggetto rispetto a una risorsa ci sono varie strutture che si possono utilizzare tra cui:

access matrix → *non scalabile*

access control list

capability list



Tra le **limitazioni** che incontriamo di DAC le principali ci sono il fatto che gestire una policy è complesso in sistemi molto grandi, dalle capability lists è difficile avere una overview dei permessi concessi su un certo oggetto e dalle access control list è difficile avere invece un'overview dei permessi dati ad un certo user.

Mandatory Access Control(MAC)

Accesso basato sulle security label degli oggetti e autorizzazioni del soggetto

se i permessi dati al soggetto sono superiori del livello di autorizzazioni necessarie per l'oggetto viene permesso l'accesso

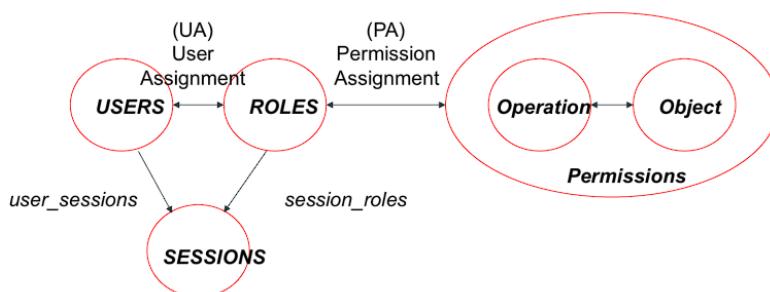
Role Based Access Control(RBAC)

Accesso basato sul ruolo di un soggetto nell'organizzazione, è un modello molto adottato, ai vari ruoli vengono assegnati i diritti di accesso alle risorse e a loro volta agli user sono assegnati dei ruoli.

Ci sono 3 tipi di RBAC:

- **RBAC_0**

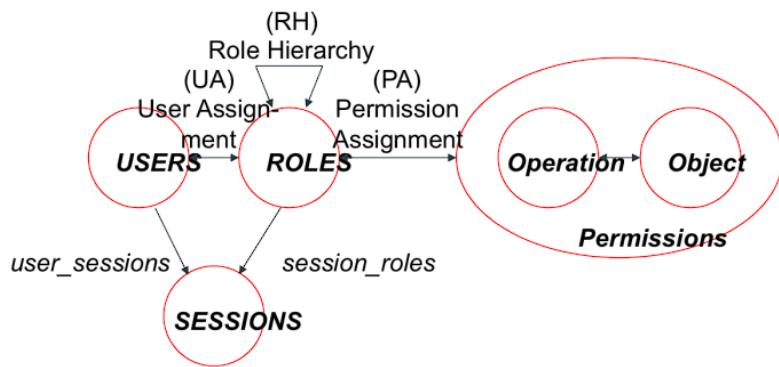
Essenzialmente qui lo user ha un ruolo, che a sua volta ha dei permessi, una volta che lo user è in una certa sessione, avrà disponibili i permessi del suo ruolo.



- **RBAC_1**

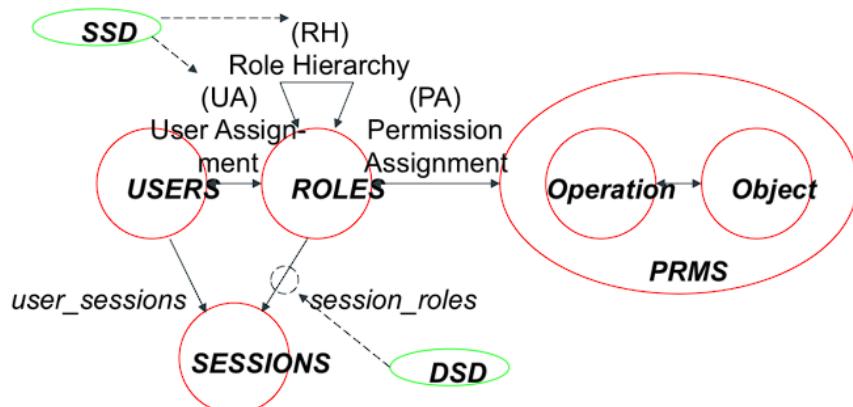
È essenzialmente RBAC_0 a cui viene fatta l'aggiunta della gerarchia dei ruoli, ogni ruolo starà sopra o sotto nella gerarchia rispetto ad altri ruoli, se un ruolo sta sopra ad altri ruoli nella gerarchia, avrà ovviamente anche tutti i permessi che tutti gli altri ruoli al di sotto di lui hanno.

↳ Capo di dipartimento
Prof
Dottorando
Studente



• RBAC_2

È RBAC_1 ma vengono aggiunti anche i **vincoli di separazione dei compiti**, possono essere **statici** → uno user non può essere assegnato a più di n ruoli nel set dei ruoli, oppure **dinamici** → un user non può attivare più di n ruoli nella sessione



Tra i **vantaggi** che incontriamo con RBAC abbiamo una gestione e monitoraggio efficiente dei permessi, difatti non c'è bisogno di assegnare manualmente agli user dei permessi perchè è fatto automaticamente assegnando un ruolo a quest'ultimo.

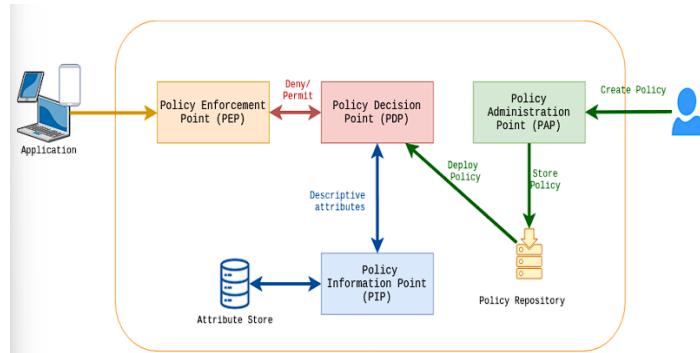
Tra le **minaccie** ad RBAC invece troviamo invece il fatto che non è un modello di access control facile da implementare correttamente, pensiamo a una banca con 50k dipendenti e 1400 reparti con più di 6mln di clienti, abbiamo un totale di 1300 ruoli e 1000 ruoli cambiano in 3 mesi, ciò comporta avere over-entitled employees, ossia dipendenti che hanno ruolo più alto di quanto non gli serva, si stima tra il 50 e il 90%

Attribute Based Access Control(ABAC)

Accesso basato sugli attributi del soggetto, l'oggetto e il contesto

XACML(extensible access control markup language) è uno standard usato per implementare ABAC, fornisce un linguaggio basato su xml per la definizione di politiche di controllo degli accessi, un protocollo di richiesta e risposta per fare decisioni di autorizzazione e un'architettura che definisce i principali componenti in un'implementazione.

Vediamone l'architettura:



- **Policy Enforcement Point**: entità che protegge le risorse, fa le richieste di decisione e applica le decisioni di autorizzazione e l'esecuzione degli obblighi
- **Policy Decision Point**: riceve ed esamina le richieste di PEP, recupera le policies applicabili, valuta tra queste la policy applicabile e ritorna la decisione di autorizzazione al PEP.
- **Policy Administration Point**: crea security policies e le salva in una repository.
- **Policy Information Point**: fa da sorgente per attributi aggiuntivi riguardo l'utente, la risorsa o il contesto.
- **Context Handler**: converte le richieste dal formato nativo al formato XACML e inversamente converte le decisioni di autorizzazione al formato nativo

L'authorization flow sarà quindi una cosa del tipo:

Il Pap scrive policy o set di policy e le rende disponibili al PDP, quando un utente richiede l'accesso a una risorsa viene mandata una richiesta al PEP, il PEP inoltra la richiesta d'accesso al context handler includendo eventualmente attributi del soggetto, della risorsa o dell'azione e contesto, a questo punto quando il context handler riceve la richiesta la inoltra al PDP, che eventualmente richiede al context handler altri attributi, se questo accade il context handler li recupera dal PIP e li dà al PDP che valuta la policy, una volta fatto ciò manda la risposta con la decisione di autorizzazione al context handler che finalmente traduce in linguaggio nativo la risposta e la manda al PEP che applica gli obblighi e se l'esito è positivo permette l'accesso alla risorsa, altrimenti lo nega.

Vediamo ora invece i componenti chiave di XACML

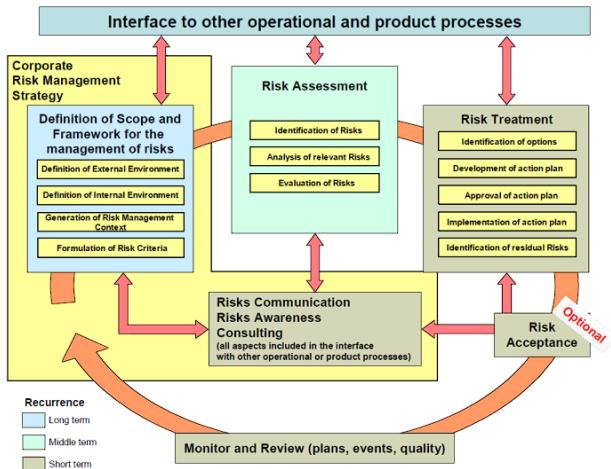
- **policy set**: è il top-level elementi aggrega altri policy set o policy
- **policy**: è composto da target, rule e obligation ed è valutato dal PDP per ottenere una decisione d'accesso.
 - **target**: definisce l'applicabilità di una policy a una risorsa
 - **rule**: esprime diverse regole di access control
 - **rule combining algorithms**: specifica come le regole possono essere combinate per fare un'authorization decision
 - **ObligationExpression**: azioni che il PEP deve svolgere con un'decisione di autorizzazione
- **rule**: fornisce condizioni che testano gli attributi importanti all'interno di una policy
 - **target**: condizione che determina se una regola è applicabile a una decision request
 - **effect**: conseguenza della valutazione a true di una regola
 - **condition**: espressione che affina l'applicabilità di una policy

- obligation(opz): operazioni/azioni da eseguire con un'authorization decision
- **target:** usato per associare una risorsa richiesta a una policy applicabile
 - AnyOf: l'accesso è consentito se almeno una condizione specificata è soddisfatta
 - AllOf: l'accesso è consentito se tutte le condizioni sono soddisfatte
 - Match: condizione di confronto tra un valore specificato e attributi
- **combining algorithm:** usati per unire le varie decisioni di policies ottenute in una singola decisione.
 - **deny overrides:** le decisioni di deny hanno la priorità su quelle di permit, se tutte le decisioni sono indeterminate il risultato è indeterminato, se tutte le decisioni sono permit, allora il risultato è permit, altrimenti è non applicabile
 - **permit overrides:** le decisioni di permit hanno la priorità su quelle di deny, se tutte le decisioni sono indeterminate, il risultato è indeterminato, se sono tutte deny il risultato è deny, altrimenti non è applicabile
 - **first-applicable:** il risultato è l'effetto delle prime rule/policy il quale target si valuta a true
 - **only one applicable:** applicabile solo ai policySet, se non c'è una policy applicabile, il risultato non è applicabile, se più di una policy è applicabile il risultato è indeterminato, se solo una policy è applicabile, allora il risultato è la valutazione della policy
- **request context:** incapsula una decision request da mandare a PDP
 - attributes: specifica gli attributi di un soggetto, risorsa, azione o ambiente
 - category: specifica se gli attributi sono relazionati
 - content:
- **response context**

3 Cyber Risk Management

Le organizzazioni devono decidere quanto tempo e denaro spendere per proteggere le loro tecnologie e servizi, uno degli obiettivi principali del risk management è di informare e migliorare queste decisioni, inoltre il risk management è un requisito di molti importanti standard e regolatori come gdpr, iso27001, ecc...

Fasi del risk management



Frame Risk

Si stabilisce il contesto in cui l'organizzazione opera, quindi le missioni e i purpose, le aree chiave e critiche, si identifica chi è responsabile di fare decisioni di cybersecurity risk management, requisiti di vario tipo (legale, regolatorio, ecc) che l'organizzazione deve soddisfare e che rischi si ritengono accettabili per l'organizzazione.

Assess Risk

Lo scopo di questa fase è di identificare:

- **rischi** all'organizzazione (operazioni, assets, ...)
- **vulnerabilità** interne e esterne all'organizzazione
- **impatto avverso** che potrebbe avvenire dato un threat che expolita le vulnerabilità
- **probabilità** che un male avvenga

Responde to Risk

In questo step si coinvolgono l'analisi e prioritizzazione dei rischi e il fare decisioni su come si gestiranno questi ultimi, ci sono quattro strategie:

- **accept the risk**
- **transfer the risk** ↗ *assicurazione*
- **avoid the risk**
- **treat the risk**

Identifichiamo inoltre 4 tipi di security:

- **procedural security:** controlli che cercano di mitigare o trattare rischi identificati seguendo policies, procedure, processi o linee guida
- **physical security:** controlli che cercano di mitigare o trattare rischi identificati tramite protezione fisica degli assets come edifici, it equip, personnel, ecc...
- **personnel security:** misura da mettere in piano per mitigare o trattare rischi da user autorizzati di cybersistemi (training e threat awareness).
- **technical security:** misure costruite nel cybersystem per mitigare o trattare rischi identificati (firewall, anti-malware sw, software updates e patching)

Comunicate the Risk

Si comunicano le scoperte e raccomandazioni alla persona o gruppo che prende le decisioni appropriato all'interno dell'organizzazione. La comunicazione deve essere significativa e appropriata in termini di livelli di dettaglio e formato utilizzati.

Implement and assure Risk

Si implementano i security controls raccomandati, mantenendo la confidenza che i controlli e le misure applicate funzionino e continuino a farlo come ci si aspetta.

Training di persone che usano, gestiscono e mantengono i sistemi e servizi richiedendo che abbiano il train e skill necessarie affinchè svolgano il loro lavoro in maniera sicura.

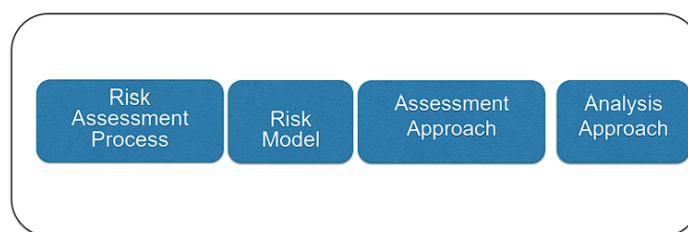
Essere sicuri che la tecnologia e i processi che l'organizzazione usa siano progettati con sicurezza

Fare testing su servizi e devices prima del deploy e mentre è in funzione, monitorando e revisionando come sono usati.

Monitor Risk

Si conferma continuamente che i controlli sono appropriati e proporzionati in termini di gestione dei rischi di cybersec, si sviluppano metriche e indicatori di performance per misurare l'effettivo impatto dei controlli e si rivisitano le valutazioni e analisi dei rischi quando qualcosa di significativo cambia(nuove vulnerabilità, tecnologie).

Componenti delle metodologia di Risk Assessment(valutazione)



Il rischio si calcola in base alla probabilità con cui la problematica si presenta e in base all'impatto che essa avrebbe

Metodologia OWASP di Risk Rating

Fornisce un set di fattori per stimare probabilità e impatto.

La probabilità è stimata basandosi su due insiemi di fattori:

- threat agent factors
- vulnerability factors

L'impatto invece è stimato basandosi su:

- technical impact factors
- business impact factors

Threat Agent Factors

- **skill level:** quanto è alto il livello di skill del gruppo?
- **motivo:** quanto motivato è il gruppo ad attaccare?
- **opportunity:** che risorse e opportunità sono richieste da questo gruppo per trovare e exploitare la vulnerabilità?
- **size:** quanto grande è il gruppo?

Vulnerability Factors

- **facilità di scoperta:** quanto facile è per il gruppo trovare la vulnerabilità?
- **facilità di exploit:** quanto facile è per il gruppo effettivamente exploitare?
- **awareness:** quanto è nota la vulnerabilità a questo gruppo?
- **intrusion detection:** quanto è probabile che un exploit sia rilevato?

Technical Impact Factors

- **perdita di confidenzialità:** quanti dati potrebbero essere divulgati e quanto sensibili sono?
- **perdita di integrità:** quanti dati potrebbero essere corrotti e come sono danneggiati?
- **perdita di disponibilità:** quanti servizi potrebbero essersi persi e quanto vitali sono?
- **perdita di accountability:** le azioni dei threat agents sono riconducibili a qualcuno?

Business Impact Factors

- **financial damage:** quanto danno finanziario porta un exploit?
- **reputation damage:** potrebbe un exploit portare a danni di reputazione che metterebbero in pericolo il business?
- **non-compliance:** quanta esposizione comporta la non conformità?
- **privacy violation:** quanta informazione personale identificabile potrebbe essere divulgata?

Determinare la gravità del rischio

Calcoliamo i valori di impact e probabilità con le seguenti tabelle:

"Threat agent factors"				"Vulnerability factors"			
Skill level	Motive	Opportunity	Size	Ease of discovery	Ease of exploit	Awareness	Intrusion detection
5	2	7	1	3	6	9	2
Overall likelihood=4.375 (MEDIUM)							

Dopodichè con il valore ottenuto avremo uno tra i seguenti livelli

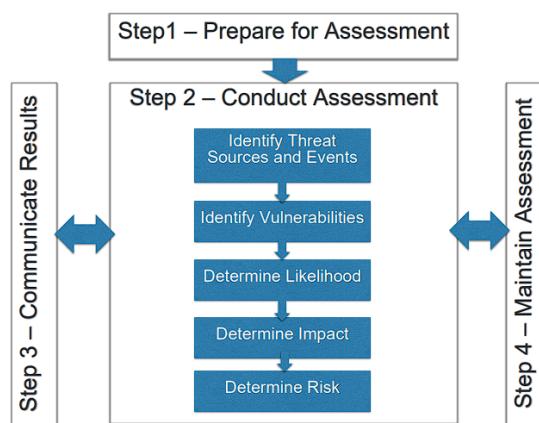
A questo punto incrociamo nella tabella sottostante e troviamo l'overall della gravità del rischio.

Technical Impact				Business Impact			
Loss of confidentiality	Loss of integrity	Loss of availability	Loss of account ability	Financial damage	Reputation damage	Non-compliance	Privacy violation
9	7	5	8	1	2	1	5
Overall technical impact=7.25 (HIGH)				Overall business impact=2.25 (LOW)			

Likelihood and Impact Levels		Overall Risk Severity			
Impact	Likelihood	HIGH	Medium	High	Critical
		MEDIUM	Low	Medium	High
		LOW	Note	Low	Medium
			LOW	MEDIUM	HIGH

Risk Assessment con NIST 800-30

È una guida con l'obiettivo di fornire degli step da seguire per condurre un risk assessment corretto



Prepare for risk assessment

L'obiettivo in questa fase è stabilire un contesto per l'assessment del rischio, tra le task che include:

- identificazione obiettivo dell'assessment
- identificazione del contesto dell'assessment
- identificare le assunzioni e vincoli associati all'assessment
- identificare il risk model, approccio dell'assessment e l'approccio dell'analisi

Conduct risk assessment

Si stila una lista di cyber security risks, tra le task da fare troviamo:

- **identificare threat source**
 - si identificano le fonti di minaccia che creano preoccupazione(outsider, avversari, user, environment, disastri, software).

Per fonti avversarie bisognerebbe chiedersi: quanto skilled, motivata e cosa sta targeting la src?

Per fonti non avversarie bisognerebbe invece chiedersi: qual'è l'effetto della threat src?
- **identificare threat events**
 - si identifica il threat event, ossia come qualcosa potrebbe accadere? Cosa attacca?

- **identificare vulnerabilità**

- valutare le vulnerabilità che un threat event può sfruttare e la loro gravità

Cosa potrebbe rendere possibile il threat event?

- **determinare likelihood**

- si determina la likelihood del threat event, lo si fa considerando la capacità, intento, targeting e quanto difficile è exploitare la vulnerabilità.

- Adversarial

TABLE G-2: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT INITIATION (ADVERSARIAL)

Qualitative Values	Semi-Quantitative Values	Description
Very High	96-100	10
High	80-95	8
Moderate	21-79	5
Low	5-20	2
Very Low	0-4	0

- Non Adversarial

Qualitative Values	Semi-Quantitative Values	Description
Very High	96-100	10
High	80-95	8
Moderate	21-79	5
Low	5-20	2
Very Low	0-4	0

- Likelihood di risultare in un impatto avverso

TABLE G-4: ASSESSMENT SCALE – LIKELIHOOD OF THREAT EVENT RESULTING IN ADVERSE IMPACTS

Qualitative Values	Semi-Quantitative Values	Description
Very High	96-100	10
High	80-95	8
Moderate	21-79	5
Low	5-20	2
Very Low	0-4	0

- Overall Likelihood

Likelihood of Threat Event Initiation or Occurrence	Likelihood Threat Events Result in Adverse Impacts				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

- **determinare impact**

- Si determina il danno potenziale causato agli assets dell'organizzazione

Type of Impact	Impact
Harm to Operations	<ul style="list-style-type: none"> Inability to perform current business functions Non compliance Direct Financial Costs Damage to image of reputation
Harm to Assets	<ul style="list-style-type: none"> Damage to or loss of physical facilities Damage to or loss of information systems or networks Damage to or loss of equipment Damage to or loss of information assets Loss of intellectual properties
Harm to Individuals	<ul style="list-style-type: none"> Loss of life Identity Theft Loss of PII Damage to the reputation
Harm to Other Organizations	<ul style="list-style-type: none"> Non compliance Direct Financial Costs Damage to image of reputation
Harm to the Nation	<ul style="list-style-type: none"> Damage to a critical infrastructure

Impact	Description
Very High	Threat event could have multiple severe or catastrophic adverse effects on organizational operations, assets, individuals, other organizations or the Nation
High	Threat event could have severe or catastrophic adverse effects on organizational operations, assets, individuals, other organizations or the Nation
Moderate	Threat event could have serious effects on organizational operations, assets, individuals, other organizations or the Nation
Low	Threat event could have limited effects on organizational operations, assets, individuals, other organizations or the Nation
Very Low	Threat event could have negligible on organizational operations, assets, individuals, other organizations or the Nation

• determinare risk

- Si determina il livello di rischio come combinazione di likelihood e impact

Adverse Impact	Likelihood of Threat Event				
	Very Low	Low	Moderate	High	Very High
Very High	Low	Moderate	High	Very High	Very High
High	Low	Moderate	Moderate	High	Very High
Moderate	Low	Low	Moderate	Moderate	High
Low	Very Low	Low	Low	Moderate	Moderate
Very Low	Very Low	Very Low	Low	Low	Low

Comunicate Results

Si comunicano i risultati dell'assessment e si condividono le informazioni legate al rischio.

Più precisamente si comunicano i risultati alle persone dell'organizzazione responsabili di supportare le risposte ai rischi e si condividono le informazioni legate ai rischi al personale che lo riguarda dell'organizzazione

Maintain Risk Assessment

Mantere la conoscenza dei rischi a cui un'organizzazione potrebbe incorrere aiuta le organizzazioni

- determinare l'effettività del rischio
- identificare cambi negli asset dell'organizzazione che potrebbero essere risk-impacting
- verificare la conformità

Riassumendo quindi il **risk management** è il processo con cui si prioritizzano i rischi identificati in termini di likelihood e sulla base di ciò minimizzare, monitorare e controllare l'impatto di questi rischi.

Il **risk assessment** invece è il processo che identifica e valuta il livello di rischio per un'organizzazione va incontro. ↗ valutazione

Threat Modeling

Modellazione delle minacce

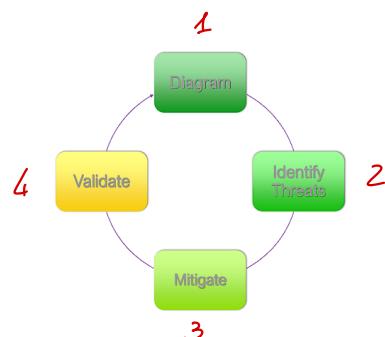
Tra le tecniche utilizzate per fare threat modeling troviamo:

- modellare e analizzare i sistemi tecnologici e i servizi
- capire come il sistema o il servizio può essere attaccato
- misure o controlli necessari per gestire il rischio di tali attacchi

La miglior applicazione delle tecniche di modellazione però è quella di informare la progettazione e la fase di sviluppo di un sistema o del ciclo di vita di un servizio

STRIDE(Microsoft)

Tecnica di threat modelling popolare, pensata da microsoft, si concentra su cosa l'attaccante cerca di ottenere, ampiamente usata nell'industria, il processo è identificato nell'immagine a fianco:

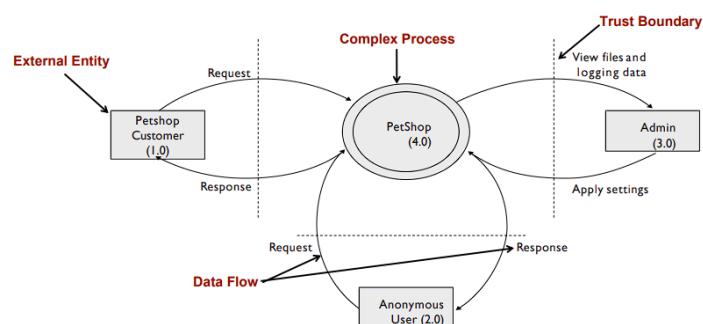


Data Flow Diagrams(step 1)

È una rappresentazione grafica del sistema sotto revisione, modella come entrano, escono e attraversano il sistema i dati, quindi tutte le src e dst e tutti i processi rilevanti in cui entrano i dati. Dei buoni Data Flow Diagrams sono fondamentali per il threat modeling.

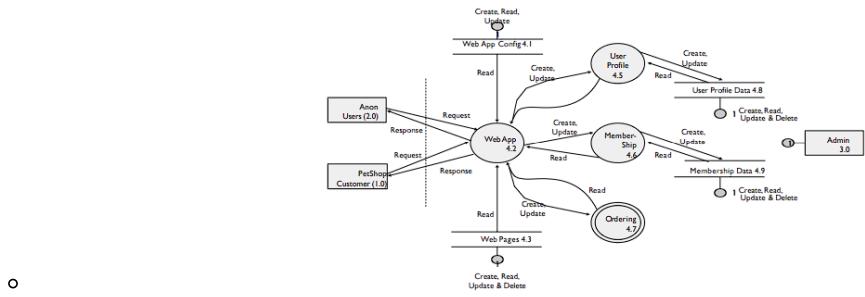
Tra gli elementi dei diagrammi troviamo:

- **entità esterne:** persone, altri sistemi
- **processi:** dll, componenti, servizi
- **data flow:** fun call, network traffic, rpc
- **data store:** database, file, shmem
- **trust boundary:** file system, process boundary



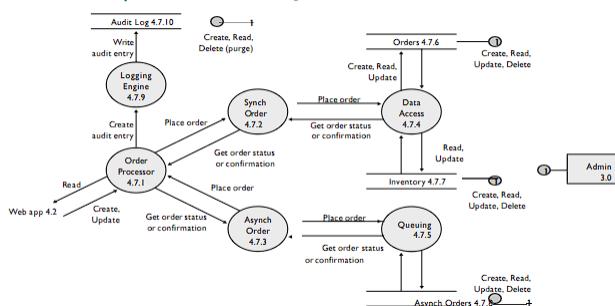
DFD decomposition consiste nell'iterare su processi, stores, e guardare dove devono essere spezzettati a loro volta, quello che si fa è:

- disegnare un **diagramma del contesto**, molto ad alto livello con software e entità esterne che interagiscono
↳ Analisi a livello di sistema, vengono identificate minacce generiche per l'intero sistema
- si passa poi al **diagramma di livello 1** di alto livello in cui compaiono i major business processes
↳ Analisi a livello di sottosistema
vengono individuate le minacce specifiche per ciascun sottosistema



- eventualmente si arriva al **livello 2 o addirittura superiori** fino a che la decomposizione è possibile

↳ Analisi a livello di componenti; vengono identificate le minacce per ciascun componente del sistema



Identify Threats(step 2)

Gli esperti fanno un brainstorm, se non si è esperti si può utilizzare **stride** per passare tra gli elementi del diagramma, otteniamo essenzialmente delle specifiche sulla manifestazione della minaccia:

Threat	Property we want
Spoofing	Authentication
Tampering	Integrity
Repudiation	Nonrepudiation
Information Disclosure	Confidentiality
Denial of Service	Availability
Elevation of Privilege	Authorization

SPOOFING

- la proprietà presa in causa è l'autenticazione, impersona qualcosa o qualcun'altro.

TAMPERING

- la proprietà presa in causa è l'integrità, modifica dati o codice.

REPUDIATION

- la proprietà presa in causa è la non-repudiation, si sostiene di non aver fatto una certa azione.

INFORMATION DISCLOSURE

- la proprietà presa in causa è la confidenzialità, si espongono informazioni a qualcuno non autorizzato a vederle.

DENIAL OF SERVICE

- la proprietà presa in causa è la disponibilità, si negano o degradano servizi all'utente.

ELEVATION OF PRIVILEGE

- la proprietà presa in causa è la authorization, si ottengono capacità senza la proper authorization

ELEMENT	S	T	R	I	D	E
External Entity	✓		✓			
Process	✓	✓	✓	✓	✓	✓
Data Store	✓	?		✓	✓	
Data Flow	✓		✓	✓		

Threat Type	DFD Elements
Spoofing	External Entities: Pet Shop Customer... Processes: Web application, Order processor
Tampering	Processes: Web application, Order processor Data stores: Audit-log data,... Data Flows: Pet Shop Customer to Web application,....
Repudiation	External Entities: Pet Shop Customer...
Information Disclosure	Data stores: Audit-log data,... Data Flows: Pet Shop Customer to Web application,....
Denial of Service	Data stores: Audit-log data,... Data Flows: Pet Shop Customer to Web application,....
Elevation of Privileges	Processes: Web application, Order processor

Quello che si vuole fare inoltre è passare dai threat generici a concreti con degli alberi, dove usiamo composizioni and/or di threat, stride fornisce 12 threat tree patterns: slide 26-38 per img.

- 1 per spoofing
- 3 per tampering
- 1 per repudiation
- 3 per inf discl
- 3 per dos
- 1 per elevation of privileges

DFD Element	Threat Type	Threat
Pet Shop Customer to Web application	Information Disclosure (I)	Observe message – No Message Confidentiality
Audit Log Data Store	Tampering (T)	Tampering with Data Store – Weak Protection
Order Processor	Elevation of Privileges (EoP)	Leverage Insufficient Authorization

Assess the risk(step 2)

Il livello di rischio ancora una volta è dato dalla combinazione di likelihood e impact, ci sono 4 livelli

- 1 very high, da fixare durante la fase di sviluppo.
- 2 high, da fixare durante la fase di sviluppo.
- 3 medium, da fixare prima che il prodotto vada in release.
- 4 low, da fixare solo se il tempo lo permette.

Microsoft SDL(security development lifecycle) nella fase di requirements dice di specificare le **bug bars**, che non fanno altro che classificare un threat basandosi sull'impatto che hanno.

In primo momento il bug è assegnato a **stride** così da piazzarlo in una categoria, poi il livello di rischio è associato al threat basandosi su varie dinamiche tra cui:

- server application vs client application
- local vs remote accessibility
- accessibilità autenticati vs admin
- ecc

STRIDE Threat Type	Client/Server	Scope	Risk Level
Denial of Service	Client	Requires reinstallation of system and/or components	2
	Client	Requires cold reboot or causes Blue Screen/Bug Check	3
	Client	Temporary DoS: restart of application	4
	Server	Anonymous user sends a small amount of data	2
	Server	Authenticated permanent DoS	3

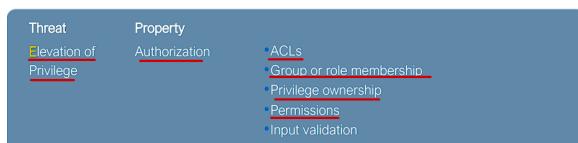
DFD Element	Threat Type	Threat	Risk Level
Pet Shop Customer to Web application	Information Disclosure (I)	Observe message – No Message Confidentiality	1
Audit Log Data Store	Repudiation(R)	Tampering with Data Store – Weak Protection	1
Order Processor	Elevation of Privileges (EoP)	Leverage Insufficient Authorization	1

Plan for mitigations(step 3)

Ci sono 4 modi per affrontare le minacce:

- do nothing
- rimuovere la feature
- accettare la vulnerabilità nel design
- contrastare il threat con la tecnologia → usare le liste di tecnologie di mitigazione

Standard mitigations



Validating threat models(step 4)

È necessario convalidare l'intero modello delle minacce, verificare se il diagramma corrisponde all'implementazione finale, assicurarsi che le minacce siano opportunamente elencate. Applicare almeno STRIDE per ogni elemento che tocca il confidence board. Controllare dunque che ogni minaccia sia mitigata adeguatamente. Verificare infine la corretta implementazione delle mitigazioni.

Nist cybersecurity framework

Sviluppato da nist per ridurre i cyber rischi alle infrastrutture critiche, è un catalogo di cybersecurity activities.

Le attività o funzioni sono 5, scomposte poi a loro volta in categorie e sottocategorie, ci riferiamo a tutto ciò come il **core**. Se le attività corrispondono a che cosa? Le categorie rispondono a che cosa/come? e sono le attività decomposte mentre le sottocategorie a come? e dicono come implementarle.

Le 5 attività sono:



Un'esempio di breakdown invece può essere:

Function	Category	Informative References	
	ID	ID.SC-1: Cyber supply chain risk management processes are identified, established, assessed, managed, and agreed to by organizational stakeholders ID.SC-2: Suppliers and third party partners of information systems, components, and services are identified, prioritized, and assessed using a cyber supply chain risk assessment process	CIS CSC 4 COBIT 5 APO10.01, APO10.02, APO10.04, APO10.05, APO12.01, APO12.02, APO12.03, APO12.04, APO12.05, APO12.06, APO13.02, BAI02.03 ISA 62443-2-1:2009 4.2.3.1, 4.2.3.2, 4.2.3.3, 4.2.3.4, 4.2.3.6, 4.2.3.8, 4.2.3.9, 4.2.3.10, 4.2.3.12, 4.2.3.13, 4.2.3.14 ISO/IEC 27001:2013 A.15.2.1, A.15.2.2 NIST SP 800-53 Rev. 4 RA-2, RA-3, SA-12, SA-14, SA-15, PM-9
			Subcategory

Identify

L'organizzazione deve identificare:

- sistemi e dati
- debolezze e forze dei sistemi
- vulnerabilità, threat, likelihood, impact e overall risk
- critical business process che dipendono dai precedenti
- tutte le risorse
- governance

Identify categories

Function	Categories
Identify (ID)	Asset Management (ID.AM) Business Environment (ID.BE) Governance (ID.GV) Risk Assessment (ID.RA) Risk Management Strategy (ID.RM) Supply Chain Risk Management (ID.SC)

Protect

Le attività di protect si concentrano su:

- assicurare una forte autenticazione e access control
- proteggere dati
- manutenzione sicura degli assets
- securing people
- assicurare che siano presenti i controlli di tutti i tipi

Protect categories

Function	Categories
Protect (PR)	Identity Management, Authentication, Access Control (PR.AC) Awareness and Training (PR.AT) Data Security (PR.DS) Information Protection Processes and Procedures (PR.IP) Maintenance (PR.MA) Protective Technology (PR.PT)

Detect

Le funzioni di detect invece:

- si concentrano su rilevazione di processi e tecnologie
- controllano anomalie e eventi inusuali
- assicurano continui monitoraggi di sicurezza e rischi

Detect categories

Function	Categories
Detect (DE)	Anomalies and Events (DE.AE) Security Continuous Monitoring (DE.CM) Detection Processes (DE.DP)

Respond

Per quanto concerne invece le attività di respond:

- pianificano risposte a incidenti e emergenze
- assicurano robustezza delle comunicazioni negli incidenti
- analizzano la causa degli incidenti
- mitigano danni a sistemi, dati ecc

Respond categories

Function	Categories
Respond (RS)	Response Planning (RS.RP) Communications (RS.CO) Analysis (RS.AN) Mitigation (RS.MI) Improvements (RS.IM)

Recover

Per finire con le funzioni di recover ci si concentra su:

- business continuity, recupero dall'incidente o planning di recovery da disastri
- mantenere le comunicazioni durante il recovery process
- improving l'effort di recovery

Recover categories

Function	Categories
Recover (RC)	Recovery Planning (RC.RP) Improvements (RC.IM) Communications (RC.CO)

CSF Tiers

Rappresentano il livello di implementazione delle attività descritte.

I tiers spaziano da parziali(T1) a adattivi(T4) e ciò ci permette di descrivere:

- un grado di rigore crescente
- quanto bene si integrano le decisioni di cybersecurity nelle decisioni di rischio più ampie
- il grado con il quale l'organizzazione condivide e riceve cybersec info da parti esterne

Al livello adaptive abbiamo un azienda che adatta le proprie pratiche di cybersecurity in base a quelle precedenti, comprese le lezioni apprese, ci si adegua adattivamente all'evoluzione delle tecnologie e delle minacce.

L'organizzazione non ha un risk management, non ha piani e i guasti non sono controllati.

(T2) Risk Informed ha informazioni sui rischi ma non ha processi di gestione del rischio.

(T3) Repeatable

In grado di elaborare i rischi.

CSF Profile

Un csf profile si ottiene unendo le 5 attività con rischi, obiettivi del business e ambiente tecnico.

4

Privacy

Il concetto di privacy è abbastanza disordinato, non c'è una vera e propria articolazione di cosa significhi, anzi ci sono varie definizioni vediamone un paio:

- "il diritto di essere lasciati da soli"
- "il diritto di un individuo di poter decidere quali informazioni riguardanti esso possano essere comunicate ad altri e sotto quali circostanze"
- "trasparenza, scopi, proporzionalità e accountability"

Proprietà della privacy

Hard Privacy

Il soggetto fornisce meno dati possibile, riduce il più possibile la necessità di fidarsi di altre entità.

Soft Privacy

Il soggetto ha già perso il controllo dei suoi dati, in pratica molto difficile per i soggetti proprietari dei dati verificare come sono collezionati e processati quest'ultimi.

Anonimità

Un attaccante non deve riuscire a identificare sufficientemente un soggetto tra un insieme di soggetti, ciò si può fare ad esempio nascondendo i link che ci sono tra identità e azione o identità e pezzi di informazione.

Pseudonimo → identificatore di un soggetto diverso dal suo nome reale.

Unlinkability

In un sistema, l'attaccante non può sufficientemente distinguere quando due o più oggetti di interesse sono relazionati o no → ad esempio voci in database diversi riguardanti la stessa persona

Undetectability

L'attaccante non può sufficientemente distinguere se esiste o no.

unobservability: undetectability dell'oggetto per i soggetti coinvolti e anonimia dei soggetti presenti nell'oggetto anche tra loro stessi non sono inoltre osservabili azioni sull'oggetto

Se invece parliamo di unobservability parliamo dell'undetectability dell'oggetto di interesse nei confronti di tutti i soggetti coinvolti e anonimia dei soggetti coinvolti nell'oggetto di interesse anche nei confronti degli altri soggetti coinvolti in quell'oggetto di interesse.

Esempio: impossibile vedere quando un utente sta accedendo a una pagina web, impossibile sapere quando una entry nel database corrisponde a una persona reale.

Plausible Deniability

Non deve essere possibile provare che un utente sa, ha fatto o ha detto qualcosa.

Confidentiality

Mantenere restrizioni autorizzate su accesso e divulgazione di informazioni includendo i mezzi per proteggere la privacy personale e informazioni proprietarie.

Compliance

È relazionata alla legislatura sulla protezione dei dati, il gdpr specifica i principi per processare dati personali in eu.

Awareness

Gli utenti dovrebbero essere messi al corrente delle conseguenze che ci sono al condividere informazioni

Attacchi alla privacy

A Taxonomy of Privacy by J.Solove

Cerca di ordinare i diversi danni che possono derivare dalle violazioni della privacy.

Troviamo tre componenti:

- **Information Collection**

- **Information Processing**

- **Information Dissemination**

- **Invasion**

Information Collection

In questa categoria troviamo:

- **sorveglianza:** guardare, ascoltare, registrare attività di un individuo.
 - *controllori smart*
Gli smart meters sono presentati come un'iniziativa per l'ambiente e il risparmio energetico. Ma è un modello altamente sorvegliante. Può dire quante docce hai fatto, quando stai cucinando, ecc..
- **interrogazione:** consiste in varie forme di domandare o sondare informazioni.
le informazioni vengono estorte forzando l'individuo a dare informazioni che normalmente non drebbe

Information Processing

Questa categoria invece include:

- **aggregazione:** coinvolge la combinazione di vari pezzi di dati di una persona
- **identificazione:** linking di informazioni a particolari individui
- **insicurezza:** coinvolge la mancanza di attenzione nella protezione di informazioni salvate da leaks e accessi impropri
- **usi secondari:** è l'utilizzo di informazioni collezionate per uno scopo, per un'altro scopo senza il consenso dell'owner.
- **esclusioni:** concerne il fallimento di consentire al proprietario dei dati di sapere che altri hanno dei suoi dati e partecipare alla manipolazione e utilizzo di questi. → *L'utente non ha modo di controllare i dati;*

Information Dissemination

In quest'altra categoria troviamo invece:

- **violazione della confidenzialità:** rompere la promessa di mantenere le info di una persona confidenziali
- **divulgazione:** rivelazione di informazioni di una persona che impattano la maniera in cui altri giudicano quest'ultima
di informazioni intime
- **exposure:** comporta la rivelazione della nudità, del dolore o delle funzioni corporee di un altro individuo
- **accessibilità increased:** si amplifica l'accessibilità di un'info
- **blackmail:** è la minaccia di rilevare informazioni personali, spesso chiedendo un riscatto
- **appropriazione:** coinvolge l'utilizzo di dati dell'identità del soggetto per obiettivi e interessi di un altro.
- **distorsione:** consiste nella disseminazione di informazioni false o equivocabili riguardo individui.

Invasion → rispetto alle altre tecniche qui abbiamo un'interazione con la vittima

Infineabbiamo:

- **intrusion:** concerne atti invasivi che disturbano la tranquillità o solitudine di un individuo
- **decisional interference:** comporta intrusioni del governo sulle decisioni dei dati di soggetti riguardanti affari privati

Privacy enhancing technologies

Sono tutti i tool, meccanismi o architetture che mirano a mitigare problemi di privacy, possono essere applicati alle comunicazioni o db esistenti e possono essere rilasciati da individui o organizzazioni.

Data protection technologies

Aiuta a progettare l'informazione, i sistemi di comunicazione e i servizi in modo che si minimizzi la collezione e l'utilizzo di dati personali e facilita la conformità alle regole di data protection.

Dovrebbero risultare in una complicazione nel rompere certe regole di protezione dei dati o comunque rendere più difficile trovarle.

Esempi di queste tecnologie sono cifratura dei dati in rest e trasmissione, authorization e authentication di dipendenti che maneggiano dati personali.

User awareness technologies

Set di tecnologie che permette allo user di scegliere se, quando e in che circostanze le sue informazioni personali sono divulgate. Aiuta gli user a fare delle scelte consapevoli che riguardano la loro protezione della privacy.

Esempi di queste sono privacy friendly defaults, clear concise e capibili privacy policies.

Data Anonymisation

→ ho un costante Tradeoff tra

Utility
Necessità riguardanti i dati raccolti e le loro analisi

Privacy
Necessità di garantire la privacy

Uno dei problemi della privacy è capire, dato un dataset di informazioni personali sensibili come computare e rilasciare funzioni del dataset proteggendo al contempo la privacy degli individui coinvolti.

In un dataset categorizziamo gli attributi in 3 classi:

- **identificatori esplicativi:** identificano un utente → nome, cognome, ci.
- **quasi-identificatori:** data di nascita, zip code, cellphone
- **attributi sensibili:** malattie, salario, ecc.

Per proteggere gli identificatori esplicativi posso fare **tokenizzazione** che genera un token unico per i dati in input oppure **substitution** che rimpiazza il valore di un attributo con valori alternativi.

Ciò però non è sufficiente per proteggere gli identificatori esplicativi, ad esempio con un record linkage possiamo incrociare dati rilasciati come anonimi con altri dati pubblici e potenzialmente trarre informazioni dai dati anonimi.

K-Anonymity

Un record deve essere indistinguibile da almeno k-1 records per quanto riguarda i quasi-identificatori.

Ogni classe di equivalenza deve contenere almeno k records che hanno gli stessi valori per i quasi-identificatori.

Original Database

Name	Zipcode	Age	Disease
Hillary	47677	29	Heart Disease
Jenny	47602	22	Heart Disease
Bob	47678	27	Heart Disease
Izzy	47905	43	Flu
John	47909	52	Heart Disease
Fred	47906	47	Cancer
Sam	47605	30	Heart Disease
Carl	47673	36	Cancer
Sarah	47607	32	Cancer

Released Database

Zipcode	Age	Disease
476**	2*	Heart Disease
476**	2*	Heart Disease
476**	2*	Heart Disease
4790*	≥40	Flu
4790*	≥40	Heart Disease
4790*	≥40	Cancer
476**	3*	Heart Disease
476**	3*	Cancer
476**	3*	Cancer

Per arrivare ad avere la k-anonymity serve:

- **generalization:** rimpiazza i quasi-identificatori specifici con dei valori meno specifici fino a che ottiene k identici valori, inoltre partiziona domini di valori ordinati in partizioni.
- **suppression:** quando la generalizzazione causa troppa perdita di informazione (comune con gli outliers), ci sono molti algoritmi.

→ avrà però perdita di informazione eliminando i record

Name	Zipcode	Age	Sex	Disease
Hilary	47677	29	F	Heart Disease
Jenny	47673	22	F	Heart Disease
Bob	47678	27	M	Heart Disease
Izzy	47905	43	F	Flu
John	47909	52	M	Heart Disease
Fred	47906	47	M	Cancer
Sam	47605	30	M	Heart Disease
Carl	47602	36	M	Cancer
Sarah	47607	32	F	Cancer

original

Zipcode	Age	Sex	Disease
47677	21-30	F	Heart Disease
47673	21-30	F	Heart Disease
47678	21-30	M	Heart Disease
47909	51-60	M	Heart Disease
47906	41-50	M	Cancer
47605	21-30	M	Heart Disease
47602	31-40	M	Cancer
47607	31-40	F	Cancer

generalization

Zipcode	Age	Sex	Disease
47677	10-29	F	Heart Disease
47673	10-29	F	Heart Disease
47678	10-29	M	Heart Disease
47909	50-69	M	Heart Disease
47906	50-69	M	Cancer
47605	30-49	M	Heart Disease
47602	30-49	M	Cancer
47607	30-49	F	Cancer

generalization

Zipcode	Age	Sex	Disease
*	10-29	*	Heart Disease
*	10-29	*	Heart Disease
*	10-29	*	Heart Disease
*	50-69	M	Heart Disease
*	50-69	M	Cancer
*	30-49	*	Heart Disease
*	30-49	*	Cancer
*	30-49	*	Cancer

generalization + suppression

Zipcode	Age	Sex	Disease
47670	10-29	*	Heart Disease
47670	10-29	*	Heart Disease
47670	10-29	*	Heart Disease
47900	50-69	M	Heart Disease
47900	50-69	M	Cancer
47600	30-49	*	Heart Disease
47600	30-49	*	Cancer
47600	30-49	*	Cancer

generalization + suppression

Tra i problemi che ha la k-anonymity c'è il fatto che non fornisce privacy se i valori sensibili di una certa classe hanno carenze di diversità e l'attaccante ha delle conoscenze di background.

↳ l'attaccante riesce a fare inferenza
(ad esempio so che popolazione giapponese
ha un basso rischio di contrarre malattie cardiache)

L-diversity

L'intuizione è che gli attributi sensibili devono presentare una diversità in ogni classe di quasi-identificatori.

Più concretamente ogni classe deve avere almeno I sensitive values ben rappresentati, inoltre non solo devono avere abbastanza valori differenti, ma devono anche essere distribuiti abbastanza uniformemente.

L'entropia della distribuzione dei sensitive values in ogni classe di equivalenza E deve essere almeno $\log(l)$, S dominio dei sensitive attribute, mentre p è la frazione di record in E che hanno s-v s:

$$\text{Entropy}(E) = - \sum_{s \in S} p(E, s) \log p(E, s)$$

Tra le limitazioni di L-diversity vediamo come sia debole a un similarity attack, sappiamo che bob ha un certo zip e una certa età, per similarità dei campi quasi-identificatori troviamo che bob ha un salario che sicuramente varia tra 3-5k e ha sicuramente qualche disturbo legato allo stomaco.

Similarity attack
A 3-diverse patient table

Similarity attack		A 3-diverse patient table			
Bob					
Zip	Age	Zipcode	Age	Salary	Disease
47678	27	476**	2*	3K	Gastric Ulcer
		476**	2*	4K	Gastritis
		476**	2*	5K	Stomach Cancer
		4790*	≥40	6K	Gastritis

L-diversity non considera la semantica dei valori sensibili

T-closeness

La distribuzione degli attributi sensibili in ogni classe di equivalenza deve essere vicina alla distribuzione che hanno nel dataset originale.

L'**earth mover distance** stima intuitivamente quanta fatica serve per trasformare una distribuzione in un'altra distribuzione, considera una distribuzione come un mucchio di terra in uno spazio e l'altra come una collezione di buchi nello stesso spazio, EMD misura il minimo lavoro necessario per riempire i buchi con la terra.

questa fatica che rappresenta la diversità, non deve essere troppo grande, altrimenti è semplice distinguere

Zipcode	Age	Salary	Disease
476**	20-40	3K	Gastric Ulcer
476**	20-40	4K	Gastritis
476**	20-40	5K	Stomach Cancer
4790*	40-60	6K	Gastritis
4790*	40-60	11K	Flu
4790*	40-60	8K	Bronchitis
476**	20-40	7K	Bronchitis
476**	20-40	9K	Pneumonia
476**	20-40	10K	Stomach Cancer

Zipcode	Age	Salary	Disease
476**	20-40	3K	Gastric Ulcer
476**	20-40	9K	Pneumonia
476**	20-40	5K	Stomach Cancer
4790*	40-60	6K	Gastritis
4790*	40-60	11K	Flu
4790*	40-60	8K	Bronchitis
476**	20-40	7K	Bronchitis
476**	20-40	4K	Gastritis
476**	20-40	10K	Stomach Cancer

In generale comunque semplicemente anonimizzare i dati non basta in quanto **non è safe**.

Privacy differenziale

Non è una tecnica, ma una proprietà da soddisfare, il ragionamento è: se prendo il dataset, effettuo l'analisi e dopo tolgo un dato il risultato dell'analisi deve essere molto simile
↳ la differenza è minore di un certo ϵ

$$Pr[M(D) \in S] \leq e^{\epsilon} \cdot Pr[M(D') \in S]$$

Con la privacy differenziale possiamo computare statistiche descrittive come conteggi, medie, mediane, istogrammi, possiamo fare task supervisionate o meno di ML come classificazione, regressione ecc o la generazione di dati sintetici

Data Protection

Partiamo col definire i dati personali come qualsiasi informazione relativa a una persona identificata o identificabile, come numeri identificativi ma anche informazione di carattere fisiologico, psicologico, mentale o sociale.

Chi è chi?

- **controller o data subject:** una persona naturale identificata o identificabile i quali personali dati sono processati
- **data controller:** una persona naturale o legale, autorità pubblica, agenzia o altro corpo che da solo o con altri determina gli scopi e mezzi con cui vengono processati i dati personali
- **data processor:** una persona naturale o legale, pubblica autorità o altri corpi che processano dati personali per conto del controller

Chi sono invece i **data controller**? Secondo l'articolo 29wp sono i service provider mentre gli user sono i **controller**. Ovviamente sia **data controller** che **data processor** avranno determinati obblighi.

Obblighi del data controller

- Deve avere una base giuridica per processare i dati
- Deve collezionare solo i dati necessari per il suo scopo
- Deve tenere dati accurati
- Deve abilitare i data subject a esercitare i loro poteri
- Deve processare i dati per uno specificato o specifico e limitato scopo
- Deve tenere i dati fintantoche sono necessari
- Deve tenere i dati sicuri
- Deve mantenere un record delle attività di processamento

Legalità

Devono avere una base giuridica, tra le possibili basi giuridiche ci sono:

- **consenso:** il data subject ha dato il consenso a processare i suoi dati per degli scopi specifici

- **contratto:** il processamento è necessario per la performance di un contratto nel quale il data subject è parte
- **obblighi legali:** il processamento è necessario per l'adempimento di un obbligo legale al quale è soggetto il data subject
- **interessi vitali:** il processamento è necessario per proteggere interessi vitali del data subject o di un'altra persona naturale
- **pubblici interessi:** il processamento è necessario per la performance di un task di pubblico interesse
- **legittimi interessi:** il processamento è necessario per scopi di legittimo interesse perseguito dal controller o terze parti, tranne dove tali interessi sono sovrascritti da interessi o diritti fondamentali e libertà del data subject che richiede protezione dei dati personali, in particolare quando il data subject è un bambino

Consenso

Per consenso del soggetto dei dati intendiamo qualsiasi indicazione liberamente espressa, specifica, informata e inequivocabile delle volontà del soggetto dei dati, mediante una dichiarazione o un'azione chiara e affermativa, che attesti l'accettazione del trattamento dei dati personali a lui o a lei relativi.

- **liberamente dato:** Non dovrebbe essere in genere una condizione preliminare per iscriversi a un servizio.
- **specifico:** Richiedi il consenso per ogni scopo e attività di trattamento.
- **informato:** Spiega in un linguaggio chiaro e conciso
 - nome del responsabile del trattamento dei dati
 - nome di eventuali terzi responsabili
 - scopi del trattamento
 - qualsiasi attività di trattamento
 - informa gli individui che possono revocare il consenso in qualsiasi momento
- **indicazione non ambigua:** Il silenzio, le caselle preselezionate o l'inattività non dovrebbero costituire consenso.

Limitazione degli scopi

- I dati personali devono essere raccolti per scopi specifici, esplicativi e legittimi e non devono essere ulteriormente trattati in modo incompatibile con tali scopi.
- I responsabili del trattamento dei dati devono:
 - specificare gli scopi nelle informazioni sulla privacy per gli individui
 - specificare il o i fini del trattamento dei dati personali nei registri di trattamento
 - non trattare i dati per scopi incompatibili con quelli iniziali.
- Gli scopi compatibili sono quelli di archiviazione nell'interesse pubblico, di ricerca scientifica o storica o di scopi statistici.

Minimizzazione dei dati

I dati personali devono essere adeguati, pertinenti e limitati a quanto è necessario in relazione agli scopi per i quali vengono trattati.

I responsabili del trattamento dei dati devono assicurarsi che i dati personali che stanno elaborando siano:

- **Adeguati:** Sufficienti per adempiere correttamente allo scopo dichiarato
- **Pertinenti:** Devono avere un legame razionale con tale scopo
- **Limitati a quanto è necessario:** Non devono essere detenuti più di quanto sia necessario per quel determinato scopo.

Accuratezza

I dati personali devono essere accurati e, quando necessario, mantenuti aggiornati; devono essere adottate tutte le misure ragionevoli per garantire che i dati personali inesatti, in relazione agli scopi per i quali vengono trattati, siano cancellati o rettificati senza indugi.

Limitazione dello stoccaggio

- I dati personali devono essere conservati in una forma che permetta l'identificazione degli interessati per un periodo non superiore a quanto necessario per gli scopi per i quali i dati personali sono trattati
- I dati personali possono essere conservati per periodi più lunghi nella misura in cui saranno trattati esclusivamente per scopi di archiviazione nell'interesse pubblico, finalità di ricerca scientifica o storica, o scopi statistici

Security

I dati personali devono essere trattati in modo che ne sia garantita la sicurezza appropriata, compresa la protezione contro il trattamento non autorizzato o illecito e contro la perdita, la distruzione o il danneggiamento accidentali, mediante l'adozione di adeguate misure tecniche o organizzative.

Responsabilità

- I responsabili del trattamento devono essere in grado di dimostrare la conformità alle obbligazioni del GDPR.
- Devono mettere in atto adeguate misure tecniche e organizzative per soddisfare i requisiti di responsabilità. Tali misure includono:
 - Adozione e attuazione di politiche sulla protezione dei dati.
 - Adozione di un approccio basato sulla "protezione dei dati per progettazione e per impostazione predefinita".
 - Stipula di contratti scritti con organizzazioni che trattano dati personali per suo conto.
 - Conservazione della documentazione sulle attività di trattamento;
 - Implementazione di adeguate misure di sicurezza.
 - Registrazione e, se necessario, segnalazione di violazioni dei dati personali.
 - Effettuazione di valutazioni dell'impatto sulla protezione dei dati per utilizzi di dati personali che sono suscettibili di comportare un rischio elevato per gli interessi degli individui.
 - Nomina di un responsabile della protezione dei dati.

Diritti del data subject

Ovviamente come il data controller ha degli obblighi da rispettare, il data subject avrà dei diritti:

1. ha il diritto di essere informato
2. ha il diritto di accedere ai dati che lo riguardano
3. ha il diritto di rettificare i dati
4. ha il diritto di far eliminare i dati se il processing non è conforme alla legge
5. ha il diritto di obiettare un certo processing quando non basato sul consenso
6. ha il diritto di non essere soggetto a decisioni basate su processi automatizzati
7. ha il diritto alla portabilità dei dati

Informativa sulla privacy

I responsabili del trattamento dei dati devono informare gli individui sul loro trattamento in modo facilmente accessibile e comprensibile. Devono utilizzare un linguaggio chiaro e semplice.

Quando vengono raccolti dati, i responsabili del trattamento devono fornire un'avviso sulla privacy che *con:*

- Il nome e i dettagli di contatto dell'organizzazione.
- Lo scopo del trattamento
- La base giuridica del trattamento
- Le categorie di dati personali ottenuti.
- I destinatari o categorie di destinatari dei dati personali.
- I dettagli sui trasferimenti dei dati personali verso paesi terzi o organizzazioni internazionali.
- I periodi di conservazione dei dati personali.
- I diritti disponibili agli individui in relazione al trattamento.

Riportare violazioni

- Il GDPR introduce l'obbligo per tutte le organizzazioni di segnalare determinate violazioni dei dati personali all'autorità di controllo competente. Devono farlo entro 72 ore dal momento in cui vengono a conoscenza della violazione, se possibile.
- Se la violazione è probabile che comporti un rischio elevato di pregiudizio ai diritti e alle libertà degli individui, devono anche informare tali individui senza indugi ingiustificati.
- Dovrebbero assicurarsi di avere procedure robuste per il rilevamento, l'indagine e la segnalazione interna delle violazioni. Ciò faciliterà la presa di decisioni su se notificare o meno all'autorità di controllo competente o agli individui interessati, o a entrambi.
- Devono anche mantenere un registro di qualsiasi violazione dei dati personali, indipendentemente dal fatto che siano tenuti a notificarlo o meno.

Sanzioni del GDPR

Ci sono due livelli di sanzioni:

- **violazioni meno gravi:** Potrebbero risultare in una multa fino a 10 milioni di euro o al 2% del fatturato annuo mondiale dell'azienda, esempio di queste infrazioni potrebbe essere la mancata segnalazione di una violazione dei dati all'autorità di protezione dei dati
- **violazioni molto gravi:** Potrebbero risultare in una multa fino a 20 milioni di euro o al 4% del fatturato annuo mondiale dell'azienda, esempio di queste infrazioni potrebbe essere la violazione dei principi di protezione dei dati o violazione dei diritti del data subject