Note sulla sicurezza informatica

Luca Battistin

June 2, 2024

Abstract

Queste note vogliono riassumere i principali concetti relativi alla sicurezza informatica vista soprattutto dal punto di vista aziendale. Vanno considerate insieme alla *note sulla crittografia* e alle *note sulla virtualizzazione*. Tenendo ben presente che la sicurezza informatica è un argomento "cappello", sotto il quale può rientrare quasi ogni aspetto informatico (oltre a questioni organizzative e di comunicazione), si propone una definizione, si precisa un po' di terminologia relativa alle vulnerabilità e si delineano le soluzioni tecnologiche principali soprattutto in termini di continuità di servizio. Si conclude con dei riferimenti normativi.

Contents

1 Definizione

La sicurezza informatica, secondo lo standard ISO 27002, è l'insieme delle misure software, hardware, strutturali, procedurali adottate da un'azienda o un ente al fine di garantire la riservatezza (Confidentiality), l'integrità (Integrity) e la disponibilità (Availability) dei dati trattati.

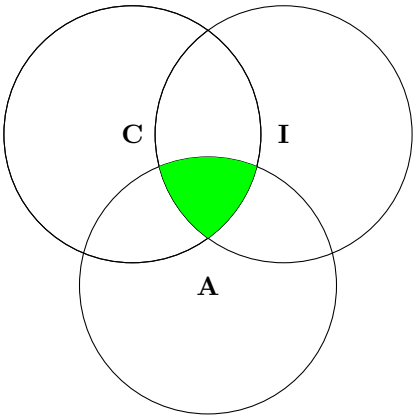

Figure 1: CIA triad

Confidentiality (Riservatezza). Un dato è riservato se è accessibile esclusivamente dal legittimo proprietario.

Integrity (Integrità). Un dato è integro se, nel trasferimento da un sistema all'altro, non è stato cancellato, corrotto o modificato per errore o per malizia.

Availability (Disponibilità). Un dato è disponibile se il legittimo proprietario ne può disporre ogni volte che ne ha bisogno. In pratica si tratta di garantire l'accesso ai dati 24/ 7

A queste tre caratteristiche, vanno poi aggiunte l'autenticità e il non ripudio.

Authenticity (Autenticità). Un dato è autentico se può essere garantita la corrispondenza con il suo legittimo autore o mittente. Spesso l'autenticità si riferisce anche ad un servizio o un'utenza.

Non repudiation (Non ripudio). Un dato è non ripudiabile se l'autore o il proprietario, dopo averlo inviato, non può negarne la paternità.

Garantire al 100% le precedenti caratteristiche è impossibile (si parla a volte dei five nines - 99,999%), perciò spesso si parla di sicurezza informatica in termini di minimizzare l'impatto o mitigare le minacce eliminando o minimizzando le vulnerabilità.

Per la riservatezza e l'integrità le principali misure tecnologiche sono date dalla **crittografia** per la quale si rimanda alle note dedicate[1] mentre per la disponibilità le varie misure sono principalmente orientate a qualche forma di ridondanza.

2 Threats and vulnerabilities

Per **vulnerabilità** si intende ogni debolezza del sistema sulla quale un attacco malevolo o un evento accidentale potrebbero insistere per intaccare una delle suddette caratteristiche della sicurezza informatica, ovvero la perdita, il furto, la corruzione o l'indisponibilità dei dati. Possono essere di tipo hardware, difetti di configurazione dei sistemi o di sviluppo software. La OWASP[2] propone la seguente definizione:

> A vulnerability is a hole or a weakness in the application, which can be a design flaw or an implementation bug, that allows an attacker to cause harm to the stakeholders of an application. Stakeholders include the application owner, application users, and other entities that rely on the application.

Un elenco delle vulnerabilità dei sistemi sarebbe lunghissimo. Di fatto ci sono database aggiornati quotidianamente che raccolgono le vulnerabilità note[3] Di seguito riportiamo solo la definizione generale di alcune:

- sistemi software/firmware obsoleti o non aggiornati
- password deboli
- configurazioni errate o con parametri di default
- mancanza di autenticazione
- software mal progettati, ad esempio input non sanitizzati (*unsanitized user inputs*)

[1] Vedi *Appunti di Crittografia* disponibili sul portale di e-learning www.v-learning.it

[2] https://owasp.org/ Open Worldwide Application Security Project (OWASP) is a non-profit foundation that works to improve the security of software

[3] Si vedano ad esempio:
https://osv.dev/ A distributed vulnerability database for Open Source
https://vuldb.com/it/ Un database sulla vulnerabilità con libero accesso.

Le minacce (**threats**) sono tutte quelle azioni messe in atto da malintenzionati che sfruttando (**exploitation**) una vulnerabilità recano danno all'azienda rubando, manomettendo o rendendo indisponibili i dati. Tra le minacce vanno considerati anche gli eventi accidentali (dalle rotture ai disastri ambientali) e gli errori umani. Come per le vulnerabilità, si citano di seguito solo le definizioni di alcune minacce più comuni:

MITM attack Il Man In The Middle attack sfrutta una debolezza nell'autenticazione tra due nodi per interporsi in maniera trasparente ai due e intercettare tutto il traffico scambiato. Tipiche applicazioni sono realizzate a livello locale mediante arp poisoning o a livello web inserendosi nel TLS handshake.

DoS Denial of Service. Mira alla disponibilità dei dati inondando un server di richieste fasulle (tipicamente dei SYN flooding). È un attacco difficile da mitigare quando proviene da molti computer (**DDoS**) preventivamente resi zombie dall'attaccante (**botnet**)

Zero Day attack è un attacco che sfrutta una vulnerabilità (hardware, software o firmware) non ancora nota e quindi non risolta dagli aggiornamenti.

Trojan horse è un tipo di malware che viene accettato dal sistema target perché camuffato da software legittimo o innocuo. Di fatto, come il mitologico stratagemma di Ulisse, nasconde al suo interno una componente dannosa, il cui scopo, spesso è quello di aprire delle falle per l'ingresso di altri malware.

Rootkit è un software che, una volta entrato nel sistema target, fa guadagnare all'attaccante diritti di amministratore (**elevation of privilege**).

Ramsonware è un malware che non ruba propriamente i dati ma, una volta iniettato nel sistema target, li rende indisponibili cifrandoli. L'attaccante chiede un riscatto per concede la chiave per decifrarli.

Phishing Questo attacco sfrutta la poca formazione degli utenti è infatti classificato come **social engineering**. Prevedere l'invio di un messaggio ingannevole (via email, telefonica o di messaggistica) con la richiesta di concedere delle credenziali (o di cliccare su un link o di fare il login su un sito fasullo).

Un attacco è quasi sempre una combinazione dei precedenti (e di altri). A titolo di esempio si può citare un vecchio malware, **stuxnet**[4], che combinava worm, rootkit e diversi zero day.

Spesso vulnerabilità, minacce e rischi vengono confusi. Una differenza essenziale per la progettazione e gestione della rete aziendale sta nel fatto che le minacce esistono sempre e non sono controllabili mentre le vulnerabilità sono interne all'azienda e vanno analizzate e possibilmente eliminate. Il **rischio** è la

[4] https://it.wikipedia.org/wiki/Stuxnet

stima di ciò che avviene quando una minaccia sfrutta una vulnerabilità. Esso, calato nella realtà di riferimento, va valutato in termini di entità del danno arrecato (più precisamente è il prodotto della probabilità del verificarsi dell'evento e dell'entità del danno arrecato all'azienda, misurato in soldi o almeno in fasce di rischio). Tanto più alto è il rischio, tanto maggiore dovrà essere lo sforzo per mitigarlo.

In questo paragrafo sono stati introdotti alcuni termini tipici della cyber security ma per un elenco un po' più completo si possono consultare i glossari del SANS [2] o del CSIRT [1]

3 Mitigazioni

Come già detto, una politica di sicurezza deve partire dall'analisi dei rischi (**Cyber Risk Assessment**) per determinare quali misure di mitigazione adottare in relazione ai vari scenari di attacco. Nei prossimi paragrafi si elencheranno le misure più comuni.

4 Difesa perimetrale

. Un **firewall** di rete è un dispositivo (e un software) che si interpone tra la rete locale e Internet per filtrare il traffico in ingresso e in uscita dalla rete. Viene anche detto **bastion host** per distinguerlo dal personal firewall, ovvero il software che filtra il traffico entrante o uscente da una singola postazione.

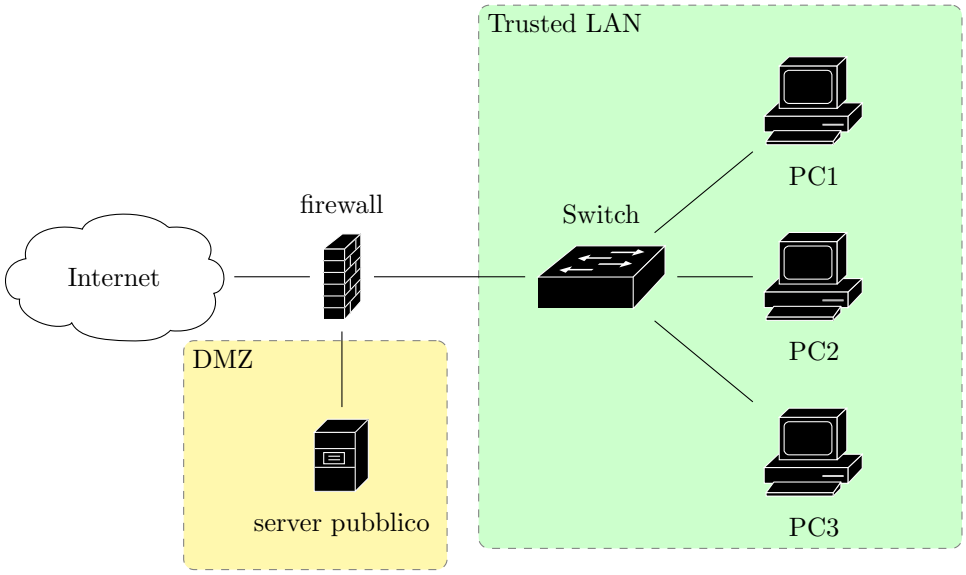

Figure 2: semplice configurazione bastion host con DMZ

Packet filtering il filtraggio si basa su regole che riguardano le intestazioni dei pacchetti, tipicamente sulla porta destinazione per questo è detto anche **port based**. Ovviamente i campi su cui il filtraggio può essere operato sono diversi, ad esempio l'indirizzo IP, il protocollo o l'URL. In questo ultimo caso si definiscono delle black list di URL non ammessi (o, meno frequentemente, una white list con i soli URL accettati)

statefull inspection il filtraggio è fatto sulla base dello stato della connessione: se essa è già stata attivata dall'interno, allora il traffico viene ammesso.

content filtering Il filtraggio è basato sul contenuto dei dati. Si impostano delle parole chiave o stringhe che, se trovate nel contenuto del traffico (tipicamente web o mail), vengono bloccate. In tal caso è necessaria la decifratura TLS del traffico. Il firewall agirà quindi da proxy[5] server aprendo un TLS handshake col servizio richiesto, mettendo in cache i contenuti dopo averli filtrati e inoltrandoli al client richiedente, se ammissibili. Si rende perciò necessario copiare in ogni postazione LAN (o almeno nei browser) il certificato del proxy server per l'autenticazione TLS. Questo filtraggio è più oneroso ma come aspetti vantaggiosi, oltre ad una maggiore sicurezza, permette una ottimizzazione di banda grazie al caching.

4.1 ACL

Le Access Control Lists sono le liste di regole (o entries) che filtrano il traffico. Noi le abbiamo viste applicate ai router Cisco nella sintassi IOS. In particolare abbiamo trattato le standard ACL per filtrare il traffico in base all'indirizzo IP sorgente quindi abbiamo accennato alle extended ACL per creare una rudimentale DMZ. La ACL va applicata ad una interfaccia di livello 3 in ingresso o in uscita. La sintassi delle **ACL standard** prevede che si specifichi solo l'indirizzo IP sorgente del traffico che si vuole filtrare scegliendo eventualmente un range di IP mediante wildcard mask. Ad esempio, se voglio che le sottoreti 192.168.0.0/26 e 192.168.0.96/27 non comunichino con la vlan 10, imposterei nel multilayer switch la seguente:

```
Central(config)#access-list 25 deny 192.168.0.0 0.0.0.63
Central(config)#access-list 25 deny 192.168.0.96 0.0.0.31
Central(config)#access-list 25 permit any
Central(config)#int vlan 10
Central(config-if)#ip access-group 25 out
```

Una nota sulla funzione della **wildcard mask**:i bit posti a 1 nella wildcard mask servono ad "ignorare" i corrispondenti bit nell'indirizzo ip. Più precisamente, quando il router controlla se l'indirizzo sorgente (del pacchetto in esame) fa il match con una entry della access-list, esegue un OR logico tra l'indirizzo

[5]proxy, letteralmente significa delegato, sostituto, chi agisce in vece di. Nel campo informatico è quindi un dispositivo che fa le richieste in vece dei client e poi inoltra le risposte.

presente nella riga e la relativa wildcard mask; se il risultato è uguale all'OR logico dell'indirizzo sorgente (del pacchetto in esame) e la medesima wildcard mask il match è positivo, la regola viene applicata e si interrompe il processo, altrimenti si prosegue con la riga successiva. Una ACL estesa, rispetto a quella standard ha molti più parametri. La sua sintassi è

```
R0(config)#access-list <id> <action> <protocol> <source IP>
           <operator> <source Port> <destination IP>
           <operator> <destination Port> [Established]...
```

dove:

id è il numero che identifica la ACL. deve appartenere al range 100-199 oppure 2000-2699

action può essere `permit` oppure `deny`

protocol è il protocollo da sottoporre a 'matching'. Possibili valori sono ip,tcp,udp,icmp

source IP indirizzo IP sorgente (da dove arriva rispetto al router) con wildcard mask

operator può essere uno tra **eq neq gt lt range**[6]

source Port porta logica Sorgente

Lo stesso vale per i parametri `destination`.

4.2 iptables

Iptables è uno dei componenti principali per quanto riguarda la sicurezza in un sistema Linux, si tratta di un firewall implementato a livello kernel che permette, tramite la creazione di regole, il filtraggio del traffico. Iptables lavora su 3 tabelle (tables) di default:

filter : regola il firewalling: quali pacchetti accettare, quali bloccare

nat : regola le attività di natting

mangle interviene sulla alterazione dei pacchetti.

Ogni tabella ha delle catene (chains) predefinite (INPUT, OUTPUT, FORWARD) a cui possono essere aggiunte catene custom. Ogni regola può contenere diversi parametri e opzioni per i quali si rimanda alla documentazione online. Si riportano un paio di esempi.

```
# iptables -A INPUT -s 192.168.0.0/24 -j DROP
```

Blocca tutto il traffico proveniente dalla rete 192.168.0.x

```
# iptables -t filter -I INPUT -p tcp --dport 80 -j ACCEPT
```

Accetta il traffico verso la porta 80 locale.

[6] eq: equal; neq: not equal; gt: greater than; lt:less than; range: si indica un intervallo di porte logiche

5 controllo degli accessi

Uno dei servizi principali per il controllo degli accessi alle risorse di rete locale è AAA (Authentication, Authorization and Accountig). Esso, soprattutto per quanto riguarda la parte di autenticazione, è stato trattato diffusamente nelle *note sulla crittografia*. Il sistema di **autorizzazione** si basa principalmente sulla divisione degli utenti in gruppi ai quali è garantito l'accesso a determinate risorse secondo alcuni privilegi (tipicamente:lettura, scrittura, esecuzione) e periodi di tempo. Disporre di un **resoconto** (accounting) delle attività svolte dai diversi utenti è imprescindibile per poter capire le cause di malfunzionamenti o attacchi. In particolare il sistema di accounting permette di tracciare:

- il tempo di sessione di ogni utente;
- le risorse accedute in ogni sessione dall'utente autenticato
- il traffico spedito e ricevuto da un utente in ogni sessione;
- gli eventuali tentativi di accedere a risorse non autorizzate;
- i comandi di sistema impartiti durante la sessione.

Poiché l'autenticazione è principalmente basata sulle password è essenziale una opportuna politica di gestione delle stesse (scegliere password che non siano parole di un dizionario, di lunghezza minima 10 caratteri, che contengano cifre e caratteri speciali, che alternino maiuscole e minuscole). Com'è noto le password vengono **oscurate** mediante una funzione di HASH, ma per capire meglio le direttive generali su come generare e mantenere una password robusta è bene conoscere i tipi di attacco al file delle password:

lookup hash table esistono delle enormi tabelle dove sono state pre-calcolati gli hash di moltissime parole e stringhe comunemente usate come password[7]. Noto il message digest della password, basta una query su tali database per ottenere in pochi millisecondi la password in chiaro. Per evitare un simile attacco si aggiunge un po' si sale alla password (**salting**)

attacco del dizionario Il file di sistema dove vengono memorizzate le password contiene il nome utente, la funzione di hash usata, il sale (ovvero una stringa pseudocasuale aggiunta alla password) e il message digest della concatenazione tra password e sale. Ciò impedisce un lookup attack ma non protegge da un attacco del dizionario, ovvero dal calcolare, per ogni utente il message digest salato di tutte le parole di un dizionario (o lista di password comuni). Questo attacco è computazionalmente molto più oneroso del precedente, ma può individuare una password debole, ovvero contenuta nelle suddette liste, nel giro di poche ore.

[7] si veda, ad esempio, carckstation (https://crackstation.net/) nella cui home page si legge: Crackstation's lookup tables were created by extracting every word from the Wikipedia databases and adding with every password list we could find.

brute force In questo caso si generano tutte le stringhe possibili, partendo da quelle più corte. E' computazionalmente intrattabile quando la stringa è lunga almeno 10 caratteri.

il software open source `john the ripper`[8] permette di testare la robustezza di una password applicando i suddetti attacchi. Esso prevede anche una modalità (single mode) in cui una stringa (ad esempio il nome utente o altre informazioni su di esso) viene manipolata generando moltissime variazioni.

5.1 Spoofing

Nel contesto dell'(assenza di) autenticazione si collocano i diversi attacchi di **spoofing** ovvero quelle situazioni in cui l'attaccante finge di essere altro da sé (arp, ip, dhcp, dns) per poi attutare un MITM attack. Ad esempio l'arp spoofing si può realizzare facilmente con un arp poisoning[9]. Per evitare tali attacchi le reti aziendali implementano sugli switch un **Dynamic Arp Inspection** (DAI), ovvero un controllo sui pacchetti ARP realizzato grazie ad un database interno allo switch dove sono mappati indirizzi IP e MAC address. Tale database potrebbe essere implementato staticamente dall'amministratore ma più comunemente è creato dinamicamente in concomitanza al **Dhcp snooping**. Si tratta in sostanza di impostare sullo switch una porta *trusted* a cui è collegato il DHCP autentico: ciò evita il DCHP spoofing perché le *DHCP offer* in ingresso dalle altre porte vengono scartate e vengono invece associati IP e MAC attendibili. Questa tabella è condivisa con lo switch.

6 backup/restore

Abbiamo già sottolineato che i dati rappresentano un bene primario per ogni tipo di azienda (ed anche per il singolo utente). Un sistema di backup/restore dei propri dati si rende quindi indispensabile. Stabilito quali sono i dati da salvare (ovvero le cartelle di cui il sistema farà una copia periodica) Le tipologie di backup possono essere distinte in

completo se tutto il volume di dati è copiato integralmente

differenziale se viene copiata solo la parte di dati che sono stati modificati rispetto all'ultimo backup completo

incrementale se viene copiata solo la parte di dati che sono stati modificati rispetto all'ultimo backup, incrementale o completo che sia.

Ogni sistema di backup stabilisce quali dati vanno copiati (tipicamente le carelle dei server ma si possono dettagliare anche cartelle di postazioni client),

[8] https://www.openwall.com/john/

[9] Abbiamo visto questo attacco l'anno scorso: l'attaccante può rispondere all'arp request di un host che richiede, ad esempio, il mac del gateway, fingendosi il gateway ed intercettando così il traffico rivolto verso l'esterno

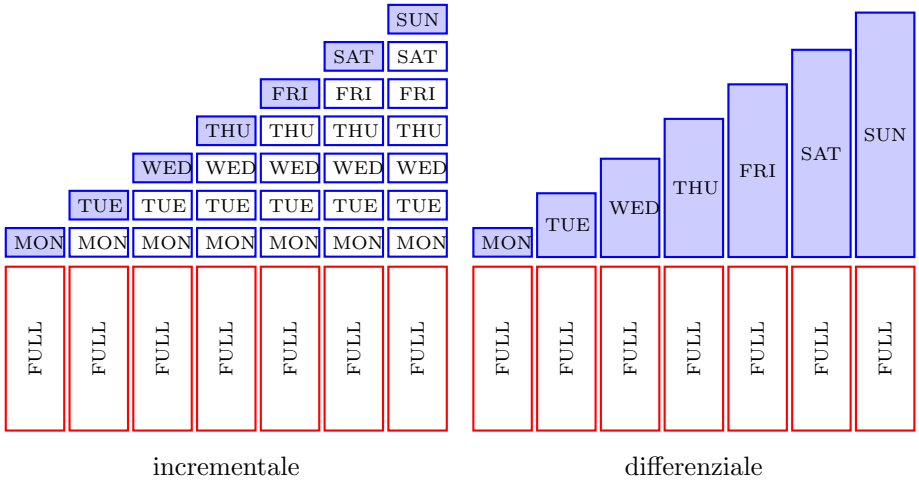

Figure 3: Backup incrementale vs differenziale

con quale frequenza (una tipica soluzione è il backup incrementale quotidiano notturno ed il backup completo settimanale) e in quali memorie di massa (tipicamente un NAS locale e un drive remoto).

In commercio esistono molte soluzioni per il backup; in ambiente Linux si distingue Amanda[10] il cui modello di lavoro prevede che sia il server a provvedere alla raccolta dei dati dalle postazioni remote e a gestire la copia.

Va sottolineata l'importanza della verifica del processo di restore, ovvero il controllo che si possono ripristinare in tempi brevi i dati sui sistemi server e client. anche in questo caso la virtualizzazione dell'hardware permette di creare degli ambienti test in cui fare tale verifica.

7 monitoraggio

Il monitoraggio delle reti ha lo scopo di controllare "lo stato di salute" della rete per ottimizzarne le prestazioni e per evidenziarne eventuali anomalie. Uno dei principali protocolli usati è SNMP (Simple Network Managment Protocol) la cui versatilità permette di adattarlo al monitoraggio di qualsiasi parametro.

7.1 basic tools

Prima di parlare dei software dedicati al monitoraggio, vale la pena ripassare gli strumenti di base che permettono una diagnosi, seppur limitata, della rete.

[10] Amanda Network Backup. Advanced Maryland Automatic Network Disk Archiver https://www.amanda.org/ originariamente sviluppato dal dipartimento di informatica dell'università del Maryland nei primi anni novanta

Con i comandi `ping`, `ifconfig` (`ip a` per linux) e `tracert` (`traceroute` per linux) si possono recuperare alcune informazioni di base sulla configurazione IP. Il già noto **telnet** permette di aprire una connessione sulla porta specificata. A titolo di esempio se ne riporta l'utilizzo nel caso si voglia ottenere la risorsa web(http) dal dominio web-02.challs.olicyber.it con pathname: server-records e query string: id=flag:

```
telnet web-02.challs.olicyber.it 80
GET /server-records?id=flag HTTP/1.1
Host:  web-02.challs.olicyber.it
```

Con il tool **nmap**[11] si possono fare scansioni più sofisticate[12]come :

`nmap -A -T4 scanme.nmap.org` esegue una scansione completa delle porte aperte sul target.

`nmap` *`192.168.1.0/24`* esegue una scansione delle porte aperte nella sottorete indicata (ovvero *192.168.1.0/24*). mostra un output del tipo:

```
Starting Nmap 7.80 ( https://nmap.org ) at 2024-04-18 19:38 CEST
Nmap scan report for 192.168.1.1
Host is up (0.0025s latency).
Not shown: 997 filtered ports
PORT    STATE SERVICE
53/tcp  open  domain
80/tcp  open  http
443/tcp open  https
...
...
Nmap done: 256 IP addresses (5 hosts up) scanned in 24.72 seconds
```

`nmap -sn` *`192.168.1.0/24`* esegue un ping scanning, ovvero ricerca tutte le NIC attive nella rete target (nell'esempio *192.168.1.0/24*) riportandone indirizzo IP e MAC ADDRESS.

netcat è un altro strumento versatile che permette il port scanning ma che viene usato principalmente per la connessione con servizi remoti da linea di comando. Può essere integrato facilmente nei linguaggi di scripting come succede nelle sfide della cyberchallenge[13]. A questi tool va sicuramente aggiunto il ben noto **Wireshark** per l'analisi dettagliata del traffico di rete.

[11] https://nmap.org/ è multipiattaforma: disponibile per windows, linux, mac e per ogni altra piattaforma grazie al codice sorgente.

[12] N.B. le scansioni fatte con nmap possono essere interpretate come degli attacchi alla rete (reconnoisense attack) per tanto vanno fatte solo sulla propria rete o su reti per le quali si è ottenuto il consenso alla scansione.

[13] https://cyberchallenge.org

7.2 advanced tools

Se con una opportuna combinazione e automatizzazione dei precedenti strumenti si può ottenere un discreto monitoraggio della rete, è sicuramente vantaggioso in termini di facilità d'uso, robustezza, versatilità e completezza servirsi di soluzioni dedicate che integrano le seguenti funzionalità:

- Un sistema di tracciamento automatico dei dispositivi connessi alla rete (con la possibilità di ipotizzare la topologia).
- Analisi istantanea e cronologia delle performance divisa per dispositivo e applicazione.
- Configurazione delle notifiche e degli alert.
- Generazione di grafici e report di analisi dell'attività sulla rete.

Si trova in commercio una vasta scelta di soluzioni; a titolo di esempio si possono citare dei prodotti open source come **zabbix**[14] **Cacti**[15] **Nagios**[16]. Il monitoraggio è un elemento fondamentale degli **Intrusion Detection System** (IDS), ovvero di quei sistemi che analizzando il traffico riescono a rilevare una intrusione nella rete. Essenzialmente essi cercano di individuare una potenziale intrusione in tempo reale rilevando delle difformità di traffico in rete rispetto ad una **baseline** di riferimento. Se oltre alla rilevazione, e conseguente alert, il sistema blocca il traffico anomalo si parla di **Intrusion Prevention System** (IPS). IDS e IPS non vanno confusi con il firewall, che applica regole predefinite, ma succede spesso che gli IPS siano integrati nel firewall il quale, in tal caso, viene definito *next generation firewall* (NGFW).

8 continuità di servizio

La continuità di servizio (o **Business continuity**) è la capacità della struttura di continuare ad erogare i servizi (ad un livello accettabile) anche nel caso si verifichino eventi critici potenzialmente causa di interruzioni. Una strategia adeguata deve partire dall'identificazione delle minacce, valutarne l'impatto e definire un piano di resilienza per ogni scenario possibile. Pertanto il BCT (Business Continuity Plan) dipende dalla realtà di riferimento. In termini generali la **ridondanza** delle strutture hardware critiche (alimentazione, connettività, server) aumenta la **fault tollerance**; la virtualizzazione dell'hardware ne permette l'ottimizzazione e la possibilità di assegnare risorse in base ai carichi. Molte delle misure già discusse (Difesa perimetrale, antimalware, aggiornamento dei sistemi, monitoraggio, formazione del personale, un efficiente backup/restore dei dati e dei sistemi software), concorrono a migliorare la continuità di servizio. Nel caso l'evento imprevisto sia devastante (calamità naturali, incendi, etc.) si parla di **disaster recovery plan**.

[14] https://www.zabbix.com/ Si ringrazia Giacomo Mattiello per aver esposto le caratteristiche di questo sistema di monitoraggio, incontrato durante il tirocinio aziendale.
[15] https://www.cacti.net/
[16] https://nagios.com

9 Normativa

La normativa (europea) in merito alla cyber security e la tutela dei dati degli utenti ha tentato di "tenere il passo" delle formidabili innovazioni tecnologiche informatiche di questi ultimi anni, con il duplice scopo di aumentare la consapevolezza dei cittadini in merito al valore e alla quantità di dati personali trattati, restituendo loro un maggiore controllo, e di regolarne, da parte delle aziende, il trattamento (ovvero la raccolta, la conservazione, il trasferimento o l'utilizzo).

9.1 GDPR

Il regolamento generale sulla protezione dei dati **General Data Protection Regulation** è stato adottato dalla UE nel 2016 (pubblicazione in gazzetta ufficiale il 4 maggio 2016[17] ed è operativo dal 25 maggio 2018. Esso garantisce a tutti i cittadini europei specifici diritti :

access diritto di accedere ai propri dati

erase diritto di cancellare i propri dati

rectification modificare i propri dati

data portability trasferire i propri dati su altra piattaforma

Per garantire tali diritti, tutte le aziende (e i loro fornitori di servizi) anche extraeuropee che gestiscono i dati personali di cittadini europei hanno obblighi precisi:

adeguate misure di sicurezza. L'azienda deve dimostrare di avere adottato, sulla base della valutazione dei rischi, misure di sicurezza adeguate al valore dei dati trattati.

Pseudonimizzazione dei dati, quando essi devono essere estratti ed aggregati per interesse di ordine collettivo.

DPO Data Protection Officer. Deve incaricare un esperto (con competenze informatiche e giuridiche) per verificare la conformità del trattamento dei dati con il GDPR

Data breach notification La eventuale perdita dei dati, a causa di un attacco o altro evento, deve essere denunciata alle autorità entro 72 ore.

[17] Il testo integrale del regolamento si può leggere, in diverse lingue al link: https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1717324329951&uri=CELEX:32016R0679, oppure sul sito del garante della privacy: https://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/6264597

Consent ottenere specifico consenso per ogni servizio (esplicito, preciso, ritrattabile in ogni momento)[18]. Al punto (32) infatti si legge:

> Il consenso dovrebbe essere espresso mediante un atto positivo inequivocabile con il quale l'interessato manifesta l'intenzione libera, specifica, informata e inequivocabile di accettare il trattamento dei dati personali che lo riguardano, ad esempio mediante dichiarazione scritta, anche attraverso mezzi elettronici, o orale.

Le sanzioni per le aziende che non rispettano gli obblighi di legge possono essere molto elevate: fino a 20 M€ o fino al 4% fatturato annuo.

9.2 DSA

Il Digital Service Act è stato approvato dal Parlamento Europeo il 5 luglio 2022 insieme al Digital Markets Act. Tale regolamento sui servizi digitali mira principalmente a proteggere i diritti degli utenti in termini di profilazione e contrastare la diffusione di contenuti illegali o fake news.

9.3 AI Act

Il 13 marzo 2024 è stato approvato dal Parlamento the AI ACT : The EU Artificial Intelligence Act[19]. Si tratta della prima legge trasversale al mondo sull'intelligenza artificiale. Introduce regole uniformi su tutto il territorio UE per quanto riguarda sviluppo, produzione, commercializzazione e uso dei sistemi AI all'interno del mercato unico UE nel rispetto dei valori tutelati e promossi dall'Unione.

References

[1] Csirt istituito presso l'agenzia per la cybersicurezza nazionale (acn).

[2] Sans institute.

[18] Ciò vale in particolare per i dati "concessi" dall'utente durante la navigazione sul web: i cookies e altri strumenti di tracciamento. Si veda a tal proposito https://www.garanteprivacy.it/faq/cookie.

[19] https://artificialintelligenceact.eu/ è un documento di oltre 450 pagine.