



SAPIENZA
UNIVERSITÀ DI ROMA

Analisi Comparativa sulla Sicurezza delle Infrastrutture di Rete Aziendali

Facoltà di Ingegneria dell'Informazione, Informatica e Statistica
Corso di Laurea in Informatica

Mattia Giordano

Matricola 1884283

Relatore

Prof. Alessandro Checco

Anno Accademico 2024/2025

Analisi Comparativa sulla Sicurezza delle Infrastrutture di Rete Aziendali
Tesi di Laurea Triennale. Sapienza Università di Roma

© 2025 Mattia Giordano. Tutti i diritti riservati

Questa tesi è stata composta con L^AT_EX e la classe Sapthesis.

Email dell'autore: mattia-giordano@hotmail.it

«Non possiamo dirigere il vento ma possiamo orientare le vele.»
Seneca.

Abstract

Le reti aziendali rappresentano un pilastro fondamentale per il funzionamento della società moderna, fondamentali anche per il funzionamento di servizi critici in ambiti sanitari, finanziari e per gli operatori di servizi essenziali. Tuttavia, la loro complessità e la crescente esposizione a minacce informatiche richiedono una progettazione e una gestione rigorosa, basata su principi di sicurezza avanzati e standard consolidati. Questa tesi analizza lo stato dell'arte delle tecnologie e strumenti esistenti nelle reti aziendali moderne, per sopprimere vulnerabilità e identificando errori comuni nelle configurazioni e negligenze nella manutenzione. Verranno anche analizzati i framework internazionali come ISO/IEC 27001, NIST CSF e COBIT2019, il tutto supportato dalla letteratura scientifica. Sono stati esaminati casi studio emblematici, come l'attacco ransomware alla Colonial Pipeline del 2021.

Il lavoro analizza le tecniche odiere per mettere in sicurezza una rete, analizzando principi quali la difesa in profondità, il minimo privilegio e l'isolamento e tecnologie come Next-Generation Firewall, i sistemi di rilevamento collaborativo e la segmentazione avanzata tramite VRF. Vengono approfonditi strumenti di monitoraggio proattivo come SIEM e SOC sono anche mostrate metodologie di manutenzione preventiva, tra cui patch management automatizzato e politiche di controllo degli accessi. Particolare attenzione nella fine dell'elaborato è dedicata all'integrazione di intelligenza artificiale e machine learning per l'analisi predittiva delle minacce e l'ottimizzazione dei processi di risposta. Il progetto è stato scritto in italiano, ma data la forte presenza della lingua inglese in materia sono presenti ingleismi o parole inglesi.

Indice

Abstract	iii
1 Introduzione	1
1.1 Analisi del Problema	2
1.2 Cosa dice la letteratura scientifica a riguardo	3
1.3 Metodologia	5
1.4 Obiettivi	5
2 Architettura e Progettazione delle Reti Aziendali	6
2.1 Problemi Comuni nelle Reti	6
2.1.1 Tipi di Rete Aziendale e Implicazioni per la sicurezza	6
2.2 Principi e Strumenti per una Progettazione Sicura delle Reti	9
2.2.1 Princípio della Difesa in Profondità	10
2.2.2 Princípio del Minimo Privilegio	10
2.2.3 Princípio della Separazione dei Poteri	10
2.2.4 Princípio della Sicurezza by Default	11
2.2.5 Princípio della Modularità	11
2.2.6 Princípio del Fallire in Maniera Sicura	12
2.2.7 Princípio di Isolamento	12
2.3 Tecnologie e strumenti per la Sicurezza nelle Reti	12
2.3.1 IDS, IPS e CIDN	13
2.3.2 Next-Generation Firewall - NGFW	13
2.3.3 Segmentazione del Network interno	13
2.4 Fondamenti per una sicurezza avanzata	15
2.5 Performance	16
2.5.1 Metriche per valutare le performance	16
3 Metodi di Gestione e Manutenzione per Reti Sicure	19
3.1 Framework e Politiche di Sicurezza	19
3.1.1 ISO/IEC 27001	19
3.1.2 NIST Cybersecurity Framework - CSF	21
3.1.3 COBIT 2019	23
3.1.4 Politiche e Strutture Interne	23
3.2 Monitoraggio della Rete	24
3.2.1 Active Network Monitoring	24
3.2.2 Passive Network Monitoring	25

3.2.3	SNMP Network Monitoring	26
3.2.4	SIEM	27
3.2.5	SOC	28
3.3	Manutenzione Preventiva	32
3.3.1	Controllo degli Accessi	32
3.3.2	Policies di Controllo degli Accessi	35
3.3.3	Patch Management	38
3.3.4	Backup e Disaster Recovery - BDR	44
3.3.5	Formazione e Coordinazione dei Reparti IT	47
3.4	Penetration Testing - VAPT	48
3.4.1	Le Vulnerabilità	49
3.4.2	Penetration Testing	51
4	Simulazione di una Rete Reale	56
4.1	Esempio di implementazione di sicurezza nella rete di Poste Italiane	56
5	Conclusioni e Nuove Tecnologie per la Sicurezza delle Reti Aziendali	58
5.1	Machine Learning e Artificial Intelligence	59
5.2	Architetture Zero Trust	61
5.3	Limiti e conseguenze	61
5.4	Riflessioni Finali	62
	Bibliografia	63

Capitolo 1

Introduzione

Al giorno d'oggi le reti di elaboratori sono fondamentali per la nostra società, le troviamo in ogni tipo di azienda e nella pubblica amministrazione. Esse ci permettono di mantenere dati e accedervi da più dispositivi, anche al di fuori della rete locale, e di vivere in un mondo sempre più interconnesso. L'importanza di questo tipo di infrastrutture è tale che vengono utilizzate quotidianamente in molteplici ambiti della società. Alla base di queste reti vi sono però delle macchine le quali, per gestire al meglio ogni tipo di dato, devono essere opportunamente configurate e gestite, infatti la creazione di queste reti non è per niente banale e richiede una particolare attenzione anche al minimo dettaglio. Esiste però un metodo standardizzato per farlo? Esistono protocolli in grado di supportare gli amministratori di rete nella creazione e gestione ottimale delle infrastrutture, evitando la presenza di vulnerabilità critiche spesso causate da incuria o configurazioni inadeguate?

Questa tesi vuole rispondere in maniera dettagliata a queste domande mostrando una situazione chiara sulle reti moderne, sui loro problemi e su come questi potrebbero essere risolti. In particolare l'elaborato è strutturato nel seguente modo: il **Capitolo 1** presenta sia la struttura dell'elaborato sia il problema, mostra cosa dice la letteratura scientifica a riguardo, la metodologia con cui è stata condotta questa analisi e mostra anche gli obiettivi di questa tesi. Il **Capitolo 2** esplora l'architettura delle reti e mostra i suoi problemi. Introduce alcuni concetti di base e sottolinea come la progettazione di una rete andrebbe realizzata, in maniera sicura, seguendo dei principi e introducendo le tecnologie adatte per supportarne la sicurezza e il funzionamento, analizzando quindi anche nuovi strumenti senza trascurare le sue performance. Il **Capitolo 3** tratta della gestione di queste reti e della loro manutenzione, in particolare andremo ad analizzare i framework di sicurezza esistenti. Daremo spazio alle politiche interne della sicurezza e all'importanza della gerarchia dei ruoli nell'azienda e parleremo poi dei metodi per gestire le reti e per mantenerle sicure nel tempo. Nel **Capitolo 4** andremo a esaminare un caso studio di una rete aziendale reale mostrandone il funzionamento e come le strategie analizzate vengono implementate. Nel **Capitolo 5** esploreremo le tendenze future in materia e le nuove tecnologie, analizzando paper che mostrano l'integrazione di queste con strumenti già esistenti. Infine parleremo delle limitazioni attuali e daremo le considerazioni finali sul lavoro.

1.1 Analisi del Problema

Le reti di elaboratori nascono con lo scopo di connettere computer e altri dispositivi digitali tra loro, così da condividere risorse e/o dati. Questo necessita di hardware, software e configurazioni particolari in base a vari fattori, come ad esempio la loro posizione in quanto potrebbero trovarsi nello stesso luogo fisico o in parti diverse del mondo, oppure, per il tipo di servizio che andranno ad offrire. Questo tipo di infrastruttura è diventata necessaria al giorno d'oggi ed è in continua evoluzione, basta pensare a come l'avvento di Internet abbia cambiato la società moderna. Questo progresso però si porta dietro diverse problematiche sotto vari punti di vista, in particolare vista l'esistenza di vari tipi di reti, ognuna ha bisogno di una configurazione diversa, di un'attenzione diversa e si possono avere anche diversi problemi legati alla sicurezza. Se alcune accortezze vengono meno e la loro creazione o manutenzione non è effettuata a regola d'arte si può verificare un ingente problema per l'azienda che potrebbe anche ripercuotersi sulla società stessa.

Dato l'ampio utilizzo sia nel settore privato che in quello pubblico, non solo per la comunicazione e la gestione dei dati aziendali, ma anche per supportare i servizi essenziali, l'utilizzo di standard sicurezza per il mantenimento di queste reti si rivela fondamentale. Basta pensare che queste tecnologie sono usate anche per servizi critici come quelli sanitari o di emergenza, dove affidabilità e sicurezza sono condizioni necessarie. Con la diffusione di pratiche come la chirurgia a distanza, abbiamo l'esigenza di garantire l'integrità e il corretto funzionamento dei sistemi, così come la trasmissione in tempo reale dei dati a distanza. In contesti come questi, una compromissione della rete potrebbe comportare conseguenze gravi.

Il ruolo sempre più centrale che le reti hanno acquisito, e continueranno ad acquisire nel tempo, si riflette anche nella percezione del networking nella società. Oggi si dà quasi per scontato che "la rete" funzioni e sia sicura senza farsi troppi problemi, ma questo non per forza implica che le infrastrutture siano state progettate e manutenute con cura, seguendo standard adeguati. Questo elaborato vuole far luce sulle problematiche che emergono quando si trascurano le buone pratiche nella costruzione o manutenzione delle reti, cercando di creare un protocollo per poterci aiutare a creare una rete solida e sicura. Vuole inoltre spiegare quanto un comportamento superficiale in questo settore possa creare danni anche gravi, analizzeremo infatti i rischi e gli effetti di una gestione negligente, mettendo in evidenza quanto sia cruciale adottare standard elevati per prevenire malfunzionamenti.

1.2 Cosa dice la letteratura scientifica a riguardo

Come possiamo notare in questo paper scritto da F. Liao sull’analisi dei problemi di sicurezza delle reti di elaboratori e sulle contromisure [49], lo stato attuale delle reti ha diversi problemi di sicurezza non derivanti dalle macchine in se ma dagli utenti, dai manutentori o dagli ingegneri della rete stessa. Questi problemi sono spesso figli di una noncuranza da parte degli utilizzatori. L’autore evidenzia alcuni dei problemi relativi ai network, anche un esempio banale riportato tra questi è addirittura la mancanza di un’adeguata sorveglianza a queste infrastrutture, il che può consentire l’accesso fisico a potenziali attaccanti. Altre reti presentano molte difficoltà con la stabilità o con la modularità, infatti data una forte ignoranza nei primi anni nella progettazione delle reti si sono formati diversi bug che permettono ad attori esterni di compromettere la rete stessa. Tuttavia questi loophole spesso sono rimasti a causa dell’importanza di tale infrastruttura dato che una successiva modifica avrebbe potuto comportare all’interruzione dei servizi offerti per tempi indeterminati. Altri problemi che i ricercatori hanno trovato nel paper precedente, riguardano le vulnerabilità nei file server, dovute in genere a politiche di accesso non regolate o regolate superficialmente, falla che troviamo anche nella configurazione di firewall, switch o altri dispositivi, spesso dovute a una negligenza, portando alla compromissione della sicurezza in queste infrastrutture.

Visto che questo tema riguarda anche organi fondamentali per governi o per la società, alcune agenzie governative predispongono dei consigli sugli errori da non fare nelle reti o sulle problematiche note, così da mettere in guardia gli ingegneri del software e gli amministratori di rete.

Enti governativi come l’NSA¹, National Security Agency, il CISA² Cybersecurity and Infrastructure Security Agency, e altri hanno creato dei programmi ad hoc per favorire questa tematica come il Alerts & Advisory [24], ossia una piattaforma dove regolarmente vengono pubblicati dei documenti scritti da degli esperti con le loro raccomandazioni e consigli su un particolare argomento. Analizzando questo report [64] del 5 Ottobre 2023 troviamo 10 degli errori più comuni nelle configurazioni delle reti.

Notiamo come al primo posto, l’errore quindi più comune, è quello di lasciare inalterate le impostazioni o le configurazioni di default dei software, le quali portano ad errori di privacy e sicurezza, infatti queste vulnerabilità possono portare ad accessi non autorizzati. Alcune configurazioni se non modificate possono includere credenziali, impostazioni e permessi di default. Un semplice esempio può essere quello di non cambiare le credenziali di un router appena installato. Un altro errore tipico è quello di non separare propriamente i permessi amministratore da quelli utente, dando a quest’ultimo più permessi di quello che necessario.

Questi sono solo alcuni degli errori più comuni menzionati nell’articolo, dove troviamo anche una scarsa gestione delle credenziali, metodi di autenticazione a fattori multipli deboli o assenti, una scarsa gestione degli aggiornamenti e altro

¹Fonente: NSA (<https://www.nsa.gov/>)

²Fonente: CISA (<https://www.cisa.gov/>)

ancora. Gli errori citati dal report sono stati trovati all'interno di reti di grandi organizzazioni, alcune tra queste sono essenziali o critiche.

Altri dei paper importanti che analizzeremo successivamente sono [2] e [54] per l'architettura di reti sicure e per la gestione [73], [80], [76] e [61] manutenzione sicura delle reti.

Un esempio di negligenza di sicurezza nella rete di un'infrastruttura critica

Quando si parla di attacchi legati a servizi essenziali spesso c'è la credenza che i malintenzionati attacchino direttamente i sistemi collegati alla fruizione dei servizi come macchinari o altro, ma in realtà viene prima preso di mira il reparto informatico. Un esempio recente è stato l'attacco alla compagnia Colonial Pipeline, il più grande sistema di oleodotti per prodotti petroliferi raffinati negli Stati Uniti [86]. Questo attacco ha bloccato l'intero dipartimento IT grazie ad un ransomware, di cui parleremo nel dettaglio più avanti, portando l'azienda a non poter fatturare i clienti. La Colonial Pipeline a quel punto ha dovuto sospendere il servizio di fornitura, lasciando tutta la costa est senza carburante per giorni, causando il panico generale. L'attacco iniziò il 7 maggio 2021 e l'azienda riaprì la fornitura il 12 maggio 2021, molte stazioni di rifornimento vennero prese d'assalto dalla popolazione per la paura che si era diffusa, l'aeroporto Charlotte Douglas International Airport in North Carolina cambiò alcuni piani di volo per la scarsità di carburante causata dall'attacco [75]. Gli attaccanti hanno rubato circa 100 GB di dati e hanno chiesto un riscatto di circa 75 Bitcoin (circa 3.5 milioni€ nel 7 maggio 2021) che l'azienda ha dovuto pagare per continuare con le sue operazioni. Questo attacco è stato causato da un account relativo a una VPN non più utilizzato. Non è ben chiaro se gli attaccanti erano entrati in possesso della password tramite o un'estorsione a un ex dipendente oppure se questa è stata reperita tramite delle altre attività online, una delle quali è stata compromessa. Per rispettare lo stato dell'arte nelle reti è buona norma implementare misure di autenticazione a due fattori anche nelle reti VPN, misura di sicurezza assente nella rete della Colonial Pipeline [37]. Diversi sono gli attacchi di questo tipo, portati avanti a causa di una carenza nella manutenzione delle reti, sappiamo come anche diverse strutture ospedaliere americane sono state colpiti da un ransomware, che viene portato a termine per una mancanza o una noncuranza del sistema patch management [33], [25].

1.3 Metodologia

La metodologia adottata per questa analisi comparativa si basa su un approccio misto, qualitativo e quantitativo, con l'obiettivo di approfondire i problemi di sicurezza delle infrastrutture di rete aziendali e identificare soluzioni pratiche e standardizzabili. La ricerca si è articolata in diverse fasi, ossia la revisione della letteratura unita all'analisi di casi studio e l'utilizzo di strumenti tecnici per la valutazione delle vulnerabilità. Inizialmente, è stata condotta una ricerca sistematica su database accademici come IEEE Xplore, ScienceDirect, ACM Digital Library, e fonti istituzionali, come NIST, CISA e altre, utilizzando parole chiave come “network security architecture”, “patch management”, “zero trust” e “enterprise cyber threats” su strumenti di ricerca, in particolare “Google Scholar”³. In particolare, la ricerca avanzata con l'utilizzo di virgolette per le parole chiave e operatori come “AND” mi ha permesso di fare una scrematura importante dei documenti più rilevanti e congruenti con la mia analisi. Inoltre ho controllato in quali paper le fonti da me utilizzate erano state citate, così da ottenere documenti sempre più attinenti all'analisi.

Grazie a questo approccio sono riuscito a condurre un'analisi completa sulla sicurezza delle reti aziendali e ad identificare i principali fattori di rischio, proponendo linee guida pratiche per migliorare la progettazione e la gestione delle infrastrutture di rete.

1.4 Obiettivi

L'obiettivo di questa tesi è approfondire come le reti aziendali dovrebbero essere progettate e configurate per ridurre al minimo le vulnerabilità, in particolare quelle che potrebbero derivare da errori o negligenze nelle loro impostazioni. Analizzeremo dei documenti di istituzioni ufficiali, enti governativi e ricercatori per capire quale sia la strada da percorrere per ottenere una rete sicura, ma soprattutto per mantenerla così nel tempo. L'obiettivo di questa ricerca è quello di mettere insieme tutte le pratiche, le tecniche e gli strumenti che sono necessari per ottenere una rete definibile “sicura”, dando delle linee guida su quali sono i passaggi da seguire, facendone capire le conseguenze della negligenza di questi con casi realmente accaduti.

³Fonente: Google Scholar (<https://scholar.google.com/>)

Capitolo 2

Architettura e Progettazione delle Reti Aziendali

2.1 Problemi Comuni nelle Reti

Alcune reti aziendali, similmente a quelle di pubblico utilizzo come quelle delle università o degli enti pubblici, mettono a disposizione dati o servizi accessibili da chiunque. Questo tipo di infrastrutture sono da sempre le vittime perfette per attacchi distribuiti nella rete, i quali puntano a paralizzare i sistemi informatici. Per mitigare questi attacchi, gli amministratori della rete possono prendere dei provvedimenti utilizzando dei dispositivi come firewall e sistemi di intrusion detection e prevention.

Ovviamente non sono solo le reti che offrono un servizio di hosting ad avere problemi di sicurezza. Notiamo infatti da questo paper [18] come la maggior parte delle piccole-medie imprese non implementino in maniera adeguata la sicurezza informatica, diventando semplici vittime di potenziali attaccanti. Secondo questo articolo [13] del Sole 24 Ore, in Italia “le piccole e medie imprese contribuiscono per il 63% al valore aggiunto e per il 76% all’occupazione”, mentre in Europa [85] “si contano oltre 23 milioni di PMI, pari al 99% delle imprese e due posti di lavoro su tre nel settore privato”. Queste sono dunque un motore chiave dell’economia nella maggior parte dei paesi e dati rubati, esposti o servizi manomessi, risultano in un danno economico per le PMI.

2.1.1 Tipi di Rete Aziendale e Implicazioni per la sicurezza

Ogni tipologia di rete aziendale presenta specifiche vulnerabilità che derivano dalla sua architettura, dalla posizione geografica e dal contesto operativo. Questi fattori influenzano direttamente le strategie di sicurezza adottabili, rendendo fondamentale un approccio mirato alla protezione di ogni tipo di infrastruttura. Di seguito i tre tipi principali di reti, con focus sulle vulnerabilità e contromisure specifiche:

- **LAN**(Local Area Network): copre un'area contenuta come case o uffici. È usata in genere per collegare computer e altri dispositivi all'interno di un'area limitata.

Rischi: Le LAN sono particolarmente vulnerabili ad accessi fisici non autorizzati, al broadcast di traffico sensibile e all'utilizzo di dispositivi personali (BYOD) non controllati, che possono introdurre potenziali punti di ingresso per gli attaccanti.

Contromisure: Per mitigare questi rischi, è fondamentale implementare misure di segmentazione come le VLAN per isolare i reparti, adottare protocolli di autenticazione come l'802.1X e monitorare continuamente il traffico per rilevare anomalie o comportamenti sospetti, come analizzato in questo articolo [7].

Esempio Reale: Stampanti non protette, ad esempio, rappresentano un rischio significativo, in quanto spesso non vengono configurate correttamente, permettendo a eventuali malintenzionati di accedere alla rete aziendale. Come evidenziato da questo articolo [10], dimostrando quanto sia importante implementare misure di protezione adeguate per dispositivi di questo tipo.

Analizzando questo articolo [23] vediamo come 28 000 stampanti sono state compromesse nel mondo per dimostrare l'importanza della messa in sicurezza di questi dispositivi. Per dimostrare la riuscita dell'esperimento sono stati stampati dei fogli con delle linee guida su come mettere in sicurezza queste stampanti. L'articolo evidenzia come sono riusciti a penetrare in 27,944 stampanti delle 50 000 previste, ottenendo un successo del 56% e stimando che su 800 000 stampanti connesse a internet circa 447 000 sono insicure.

- **WAN**(Wide Area Network): a differenza della LAN è pensata per coprire una vasta area. È utilizzata per collegare le reti locali tra di loro, è quindi in grado di collegare sedi remote.

Rischi: I rischi principali per questo tipo di rete sono: l'intercettazione del traffico su collegamenti pubblici, gli attacchi DDoS verso i router perimetrali o le configurazioni errate dei BGP.

Contromisure: Le contromisure adottabili sono: la crittografia del traffico tra le reti, usando VPN IPsec o TLS, implementazioni di protocolli sicuri come BGPSEC o l'utilizzo di firewall NGFW (Next-Generation Firewall) con filtraggio deep packet inspection [5].

Esempio Reale: In questo articolo [12] viene descritto come nella competizione Pwn2Own¹ una squadra ha trovato una vulnerabilità in un router TP-Link, connesso alla WAN che gli ha permesso di inserirsi nella LAN, attaccando successivamente una telecamera Synology.

¹Fonte: Wikipedia (<https://it.wikipedia.org/wiki/Pwn2Own>)
Competizione tra hacker con l'obiettivo di trovare delle fallo in software e hardware di ultima generazione ritenuti o che erano stati dichiarati privi di vulnerabilità

- **Cloud Networks:** può essere visualizzato come una rete virtualizzata ospitata su un servizio cloud, togliendo il peso della gestione e della configurazione all'utilizzatore. Questo tipo di reti sono composte anche da router virtuali, firewall e altri componenti.

Rischi: Le problematiche principali sono quella della mal configurazione di gruppi di sicurezza, accessi non autorizzati tramite API key compromesse e attacchi cross-tenant in ambienti multi-tenant [34].

Contromisure: Per aggirare i problemi di questo tipo di rete spesso è buona norma usare un approccio “Zero Trust”, con autenticazione multifattoriale. L'adozione di un'automazione della sicurezza tramite vari strumenti, come AWS Config per rilevare configurazioni rischiose [58], e l'utilizzo di una crittografia end-to-end per dati in transito e a riposo.

Esempio reale: Nel 2024, un'azienda ha subito una violazione dati su AWS a causa di un bucket S3 configurato come pubblico [47]. L'implementazione di policy IAM granulari ha risolto il problema.

Confronto tra le Vulnerabilità		
Tipo di Rete	Vulnerabilità Critiche	Best Practice di Sicurezza
LAN	Accesso fisico, ARP Spoofing	VLAN, 802.1X, NAC(Network Access Control)
WAN	DDoS, BGP hijacking	VPN, BGPsec, NGFW con mitigazione DDoS
Cloud	Misconfigurazioni IAM/S3	Zero Trust, automazione strumenti CSPM

Tabella 2.1. Analisi delle vulnerabilità sui vari tipi di rete.

La costruzione di queste reti richiede l'utilizzo di vari componenti hardware, tra cui modem, switch, router, access point, client, server, load balancer, proxy e altri. A questi si affiancano diversi componenti software, principalmente i protocolli di rete, che implementano i livelli astratti dei modelli concettuali per l'architettura delle reti, come il livello fisico, di collegamento (datalink) e di trasporto, che verranno approfonditi successivamente. La scelta di ognuna di queste cose è dettata dal tipo di esigenze che servono e da priorità di sicurezza diverse. Standardizzare le configurazioni e allinearsi a framework come ISO 27001 permette di creare reti sicure by design.

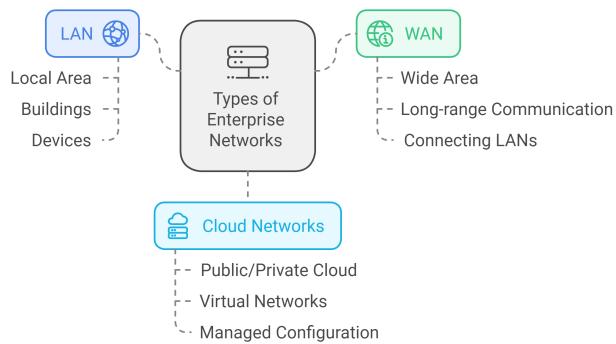


Figura 2.1. Rappresentazione dei tipi di Rete.

2.2 Principi e Strumenti per una Progettazione Sicura delle Reti

Analizzando il paper [2] e [54], diamo delle linee guida su qual è lo stato dell'arte da seguire per la progettazione di una rete aziendale sicura, la quale richiede l'integrazione di principi fondamentali come la modularità, l'isolation e il secure-by-default, fondamentali per assicurare un sistema in grado di anticipare le minacce, ridurre la superficie di attacco, garantire resilienza e che si possa recuperare in maniera sicura da fallimenti.

A partire dal modello “CIA triad”, troviamo tre concetti fondamentali per costruire una rete, e sono:

- Confidentiality: Protezione di dati sensibili da accessi non autorizzati. Per farlo si usa la crittografia, controllo degli accessi e altre misure.
- Integrity: Garanzia che i dati non siano alterati in alcun modo grazie a certificati digitali o a tecniche di hashing
- Availability: Possibilità di accedere ai dati e alle risorse quando serve. Per farlo vengono utilizzati sistemi ridondanti o di backup.

Un sistema sicuro si costruisce a partire da questi tre principi. In base al tipo di attività che si andranno a svolgere con la rete si possono bilanciare alcuni concetti.

Ci sono poi alcuni principi come l'utilizzo del machine learning, ML, e dell'intelligenza artificiale, di cui parleremo più avanti, che possono aumentare la sicurezza di alcuni sistemi.

Per difendersi quindi vengono sviluppati algoritmi in grado di rilevare e mitigare problemi di sicurezza in tempo reale, oppure grazie al ML si possono identificare pattern e anomalie. È fondamentale scrivere codice in maniera sicura e usare quindi programmi pensati per prevenire attacchi noti come quelli di Buffer overflow, SQL injection, e cross-site scripting.

Andiamo ora ad approfondire dei punti cardine necessari per costruire un sistema sicuro. È importante ricordare che l'applicazione di queste linee guida si deve adattare alla situazione per cui il sistema verrà usato. Infatti dobbiamo prima stabilire il contesto, gli obiettivi e le potenziali minacce, capire il rischio accettabile e cosa è necessario per eseguire il sistema. Sappiamo che attaccanti poco abili abbandonano l'attacco facilmente dopo qualche tentativo fallito, dobbiamo quindi fare in modo che il sistema sia difficile da attaccare. Bisogna anche prevedere diversi sistemi o livelli di autenticazione in quanto i malintenzionati preferiscono portare a termine i propri attacchi con tecniche di social engineering, email phishing e replay.

2.2.1 Principio della Difesa in Profondità

Per proteggere completamente un sistema non basta un singolo apparato di sicurezza, ma bisogna utilizzare una serie di strumenti e procedure che possono aiutare a fermare gli attacchi in corso e consente all'organizzazione di mitigare una serie di pericoli. Con il principio della difesa in profondità (defense-in-depth) mettiamo le basi per una sicurezza stratificata e ridondante. Se una linea di difesa viene compromessa infatti questo metodo ci permette di limitare i danni nel network; per di più, utilizzare un solo metodo di sicurezza introduce la problematica del “single point of failure” che, se viene compromesso, mette in pericolo l'intero sistema. Per implementare questo principio possiamo utilizzare, ad esempio, dei rilevatori. Se un sistema ha due rilevatori, essi possono essere usati in serie o in parallelo in base alla quantità di falsi positivi o negativi ottenuti e in base al sistema richiesto.

2.2.2 Principio del Minimo Privilegio

Questo principio ci suggerisce di fornire a ogni utente il minimo numero di permessi possibile richiesti per completare il proprio lavoro. Questo principio si applica anche ai programmi usati all'interno di un network, lasciando il numero minimo di permessi necessari per essere eseguito in maniera corretta, cercando di minimizzare il livello di privilegi dato a ogni programma.

2.2.3 Principio della Separazione dei Poteri

L'idea alla base di questo principio è quella di non dare a nessun utente troppo potere su un sistema, anzi il suggerimento è quello di dividere le responsabilità su più utenti, cercando di ridurre così la possibilità di rischi di sicurezza.

2.2.4 Principio della Sicurezza by Default

In questo fondamento ci assicuriamo che ogni impostazione di sicurezza sui vari programmi usati sia attiva di default, come:

- L'autenticazione a 2 fattori (2FA): meccanismo che richiede due metodi di identificazione all'utente che vuole accedere, e quindi la sola password non sarà sufficiente.
- Crittografia: la crittografia delle informazioni permette la lettura dei dati solo da parte di utenti autorizzati.
- Firewall: un dispositivo che permette di controllare il network e restringere il suo traffico basandosi su regole di sicurezza predefinite.
- Secure Boot: una caratteristica dove solo software autorizzato viene caricato all'accensione del sistema.

2.2.5 Principio della Modularità

Questo fondamento consiste nello smontare un sistema in piccoli componenti indipendenti o modulabili per aumentare la sicurezza. Un esempio di questo principio sono i microservizi, un metodo per sviluppare software modulare dove le grandi applicazioni sono divise in piccoli pezzi e usati indipendentemente. Questa tecnica punta a diminuire la superficie su cui si propaga l'attacco e limita gli effetti di questi. Un altro esempio è quello dell'hardware modulare, dove il sistema è smontato in componenti più piccoli che possono essere facilmente cambiati. Questo incrementa la sicurezza poiché rende più facile identificare problemi nelle patch dei singoli componenti. Un esempio di hardware modulare sono il processore, la RAM e i dispositivi di I/O. Un'altra pratica utilizzata è quella della virtualizzazione, ossia quella tecnologia che permette a più sistemi operativi o applicazioni di essere eseguiti su una singola macchina fisica. Questo aumenta la sicurezza in quanto isola ogni applicazione l'una dall'altra rendendo più difficile per un attaccante spostarsi all'interno del sistema. Questa tecnica fornisce un livello di isolamento che permette di limitare l'impatto di un sistema compromesso o può impedire che un attacco venga portato a termine.

2.2.6 Principio del Fallire in Maniera Sicura

Tutti i tipi di sistemi possono fallire, anche i più sicuri. È importante essere preparati a questo tipo di eventi per minimizzare l'impatto e questa strategia è alla base di ogni sistema sicuro di successo. Ci sono alcuni punti da seguire per ottenere ciò:

- Fallire con grazia (Fail Gracefully): ossia i sistemi e le applicazioni devono essere costruite per questa eventualità così da fare in modo che funzionino il più possibile anche sotto attacco. Per esempio se un sito di un ristorante d'asporto viene compromesso gli utenti devono avere la possibilità di vedere il menù ma no di piazzare ordini.
- Accesso Limitato: l'accesso a dati sensibili deve essere limitato solo agli utenti che lo necessitano veramente, per minimizzare l'impatto di un possibile attacco.
- Test e Aggiornamenti Frequenti: per prevenire le vulnerabilità è importante aggiornare con frequenza un sistema e testarlo con dei metodi di pentesting per assicurarsi della sua sicurezza.
- Crittografia: I dati sensibili devono essere crittografati, sia quando vengono mossi (inviati) sia quando vengono solo tenuti in memoria, da accessi non autorizzati.

2.2.7 Principio di Isolamento

Uno dei punti chiave per avere un sistema sicuro in ambito informatico è quello dell'isolamento, che ci aiuta a tenere varie parti del sistema o del network separate, prevenendo la distribuzione di malware. Possiamo applicare questo principio in varie aree della sicurezza informatica, come:

- Network Isolation: consiste nell'isolare parti diverse di un network per evitare che accessi non autorizzati o malware si possano propagare facilmente all'interno di questo. Per ottenere questo tipo di isolamento usando strumenti come firewall, VPN e tecniche di segmentazione della rete, VLAN. Questo permette di separare ad esempio i reparti all'interno di un'organizzazione.
- Process Isolation: separa processi o applicazioni diverse eseguite su un computer per evitare che del malware possa propagarsi tra di loro, per fare ciò sono usate tecniche di sandboxing² o di containerization.
- Data Isolation: separiamo i dati sensibili dal resto del sistema o del network per prevenire gli accessi non autorizzati, per farlo usiamo tecniche di encryption, accessi controllati e archiviazione sicura.

2.3 Tecnologie e strumenti per la Sicurezza nelle Reti

Analizziamo ora alcuni strumenti e tecniche utili per mettere in sicurezza le reti. Seguiremo i paper citati precedentemente.

²Un ambiente di prova.

Fonte: Wikipedia (<https://it.wikipedia.org/wiki/Sandbox>)

2.3.1 IDS, IPS e CIDN

Per mettere in sicurezza le reti a partire dai primi anni 2000, sono stati inseriti sistemi come l’Intrusion Prevention System (IPS) e l’Intrusion Detection System (IDS), all’interno dei firewall. Questi sistemi uniti insieme vennero ampiamente utilizzati e hanno aiutato a contrastare molti attacchi hacker negli anni. Con il passare del tempo però gli attacchi sono diventati sempre più sofisticati e questi due sistemi da soli non bastavano. Nasce così un nuovo concetto, quello del Collaborative Intrusion Detection Network, CIDN. Integrato negli ultimi anni all’interno dei firewall di nuova generazione, NGFW. Questo nuovo meccanismo, non lavora più autonomamente, ma utilizza dei nodi, chiamati peer, come IDS, questo permette al sistema di creare una collaborazione tra i peer, i quali condividono quello che hanno imparato dagli attacchi. Ci sono dei prerequisiti principali per la costruzione di una CIDN come: la comunicazione efficiente a distanze medio-brevi, la robustezza dei peer, la scalabilità e la partecipazione di tutti i nodi. Purtroppo anche i nodi stessi possono essere vittime di attacchi, compromettendo l’intera CIDN.

2.3.2 Next-Generation Firewall - NGFW

Il firewall è una soluzione che permette di mettere in sicurezza le reti; questo può essere sotto forma di software o di dispositivo fisico. Il suo intento è quello di monitorare e rafforzare i controlli nel traffico dati, anche controllando gli accessi. Qualsiasi tipo di traffico, sia interno che esterno, viene analizzato dal firewall e verrà “fatto passare” solo se rispetta le regole (o policy) di sicurezza che sono state create. Negli anni sono stati fatti investimenti e studi importanti da parte delle aziende per rendere questi dispositivi più sicuri, soprattutto per quello che riguarda il packet inspection e la profilazione del traffico. Alcuni firewall possono anche essere cloud-hosted al giorno d’oggi. Aiutano a intercettare e a bloccare anche attacchi di grande importanza e avanzati. Rispetto ai firewall di vecchia generazione, basati su regole, questi hanno fasi di costante apprendimento, aggiornando anche il loro database di attacchi e malware conosciuti, offrendo una maggiore protezione ogni volta che si verificano delle violazioni. Per questi nuovi dispositivi è anche possibile decifrare, analizzare e criptare il traffico SSL/TLS, agendo come un proxy, fondamentale per le connessioni HTTPS. Grazie poi alle possibilità di analizzare il traffico in maniera intelligente, mettere in quarantena potenziali virus, segmentare la rete e altre tecniche, riusciamo a rendere l’utente più sicuro concedendogli un controllo maggiore delle applicazioni e dei servizi, senza tralasciare le performance.

2.3.3 Segmentazione del Network interno

La segmentazione del network è una pratica fondamentale per migliorare la sicurezza e l’efficienza delle reti aziendali. Questa tecnica può essere implementata a diversi livelli del modello OSI³, come i layer 2 e 3, utilizzando strumenti come le Virtual Local Area Network, VLAN. Tuttavia, per scenari più complessi, come quelli che coinvolgono grandi infrastrutture o reti geograficamente distribuite, tecnologie avanzate come

³Fonte: Wikipedia (https://it.wikipedia.org/wiki/Modello_OSI)

Virtual Routing and Forwarding (VRF), Multi-Protocol Label Switching (MPLS) e il Border Gateway Protocol (BGP) giocano un ruolo cruciale.

- Virtual Routing Forwarding (VRF): consente di creare multiple istanze di routing virtualizzate su un singolo dispositivo fisico, utilizzando tabelle di routing indipendenti. Questo permette di isolare logicamente segmenti di rete senza richiedere hardware dedicato, riducendo i costi e migliorando la sicurezza attraverso la separazione del traffico.
- Multi Protocol Label Switching (MPLS): integra la segmentazione fornendo un routing efficiente tra le reti virtuali create con VRF. Utilizzando etichette anziché indirizzi IP, MPLS ottimizza il data forwarding, riducendo la latenza e migliorando la gestione del traffico in reti complesse. In combinazione con VRF, MPLS supporta la creazione di reti private virtuali, VPN, a livello di layer 3, ideali per connettere sedi remote in una WAN aziendale.
- Border Gateway Protocol (BGP): agisce come il collante che connette diverse reti autonome, AS, in un sistema globale. Nel contesto della segmentazione, BGP viene utilizzato per gestire il routing tra diverse istanze VRF o domini MPLS, assicurando che il traffico rimanga isolato e coerente anche quando attraversa confini organizzativi o geografici. Ad esempio, in una rete WAN, BGP può essere configurato per scambiare rotte solo tra specifiche istanze VRF, garantendo che il traffico critico non venga instradato attraverso percorsi non sicuri.

Insieme, VRF , MPLS e BGP formano un framework robusto per la segmentazione del network interno. Queste tecnologie lavorano in sinergia per garantire che il traffico sia isolato, instradato in modo efficiente e protetto da accessi non autorizzati.

Ad esempio, in un'organizzazione con sedi multiple, MPLS può essere utilizzato per instradare il traffico tra le sedi, mentre VRF garantisce che il traffico di reparti diversi (come Operativo e Tecnologico) rimanga separato. Allo stesso tempo, BGP assicura che le rotte tra le sedi siano ottimizzate e sicure, evitando che il traffico critico venga esposto a rischi durante il transito. Questo approccio integrato non solo migliora la sicurezza della rete, ma offre anche vantaggi in termini di scalabilità e flessibilità, rendendolo ideale per infrastrutture aziendali complesse e distribuite.

Esempio di integrazione

Immaginiamo un'azienda con sedi distribuite in diverse città che vuole separare il traffico IT (sistemi informatici) dal traffico OT (sistemi industriali). Per farlo, implementa una soluzione integrata basata su VRF , MPLS e BGP.

Sul router centrale, vengono configurate due istanze VRF : una per il traffico IT e una per il traffico OT. Questa separazione logica garantisce che i due tipi di traffico non si mescolino mai, riducendo il rischio di interferenze o accessi non autorizzati.

Per instradare il traffico tra le sedi in modo efficiente, viene utilizzato MPLS . I pacchetti IT vengono etichettati con una label MPLS dedicata (es. 100), mentre i pacchetti OT usano un'altra label (es. 200). Questo meccanismo assicura che il traffico segua percorsi predefiniti e rimanga isolato anche quando viaggia sulla stessa rete principale.

Infine, BGP gestisce il routing tra le sedi, scambiando rotte solo all'interno delle rispettive istanze VRF. Ad esempio, le rotte IT non vengono mai annunciate nella VRF_OT, garantendo che il traffico critico OT non sia esposto a rischi durante il transito.

Grazie a questa combinazione di tecnologie, l'azienda ottiene una rete sicura, scalabile e performante. Se una nuova sede viene aggiunta, è sufficiente configurare nuove istanze VRF e aggiornare le politiche BGP, senza dover riconfigurare l'intera infrastruttura.

2.4 Fondamenti per una sicurezza avanzata

Ricapitolando abbiamo visto finora delle misure di sicurezza convenzionali, che possono includere anche:

- IDS con:
 - Firewall a 2-stage.
 - DMZ.
- IPS con:
 - Ispezione del Knowledge Database (KDB).
 - Logging.
- Anti-Malware con:
 - Anti-spam, Anti-phishing, Anti-ransomware.
 - Funzionalità di quarantena.

Per una sicurezza più avanzata utilizziamo invece nuove tecniche e dispositivi come NGFW, CIDN visti sopra ma anche l'honeypotting (HP), tecnica che opera con risorse buone, ma “finte” e poco protette intenzionalmente, per attirare l'attenzione di potenziali attaccanti e distrarli dall'obiettivo principale o da risorse più importanti.

HoneyPotting

Questa strategia può essere usata in combinazione con le altre tecniche di firewall, IDS/IPS, CIDN. I suoi scopi sono molteplici tra cui: eludere potenziali intrusi, collezionare e analizzare informazioni su potenziali attacchi, monitoraggio delle vulnerabilità e controllo degli attacchi dall'interno. Questa tecnica collabora ampiamente con i gateway, i firewall del network e i knowledge database, come il MITRE ATT&CK. Questi HP simulano degli host fisici, come: macchine virtuali, dispositivi IoT⁴ o software fatti apposta per attirare gli attaccanti e distrarli. In caso di violazione del network, gli HP sono quelli con più probabilità di essere attaccati per primi in quanto sono, volutamente, meno sicuri. Questi dispositivi possono essere implementati in più modi:

⁴Fonte: Wikipedia (https://it.wikipedia.org/wiki/Internet_delle_cose)

- Server-Side Honeypotting: ossia che simulano un'applicazione lato server, dove l'intruso sarà attratto in un'area isolata e appena inizierà l'attacco l'honeypot inizierà a registrare le attività dell'attaccante e ad applicare contromisure specifiche.
- Client-Side Honeypotting: il suo obiettivo è quello di imitare un'applicazione come ad esempio un browser che accede siti non sicuri o pericolosi per poi loggare gli attacchi che subisce.

In conclusione, l'integrazione di tecnologie avanzate come gli honeypot con le soluzioni di sicurezza quali NGFW, CIDN e framework di segmentazione, permette di costruire un sistema di sicurezza multi livello, capace non solo di rispondere alle minacce esistenti ma anche di prevenirne di nuove, creando un ecosistema di difesa stratificato e resiliente, in grado di adattarsi alle crescenti minacce cyber e di fornire alle organizzazioni gli strumenti necessari per anticipare, identificare e mitigare efficacemente gli attacchi informatici, ponendo le basi per una strategia di sicurezza robusta.

2.5 Performance

Le reti aziendali moderne devono conciliare due obiettivi apparentemente contrastanti: garantire un alto livello di sicurezza e mantenere prestazioni ottimali. Misure di protezione come quelle prima citate possono introdurre overhead, latenza o complessità, influenzando l'efficienza operativa.

Questo capitolo analizza l'impatto delle tecnologie di sicurezza sulle performance delle reti, identificando metriche chiave, criticità e strategie per bilanciare sicurezza ed efficienza.

2.5.1 Metriche per valutare le performance

Per valutare le prestazioni di una rete aziendale sicura è essenziale monitorare alcune metriche fondamentali:

- Latenza: il tempo impiegato da un pacchetto dati per viaggiare dalla sorgente alla destinazione. Una latenza elevata può rallentare le applicazioni in tempo reale.
- Throughput: la quantità di dati che possono essere trasferiti in un determinato intervallo di tempo.
- Jitter: la variazione nel ritardo dei pacchetti.
- Disponibilità (Up-Time): la percentuale di tempo in cui la rete è operativa e accessibile.
- Packet Loss: la percentuale di pacchetti persi durante la trasmissione.

Queste metriche devono essere monitorate continuamente per identificare eventuali colli di bottiglia o inefficienze nella rete, o anche come metro di paragone per cercare di capire eventuali problemi.

Per garantire un network oltre che sicuro anche performante, dobbiamo adottare alcune strategie di ottimizzazione, come il Load Balancing che ci permette di ridurre il sovraccarico sui singoli componenti distribuendo il traffico tra più dispositivi. Possiamo anche fare utilizzo di tecniche di caching per i contenuti richiesti frequentemente così da migliorare il throughput. Possiamo anche adottare tecniche di Quality of Service (QoS), ossia una serie di meccanismi per controllare il traffico e assicurarci che alcune applicazioni critiche funzionino bene anche con una capacità della rete limitata. Consente quindi a un dispositivo di rete di differenziare il traffico e di applicare a questo comportamenti diversi per dare priorità al traffico critico, come il VoIP o le applicazioni aziendali più importanti, garantendo che le prestazioni rimangano elevate anche durante periodi di alto carico. Inoltre grazie a strumenti come Netflow, Wireshark o SNMP possiamo analizzare le prestazioni della nostra rete così da poterci regolare di conseguenza.

Notiamo ora come, secondo questo studio [66] più di un terzo del personale IT di un'azienda disabilita funzionalità importanti dei firewall o declina l'abilitazione di certe misure di sicurezza per aumentare le performance della rete. Vediamo come la funzionalità più disabilitata è quella del Deep Packet Inspection, DPI, che il 31% delle aziende ammette di disabilitare in quanto è la più pesante sulla rete. Guardando il grafico, notiamo che è seguita da anti-spam, anti-virus e VPN.

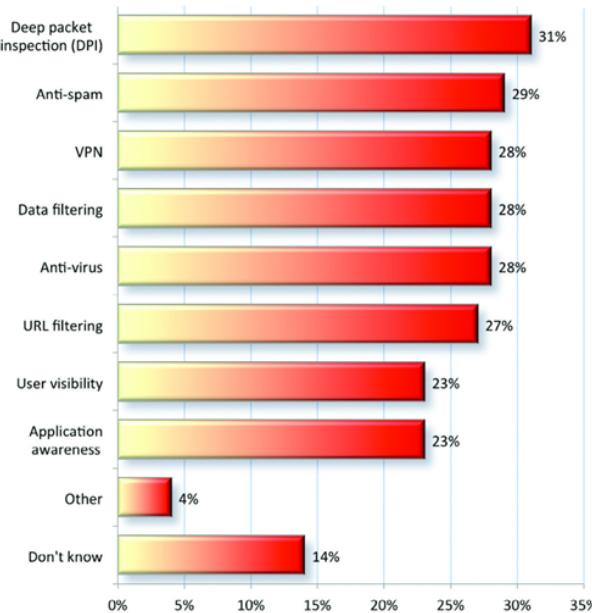


Figura 2.2. Risposta a: “Quale funzionalità di sicurezza è disabilità per favorire le performance?” [60].

Spesso i manager e i direttori operativi delle organizzazioni non sono al corrente dello stato di sicurezza delle loro reti, e lo scoprono quando è troppo tardi. Tra i vari reparti IT tutti vogliono supportare l'organizzazione dal punto di vista informatico, ma a volte alcune mansioni, come ad esempio la gestione delle regole del firewall, vengono assegnati a reparti che sottostimano i rischi di sicurezza, preferendo le performance.

Un altro rischio che viene citato nel paper è quello dei BYOD, i quali possono essere punti di entrata per potenziali attaccanti. Per fare un esempio basta pensare agli attacchi di tipo AET, Advanced Evasion Techniques, attacchi sofisticati che usano diverse tecniche di evasione per rimanere inosservati nella rete per molto tempo; utilizzando tecniche come la frammentazione, bypassano gli IPS. Gli AET dividono il loro payload in piccoli pezzi che vengono consegnati contemporaneamente per poi venire riassemblati e completare l'attacco. Il 40% degli addetti ai lavori ha sperimentato un attacco dove la tecnica AET ha giocato un ruolo chiave per la riuscita di quest'ultimo.

Per risolvere questo problema bisognerebbe testare frequentemente la propria attrezzatura, assicurandosi di bilanciare correttamente la performance senza trascurare la sicurezza e collaborando tra i vari reparti IT per raggiungere questo compromesso. Inoltre i direttori operativi dovrebbero considerare di investire di più nella loro sicurezza, rendendo la loro rete scalabile per facilitare il compromesso tra sicurezza e prestazioni. Leggiamo nel paper menzionato come già aggiungere un NGFW a un cluster di 3 o più può incrementare le performance di almeno il 75% e dovrebbero inserire delle routine organizzate per testare la loro rete più frequentemente.

Capitolo 3

Metodi di Gestione e Manutenzione per Reti Sicure

La sola implementazione delle soluzioni descritte precedentemente per costruire una rete sicura non basta. È fondamentale adottare una metodologia per la gestione e la manutenzione delle reti, al fine di preservare l'integrità e la sicurezza nel tempo. Vedremo i processi e le best practice per una corretta amministrazione delle infrastrutture di rete. Particolare attenzione sarà dedicata alla definizione di procedure standardizzate che permettano di mantenere nel tempo un elevato livello di sicurezza, riducendo al minimo gli errori umani e le vulnerabilità derivanti da configurazioni inappropriate.

L'obiettivo è quello di identificare un framework operativo che consenta agli amministratori di rete di gestire in modo efficace e sistematico le complesse infrastrutture moderne, bilanciando le esigenze di sicurezza con quelle di performance e disponibilità del sistema.

3.1 Framework e Politiche di Sicurezza

Per una gestione efficace bisogna costruire delle linee guida e seguire degli standard all'interno dell'azienda. Analizziamo alcuni dei framework più conosciuti.

3.1.1 ISO/IEC 27001

L'Organizzazione Internazionale per la Normazione è la più importante organizzazione a livello mondiale per la definizione di norme tecniche che, insieme alla Commissione Elettrotecnica Internazionale, hanno redatto un documento per definire dei requisiti specifici per l'implementazione di un Sistema di Gestione della Sicurezza delle Informazioni (SGSI). Questo documento è fondamentale per aiutare le aziende a mantenere la sicurezza delle loro informazioni. Data la costante crescita delle tecnologie, questo standard viene aggiornato periodicamente, con l'ultima versione redatta nel 2022. Lo scopo di questo standard è certificativo, permettendo di costituire un sistema completo per garantire la gestione della sicurezza nella tecnologia dell'informazione.

La norma si basa sul modello PDCA (Plan-Do-Check-Act) e segue un approccio basato sulla gestione del rischio. I punti principali di questo approccio sono:

- Pianificazione e Progettazione. In particolare, qua è richiesta una fase di risk assessment, che viene suddivisa in:
 - Identificazione dei rischi.
 - Analisi e valutazione.
 - Selezione degli obiettivi di controllo e attività di controllo per la gestione dei rischi.
 - Assunzione del rischio residuo da parte del management.
 - Definizione dello Statement of Applicability, ossia gli obiettivi di controllo adottati e i controlli implementati dall'organizzazione rispetto ad una lista di obiettivi di controllo previsti dalla norma.
- Implementazione (processi operativi).
- Monitoraggio.
- Miglioramento.

Di fondamentale importanza è l'Annex A “Control objectives and controls” che contiene i 133 “controlli” a cui l'organizzazione che intende applicare la norma deve attenersi; infatti, questo allegato descrive le azioni necessarie per garantire la sicurezza dei sistemi IT. Si occupa anche di importanti aspetti della sicurezza dei dati, come la sicurezza fisica, la protezione legale, la gestione delle risorse umane e le questioni organizzative.

Questa norma è applicabile a tutte le imprese o aziende pubbliche, dato che non si basa su uno specifico settore di business o organizzazione. Bisogna tener presente che l'adozione e gestione di un SGSI richiede un impegno di risorse significativo e quindi deve essere seguita da un ufficio specifico.

ISO/IEC 27002

Questo è un documento aggiuntivo costituito da una raccolta di “best practices” che possono essere adottate per soddisfare i requisiti della norma ISO 27001 al fine di proteggere le risorse informative. A differenza della norma 27001, la 27002 non è certificabile in quanto è una raccolta di semplici raccomandazioni. Anche questo documento, seppur non certificabile, ha la sua importanza tecnica proprio per le linee guida che fornisce ed è complementare alla 27001, andando a spiegare ogni controllo presentato nell'allegato A prima citato e come essi possano essere implementati.

3.1.2 NIST Cybersecurity Framework - CSF

Sviluppato dal National Institute of Standards and Technology, NIST¹, il Cybersecurity Framework è un insieme di linee guida progettate per aiutare le organizzazioni a valutare e migliorare la loro capacità di prevenire, rilevare e rispondere ai rischi di sicurezza informatica. È stato progettato per essere flessibile e adattabile, fornendo una guida di alto livello che consente alle singole organizzazioni di determinare le specifiche di implementazione in base alle loro esigenze uniche e ai profili di rischio. Sebbene ampiamente elogiato, è stato criticato per i costi e la complessità connessi alla sua attuazione, in particolare per le piccole e medie imprese. Il CSF è formato da 3 componenti principali:

- Core. Il quale offre un insieme strutturato di attività e linee guida correlate ai diversi aspetti della cybersecurity. Al suo interno, definisce 6 funzioni fondamentali, articolate in 23 sottocategorie distinte, tra cui:
 - **Identificare.** Questa funzione è orientata a rafforzare la consapevolezza sugli asset aziendali e sui rischi correlati, ottimizzando anche i processi di gestione patrimoniale.
 - **Proteggere.** La finalità di questa funzione è preservare l'integrità di dati sensibili e infrastrutture tecnologiche, rilevando accessi illeciti, violazioni e potenziali attacchi informatici.
 - **Rilevare.** Questa funzione include una sorveglianza sistematica degli incidenti di cybersecurity, attraverso attività come l'identificazione di intrusioni e il tracciamento log e il monitoraggio degli eventi.
 - **Rispondere.** Lo scopo di questa funzione è di attivare tempestive contromisure in caso di incidenti, attraverso una gestione coordinata delle risorse al fine di contenere gli impatti e accelerare il ripristino delle funzionalità.
 - **Recuperare.** Si focalizzata sul ripristino dell'operatività post-incidente, questa funzione garantisce una transizione efficiente verso la regolare attività, integrando al contempo azioni correttive per potenziare le difese future.
 - **Govern.** Introdotta con l'aggiornamento 2024 del framework, questa funzione rappresenta un nuovo pilastro strategico: guida all'integrazione coerente delle altre cinque funzioni, estendendo la sua applicabilità a tutti gli asset tecnologici dell'organizzazione.

¹Fonente: NIST (<https://www.nist.gov/>)

- Implementation Tiers. Si tratta di livelli progettati per supportare le organizzazioni nella valutazione dell'efficacia delle proprie strategie di cybersecurity e del loro grado di evoluzione. La suddivisione prevede 4 livelli, così definiti:
 - **Tier 1 – Parziale.** Le organizzazioni dimostrano una consapevolezza parziale delle minacce informatiche, gestendo la sicurezza con criteri disorganizzati e privi di un piano strutturato.
 - **Tier 2 – Informato.** Le organizzazioni delineano una strategia di gestione del rischio più articolata, avviando l'integrazione graduale di un programma cybersecurity strutturato e documentato.
 - **Tier 3 – Ripetibile.** Le organizzazioni dispongono di un framework cybersecurity consolidato, accompagnato da meccanismi di mitigazione del rischio e un monitoraggio periodico delle prestazioni di sicurezza.
 - **Tier 4 – Adattivo.** Le organizzazioni adottano un approccio alla cybersecurity avanzato e dinamico, caratterizzato da un orientamento proattivo alla gestione del rischio, ai processi di ottimizzazione continui e alla capacità di risposta rapida ed efficace agli incidenti.
- Profiles. Strumenti flessibili che permettono di personalizzare il framework in base alle esigenze organizzative e al profilo di rischio. Tipicamente, le organizzazioni definiscono un “Profilo corrente” per catalogare le pratiche e i risultati già attivi in ambito sicurezza. In seguito, costruiscono un “Profilo obiettivo” per identificare i traguardi desiderati e pianificare le iniziative di transizione. Alternativamente, è possibile adottare un profilo predefinito, calibrato su standard di settore o su specificità operative rilevanti.

Anche questo framework ha subito diversi aggiornamenti per stare al passo con la tecnologia, arrivando all'ultima versione, la 2.0 del 2024, aggiungendo nuove linee guida sulla governance della sicurezza informatica.

Unione tra ISO/IEC 27001 e NIST CSF

L'unione tra i due framework rappresenta un approccio strategico vincente per rinforzare la sicurezza informatica di un'organizzazione, permette di potenziare la capacità di gestione del rischio, di ottenere una certificazione internazionale e di promuovere un miglioramento continuo alle pratiche di sicurezza, ma nonostante i vantaggi, l'integrazione presenta sfide significative. Mantenere infatti l'allineamento dei diversi requisiti, così come la certificazione nel caso di ISO 27001, personalizzando allo stesso tempo gli approcci per adattarli al proprio contesto, come suggerito dal CSF, non è un lavoro da poco. Le organizzazioni devono gestire queste difficoltà con attenzione per definire una strategia di cybersecurity coerente, in grado di affrontare sia le minacce in evoluzione sia le richieste normative, garantendo al contempo una solida gestione della sicurezza delle informazioni.

Per affrontare queste sfide, sviluppare un piano di integrazione che combini i punti di forza di entrambi i modelli e che implementi i controlli, dando priorità ad aree critiche necessarie, è fondamentale per far convivere entrambi i framework insieme creando una struttura solida. Le organizzazioni disposte a investire in un

programma completo di sicurezza informatica che incorpora entrambi i modelli possono trovare vantaggi strategici a lungo termine. Stabilendo una solida base con ISO 27001 e migliorando la flessibilità attraverso CSF, le organizzazioni possono sviluppare una strategia di sicurezza informatica solida e resiliente su misura per le loro esigenze e obiettivi unici [38], [73].

3.1.3 COBIT 2019

Tra i vari framework troviamo anche il COBIT, ossia il Control Objectives for Information and Related Technologies, sviluppato in particolare per la governance IT, che garantisce sicurezza, integrità e conformità normativa adattandosi bene a organizzazioni di ogni tipo, grandi o piccole. La sua struttura è composta da 6 punti chiave, ed essi sono:

- **Processi.** Attività e pratiche necessarie per raggiungere specifici obiettivi IT.
- **Strutture Organizzative.** Organi che prendono decisioni nella governance.
- **Principi, politiche e framework.** Linee guida per allineare l'IT alla società.
- **Flussi di informazioni.** Dati essenziali per la governance.
- **Cultura, etica e comportamenti.** Come i comportamenti di un individuo o di un gruppo impattano sulla governance.
- **Persone, skill e competenze.** Risorse umane critiche per raggiungere gli obiettivi di governance.

L'approccio strutturale di questo modello è molto flessibile e permette alle organizzazioni di adattarsi al framework in base alle loro necessità e lo rende facile da implementare. Questo modello promuove anche il cambiamento, aiutando le aziende ad adattarsi agilmente ai cambiamenti tecnologici; inoltre facilita la comunicazione e la collaborazione tra i diversi software interni di un business, supportando il management IT [1]. Questo modello è sicuramente il più adatto per la manutenzione continua e il management di una rete, essendo stato pensato per questo, fornendo allo stesso tempo solidi principi di sicurezza. Fornisce una struttura e un metodo d'approccio chiaro che cerca di legarsi agli obiettivi aziendali [83]. Si concentra molto sull'importanza della manutenzione, sul controllo della rete, cercando sempre una risposta proattiva alla sicurezza, tenendo conto anche del fattore umano. Allo stesso tempo, la troppa flessibilità di questo framework e i diversi controlli che ha possono essere travolgenti per una società con poche risorse, in particolare quelle che non hanno un reparto IT dedicato [30].

3.1.4 Politiche e Strutture Interne

La chiara definizione dei ruoli e delle responsabilità è un pilastro fondamentale per creare una governance efficace della sicurezza informatica. Senza una struttura organizzativa ben delineata, anche le policy più rigorose rischiano di rimanere teoriche. Vediamo l'importanza di alcuni ruoli come il Chief Information Security Officer, CISO, il responsabile strategico della sicurezza informatica il quale ha un ruolo trasversale

che collega la direzione esecutiva, i reparti operativi e gli standard normativi. Questa figura si occupa infatti di sviluppare e implementare processi e sistemi sicuri per prevenire, rilevare e recuperare da attacchi, di definire gli obiettivi a lungo termine, di allineare il rischio aziendale ai vari framework di cui abbiamo parlato in precedenza e di implementare le policy di sicurezza che l'azienda deve seguire. Si occupa inoltre di allocare fondi per gli strumenti tecnologici, per la formazione del personale e di progettare e realizzare il piano di cybersecurity aziendale, per tenere al sicuro le risorse informatiche societarie. Si assume la responsabilità di garantire l'aderenza a normative come il GDPR (normativa per la privacy²) e altre. Il suo ruolo è estremamente versatile, con compiti che non si limitano alla sicurezza informatica ma anche alla gestione aziendale, per cui non bastano solide basi in ambito IT ma sono necessarie anche competenze in ambito finanziario e amministrativo [20]. Questo ruolo in genere nelle imprese di medio-piccole dimensioni viene ricoperto da un membro del personale IT se presente, altre volte viene appaltato esternamente, mentre nel 40% dei casi viene completamente ignorato [67]. Non in tutte le grandi imprese invece viene definito questo ruolo, infatti spesso viene affidato al CIO, Chief Information Officer, il quale si occupa però di tutta l'area IT e non solo della sicurezza; questo può portare a una negligenza di quest'ultima. Con il passare del tempo, la figura del CISO si è sempre più affermata e insieme a questa si è andato ad affiancare il ruolo di Cyber Security Manager. Questa figura ha un ruolo più tecnico ma meno manageriale rispetto al CISO, con il quale divide la responsabilità della sicurezza informatica aziendale. Contribuisce alla stesura delle policy di sicurezza e si occupa di farle rispettare, valuta rischi minacce e possibili conseguenze e gestisce il piano di Incident Response [67].

3.2 Monitoraggio della Rete

Il monitoraggio della rete è un aspetto fondamentale non solo per il corretto funzionamento o per il controllo delle performance di queste, ma anche per la loro sicurezza. Queste tecnologie si occupano di identificare componenti del sistema lenti e/o compromessi, così da poter rilevare, rispondere e mitigare potenziali attacchi per garantire la sicurezza del sistema. Al giorno d'oggi sono diverse le soluzioni per monitorare il network, come l'analisi del traffico, l'alerting in tempo reale e altre. Analizziamo ora i diversi tipi di monitoraggio del traffico.

3.2.1 Active Network Monitoring

Consiste nel generare traffico con pacchetti specifici all'interno della rete per testare la performance, l'availability e la reattività di quest'ultima. Questa tecnica di monitoring ha un approccio proattivo che permette la simulazione di breach nella rete per vedere la risposta del network sotto varie condizioni, misurando la performance con metriche tipo il response time, la latency, la percentuale di pacchetti persi e il throughput. Questa soluzione coinvolge l'implementazione di monitoring agents o sensori in punti strategici della rete per monitorare il traffico end-to-end che

²Fonte: Wikipedia (https://it.wikipedia.org/wiki/Regolamento_generale_sulla_protezione_dei_dati)

permettono il funzionamento prima descritto. Questo tipo di monitoraggio è comodo per una rete grande in quanto è scalabile e accomoda anche sistemi distribuiti [65].

Anche se alcune grandi aziende potrebbero sviluppare dei propri tool di monitoring in-house, alcune imprese potrebbero preferire la possibilità di fare out-sourcing di questo servizio. Tra gli applicativi leader per le grandi imprese abbiamo SolarWinds³, dato che è in grado di gestire reti complesse grazie alla sua scalabilità. Questo strumento è in grado di offrire rapporti dettagliati della rete, real-time monitoring, alerts automatici e altro. Questo applicativo comporta una spesa iniziale non solo per il programma in sé quanto per la difficoltà di gestione [65].



Figura 3.1. Pannello di controllo SolarWinds³.

3.2.2 Passive Network Monitoring

Questo tipo di monitoring cattura il traffico della rete implementando sensori al suo interno. A differenza dell'Active Monitoring, questo metodo non è proattivo, non interferirà quindi con le operazioni della rete, ma osserva semplicemente il traffico, fornendo un'analisi in tempo reale anche sui dati passati, facilitando l'identificazione di un pattern. Questi strumenti sono utili per individuare la causa di anomalie della rete, misurare la performance delle applicazioni, analizzare il comportamento della rete, anche durante attacchi esterni, mantenendo dei log dettagliati dell'attività nel network. Nelle varie implementazioni di questo tool non è raro trovare dei strumenti di monitoring chiamati "network tap" che catturano i pacchetti, analizzandone il contenuto ed estraendone informazioni importanti sulla performance, sicurezza e comportamento del network [45].

Questo tipo di monitoraggio viene preferito quando si vogliono catturare informazioni utili dal traffico della rete senza interferire con le operazioni di quest'ultima.

³ Sito: (<https://www.solarwinds.com/>)

Uno dei strumenti più utilizzati sia nelle aziende di grandi dimensioni che più piccole, ma anche da utenti privati, è Wireshark⁴, programma open source in grado di essere eseguito sui sistemi operativi più utilizzati e che permette all'utente di osservare tutto il traffico presente sulla rete tramite interfaccia grafica.

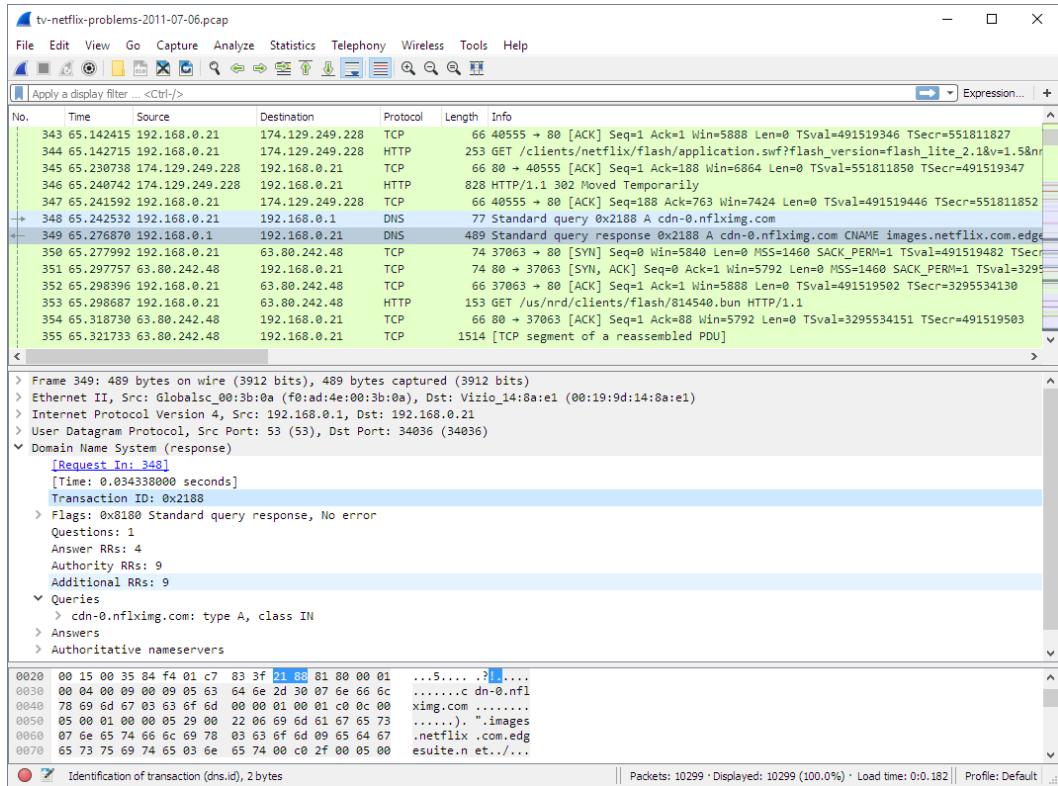


Figura 3.2. Pannello di controllo Wireshark⁴.

3.2.3 SNMP Network Monitoring

Il Simple Network Management Protocol è un protocollo di management della rete molto utilizzato per sorvegliare i dispositivi nel network e i suoi sistemi. È un protocollo di rete che permette ai network administrator di raccogliere informazioni dai dispositivi nella rete, così da monitorare le loro performance e gestirli da remoto. Permette di raccogliere parametri importanti come la banda utilizzata, l'utilizzo di risorse hardware e la percentuale di errori. Fornisce una visione in real time dell'infrastruttura di rete e consente un troubleshooting proattivo. Per implementare questa tecnica di controllo, i dispositivi devono avere un software con un agente SNMP installato così da poter fornire dati all'SNMP manager. Questa tipologia di monitoring offre diverse funzionalità utili agli amministratori della rete per gestire la rete. Il device discovery permette di scoprire i dispositivi nella rete in automatico, semplificando il processo di aggiunta dei dispositivi al sistema di monitoring. Permette anche di rilevare anomalie nei dispositivi collegati alla rete generando notifiche e alert per permettere una risposta pronta in situazione critiche. Grazie

⁴Sito: (<https://www.wireshark.org/>)

agli agenti precedentemente menzionati è anche possibile modificare le configurazioni dei dispositivi anche da remoto, garantendo una gestione più facile e rapida su più device, assicurando una coesione ai standard della rete [45]. Uno dei software utilizzati dalle grandi aziende è Obkio⁵.



Figura 3.3. Pannello di controllo Obkio⁵.

3.2.4 SIEM

Per gestire e poter utilizzare tutte le informazioni, gli alert e i dati provenienti dal monitoring della rete è necessario un sistema di **Security Information and Event Management**, SIEM. Questo strumento raccoglie tutti i dati e gli eventi relativi alla sicurezza da diverse fonti di una rete, i quali sono rappresentati tramite schemi diversi, spesso prioritari di qualche brand. I SIEM includono anche informazioni di contesto che possono essere utili nell'analisi, come dati aggiornati sugli asset aziendali, regole e priorità degli alert. Il compito di questo sistema è quello di correlare tra loro i log provenienti da fonti diverse, trovando attributi comuni così da poter definire un pattern per degli attacchi o scenari che possono allertare i Security Analysts. I SIEM lavorano con gli strumenti di monitoring definiti in precedenza e utilizzano vari sensori e applicazioni presenti sui dispositivi e nella rete per monitorare il comportamento di questi, se necessario inoltre archivia in un database eventi per cui potrebbe essere opportuna un'analisi a lungo termine, così da non tralasciare malware potenzialmente resiliente. Vengono create delle regole generate algoritmamente, le quali catturano informazioni su comportamenti malevoli, il rischio però è che se queste regole sono mal configurate si rischia di trasformare il SIEM in un sistema di big data, che renderebbe l'archiviazione, la ricerca, l'analisi e la condivisione una sfida. Un altro problema più importante riguarda quello dei falsi positivi; infatti, se le regole dovessero generare troppi falsi positivi tra gli allarmi, l'analisi degli eventi potrebbe diventare difficile da gestire. Allo stesso modo, un numero alto di falsi negativi potrebbe compromettere la rete; bisogna quindi trovare il giusto compromesso tra i due, così da poter individuare il

⁵Sito: (<https://obkio.com/>)

maggior numero possibile di attacchi senza però raccogliere troppi dati inutili ai fini della sicurezza [8].

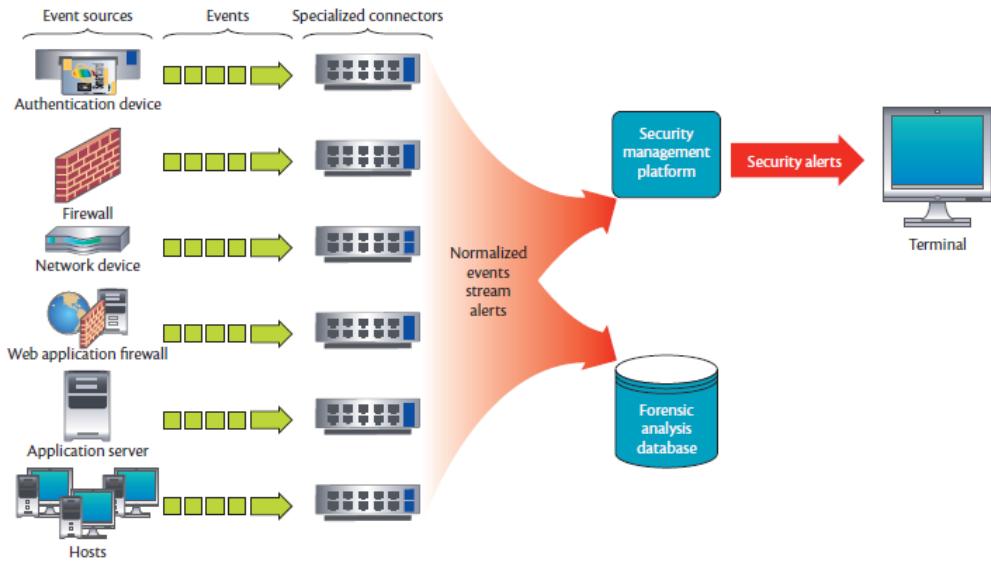


Figura 3.4. Un'architettura generica di un SIEM. Il SIEM accetta gli input dai vari dispositivi di sicurezza e sensori. Dopo averli ricevuti li normalizza in un formato comune [8].

Questo strumento è particolarmente utile nella manutenzione per riconoscere minacce in tempo reale, migliorare l'efficienza organizzativa, grazie a dashboard centrali che permettono una risposta rapida ed efficiente alle minacce e agli incidenti. Permette inoltre di condurre indagini forensi all'interno della rete, analizzando attività sospette e imparando da incidenti passati. Fornisce inoltre un grande supporto di sicurezza alla rete, mitigando e monitorando i BYOD, tracciando le attività di rete di tutti gli utenti, i dispositivi e le applicazioni, migliorando notevolmente la trasparenza dell'intera infrastruttura e rilevando le minacce indipendentemente da dove si accede agli asset [8].

3.2.5 SOC

Per monitorare gli eventi, tutte le informazioni contenute nella rete e i suoi asset, avremmo bisogno di un **Security Operation Center**, SOC. Si tratta di un'infrastruttura dove risiede un team specializzato incaricato di monitorare, analizzare e rispondere agli incidenti della rete in tempo reale. Questo reparto riceve in continuazione informazioni sugli eventi dai sensori, dai log e dagli alert di cui abbiamo parlato in precedenza. Quando un alert viene azionato e notificato, il personale del SOC deve determinare se si tratta di un falso positivo o meno e il suo compito è quello di proteggere gli asset aziendali. Un SOC può essere in-house, e quindi interno all'organizzazione, o preso in out-sourcing, ossia appaltato a un'azienda esterna. In genere la seconda via è quella percorsa dalla maggior parte delle organizzazioni in quanto la prima risulta essere troppo costosa. Queste strutture possono essere fisiche o cloud-based e il personale che compone questa struttura è personale specializzato

in sicurezza informatica [16]. Questa divisione ha diverse funzioni come il threat hunting e il threat intelligence, ossia il compito di fornire informazioni aggiornate sui rischi di cyber sicurezza moderni. Questa funzione permette anche di tenere il SOC, e di conseguenza l'organizzazione, in costante sviluppo per proteggersi. Il threat hunting consiste nell'identificare e investigare attivamente gli attacchi che potrebbero avere bypassato i controlli di sicurezza. Abbiamo poi una sezione che si occupa di mantenere gli strumenti utilizzati dal SOC e i suoi logs, assicurandosi il corretto funzionamento dell'organizzazione. Questa si occupa anche di gestire gli incidenti quando ci sono, ossia di investigarne la causa. Il loro obiettivo è mitigare l'impatto dell'attacco e questo viene anche segnalato al reparto che si occupa di Incident Management, che si occupa della parte gestionale dell'incidente. Un altro reparto importante in questa struttura è quello che gestisce le vulnerabilità; il loro compito è trovarle all'interno dell'organizzazione e questo compito richiede risorse, competenze e strumenti proprio per il pentesting. Troviamo poi la funzione di Insider Threat che si occupa di individuare gli attacchi provenienti dall'interno utilizzando tecniche e strumenti diversi rispetto agli attacchi esterni [16].

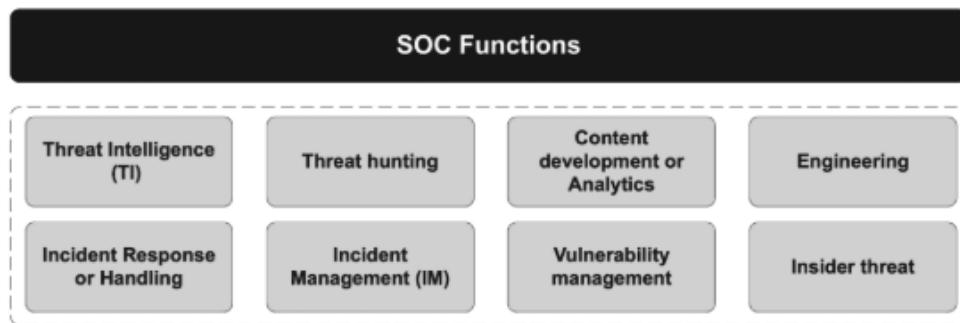


Figura 3.5. Descrizione delle funzionalità di un SOC [16].

Questa infrastruttura segue una struttura particolarmente gerarchica e divide infatti il proprio personale in analisti di sicurezza di diverso livello, che vanno in genere dall'uno, coloro che troviamo in prima fila che sorvegliano continuamente l'infrastruttura della rete aziendale, al terzo, che in genere corrisponde al CISO o al Cyber Security Manager di cui abbiamo parlato in precedenza. Per il SOC è fondamentale agire secondo dei framework e delle politiche di sicurezza prestabilite e ben delineate, manutenendosi secondo delle politiche di governance da rispettare. Un altro strumento di cui abbiamo parlato in precedenza e di cui il SOC ne fa ampio utilizzo è il SIEM.

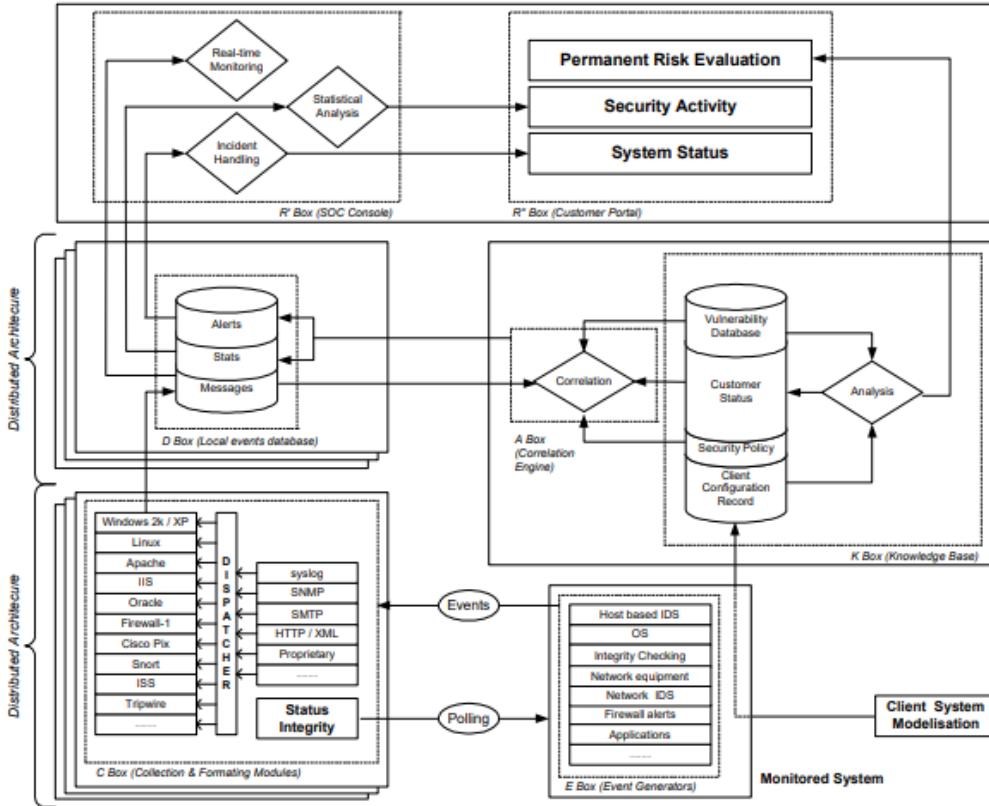


Figura 3.6. Descrizione dell'architettura di un SOC [9].

MITRE ATT&CK

Abbiamo citato in precedenza i Knowledge Database, ossia delle banche dati dove sono raccolte tutte le tecniche e tattiche di attacco già conosciute, utili per poter prevenire e rilevare le offensive informatiche. Tra i Knowledge Database più utilizzati troviamo il MITRE ATT&CK, un database accessibile a tutti contenente la maggior parte degli attacchi conosciuti e in continuo aggiornamento per mitigare questo problema. Questo strumento funziona basandosi su una vasta Threat Intelligence Mapping, infatti grazie alle tattiche, tecniche e procedure (TTP), utilizzate in passato nei vari attacchi, si è in grado di prevedere il comportamento futuro di un attaccante, informazione fondamentale per poter difendersi al meglio. Questo è possibile grazie al continuo aggiornamento di questo strumento, ma anche grazie a una struttura organizzata delle TTP usate. Un'altra funzionalità chiave di questo strumento, chiamata Data Source Gap Identification, è un processo che identifica le lacune nei dati disponibili per rilevare tecniche specifiche. Il MITRE ATT&CK elenca per ogni tecnica i data source necessari, come: log di processo, registri di autenticazione, dati di rete e altri, permettendo alle organizzazioni di valutare se dispongono degli strumenti per monitorare quelle attività [4].

L'utilizzo del MITRE ATT&CK può essere fondamentale nei SOC, in quanto fornisce la conoscenza necessaria per le loro operazioni base, ossia rilevare, rispondere e mitigare le minacce cibernetiche, fornendo conoscenze standardizzate e dettagliate per capire le tecniche e tattiche avversarie. Il framework è organizzato in diverse categorie, tra cui le tattiche. Queste rappresentano ad alto livello gli obiettivi a cui un attaccante mira. Ognuna di queste tattiche ha diverse tecniche che specificano i dettagli dei metodi usati per raggiungere l'obiettivo della tattica. Altri componenti del framework contengono le sotto-tecniche, che offrono metodi più dettagliati per gli obiettivi tattici di difesa, le procedure, che descrivono in maniera specifica che tipo di avversario applica certe tecniche o sotto-tecniche e le mitigazioni, che specificano misure difensive per prevenire la riuscita di un attacco.

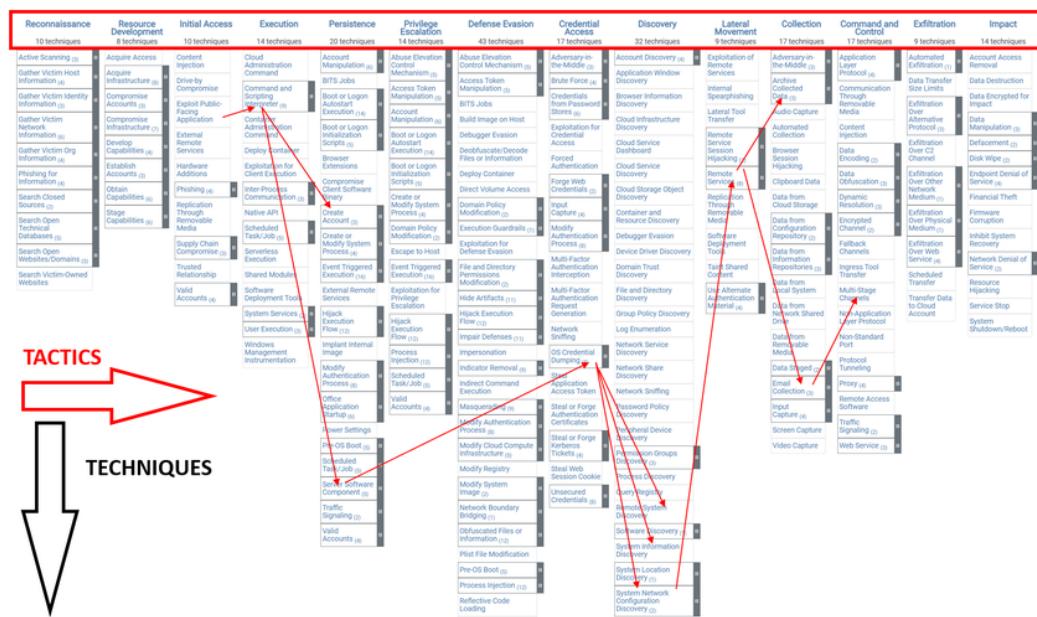


Figura 3.7. Il layout della matrice del MITRE ATT&CK per il dominio Enterprise⁶. Le tattiche sono organizzate per colonne mentre le tecniche per righe [3].

Grazie a questo strumento i SOC hanno un aiuto per allineare le loro strategie anche in base alle potenziali intenzioni di un attaccante, aumentando l'efficienza e la risposta alle minacce della cyber sicurezza e tenendosi sempre aggiornati in materia, permettendo di reagire proattivamente alla minaccia. In un campo in continuo cambiamento come la cyber security è cruciale per i Security Operation Centers capire le tattiche e le tecniche avversarie per sviluppare una strategia di risposta funzionale. Vediamo come in questi paper [42], [19] l'integrazione di questo knowledge database ha migliorato le strategie dei SOC, i paper forniscono esempi concreti di come lo strumento ha minimizzato i potenziali danni e perdite. Migliorando anche i rapporti di rilevazione e abbassando i tempi di risoluzione degli incidenti. Ricordiamo che questo strumento si basa sugli attacchi già conosciuti, è quindi fondamentale non utilizzare questo come unica risorsa di difesa, rendendo comunque fondamentale

⁶Il termine dominio Enterprise si riferisce a un insieme di sistemi, reti e tecnologie utilizzate all'interno di organizzazioni aziendali o imprese.

l'allocazione di risorse per la formazione del personale e di altri strumenti necessari per combattere le minacce [3].

3.3 Manutenzione Preventiva

La manutenzione preventiva consiste in un approccio cautelare nei confronti degli asset digitali dell'organizzazione e delle sue infrastrutture, cercando di prevenire, appunto, violazioni nella rete. Questa è una strategia che sta acquistando sempre più importanza tra le società. Grazie alla prevenzione, tramite strumenti come il controllo degli accessi, il patch management, i backup, e altri, si è in grado di rispondere meglio agli attacchi e di fornire continuità ai servizi o alle risorse in maniera più rapida. Questa tecnica cerca quindi di identificare e correggere i potenziali problemi prima che si trasformino in vulnerabilità o incidenti. Un punto chiave della manutenzione preventiva è anche la formazione del personale. Mettere in guardia e informare i propri dipendenti dei pericoli a cui l'infrastruttura di rete è soggetta, li potrà aiutare a riconoscere e a rispondere a comportamenti pericolosi. A differenza della manutenzione classica, quella preventiva permette dei down time minori, ma previene anche potenziali perdite di dati e violazioni di sicurezza.

3.3.1 Controllo degli Accessi

Uno dei metodi più antichi di prevenzione è il controllo degli accessi. Il compito di questa funzione di sicurezza è quello di limitare le attività di utenti legittimi. Tramite un reference monitor⁷ controlliamo i tentativi di accesso da parte di un utente (o un programma eseguito da un utente) verso un oggetto nel sistema. Il reference monitor consulta un database di autorizzazioni per determinare se un utente può effettivamente fare un'operazione o meno. Le autorizzazioni in questo database sono gestite da un security administrator⁸ basandosi sulle policy interne di sicurezza dell'organizzazione. È importante distinguere l'autenticazione dal controllo degli accessi, infatti stabilire correttamente l'identità di un utente è responsabilità dei servizi di autenticazione mentre il controllo degli accessi prende per buona l'identità dell'utente in quanto non è di sua competenza. Notiamo inoltre che in una rete il processo di autenticazione è più difficile da gestire in quanto un potenziale intruso potrebbe osservare il traffico del network e può replicare i protocolli di autenticazione per mascherarsi come utente legittimo, attacco noto come masquerade attack. Dobbiamo fare una distinzione anche tra politiche e meccanismi di sicurezza. Le politiche sono linee guida di alto livello che determinano come vengono controllati gli accessi e come vengono prese le decisioni di accesso. I meccanismi sono funzioni software e hardware di basso livello che possono essere configurate per implementare una politica. In generale non esistono politiche migliori di altre in quanto alcune potrebbero essere adatte per un sistema ma non per un altro. Negli anni sono state sviluppate diverse idee astratte per implementare questa funzionalità, come la matrice degli accessi. Alla base di queste idee troviamo sempre una divisione tra oggetti e soggetti. Gli oggetti sono i dati che troviamo memorizzati in un sistema, la

⁷Fonente: Wikipedia (https://en.wikipedia.org/wiki/Reference_monitor)

⁸Fonente: Wikipedia (<https://it.wikipedia.org/wiki/Sistemista>)

cui protezione è il requisito fondamentale, mentre le entità che iniziano delle attività sono chiamati soggetti, ossia utenti o programmi eseguiti da utenti. Un utente si autentica al sistema con soggetti differenti in occasioni differenti in base al tipo di privilegio di cui ha bisogno. Il soggetto inizia quindi operazioni sugli oggetti che saranno permesse o meno in base alle autorizzazioni prestabilite nel sistema.

	File 1	File 2	File 3	File 4
User 1	Read	Write	Own	—
User 2	Write	Own	—	—
User 3	Own	—	—	Read
User 4	Read	Read	Read	Own

Figura 3.8. Un esempio di matrice di controllo degli accessi con i suoi permessi [32].

In questo modello concettuale troviamo delle righe per ogni soggetto e delle colonne per ogni oggetto e ogni cella della matrice specifica i permessi di accesso per ogni soggetto nella riga e ogni oggetto nella colonna.

Le autorizzazioni sono espresse in termini di diritti di accesso e dipendono dal tipo di oggetto in questione, per i file i diritti di accesso saranno “read”, “write”, “execute” e “own”, in particolare l’attributo di proprietà può controllare chi può cambiare i diritti di accesso per il file. Se l’oggetto dovesse essere per esempio un conto bancario i diritti saranno tipo “inquiry”(consultare), “credit”(accreditare) e “debit”(addebitare) che corrisponderanno alle operazioni basiche che possono essere effettuate su un conto.

Dato che nei sistemi reali una matrice di questo tipo avrebbe dimensioni enormi, si è pensato a degli approcci implementativi diversi.

Access Control List - ACL

Ogni oggetto è associato a una ACL, che specifica, per ogni soggetto nel sistema, gli accessi che il soggetto è autorizzato a eseguire sull’oggetto. Questo approccio si limita quindi a memorizzare le colonne della matrice precedentemente menzionata. Guardando all’ACL di un oggetto, è facile determinare gli attributi per cui un soggetto è attualmente autorizzato. Questo ha però lo svantaggio di rendere difficile la determinazione di tutti gli accessi che un soggetto ha; sarebbe infatti necessario analizzare l’ACL di tutti gli oggetti nel sistema in base a un particolare soggetto. Allo stesso modo, per rimuovere tutti i permessi per un particolare utente, tutti gli ACL dovrebbero essere analizzati; nella realtà si fa prima a eliminare l’istanza

dell’utente corrispondente, anche se questo non si applica se è necessaria solo la modifica di alcuni permessi per un utente, rendendola comunque un’operazione complessa.

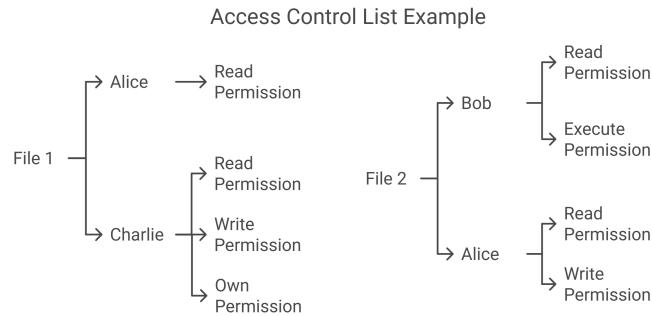


Figura 3.9. Rappresentazione concettuale di controllo degli accessi tramite ACL con i suoi permessi.

Capabilities

L’approccio delle capability list è il duale dell’access control list, dove ad ogni soggetto è associato con una lista, chiamata capability list, che indica per ogni oggetto nel sistema quale attributo un determinato soggetto possiede per quell’oggetto. In questo tipo di approccio è più facile analizzare tutti gli attributi di un utente analizzando la capability list di questo, allo stesso modo determinare tutti i soggetti che possono accedere a un particolare oggetto richiede l’analisi di ogni capability list di ogni soggetto.

È possibile combinare i metodi di ACL e di Capabilities, infatti in sistemi distribuiti questo comporta il vantaggio di non dover ripetere l’autenticazione di un utente in base al tipo di operazioni che deve compiere, permettendo al soggetto di autenticarsi una sola volta e di ottenere le sue capability list e di ottenere i servizi dai vari server nel sistema e se sono necessari ulteriori permessi ogni server può fornire l’ACL. Lo svantaggio di questo approccio varia in base all’ordine logico della tabella dei permessi, infatti se questa è ordinata in base ai soggetti otteniamo i vantaggi della capability list, altrimenti delle ACL.

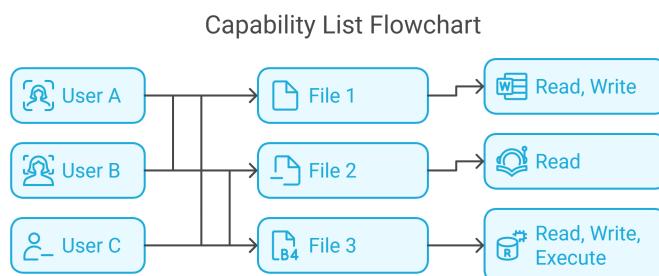


Figura 3.10. Rappresentazione di un esempio di controllo degli accessi tramite capabilities con i suoi permessi.

3.3.2 Policies di Controllo degli Accessi

Analizziamo ora 3 tipi di policy di controllo degli accessi più utilizzate. Alcune policies sono categorizzate in discretionary e non-discretionary, o mandatory.

Classical Discretionary Policies - DAC

Le classical discretionary policies, anche chiamate **DAC**, regolano l'accesso degli utenti alle informazioni sulla base dell'identità dell'utente e delle autorizzazioni che specificano, per ogni utente, o gruppo di utenti, e per ogni oggetto nel sistema, gli attributi di accesso (“read”, “write” e “execute”) consentiti all'utente sull'oggetto. Ogni richiesta di accesso a un oggetto da parte di un utente viene verificata rispetto alle autorizzazioni definite. Se esiste un'autorizzazione che stabilisce che l'utente può accedere all'oggetto nella modalità specificata, l'accesso viene concesso; in caso contrario, viene negato.

Tuttavia, queste politiche di controllo degli accessi presentano lo svantaggio di non garantire un controllo effettivo sul flusso delle informazioni all'interno di un sistema. È semplice aggirare le restrizioni di accesso definite tramite le autorizzazioni. Ad esempio, un utente in grado di leggere dati può condividerli con altri utenti non autorizzati, senza che il proprietario ne sia a conoscenza. Ciò accade perché le politiche discrezionali non impongono alcuna restrizione sull'utilizzo delle informazioni da parte di un utente dopo che quest'ultimo le ha ottenute, ovvero la diffusione delle informazioni non è controllata. Questo problema non lo troviamo nelle politiche di accesso di tipo mandatory, che vedremo dopo.

Inoltre, dato che sono basate su autorizzazioni esplicitamente specificate, sono definite chiuse, le quali garantiscono l'accesso solo se esiste un riscontro positivo con le autorizzazioni, altrimenti viene negato. Concetto simile a quello del whitelisting. Politiche opposte, chiamate aperte, negano l'accesso se esiste un divieto nelle autorizzazioni, come una sorta di blacklisting. Ogni richiesta di accesso da parte di un utente viene verificata rispetto alle autorizzazioni negative definite e viene concessa solo se non esistono autorizzazioni che negano l'accesso.

Questo tipo di politiche sono basate su ACL o Capabilities.

Classical Mandatory Policies - MAC

Le Classical Mandatory Policies, anche chiamate MAC, regolano l'accesso sulla base della classificazione di soggetti e oggetti nel sistema. A ogni utente e oggetto del sistema viene assegnato un livello di sicurezza, chiamato “sensitivity label”. Il livello di sicurezza associato a un oggetto riflette la sensibilità delle informazioni in esso contenute, ossia il potenziale danno derivante dalla loro divulgazione non autorizzata. Il livello di sicurezza associato a un utente, denominato anche “clearance”, riflette l'affidabilità dell'utente nel non divulgare informazioni sensibili a utenti non autorizzati ad accedervi. L'accesso a un oggetto da parte di un soggetto è permesso solo se qualche relazione tra i loro livelli di sicurezza è soddisfatta.

Per garantire il corretto flusso delle informazioni, sono richiesti due principi fondamentali:

- **Read Down:** la clearance del soggetto deve dominare il livello di sicurezza dell'oggetto che si desidera leggere.
- **Write Up:** la clearance del soggetto deve essere dominata dal livello di sicurezza dell'oggetto che si desidera scrivere.

Il rispetto di questi principi impedisce che informazioni contenute in oggetti di livello alto (quindi più sensibili) possano fluire verso oggetti di livello più basso, consentendo di fatto solo un flusso di informazioni verso l'alto (o all'interno della stessa classe di sicurezza). È importante anche comprendere la relazione tra utenti e soggetti in questo contesto. Per esempio se l'utente umano Bell ha una clearance di livello S (Secret), e si autentica sempre come un soggetto S, questo soggetto non potrà leggere gli oggetti TS (Top Secret), a causa della regola read down, però con la regola write up ci sono due aspetti che possono sembrare contro intuitivi all'inizio. Infatti lo stesso soggetto potrà scrivere sugli oggetti TS, anche se non può leggerli. Molti sistemi a causa di questo inconveniente non consentono la regola di write up, limitando i permessi di scrittura allo stesso livello del soggetto. La regola write up è stata pensata per poter permettere agli utenti di livelli inferiori di interfacciarsi con quelli di livelli superiori. Notiamo come questo tipo di regole non permette il contrario, infatti i soggetti con permessi superiori non possono interagire con quelli con permessi inferiori, per farlo devono registrarsi come soggetti con permessi inferiori. Qual è quindi l'utilità di queste restrizioni?

Questa implementazione è la FSM Bell-LaPadula, questo modello è stato sviluppato per essere utilizzato nel dipartimento della difesa americano⁹. Questo modello considera infatti più sicuri gli umani e previene il leak di informazioni da parte di software malevoli dai livelli superiori a quelli inferiori.

Il MAC può essere applicato anche per la protezione dell'integrità delle informazioni. Ad esempio, i livelli di integrità potrebbero essere Cruciale (C), Importante (I) e Sconosciuto (U). Il livello di integrità associato a un oggetto riflette il grado di fiducia che può essere riposto nelle informazioni in esso memorizzate, nonché il potenziale danno derivante da modifiche non autorizzate a tali informazioni. Il livello di integrità associato a un utente riflette l'affidabilità dell'utente nell'inserire, modificare o eliminare dati e programmi a quel livello. Principi analoghi a quelli definiti per la segretezza devono essere rispettati, come segue:

- **Read Up:** Il livello di integrità di un soggetto deve essere dominato dal livello di integrità dell'oggetto che viene letto.
- **Write Down:** Il livello di integrità di un soggetto deve dominare il livello di integrità dell'oggetto che viene scritto.

Notiamo quindi che l'essenza del MAC è il flusso di informazioni unidirezionale in una rete di etichette di sicurezza.

⁹Fonte: Wikipedia (https://en.wikipedia.org/wiki/United_States_Department_of_Defense)

Role-Based Policies - RBAC

Questo tipo di policy, **RBAC**, nasce per un'esigenza di soddisfare le aziende private. Questo tipo di policy per il controllo degli accessi è di tipo MAC e definisce condizioni specifiche per l'accesso a un oggetto. Queste politiche consentono di specificare le autorizzazioni da concedere agli utenti (o ai gruppi) sugli oggetti, come nell'approccio discrezionale, combinando tale possibilità con la definizione di restrizioni, simili a quelle dell'approccio MAC, sull'assegnazione o sull'utilizzo di tali autorizzazioni. Le politiche role-based regolano l'accesso degli utenti alle informazioni in base alle attività che questi svolgono nel sistema. Tali politiche richiedono l'identificazione di ruoli all'interno del sistema. Un ruolo può essere definito come un insieme di azioni e responsabilità associate a una specifica attività lavorativa. Invece di specificare tutti gli accessi che ciascun utente è autorizzato a eseguire, le autorizzazioni di accesso sugli oggetti sono specificate per i ruoli. Agli utenti vengono assegnate le autorizzazioni per assumere determinati ruoli. Vediamo come in questo studio del NIST conferma che i ruoli rappresentano un approccio utile per molte organizzazioni commerciali e governative [27].

L'utente che assume un determinato ruolo è autorizzato a eseguire tutte le operazioni per cui quel ruolo è abilitato. In generale, un utente può ricoprire ruoli diversi in momenti diversi. Inoltre, lo stesso ruolo può essere assegnato a più utenti, anche contemporaneamente. Alcune implementazioni sul controllo degli accessi basato sui ruoli permettono a un utente di svolgere più ruoli in contemporanea, mentre altre limitano l'utente a un solo ruolo alla volta o stabiliscono che alcuni ruoli possano essere combinati, mentre altri devono essere esercitati in modo esclusivo. Non esistono standard consolidati in questo ambito, quindi è probabile che diversi sistemi adottino approcci differenti.

L'approccio basato sui ruoli offre numerosi vantaggi come: i **ruoli gerarchici**, in molti contesti esiste una gerarchia naturale di ruoli, basata sui principi familiari di generalizzazione e specializzazione. Questi semplificano ulteriormente la gestione delle autorizzazioni. Garantiscono inoltre l'accesso con il **minor privilegio** necessario per il compito da svolgere. Gli utenti autorizzati a ruoli potenti non hanno bisogno di esercitarli fino a quando quei privilegi non sono effettivamente necessari. Questo riduce al minimo il rischio di danni causati da errori involontari o da intrusi che si spacciano per utenti legittimi. La **separazione dei compiti**, ossia quel principio per cui nessun utente dovrebbe avere abbastanza privilegi da poter abusare del sistema autonomamente. Ad esempio, la persona che autorizza un assegno non dovrebbe essere la stessa che lo prepara. La separazione dei compiti può essere applicata in modo statico, ossia con ruoli che non possono essere eseguiti dallo stesso utente, o dinamico, applicando il controllo al momento dell'accesso. Un esempio di separazione dinamica dei compiti è la regola dei due responsabili. Il primo utente che esegue un'operazione che richiede due persone può essere qualsiasi utente autorizzato, mentre il secondo utente deve essere un altro utente autorizzato, diverso dal primo. Le politiche basate sui ruoli forniscono una classificazione degli utenti in base alle attività che svolgono. Allo stesso modo, dovrebbe essere fornita una classificazione per gli oggetti. Dando un esempio, generalmente un impiegato avrà bisogno di accedere ai conti bancari, mentre una segretaria avrà accesso a lettere e memo (o a un sottoinsieme di essi). Gli oggetti possono essere classificati

in base al loro tipo (come lettere, manuali, ecc...) o al loro ambito di applicazione (lettere commerciali, lettere pubblicitarie, e così via). Le autorizzazioni di accesso per ruoli dovrebbero quindi essere basate sulle **classi di oggetti**, piuttosto che sugli oggetti specifici. Riprendendo l'esempio, al ruolo di segretaria può essere concessa l'autorizzazione a leggere e scrivere l'intera classe delle lettere, invece di fornire autorizzazioni esplicite per ciascuna singola lettera. Questo approccio ha il vantaggio di rendere l'amministrazione delle autorizzazioni molto più semplice e meglio controllata.

3.3.3 Patch Management

Negli anni si ha avuto un costante sviluppo della tecnologia e con questa anche di malware e vulnerabilità. Nasce quindi la necessità di un rilascio costante di aggiornamenti software, per fare in modo di proteggere i propri strumenti, hardware o software, da vari attacchi, sempre più nuovi. Ogni organizzazione deve stabilire una policy di gestione degli aggiornamenti e fare in modo che essa venga seguita. Questo processo consiste nell'applicazione degli aggiornamenti rilasciati dal fornitore per chiudere le vulnerabilità di sicurezza e ottimizzare le prestazioni di software e dispositivi. La gestione delle patch è talvolta considerata parte della gestione delle vulnerabilità ed è fondamentale nella sicurezza della rete per impedire agli hacker di sfruttare le potenziali vulnerabilità presenti nei software per poi compromettere l'azienda [35]. Secondo dei dati dell'FBI e dell'università Carnegie Mellon, più del 90% degli attacchi sono portati a termine tramite una vulnerabilità software causata da un mancato aggiornamento [72].

Con infrastrutture di rete sempre più complesse nasce il bisogno di un sistema di aggiornamento adeguato, dato che le patch sono fondamentali nel mondo IT in quanto migliorano non solo la sicurezza ma anche le prestazioni e la produttività. Gli aggiornamenti possono infatti essere di vario tipo:

- **Aggiornamenti di Sicurezza.** Si focalizzano sul mettere in sicurezza i software, risolvendo vulnerabilità prima non note. Questo è uno dei punti di ingresso principali nella rete da parte degli hacker e il mancato aggiornamento può lasciare una porta di ingresso aperta per loro.
- **Aggiornamenti delle Funzionalità.** Questo tipo di patch punta a migliorare i software rilasciando nuove funzionalità.
- **Correzioni di Bug.** Queste correzioni risolvono problemi minori nell'hardware o nel software, in genere questi non causano problemi di sicurezza ma influiscono comunque sulle prestazioni.

Uno degli eventi più importanti nella storia della cyber security che ricordiamo ancora oggi e che porta alla luce l'importanza di questo argomento è stato l'attacco WannaCry del 2017, che sfruttando una vulnerabilità nella funzionalità SMB¹⁰ di Windows, che fu corretta da Microsoft il 14 Marzo 2017, e quindi prima della diffusione che datiamo al 14 Aprile 2017, quando fu scoperta e pubblicata dall'NSA [87]. Questo worm si diffuse però proprio per la negligenza in diversi computer non aggiornati,

¹⁰Fonete: Wikipedia (https://it.wikipedia.org/wiki/Server_Message_Block)

creando il panico in sistemi, anche critici, nella nostra società. A partire da quel momento venne presa molto più seriamente l'operazione di patch management.

Le case produttrici hanno iniziato a rilasciare aggiornamenti più velocemente rispetto a prima per cercare di combattere la rapidità con cui gli exploit vengono diffusi al giorno d'oggi. Basta guardare a questo esempio, dove Microsoft [44] ha rilasciato un aggiornamento per “fixare” 63 vulnerabilità nei suoi vari applicativi, oppure ad esempi come [63] e [43], dove due case costruttrici hanno trovato vulnerabilità critiche¹¹ nei loro prodotti.

Ci viene da chiederci quindi, se quindi siamo consapevoli di questi rischi, perché tali problemi ci sono ancora oggi e continuano ad essere sfruttati?

La risposta è più complessa di quello che si può pensare, infatti i reparti IT operano spesso in condizioni di carenza di personale e sovraccarico, divisi tra manutenzione ordinaria, supporto tecnico e emergenze. Gestire l'applicazione di patch su migliaia di dispositivi, anche diversi, considerando il flusso incessante di aggiornamenti settimanali, supera le capacità umane quando affidata esclusivamente a processi manuali; inoltre, in alcuni sistemi, con il passare del tempo, sono state applicate talmente “toppe” che la sola idea di introdurre una qualunque modifica suscita timore e incertezza tra il personale di supporto. L'inserimento di una nuova patch, infatti, rischia di causare più problemi di quanti ne risolva. Non esiste poi una soluzione unitaria per tutti i tipi di business ed è anche per questo motivo che il patch management è diventato un problema sempre più gravoso per le aziende [72]. Un altro fattore da considerare è che i fornitori spesso smettono di supportare le versioni più vecchie dei propri prodotti: ciò implica che non verranno più rilasciate patch per le nuove vulnerabilità, rendendo queste versioni meno sicure con il passare del tempo [80].

Un programma efficace di gestione delle patch si articola in più fasi. Il numero di fasi può variare da un'azienda all'altra in base alla sua infrastruttura IT e ad altri fattori chiave, come la dimensione, la diversità nelle piattaforme, nei sistemi e nelle applicazioni, il livello di automazione e aggiornamento, la centralizzazione o decentralizzazione dell'IT e la disponibilità di risorse.

Riprendiamo ora dal paper del NIST [80], sulla guida al patch management per le aziende, l'importanza di questa pratica e capiamo che la gestione delle patch è il processo di identificazione, acquisizione, installazione e verifica delle patch per prodotti e sistemi. Le patch correggono problemi di sicurezza e funzionalità nel software e nel firmware. Dal punto di vista della sicurezza, le patch sono di particolare interesse poiché contribuiscono a mitigare le vulnerabilità causate da difetti nel software; l'applicazione delle patch per eliminare queste vulnerabilità riduce significativamente le opportunità di ingresso. Inoltre, le patch sono generalmente il metodo più efficace per mitigare le vulnerabilità dei difetti nel software e spesso rappresentano l'unica soluzione pienamente efficace [80].

¹¹Fonente: NIST - NVD (<https://nvd.nist.gov/vuln-metrics/cvss>)

Le difficoltà nel patch management - Tempistica, Priorità e Testing

La gestione delle patch aziendali ruota attorno a tre aspetti fondamentali: tempistiche, priorità e test. Installare immediatamente ogni nuova patch riduce la finestra di esposizione a eventuali vulnerabilità, ma le risorse limitate e i rischi operativi legati a patch non testate impongono di stabilire un ordine di priorità. Molti fornitori semplificano il processo rilasciando patch in “bundle” (ad esempio mensili o trimestrali), permettendo di effettuare i test e di distribuire gli aggiornamenti in un'unica soluzione. Ciò può però prolungare il tempo tra la scoperta di una vulnerabilità e il rilascio della patch, lasciando una finestra più ampia per eventuali attacchi, a meno che non si decida di pubblicare subito un aggiornamento urgente in caso di exploit attivo.

Inoltre, il rilascio di una patch può fornire indicazioni utili agli aggressori, tramite reverse engineering, spingendo alcune organizzazioni a installarla immediatamente, anche senza test approfonditi, purché siano disponibili procedure di rollback (come gli snapshot di macchine virtuali). Va infine considerato che, per rendere effettive le patch, spesso è necessario riavviare servizi o interi sistemi, con un impatto diretto sulla continuità operativa. In definitiva, non conta solo quando la patch viene installata, ma quando diventa effettivamente operativa.

Troviamo fondamentale per la gestione delle patch a livello aziendale un inventario aggiornato e completo di software, applicazioni e sistemi operativi, installato su ogni host, incluse le versioni in uso. Senza queste informazioni, è impossibile identificare, reperire e installare correttamente le patch necessarie, oltre a rilevare eventuali versioni obsolete che richiedono aggiornamenti.

L'installazione di una patch può generare effetti collaterali indesiderati. Ad esempio, può modificare inavvertitamente alcune impostazioni di sicurezza già presenti o introdurne di nuove, creando di fatto nuovi problemi di sicurezza proprio mentre si cerca di risolvere la vulnerabilità originaria.

Una patch installata potrebbe non essere attiva finché il software non viene riavviato o modificato. Verificarne l'efficacia è complesso, soprattutto senza indicazioni chiare su eventuali riavvii richiesti. Testare la vulnerabilità è un'opzione rischiosa e fattibile solo se esiste già un exploit.

Tecnologie per il Patch Management Aziendale

Le tecnologie di patch management enterprise condividono un'architettura simile ad altre soluzioni di sicurezza: server centralizzati per gestione/reporting e console operative. Ciò che le differenzia è la metodologia di rilevamento delle patch mancanti, articolata in tre approcci:

- **Agent-Based.** Le tecnologie di patch management agent-based richiedono un agente installato su ciascun dispositivo, con server centrali che coordinano il processo. L'agente individua il software vulnerabile, scarica e applica le patch tramite privilegi amministrativi. Questo approccio è ideale per dispositivi remoti, come laptop o smartphone, grazie alla gestione decentralizzata.

Le limitazioni di questo approccio possono essere, l'incompatibilità, come ad esempio per i sistemi embedded e il supporto limitato per dispositivi simili.

- **Agentless Scanning.** Operano tramite server centrali che scansionano la rete per identificare patch mancanti, richiedendo privilegi amministrativi sui dispositivi per installare aggiornamenti e gestire riavvii. Il vantaggio principale è l'assenza di agenti installati localmente, semplificandone la gestione. Presentano alcune criticità come; i dispositivi remoti esclusi, tipo laptop in smart working, poiché non raggiungibili via rete locale, l'interferenza di rete: Firewall o NAT possono bloccare le scansioni, compromettendo l'accuratezza e il supporto limitato per piattaforme specializzate, analogamente alle soluzioni agent-based.
- **Monitoraggio passivo della rete.** Analizzano il traffico locale per individuare applicazioni non aggiornate. A differenza delle soluzioni agent-based e agentless, questo approccio non richiede privilegi sui dispositivi, rendendolo ideale per monitorare sistemi non gestiti dall'organizzazione, come dispositivi di operatori esterni o visitatori. Questa tecnica offre un valore unico nel rilevare vulnerabilità "nascoste" e sistemi non gestiti, ma la sua efficacia è vincolata a contesti specifici. Per una copertura completa, è essenziale integrarlo con approcci agent-based e agentless, sfruttando i punti di forza di ciascuna metodologia in uno schema di difesa stratificato.

Confronto delle Tecniche			
Caratteristica	Agent-Based	Agentless Scanning	Passive Network Monitoring
Privilegi amministrativi richiesti sugli host?	Sì	Sì	No
Supporta host non gestiti?	No	No	Sì
Supporta host remoti?	Sì	No	No
Supporta appliance?	No	No	Sì
Larghezza di banda necessaria per la scansione?	Minima	Da moderata a eccessiva	Nessuna
Possibile gamma di applicazioni rilevate?	Completa	Completa	Solo quelle che generano traffico non cifrato

Tabella 3.1. Confronto delle architetture [80].

Capacità di Sicurezza e Gestione Operativa nelle Tecnologie di Patch Management

Le tecnologie di patch management rappresentano un pilastro critico nella difesa delle infrastrutture informatiche moderne, integrando tre dimensioni fondamentali: gestione dell'inventario, gestione delle patch e mitigazione dei rischi operativi. Centrali in questo contesto sono i protocolli come lo SCAP (Security Content Automation Protocol) [69], che standardizzano l'organizzazione e l'analisi delle informazioni di sicurezza, garantendo coerenza e interoperabilità tra sistemi eterogenei.

La gestione dell'inventario costituisce la base operativa, permettendo il rilevamento preciso del software installato, delle relative versioni e delle vulnerabilità associate. Le tecnologie di patch management sono progettate per identificare il software installato su ciascun host, comprese le versioni specifiche, con un focus prioritario sul rilevamento di quelle vulnerabili. Oltre alla mappatura, molte soluzioni integrano funzionalità avanzate per gestire il ciclo di vita del software: installare aggiornamenti, aggiungere/rimuovere componenti specifici, come plugin o librerie, o disinstallare intere applicazioni. Queste capacità le rendono strumenti polivalenti, non solo per la sicurezza ma anche per l'ottimizzazione delle risorse IT. Ovviamente, gli strumenti di patch management hanno diverse funzionalità, come: l'identificazione delle patch necessarie, il bundling e la prioritizzazione, la flessibilità operativa o l'installazione automatizzata e verifica.

Dopo aver creato un sistema di patch management, i suoi amministratori devono testare, distribuire la soluzione e mantenere le sue operazioni e sicurezza.

L'adozione di strumenti aziendali per il patch management, seppur potenzialmente portatrice di nuovi rischi, rappresenta una scelta strategica per mitigare minacce ben più gravi derivanti dall'inazione. Le organizzazioni che trascurano gli aggiornamenti sistematici espongono infatti i propri sistemi a vulnerabilità critiche, con conseguenze spesso catastrofiche. Gli strumenti di patching offrono un bilancio netto positivo: i benefici in termini di sicurezza superano ampiamente i rischi residui. I potenziali rischi possono essere: una patch alterata, credenziali utilizzate impropriamente, vulnerabilità nei componenti della soluzione, un'entità potrebbe monitorare le comunicazioni dello strumento per identificare vulnerabilità. Le organizzazioni devono ridurre questi rischi con tecniche che dovrebbero essere seguite quando si rilascia una qualsiasi applicazione critica per l'azienda.

Le organizzazioni dovrebbero distribuire gli strumenti di patch management adottando un approccio a fasi, che consenta di affrontare problematiche procedurali e di comunicazione con un gruppo limitato di utenti prima di un rollout universale. Inizialmente, è comune focalizzarsi su sistemi standardizzati, come desktop omogenei e server farm a singola piattaforma con configurazioni simili. Una volta consolidata questa fase, è possibile affrontare contesti più complessi, come ambienti multi-piattaforma, desktop non standard, computer legacy o con configurazioni insolite. Per sistemi operativi, applicazioni non supportate da strumenti automatizzati o dispositivi con configurazioni particolari, tipo sistemi embedded, controlli industriali, dispositivi medici o sperimentali, potrebbe essere necessario ricorrere a metodi manuali. In tali casi, è essenziale definire procedure scritte e formalizzate per garantire un processo di patching manuale strutturato e tracciabile.

Le società devono bilanciare sicurezza, usabilità e disponibilità operativa.

Ad esempio, le patch potrebbero compromettere altre applicazioni, problema mitigabile testandole prima del deployment. Forzare riavvi di applicazioni, OS o modifiche allo stato degli host può interrompere servizi o causare perdite di dati. È quindi cruciale equilibrare l'applicazione tempestiva delle patch con la necessità di mantenere la continuità operativa.

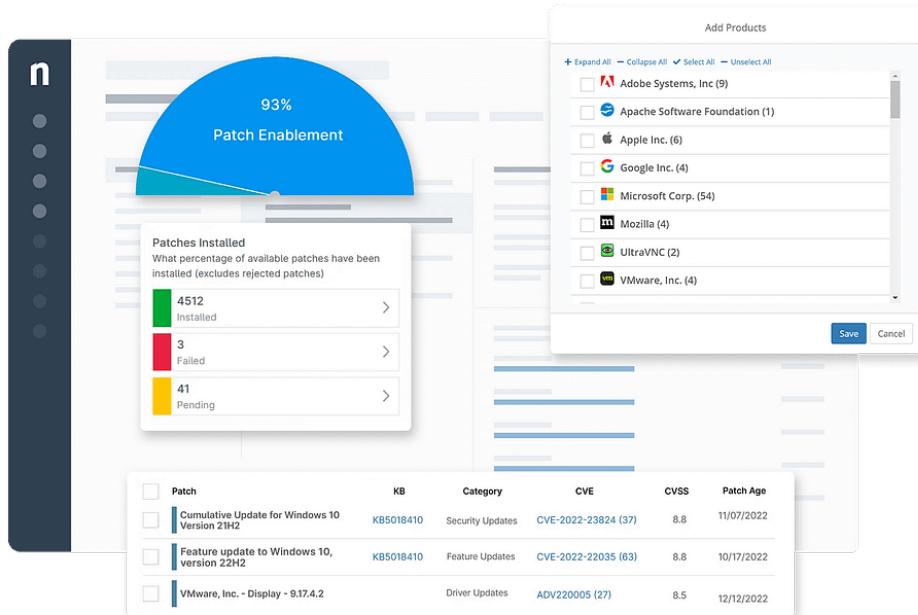


Figura 3.11. La dashboard di un programma di patch management¹².

Framework per il Patch Management - ACVRM

Analizziamo come in questo studio [61] viene proposto un framework innovativo progettato per automatizzare la gestione delle vulnerabilità in contesti IT complessi, chiamato **Automated Context-aware Vulnerability Risk Management, ACVRM**. Con l'aumento esponenziale delle vulnerabilità segnalate, 25.064 nel 2022, di cui il 57,69% classificate come critiche o ad alto rischio [11], e normative sempre più stringenti, come negli USA dove si danno 15 giorni¹³ per patch critiche, le organizzazioni affrontano sfide significative nel mantenere sistemi sicuri e conformi. ACVRM risponde a queste esigenze integrando un approccio contestuale e cicli di feedback per ottimizzare l'intero processo di remediation.

Il framework si articola in tre fasi principali. La **Fase 1** raccoglie e normalizza i dati sulle vulnerabilità da fonti pubbliche come il NIST National Vulnerability Database, NVD, adattando i punteggi di gravità al profilo specifico dell'organizzazione. La **Fase 2** identifica le vulnerabilità negli asset aziendali e calcola un Patch Score, PS, basato su criteri ponderati come impatto operativo e rischio residuo.

¹²Fonte: Ninja One (<https://www.ninjaone.com/it/gestione-patch/>)

¹³Fonte: CISA (<https://www.cisa.gov/binding-operational-directive-19-02>)

Il cuore dello studio risiede nella **Fase 3**, dedicata al Patch Management: qui, le patch vengono testate in ambienti controllati mirror della produzione, verificate in tre step, ossia: deploy, controllo versione, test funzionali e ottimizzate attraverso un feedback loop che incorpora errori storici per migliorare le priorità future. Un elemento chiave è l'Automated Review, AR, che elimina patch ridondanti e riordina le dipendenze, riducendo conflitti e inefficienze.

Nel paper è stato condotto un esperimento, su un ambiente simulato con 8 server Ubuntu e 21 vulnerabilità iniettate, è stato dimostrato l'efficacia di ACVRM. Senza automazione (Caso 1), solo il 33% delle patch aveva successo, con il 48% di interventi umani. Introducendo l'AR (Caso 2), il successo è salito al 60%, riducendo gli interventi al 10%. Considerando le dipendenze tra patch (Caso 3), l'efficacia ha raggiunto l'80%, azzerando completamente la necessità di esperti. Questi risultati evidenziano come l'automazione contestuale e l'apprendimento dagli errori possano trasformare la gestione delle vulnerabilità da processo reattivo a strategia proattiva.

Le conclusioni sottolineano i vantaggi di ACVRM: riduzione dei tempi di remediation, adattamento dinamico al contesto organizzativo e minimizzazione del carico operativo per gli esperti IT.

3.3.4 Backup e Disaster Recovery - BDR

In un contesto dove attacchi informatici, errori umani e disastri fisici, come guasti hardware, eventi naturali, possono compromettere l'integrità dei dati, il Backup e Disaster Recovery (**BDR**) emergono come elementi fondamentali per la continuità operativa. Queste strategie non solo preservano le informazioni critiche, ma permettono un ripristino rapido delle funzionalità, minimizzando downtime e perdite economiche. Ci sono alcuni eventi, in particolare più recenti come il precedentemente citato WannaCry [87], che hanno spinto le aziende a investire di più in questi reparti, acquistando sempre più importanza.

Queste pratiche consistono nel creare o aggiornare periodicamente più copie di file, destinati poi all'archiviazione in una o più località remote, pronte per essere utilizzate per riprendere le operazioni aziendali nel caso di una perdita di dati, dovuta a fattori come: file danneggiati, corruzione dei dati, attacchi hacker o disastri naturali [36]. Notiamo come il **Backup** e il **Disaster Recovery** siano due processi ben distinti, il primo consiste nel processo di fare copie di file, mentre il secondo è un insieme di piani e processi che consentono di ristabilire rapidamente l'accesso ad applicazioni, dati e risorse IT dopo un'interruzione.

Nel definire queste strategie, è essenziale considerare parametri come il Recovery Time Objective (RTO), ovvero il tempo necessario per riprendere le normali operazioni aziendali dopo un'interruzione, e il Recovery Point Objective (RPO), che indica la quantità di dati che si può permettere di perdere in caso di disastro. Inoltre, processi come il failover, che trasferisce automaticamente i compiti ai sistemi di backup in modo trasparente per gli utenti, e il fallback, che riporta le operazioni ai sistemi originali una volta risolto il problema, giocano un ruolo cruciale nel garantire continuità. Il restore, invece, è il processo di trasferimento dei dati di backup al sistema primario, essenziale per ripristinare le funzionalità.

Molte organizzazioni, infatti, stabiliscono diversi RTO e RPO a seconda dell'importanza dei carichi di lavoro. Ad esempio, per una grande banca, il sistema di online

banking rappresenta un carico di lavoro critico, con la necessità di minimizzare il tempo di inattività e la perdita di dati. Al contrario, un'applicazione meno critica, come quella per il tracciamento delle ore dei dipendenti, potrebbe tollerare tempi di inattività più lunghi senza un impatto significativo sul business. Analizzando sempre [36] capiamo che classificare i carichi di lavoro in livelli, come Tier 1, Tier 2 o Tier 3, aiuta a definire un piano di ripristino di emergenza più strutturato.

Una volta stabiliti gli obiettivi di recupero, il passo successivo è valutare le opzioni di implementazione. Le aziende devono decidere se mantenere alcune funzioni di backup o ripristino on-premises oppure optare per soluzioni basate su cloud pubblico o ibrido. Negli ultimi anni, le soluzioni di backup e ripristino basate su cloud sono diventate sempre più popolari, grazie alla loro capacità di fornire infrastrutture scalabili e strumenti avanzati per gestire i processi di backup e ripristino. Scegliendo una soluzione basata su cloud, le organizzazioni possono evitare grandi investimenti iniziali per l'infrastruttura e ridurre i costi di gestione dell'ambiente. Inoltre, il cloud offre vantaggi come la scalabilità rapida e la distanza geografica necessaria per proteggere i dati in caso di disastro regionale. Alcune aziende scelgono un approccio ibrido, archiviando i dati di backup nel cloud mentre mantengono l'ambiente di produzione on-premises.

Questo modello consente di ottenere i benefici della scalabilità e della separazione geografica senza dover spostare completamente l'ambiente di produzione. In alternativa, un modello cloud-to-cloud può essere utilizzato quando sia la produzione che il ripristino di emergenza sono ospitati nel cloud, ma in siti diversi per garantire una sufficiente separazione fisica [36].

Tuttavia, in alcuni casi, mantenere alcuni processi di backup o ripristino on-premises può essere vantaggioso, specialmente per recuperare dati rapidamente o per rispettare normative severe sulla privacy o sulla sovranità dei dati. Un piano di ripristino interamente basato su un ambiente on-premises, tuttavia, presenta limiti significativi. Se un disastro naturale o un blackout colpisce, l'intero data center – con sistemi primari e secondari – potrebbe essere compromesso. Per questo motivo, la maggior parte delle strategie di ripristino prevede l'utilizzo di un sito secondario situato a una certa distanza dal data center principale. La scelta della posizione di questo sito dipende da fattori come prestazioni, conformità normativa e accessibilità fisica.

A seconda delle opzioni di implementazione scelte, diverse tecnologie possono essere utilizzate per il backup e il ripristino di emergenza. I nastri magnetici tradizionali, nonostante la loro longevità, continuano a svolgere un ruolo nel backup grazie alla loro affidabilità e costo contenuto. Tuttavia, questa tecnologia non è adatta al ripristino di emergenza, poiché richiede tempi di accesso più lunghi rispetto allo storage basato su disco. Inoltre, il recupero fisico di un nastro da un deposito esterno potrebbe comportare la perdita di ore o addirittura giorni di disponibilità. Un'alternativa più moderna è la replica basata su snapshot, che cattura lo stato corrente di un'applicazione o disco in un determinato momento. Questo metodo scrive solo i dati modificati dall'ultimo snapshot, preservando lo spazio di archiviazione [36].

Tuttavia, i dati saranno completi solo fino all'ultimo snapshot: se gli snapshot vengono eseguiti ogni ora, si deve essere disposti a perdere un'ora di dati. Infine, molte organizzazioni stanno adottando la replica continua, che replica costantemente

l'ultima versione di un disco o applicazione in un'altra posizione o nel cloud, riducendo al minimo i tempi di inattività e fornendo punti di recupero più granulari.

In entrambi gli ambiti la pianificazione è fondamentale, infatti un'organizzazione non può permettersi di trascurare il backup o il ripristino di emergenza. Se ci vogliono ore per recuperare dati persi dopo una cancellazione accidentale, i dipendenti rimarranno inattivi, incapaci di completare processi aziendali critici che dipendono dalla tecnologia. Inoltre, se occorrono giorni per riportare online l'attività dopo un disastro, si rischia di perdere clienti in modo permanente. Considerando il tempo e i soldi che si potrebbero perdere, gli investimenti in metodologie di backup e piani di ripristino di emergenza sono completamente giustificati.



Figura 3.12. Report di Sophos sui ransomware nel 2024 [79].

Esistono inoltre diverse tipologie di backup, e la scelta del sistema da usare dipende dalle esigenze specifiche dell'organizzazione e dai vincoli di budget, con opzioni che includono backup completi, incrementalni, differenziali e la protezione continua dei dati, CDP, ognuna con vantaggi e limitazioni specifiche.

I backup completi catturano tutti i dati regolarmente, offrendo una protezione esauritiva e semplificando il processo di ripristino, poiché richiedono solo l'ultimo backup per recuperare i dati. Tuttavia, questo approccio richiede spazio di archiviazione significativo e tempi di esecuzione prolungati, rendendolo meno pratico per ambienti con grandi volumi di dati o risorse limitate.

I backup incrementali, invece, si concentrano solo sulle modifiche apportate ai dati dall'ultimo backup, offrendo efficienza in termini di spazio e tempo. Questo metodo riduce il carico sulle risorse di archiviazione e accelera il processo di backup, ma necessita di un backup completo per il ripristino totale, aumentando la complessità e il tempo richiesto in caso di recupero.

I backup differenziali rappresentano un compromesso tra efficienza e velocità di recupero, poiché salvano tutte le modifiche apportate dal precedente backup completo. Rispetto ai backup incrementali, semplificano il processo di ripristino, ma richiedono più spazio di archiviazione man mano che il tempo tra due backup completi aumenta.

Il CDP consente la replica in tempo reale, riducendo al minimo la perdita di dati anche durante frequenti interruzioni. Questo approccio è particolarmente utile per organizzazioni che non possono tollerare alcuna perdita di dati, ma richiede infrastrutture robuste e può comportare costi elevati, sia in termini di hardware che di larghezza di banda. I sistemi di backup efficaci si basano su componenti chiave come software di backup automatizzato, soluzioni di archiviazione locale, cloud o nastri, e infrastrutture di rete progettate per garantire trasferimenti sicuri ed efficienti. Le strategie di implementazione variano tra backup locale, remoto e cloud, con la regola 3-2-1 che offre un approccio bilanciato per la protezione dei dati. Per massimizzare l'efficacia, è fondamentale adottare best practice come test regolari, politiche chiare per la gestione dei dati, misure di sicurezza robuste e automazione dei processi. Tuttavia, l'implementazione del backup di rete presenta sfide significative, tra cui la complessità della gestione in reti distribuite, i costi elevati, la necessità di scalabilità e la crescente minaccia di attacchi informatici. Un'implementazione di successo richiede una pianificazione accurata, valutando dati critici, tempi di inattività accettabili e vincoli di budget, seguita da una configurazione attenta, test approfonditi e formazione degli utenti, con un monitoraggio continuo per garantire il corretto funzionamento e l'adattamento alle esigenze future.

3.3.5 Formazione e Coordinazione dei Reparti IT

L'introduzione di nuovi strumenti IT in azienda richiede una formazione adeguata per garantire che i dipendenti siano in grado di utilizzarli efficacemente, minimizzando interruzioni e massimizzando la produttività. Una formazione insufficiente può portare a errori operativi, violazioni della sicurezza e un uso limitato delle funzionalità, come dimostra il caso Target del 2013, in cui la mancanza di preparazione ha causato una grave violazione dei dati [82].

Prima di avviare la formazione, è fondamentale valutare il livello di competenza attuale dei dipendenti, identificare gli obiettivi formativi e selezionare gli strumenti IT più adatti alle esigenze aziendali. La pianificazione deve includere tempistiche realistiche, risorse necessarie e tappe di monitoraggio per garantire un approccio strutturato.

I metodi di formazione devono essere diversificati per adattarsi ai diversi stili di apprendimento. I workshop favoriscono l'apprendimento collaborativo, l'e-learning offre flessibilità per i dipendenti remoti, mentre le sessioni pratiche permettono di acquisire esperienza diretta. La scelta tra formatori interni ed esterni dipende dalla complessità dello strumento e dalle esigenze organizzative, con una combinazione spesso ideale per coprire sia aspetti tecnici che organizzativi. Materiali come manuali, video tutorial e guide rapide sono essenziali per supportare l'apprendimento.

Per mantenere l'impegno dei dipendenti, è importante evidenziare i benefici degli strumenti per il loro ruolo, integrando elementi interattivi come quiz o esercitazioni pratiche. Incentivi e un ambiente favorevole alle domande possono ulteriormente motivare il personale.

L'implementazione del programma di formazione deve seguire un approccio graduale, iniziando con piccoli gruppi per raccogliere feedback e affinare il processo. Le sessioni vanno programmate in orari non critici, garantendo l'accesso a tutte le risorse necessarie, come software aggiornati e ambienti di prova realistici. Durante la formazione, è cruciale monitorare i progressi e raccogliere feedback per apportare miglioramenti in tempo reale.

Dopo la formazione, un supporto continuo è essenziale per risolvere dubbi e prevenire problemi. Promuovere una cultura di apprendimento continuo e offrire corsi di aggiornamento periodici aiuta i dipendenti a rimanere al passo con le evoluzioni degli strumenti. Monitoraggi regolari e valutazioni delle prestazioni consentono di misurare l'efficacia del programma e identificare aree di miglioramento.

Casi di studio evidenziano l'importanza di una formazione ben strutturata: un'azienda di vendita al dettaglio ha aumentato l'efficienza operativa del 25% grazie a un approccio misto di workshop, e-learning e sessioni pratiche, mentre una società finanziaria ha fallito nell'adozione di un nuovo software a causa di una formazione inadeguata.

Le principali sfide nella formazione IT includono la resistenza al cambiamento, risorse limitate e la diversità nei ritmi di apprendimento. Soluzioni come l'e-learning, il coinvolgimento precoce dei dipendenti e l'offerta di metodi formativi vari possono mitigare questi ostacoli. Infine, la valutazione del successo della formazione si basa su metriche come aumento della produttività, riduzione degli errori e feedback qualitativo, che guidano eventuali aggiustamenti futuri.

3.4 Penetration Testing - VAPT

Individuare le vulnerabilità nei sistemi accessibili sia internamente che esternamente è fondamentale per valutare il livello di rischio di un'organizzazione. Effettuare regolarmente controlli delle vulnerabilità, tramite scansioni automatizzate e revisioni manuali, permette di stabilire le priorità per le attività di mitigazione e di aggiornare le politiche di sicurezza. Adottare questo approccio preventivo è essenziale per difendersi da possibili attacchi e garantire il rispetto delle normative in materia di sicurezza informatica. Dato poi l'esponenziale evoluzione della tecnologia, anche gli attacchi sono diventati sempre più complessi. Uno dei metodi migliori per capire le vulnerabilità della propria rete è quello del **Vulnerability Assessment and Penetration Testing, VAPT**.

Questa tecnica aiuta le organizzazioni a capire se la propria infrastruttura informatica funziona a dovere. Notiamo che questa strategia è composta da due fasi, la prima **VA**, per scovare le vulnerabilità e la seconda, **PT**, dove si provano a sfruttare queste vulnerabilità per ottenere accessi non autorizzati ed effettuare possibili attività dannose. Questo programma ci restituisce molte informazioni utili su quali possono essere i pericoli della nostra azienda e sull'entità dei danni che possono essere inflitti da un potenziale attacco.

3.4.1 Le Vulnerabilità

In genere gli attaccanti provano a sfruttare fallo già note sperando (e riuscendo molto spesso a trovarle) in aggiornamenti mancati, dovuti a scarse politiche di aggiornamento o alla novità della falla trovata. Per mettere in sicurezza la rete, trovare queste vulnerabilità è fondamentale. Molte organizzazioni e framework citati precedentemente richiedono una regolarità nei VA, per accertarsi di avere una rete sicura; questo è particolarmente vero per le PCI DSS¹⁴ [84], [77]. Analizzando i tipi di vulnerabilità, capiamo che uno dei grandi problemi che viene riscontrato è come queste siano categorizzate; infatti, per non confondersi, sono state create delle organizzazioni per gestire al meglio questo compito come la CVE e la CWE, entrambe collegate alla MITRE di cui abbiamo parlato in precedenza. La Common Vulnerabilities and Exposure List, **CVE** è uno schema standardizzato dove vengono nominate in base a una convenzione le vulnerabilità, rendendone più facile la documentazione [21]. La Common Weakness Enumeration, **CWE**, è invece un sistema che provvede a categorizzare queste vulnerabilità [22]. Il processo di Vulnerability assessment si divide in 4 fasi che sono:

- **Target Discovery.** Vengono raccolte le informazioni essenziali sul sistema da analizzare, come dettagli su reti, tecnologie utilizzate, applicazioni e infrastrutture. Questi dati permettono di comprendere l'architettura di sicurezza del target e definire le strategie di test. Tra le attività svolte ci sono, ad esempio, lo scanning Whois per ottenere informazioni sul dominio e l'analisi degli header HTTP per valutare le risposte del server web. Qui è dove vengono concentrate la maggior parte delle risorse.
- **Scanning.** Viene analizzato l'intero sistema per individuare vulnerabilità come servizi non necessari, porte aperte, connessioni remote o password deboli. Utilizzano strumenti e tecniche specifiche, come lo Half TCP Scan: inviano un pacchetto TCP_SYN alla porta target e, in base alla risposta (ACK per porta aperta, RST per chiusa, timeout per non risposta), determinano lo stato delle porte. Questo metodo è efficiente perché evita il completamento del processo di handshake TCP, riducendo i tempi e abbassando le probabilità di far scattare un IDS o IPS. Questa tecnica è presente anche nello strumento nmap¹⁵ di cui parleremo dopo. Successivamente, con strumenti automatizzati, eseguono scansioni di rete e applicazioni web per identificare errori di configurazione o criticità, generando report dettagliati sui rischi rilevati.

¹⁴Fonte: Wikipedia (https://it.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard)

¹⁵Sito: Nmap (<https://nmap.org/>)

- **Result Analysis.** Valutiamo le vulnerabilità e le minacce individuate durante lo scanning. L'obiettivo è selezionare e classificare i problemi in base alla loro gravità e all'impatto potenziale sul sistema. Poiché i dati iniziali spesso includono molti falsi positivi, questa fase serve a filtrarli, ottenendo una lista più precisa e affidabile. Le vulnerabilità vengono quindi ordinate per priorità, creando un elenco finale che viene comunicato al team per la risoluzione o per ulteriori approfondimenti.
- **Reporting.** Documentiamo tutte le operazioni e i risultati ottenuti durante la valutazione delle vulnerabilità, producendo un report dettagliato che elenca le vulnerabilità identificate, il loro livello di gravità e altre informazioni rilevanti. Questo documento serve all'organizzazione per pianificare interventi correttivi.



Figura 3.13. Le fasi nel Vulnerability Assessment.

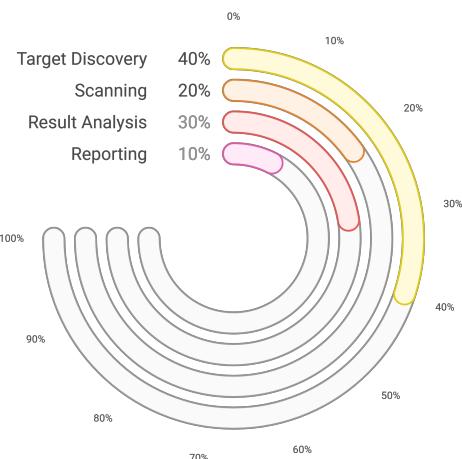


Figura 3.14. Percentuale del lavoro richiesto per le singole fasi [77].

Tecniche di Vulnerability Assessment

Questa strategia si può effettuare in due modi, manualmente o automaticamente. Nel **testing manuale**, il tester usa le sue competenze e sottopone l'obiettivo a vari test e osserva manualmente i risultati e i cambiamenti, i quali, se non sono in linea con quello che si aspetta, fanno dichiarare il software come vulnerabile. A sua volta, il metodo manuale viene diviso in:

- **Test Manuale Esplorativo.** Qua il tester naviga per il sistema trovando vulnerabilità senza un piano d'azione. L'affidabilità di questa tecnica è puramente basata su chi conduce il test [6].
- **Test Manuale Sistematico.** Questa tecnica abbiamo un piano d'azione definito, chiamato Test Plan. Qua il tester studia il sistema, i suoi componenti e le sue caratteristiche, sulle quali sviluppa un test plan efficiente e ad hoc per il sistema.

Invece nel **testing automatico**, il tester utilizza strumenti automatici per eseguire test ripetitivi, riducendo il tempo e l'intervento umano. Questi strumenti confrontano i risultati attesi con quelli reali del sistema, segnalando anomalie che potrebbero indicare vulnerabilità o errori di configurazione [6]. Nel testing automatico vengono usate due tecniche:

- **Analisi statica.** Valuta il sistema e i suoi componenti basandosi sulla sua forma, struttura, contenuto o documentazione, che in ogni caso non richiede l'esecuzione del programma. A differenza della code review, che è manuale, questa tecnica si avvale di tool automatizzati, risultando più efficiente, soprattutto per il codice sorgente. Questa tecnica è ulteriormente caratterizzata in **Static Analysis for Source Code** e **Static Analysis for Machine Code** [51].
- **Fuzzing.** Questa tecnica invia input casuali, invalidi o inaspettati al sistema per rilevare crash o comportamenti anomali. È efficace contro vulnerabilità come buffer overflow o SQL injection, ma meno utile contro minacce come keylogger. Si divide in due approcci:
 - **Mutation Based Fuzzing.** Modifica gli input in modo casuale senza conoscere il formato, come ad esempio il bit-flipping.
 - **Generation Based Fuzzing.** Richiede una comprensione dettagliata del formato dei dati per generare input mirati.

Ogni tecnica ha vantaggi e limiti. Ad esempio, il fuzzing mutation-based è veloce ma poco preciso, mentre quello generation-based è più accurato ma complesso. La scelta della tecnica dipende dal tipo di target e dagli obiettivi del test: un tester esperto deve valutare pro e contro per ottimizzare i risultati ed evitare rischi inutili.

3.4.2 Penetration Testing

Il penetration testing è un processo che simula l'acquisizione illegittima di autorità legittima per valutare la sicurezza di un sistema. È uno strumento cruciale per le aziende, poiché permette di identificare rischi prima che si trasformino in violazioni concrete, proteggendo l'organizzazione da perdite finanziarie e danni alla reputazione [78]. Il processo si divide in quattro fasi principali e sono:

- **Planning and Preparation Phase.** Qui il tester e l'organizzazione concordano tempi, ambito e modalità del test. Viene raccolta informazioni sul target attraverso ricognizione passiva, senza interagire direttamente con la rete, e ricognizione attiva, con test diretti per ottenere risposte dal sistema.
- **Detection and Penetration Phase.** Il tester sfrutta strumenti e tecniche per compromettere il sistema, sfruttando vulnerabilità logiche o fisiche. Esempi includono l'acquisizione dell'accesso iniziale (perimeter penetration) e l'escalation dei privilegi.
- **Post Exploitation and Data Exfiltration.** Qui documentiamo i percorsi per accedere ai dati sensibili, valutando punti di accesso, impostazioni di configurazione e impatto sui canali di comunicazione.

- **Reporting and Clean Up.** Viene in fine redatto un report dettagliato sulle vulnerabilità identificate, le modalità di sfruttamento e le raccomandazioni per mitigarle. Si eliminano inoltre tutti gli elementi creati durante il test.

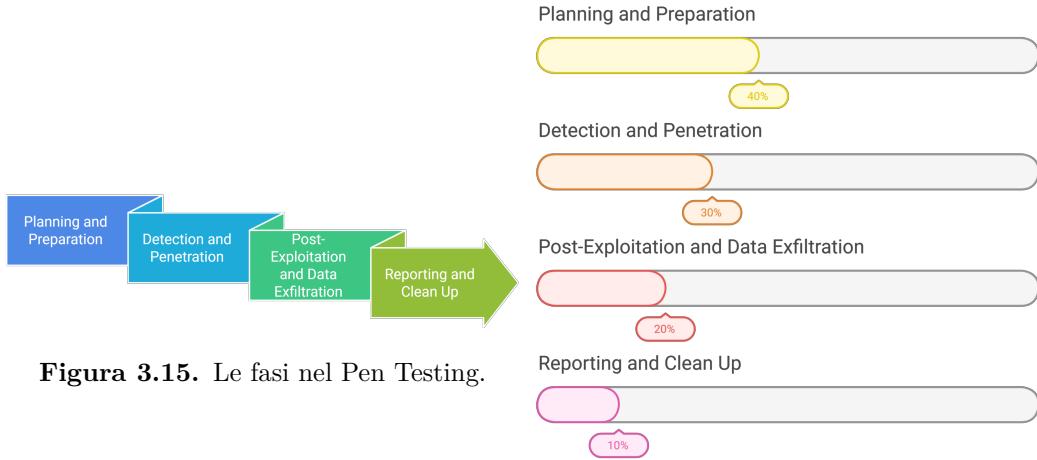


Figura 3.15. Le fasi nel Pen Testing.

Figura 3.16. Percentuale del lavoro richiesto per le singole fasi [77].

Strategie di Penetration Testing

Prima di analizzare queste strategie, notiamo come il MITRE ATT&CK precedentemente citato sia molto usato nelle strategie di pentesting [59]. Il penetration testing per siti web si basa su tre metodologie principali [78], ognuna con approcci e obiettivi distinti:

- **Black Box Testing.** Simula un attacco esterno, dove il tester non ha alcuna conoscenza preliminare del sito (codice, documentazione, configurazioni). Inizia con attività di cognizione come scansione delle porte o mappatura della rete per identificare punti deboli, sfruttando poi strumenti automatizzati e tecniche manuali per violare il sistema. Questo approccio offre una visione realistica della sicurezza, poiché replica le condizioni di un aggressore reale, ma richiede tempo e risorse elevate a causa della necessità di raccogliere informazioni da zero[74].
- **White Box Testing.** In questo caso invece il tester ha accesso completo al codice sorgente, all'architettura e alla documentazione interna. Questo permette analisi approfondite, come scansioni avanzate o test sul design del sistema, identificando vulnerabilità prima del deployment. È ideale per ottimizzare la sicurezza in fase di sviluppo, ma potrebbe sovrastimare le difese, poiché un attaccante esterno non disporrebbe delle stesse informazioni. Inoltre, richiede competenze specializzate e può risultare costoso [28], [17].

- **Grey Box Testing.** Qua combiniamo elementi delle prime due: il tester riceve informazioni parziali, come credenziali utente, diagrammi di rete, per simulare attacchi da parte di insider o hacker con accesso limitato. Ad esempio, potrebbe utilizzare dati forniti per eseguire attacchi brute-force o analizzare configurazioni specifiche. Offre un equilibrio tra realismo e profondità, ma dipende dalla collaborazione con gli amministratori e non riflette pienamente le minacce esterne pure [39].

Confronto tra Black Box, White Box e Grey Box			
Aspetto di confronto	Black Box	White Box	Grey Box
Informazioni sul target	Nessuna informazione o accesso	Accesso completo	Accesso parziale
Natura del testing	Test di accettazione utente	Solo sviluppatori/tester	Test di accettazione utente
Tempo e sforzo	Molto elevato	Ridotto	Intermedio
Granularità del test	Bassa	Alta	Media
Fondamenti	Eccezioni esterne (comportamenti interni sconosciuti)	Eccezioni interne/esterne (comportamenti noti)	Diagrammi di database e stati interni
Ambito del testing	Trial-and-error, limiti esterni	Dati e limiti interni	Limiti interni/esterni, overflow
Limitazioni	Non adatto per algoritmi	Adatto a tutti	Non adatto per algoritmi

Tabella 3.2. Confronto delle metodologie di testing [77].

Software per il VAPT

Vediamo ora due software, come Vuls e Nmap, entrambi open-source e utilizzati apposta per la scansione delle reti propedeutici al tracciamento delle vulnerabilità.

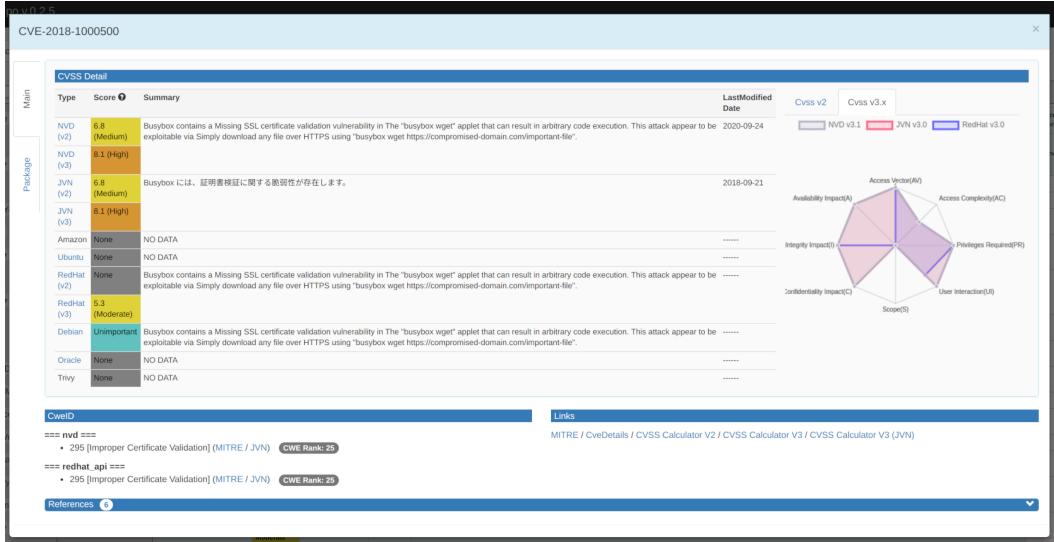


Figura 3.17. L’interfaccia web di Vuls¹⁶, con i dettagli di una vulnerabilità CVE, i punteggi di gravità CVSS e un grafico radar che riassume il livello di rischio, insieme a riferimenti e metadati utili per la gestione della minaccia.

```

Device type: general purpose
Running: Microsoft Windows 10
OS CPE: cpe:/o:microsoft:windows_10
OS details: Microsoft Windows 10 1809 - 21H2
Network Distance: 0 hops
TCP Sequence Prediction: Difficulty=255 (Good luck!)
IP ID Sequence Generation: Incremental
Service Info: OS: Windows; CPE: cpe:/o:microsoft:windows

Host script results:
| smb2-time:
|   date: 2025-03-05T17:44:13
|_ start_date: N/A
| smb2-security-mode:
|   3:1:1:
|_ Message signing enabled but not required

NSE: Script Post-scanning.
Initiating NSE at 18:44
Completed NSE at 18:44, 0.00s elapsed
Initiating NSE at 18:44
Completed NSE at 18:44, 0.00s elapsed
Initiating NSE at 18:44
Completed NSE at 18:44, 0.00s elapsed
Read data files from: E:\nmap
OS and Service detection performed. Please report any incorrect results at https://nmap.org/submit/.
Nmap done: 1 IP address (1 host up) scanned in 107.99 seconds
          Raw packets sent: 1028 (46.106KB) | Rcvd: 2099 (90.346KB)
|

```

Figura 3.18. L’interfaccia gui di nmap¹⁷, rappresenta una scansione di una rete locale. Mostra i dettagli di un host trovato in rete.

¹⁶Fonte: Vuls (<https://vuls.io/docs/en/vulsrepo.html>)

¹⁵Fonte: Nmap (<https://nmap.org/>)

```

nmap -T4 -A -v localhost
Initiating NSE at 12:45
Completed NSE at 12:45, 0.00s elapsed
Initiating NSE at 12:45
Completed NSE at 12:45, 0.00s elapsed
Initiating NSE at 12:45
Completed NSE at 12:45, 0.00s elapsed
Initiating NSE at 12:45
Completed NSE at 12:45, 0.00s elapsed
Initiating Parallel DNS resolution of 1 host. at 12:45
Completed Parallel DNS resolution of 1 host. at 12:45, 0.00s elapsed
Initiating SYN Stealth Scan at 12:45
Scanning localhost (127.0.0.1) [1000 ports]
Discovered open port 445/tcp on 127.0.0.1
Discovered open port 3306/tcp on 127.0.0.1
Discovered open port 135/tcp on 127.0.0.1
Discovered open port 9010/tcp on 127.0.0.1
Discovered open port 5357/tcp on 127.0.0.1
Discovered open port 8090/tcp on 127.0.0.1
Discovered open port 9100/tcp on 127.0.0.1
Discovered open port 2968/tcp on 127.0.0.1
Discovered open port 9080/tcp on 127.0.0.1
Discovered open port 5432/tcp on 127.0.0.1
Discovered open port 12345/tcp on 127.0.0.1
Discovered open port 7070/tcp on 127.0.0.1
Completed SYN Stealth Scan at 12:45, 0.04s elapsed (1000 total ports)
Initiating Service scan at 12:45
Scanning 11 services on localhost (127.0.0.1)
Completed Service scan at 12:47, 86.10s elapsed (12 services on 1 host)
Initiating OS detection (try #1) against localhost (127.0.0.1)
NSE: Script scanning 127.0.0.1.
Initiating NSE at 12:47
Completed NSE at 12:47, 14.26s elapsed
Initiating NSE at 12:47
Completed NSE at 12:47, 7.13s elapsed
Initiating NSE at 12:47
Completed NSE at 12:47, 0.00s elapsed
Nmap scan report for localhost (127.0.0.1)
Host is up (0.036s latency).
Other addresses for localhost (not scanned): ::1
rDNS record for 127.0.0.1: localhost.lan
Not shown: 988 closed tcp ports (reset)
PORT      STATE SERVICE      VERSION
135/tcp    open  msrpc        Microsoft Windows RPC
445/tcp    open  microsoft-ds?
2968/tcp   open  enpp?
3306/tcp   open  mysql        MySQL 8.0.36
|_ssl-date: TLS randomness does not represent time

```

Figura 3.19. L'interfaccia gui di nmap, rappresenta una scansione di una rete locale. La scansione è stata effettuata in modalità “Intense Scan”¹⁸ e l'output ci mostra le porte trovate aperte in quella rete e i servizi collegati a quella rete.

¹⁸Fonte: Nmap (<https://nmap.org/book/zenmap-scanning.html>)

Capitolo 4

Simulazione di una Rete Reale

4.1 Esempio di implementazione di sicurezza nella rete di Poste Italiane

Analizzando la rete della società Poste Italiane¹ notiamo che si configura come un caso emblematico dell'applicazione pratica dei principi di sicurezza illustrati in questa tesi, integrando concetti teorici e strumenti operativi per la protezione delle reti. A livello organizzativo, Poste Italiane ha istituito una struttura di governance dedicata alla cybersecurity, affidando la responsabilità complessiva della sicurezza informatica al Chief Information Security Officer (CISO). Questa scelta rispecchia il principio, ampiamente evidenziato nel **Capitolo 3** di questo elaborato, secondo cui una chiara definizione di ruoli e responsabilità è fondamentale per garantire una gestione efficace della sicurezza.

Sul versante tecnologico, l'adozione di infrastrutture e metodologie all'avanguardia da parte di Poste Italiane si integra perfettamente con i modelli di progettazione di reti sicure presentati nel **Capitolo 2**. L'azienda ha attivato tre poli distinti: il Security Innovation Lab, il Computer Emergency Response Team (CERT) e il Distretto Tecnologico Cyber Security di Cosenza. Il primo di questi centri operativi è impegnato nella ricerca applicata per lo sviluppo tecnologico, il secondo si occupa invece della risposta immediata agli incidenti e il terzo dello sviluppo di prototipi evolutivi per la protezione dei pagamenti elettronici. L'obiettivo ultimo di questa struttura si configura come un esempio tangibile dell'applicazione dei principi della difesa in profondità e dell'approccio "Zero Trust" per attenuare le vulnerabilità, concentrandosi sulla definizione e implementazione di modelli, metodologie e prototipi innovativi per l'analisi delle minacce cyber e la tutela dei dati personali, in modo da rafforzare le capacità difensive e di risposta di Poste Italiane e assicurare una gestione efficace ed efficiente della privacy all'interno del Gruppo [68].

Il framework di sicurezza adottato da Poste Italiane si fonda su una rigorosa definizione di policy, sull'analisi dei rischi e sulla gestione centralizzata degli incidenti, elementi che richiamano direttamente i modelli normativi e metodologici esposti in questa tesi, quali ISO/IEC 27001 per cui troviamo la certificazione [15]. Notiamo anche dall'analisi fatta in questo articolo [14] come la società abbia preso seriamente la sicurezza delle loro reti.

¹Poste Italiane: (<https://www.poste.it/>)

Dalla nostra analisi siamo anche venuti a conoscenza di uno strumento proattivo utilizzato da Poste per mantenere le loro infrastrutture sicure, ossia Microsoft Defender XDR². Si tratta di una suite di strumenti pensata apposta per la difesa aziendale che fornisce una sicurezza multi-livello, andando a proteggere gli end point, le email e le applicazioni SaaS (cloud). Nell'infrastruttura del Gruppo è presente anche un sistema di monitoraggio della rete. Tutte le informazioni che transitano nel network della società, provenienti sia da dispositivi BYOD che da apparecchiature di rete interne, vengono analizzate e inviate a un server centrale. Quest'ultimo, grazie all'applicativo precedentemente menzionato, correla gli eventi utilizzando l'integrazione con il MITRE ATT&CK già affrontato. Tale correlazione permette di individuare le attività malevoli su tutti i dispositivi della rete e cerca di risolverle automaticamente, tramite intelligenza artificiale, segnalando a prescindere l'incidente agli analisti. Abbiamo nominato anche la protezione delle email, infatti questo software analizza gli allegati e gli URL nelle mail che, se considerati malevoli, vengono rimossi. Altra funzionalità fondamentale per gli analisti sono i log che permettono di investigare gli eventi che occorrono nella rete, facilitando la verifica del corretto funzionamento dell'infrastruttura. All'interno di questa suite troviamo anche la possibilità di integrazione con un SIEM, Microsoft Sentinel³, che oltre a funzionare come un SIEM, di cui abbiamo discusso il funzionamento, permette anche di effettuare delle query su tutti i dati che sono analizzati dal Defender XDR tramite linguaggio KQL⁴. Grazie a tool come questi, il carico sul reparto IT si riduce notevolmente: da un lato si minimizza la superficie d'attacco, dall'altro si accelerano i tempi di risposta agli incidenti e di investigazione. Nella nostra analisi siamo venuti a conoscenza dell'utilizzo da parte di Poste anche di NGFW, IDS e IPS avanzati, integrati con questo strumento appena descritto di cui però non possiamo ottenere i dettagli.

²Sito: (<https://www.microsoft.com/it-it/security/business/siem-and-xdr/microsoft-defender-xdr>)

³Sito: (<https://azure.microsoft.com/it-it/products/microsoft-sentinel>)

⁴Fonente: Microsoft (<https://learn.microsoft.com/it-it/kusto/query/?view=microsoft-fabric>)

Capitolo 5

Conclusioni e Nuove Tecnologie per la Sicurezza delle Reti Aziendali

In questo capitolo andremo ad analizzare le conclusioni della nostra tesi, descrivendo le nuove tecnologie e le limitazioni e approfondendo anche il caso reale citato inizialmente. L'intelligenza artificiale, AI, e il machine learning, ML, stanno rivoluzionando la sicurezza nelle aziende, potenziando la capacità di individuare e gestire le minacce. Grazie a queste tecnologie, molti processi di sicurezza vengono automatizzati, riducendo la necessità di intervento umano e accelerando la risposta a potenziali attacchi. I sistemi di AI analizzano automaticamente i comportamenti sospetti e prevengono violazioni, bloccando gli attacchi in tempo reale. Questo approccio è diventato fondamentale per contrastare minacce informatiche sempre più avanzate e complesse. Un altro modello che sta prendendo sempre più piede è quello dei framework Zero-Trust: l'approccio di questo principio si basa sul “never trust, always verify” ovvero si vuole far capire che tutti gli utenti, esterni e interni all'organizzazione, devono autenticarsi ed essere sempre validati¹ prima di ricevere i permessi su risorse critiche. Stare al passo in un ambiente dove malware, ransomware e vari tipi di attacchi sono in costante sviluppo non è facile per le organizzazioni, abbiamo visto in precedenza come l'aumento di attacchi di questo tipo ha creato il bisogno per un avanzamento tecnologico per le misure di sicurezza nelle reti. Non è quindi facile adeguarsi, soprattutto a causa dei continui investimenti richiesti e la costante ricerca di personale con le necessarie competenze. Questi fattori rappresentano un ostacolo per la maggior parte delle aziende.

¹Fonte: (<https://cybersecurityvalidation.com/what-is-security-validation/>)

5.1 Machine Learning e Artificial Intelligence

Questi strumenti possono essere utilizzati per analizzare il traffico e per l'identificazione di pattern pericolosi. Un esempio di implementazione di intelligenza artificiale nella sicurezza delle reti è quello di Darktrace con il suo prodotto che lo utilizza per rilevare e rispondere alle minacce in tempo reale². Questi strumenti trovano grande applicazione nell'analisi dei dati. Al giorno d'oggi i sistemi di IDS e IPS, di cui abbiamo parlato in precedenza, sono il collo di bottiglia per molte reti; infatti, questi sistemi utilizzano macchine per analizzare volumi enormi di traffico [50]. Con sistemi come ML e il Deep Learning, DL, si possono creare algoritmi e strumenti in grado di prevedere il traffico. Questo comporta, non solo un aumento dell'efficienza delle prestazioni della rete, come con gli Access Point nel compiere controlli come degli accessi o il load balancing, ma aiuta a mettere in sicurezza i sistemi e ad alleggerire il carico su macchine e reparti IT. L'AI e reti neurali leggiamo da [40] come le Artificial Neural Network, ANN, siano state spesso proposte anche loro per la predizione del traffico, dato che teoricamente cattura ogni relazione tra l'output e l'input, non è però di facile implementazione. Il ML, unito ad AI, è capace di scoprire autonomamente e quindi di imparare. Questo è cruciale per la rilevazione di nuovi tipi di attacchi, ancora sconosciuti, grazie ai data set enormi da cui apprende ed è capace di integrarsi anche con banche dati come il MITRE ATT&CK menzionato precedentemente. Gli IDS basati su questa tecnologia raggiungono livelli di rilevamento soddisfacenti quando sono disponibili dati di addestramento sufficienti e i modelli mostrano una buona generalizzazione, permettendo di identificare sia varianti di attacchi esistenti che minacce completamente nuove, ma anche di ridurre sensibilmente i falsi negativi, alleggerendo quindi il carico. Un vantaggio aggiuntivo è che questi sistemi non dipendono eccessivamente da conoscenze specifiche del dominio, rendendoli più semplici da progettare e implementare. Il deep learning, una branca avanzata del machine learning, si distingue per le sue prestazioni eccezionali, superando le tecniche tradizionali nella gestione dei dati. I metodi di deep learning si differenziano proprio perché apprendono autonomamente le rappresentazioni delle caratteristiche direttamente dai dati grezzi, operando in modalità end-to-end e garantendo un approccio pratico ed efficiente [52].

Un altro strumento che beneficia particolarmente di queste tecnologie sono i SIEM, i quali devono monitorare una grande quantità di dati, limitando le prestazioni e richiedendo molte risorse. L'integrazione di intelligenza artificiale e machine learning negli strumenti SIEM sta rivoluzionando il modo in cui le organizzazioni rilevano, analizzano e rispondono agli incidenti di sicurezza. Questo studio [56] esplora il futuro dei SIEM nel contesto di un panorama cybersecurity in continua evoluzione, approfondendo come le aziende possano prepararsi all'adozione di sistemi SIEM potenziati dal ML. Queste soluzioni avanzate amplificano le capacità dei SIEM tradizionali, consentendo di identificare e gestire sia minacce note che emergenti con maggiore efficacia. Per sfruttare appieno il potenziale di queste tecnologie, è essenziale che le organizzazioni sviluppino una strategia dati solida, investano nella formazione di personale qualificato e adottino i SIEM abilitati al ML in modo graduale. Restare aggiornati sulle ultime tendenze in ambito ML e cybersecurity è

²Fonente: Darktrace (<https://darktrace.com/products>)

altrettanto cruciale per massimizzare i vantaggi offerti da questi strumenti innovativi. Come detto nei capitoli precedenti troviamo i SIEM al centro dei SoC, infatti anche queste infrastrutture hanno iniziato a sfruttare il ML per rilevare con più precisione ed efficienza le minacce. Analizzando la letteratura scientifica vediamo come in questi studi [55], [53] si parlava già di “SoC Intelligente”, evidenziando come l’analisi predittiva e l’adattamento dinamico alle minacce possano ottimizzare le operazioni nei centri. Vediamo anche come in questi lavori [26], [41], [70], viene approfondito il ruolo dell’automazione nei Security Operation Centers, definendola come un pilastro per la cyber security moderna. Queste ricerche dimostrano come l’automazione possa snellire processi complessi e liberare risorse per attività critiche grazie a meccanismi già in uso. Questi modelli hanno ispirato lo sviluppo di framework interni per l’automazione nei SOC, migliorando efficienza e tempi di risposta. Un altro aspetto cruciale emerso riguarda la sinergia tra Threat Intelligence e Threat Hunting in contesti abilitati dal ML. L’integrazione di queste discipline permette non solo di contrastare minacce note, ma anche di individuare pattern anomali e attacchi avanzati, potenziando la capacità proattiva delle organizzazioni. Questo approccio trasforma i SIEM da semplici strumenti di monitoraggio a sistemi dinamici, capaci di anticipare rischi e adattarsi a scenari in evoluzione. Per ottenere questa automazione sono necessari algoritmi di ML, in grado di analizzare dati diversi di ogni tipo, infatti l’elaborazione del linguaggio naturale, NLP gioca un ruolo cruciale, trasformando i dati non strutturati in modelli normalizzati. Questo sistema monitora dinamicamente le attività, identificando comportamenti sospetti che potrebbero sfuggire a metodi tradizionali, migliorando così la capacità di risposta proattiva alle minacce. Per avere un “SoC Intelligente”, come detto in precedenza, dobbiamo sfruttare anche le ANN, usate per prevedere le vulnerabilità sfruttabili su una rete. Come abbiamo detto in precedenza il Machine Learning, è ottimo per manipolare i dati [48], e grazie ad algoritmi basati su questa tecnica, ottimizzati in base allo scenario, possono essere sfruttati anche per il penetration testing. I pen tester infatti [71], [29], [46] potrebbero non essere accurati e possono farsi influenzare negativamente dal loro istinto, i sistemi ML invece sono più accurati in quanto non si fanno influenzare dal contesto, riuscendo a isolare meglio attacchi reali e falsi positivi. L’utilizzo quindi da parte dei pen tester di questi strumenti, unito con le loro competenze, rappresenta la scelta migliore perché combina i punti di forza distintivi delle due componenti, superando i limiti intrinseci di ciascuna. Da un lato, il Machine Learning offre la capacità di analizzare enormi volumi di dati in tempi rapidi, identificando schemi complessi, anomalie o correlazioni che sfuggirebbero all’analisi umana, soprattutto in scenari dinamici e ad alto carico di informazioni, il che permette anche di ridurre il così detto “rumore” nei dati. L’integrazione quindi tra le due soluzioni è la scelta migliore, riuscendo ad aumentare l’efficienza, riducendo gli errori e aumentando la precisione e riuscendo ad adattarsi anche agli scenari più complessi, infatti grazie all’utilizzo dell’output del ML per generare ipotesi mirate, testarle in modo dinamico e adattare le strategie di difesa in tempo reale, anche in presenza di minacce sconosciute [57], [31].

5.2 Architetture Zero Trust

Abbiamo anche parlato di framework Zero-Trust, ossia un principio che presuppone che nessuna fiducia implicita venga concessa ad asset o account utente basandosi esclusivamente sulla loro posizione fisica o nella rete o sulla proprietà degli asset, che si concentra sulla protezione delle risorse, dove autenticazione e autorizzazione, sia del soggetto che del dispositivo, sono funzioni distinte eseguite prima che una sessione verso una risorsa aziendale venga stabilita. Analizzando questo paper [81] del NIST capiamo come questa architettura è nata come risposta ai trend delle reti aziendali, come utenti remoti, politiche BYOD, di cui abbiamo parlato e asset cloud non situati entro i confini di reti di proprietà aziendale. Lo Zero Trust si concentra sulla protezione delle risorse, anziché sui segmenti di rete, poiché la posizione della rete non è più considerata l'elemento principale per la postura di sicurezza della risorsa.

All'inizio di questo capitolo abbiamo parlato di framework Zero-Trust, un approccio che parte dall'idea che non si debba dare per scontata la sicurezza di dispositivi o account solo perché sono “dentro” la rete aziendale o perché appartengono all'organizzazione. Nello Zero Trust, anche se un utente è collegato alla LAN o usa un dispositivo aziendale, non viene automaticamente considerato affidabile: prima di concedere l'accesso a qualsiasi risorsa, sia le persone che i dispositivi devono superare controlli di identità, tramite il processo di autenticazione e verifiche sui permessi, grazie al processo di autorizzazione, indipendentemente da dove si trovano. Questo modello è nato per rispondere a scenari moderni come il lavoro da remoto, l'uso di dispositivi personali, i BYOD di cui abbiamo parlato nei paragrafi precedenti e il cloud, dove dati e servizi spesso risiedono al di fuori dei confini tradizionali della rete aziendale. Invece di concentrarsi su “zone sicure” come le VLAN o i firewall perimetrali, lo Zero Trust protegge direttamente le risorse critiche, come file, applicazioni, server, trattando ogni accesso come potenzialmente rischioso. La logica è semplice: oggi un laptop connesso alla rete interna può essere compromesso tanto quanto un device collegato da casa, quindi la posizione in rete non basta più come garanzia di sicurezza.

5.3 Limiti e conseguenze

Durante questa analisi abbiamo analizzato come una rete aziendale dovrebbe essere implementata, nel caso generale, capendo che non può esistere un modello che vada bene per ogni situazione ma che bisogna adattare in ogni caso diversi principi in base al proprio use case. Implementare lo stato dell'arte nella sicurezza delle reti però non è un compito facile e richiede una grande quantità di competenze. Una sezione che abbiamo affrontato è quella sull'importanza della formazione del personale, sia tecnico che non, permettendo una maggiore esperienza nell'ambito. Fare questo investimento per le aziende significa avere un ritorno in termini di sicurezza sulla propria infrastruttura di rete. Per le piccole-medie imprese questo investimento non è facile in quanto può pesare sulla loro economia, ma deve comunque essere preso in considerazione per il corretto funzionamento del business.

Per le aziende grandi, prevedere corsi per la formazione del personale tecnico e la sensibilizzazione, in termini di sicurezza informatica, del personale meno specializzato, dovrebbe essere all'ordine del giorno. Quando questa pratica viene trascurata possono succedere disastri, come quello citato in precedenza della Colonial Pipeline [37]. Nella nostra analisi sono stati citati diverse volte dei software open-source³ i quali potrebbero aiutare le aziende che hanno meno possibilità di investimento, garantendo un livello di sicurezza elevato.

Il problema non si limita solo ad una questione di costi e di competenze, ma dobbiamo anche tener conto, come abbiamo ripetuto diverse volte durante l'analisi, che i malware e gli attacchi sono sempre più avanzati e diventano sempre più complessi ogni giorno. Infatti, anche gli strumenti citati in precedenza possono aiutarci a prevenire molti di questi, così da alleggerire il carico di lavoro, ma non garantendo al 100% la sicurezza di un'infrastruttura di rete, tesi sostenuta anche dal ricercatore Jose Nazario in questo paper [62].

5.4 Riflessioni Finali

L'obiettivo di questa analisi, come menzionato in precedenza, è quello di mettere insieme tutte le "best-practice" necessarie per creare una rete sicura all'interno di ogni azienda, mostrando degli esempi di alcuni software, e facendo capire l'importanza dell'implementare tali strumenti, soprattutto per le aziende operatrici di servizi essenziali, OSE⁴, che spesso tralasciano misure di sicurezza ritenute "meno importanti". A mio avviso questa analisi mi ha permesso di indagare più a fondo una materia che mi ha sempre incuriosito e mi ha dato gli strumenti per permettermi di rispondere alle domande iniziali. Esistono quindi più modi, standardizzati, per mettere in sicurezza le reti ed è bene adoperarli. Da questo elaborato possiamo anche capire quali sono gli strumenti necessari per definire una rete "sicura" e abbiamo esplorato anche vari mezzi che possono alleggerire e supportare non solo gli amministratori di rete, ma anche tutto il personale IT, aiutando a ridurre al minimo le negligenze. Inoltre mi ha anche lasciato un senso di responsabilità per questa disciplina scientifica, in quanto nella società di oggi è tutto connesso e non curarsi della sicurezza di queste infrastrutture di rete può creare disagi importanti che possono riversarsi anche sulla nostra società.

³Fonte: Wikipedia (https://it.wikipedia.org/wiki/Open_source)

⁴Fonte: CyberSecurity360 (<https://www.cybersecurity360.it/cybersecurity-nazionale/operatori-di-servizi-essenziali-ose-chi-sono-e-quali-obblighi-di-sicurezza-hanno/>)

Bibliografia

- [1] ADAMS, N.-R. COBIT 2019: IT governance framework. *ITLawCo*, (2024). Disponibile su: <https://itlawco.com/cobit-2019-it-governance-framework/#:~:text=What%20is%20COBIT%202019%3F,govern%20and%20manage%20IT%20effectively>.
- [2] AGBOOLA, T. O. Design Principles for Secure Systems. EasyChair Preprint 10435 (EasyChair, 2023).
- [3] AL-SADA, B., SADIGHIAN, A., AND OLIGERI, G. Analysis and Characterization of Cyber Threats Leveraging the MITRE ATT&CK Database. *IEEE Access*, **PP** (2023), 1. DOI:10.1109/ACCESS.2023.3344680.
- [4] ALSHEH, E. Creating a smarter SOC with the MITRE ATT&CK framework. *CyberProof*, (2023). Disponibile su: <https://www.cyberproof.com/blog/creating-a-smarter-soc-with-the-mitre-attck-framework/>.
- [5] AREFIN, M. T., UDDIN, M. R., EVAN, N. A., AND ALAM, M. R. Enterprise Network: Security Enhancement and Policy Management Using Next-Generation Firewall (NGFW). In *Computer Networks, Big Data and IoT* (edited by A. Pandian, X. Fernando, and S. M. S. Islam), pp. 753–769. Springer Singapore, Singapore (2021). ISBN 978-981-16-0965-7.
- [6] AUSTIN, A. AND WILLIAMS, L. One Technique is Not Enough: A Comparison of Vulnerability Discovery Techniques. In *2011 International Symposium on Empirical Software Engineering and Measurement*, pp. 97–106 (2011). DOI: 10.1109/ESEM.2011.18.
- [7] BELLA, G., BIONDI, P., AND BOGNANNI, S. Multi-service threats: Attacking and protecting network printers and VoIP phones alike. *Internet of Things*, **18** (2022), 100507. Disponibile su: <https://www.sciencedirect.com/science/article/pii/S2542660522000130>, DOI:<https://doi.org/10.1016/j.iot.2022.100507>.
- [8] BHATT, S., MANADHATA, P. K., AND ZOMLOT, L. The Operational Role of Security Information and Event Management Systems. *IEEE Security & Privacy*, **12** (2014), 35. DOI:10.1109/MSP.2014.103.
- [9] BIDOU, R. Security operation center concepts & implementation. *CiteSeer*, (2005). Disponibile su: <http://www.iv2-technologies.com>.

- [10] BLANCAFLOR, E. B. AND MONTOYA, A. J. Vulnerabilities in Office Printers, Multifunction Printers (MFP), 3D Printers, and Digital Copiers: A Gateway to Breach Our Enterprise Network. In *International Conference on Cloud Computing and Computer Networks* (edited by L. Meng), pp. 53–62. Springer Nature Switzerland, Cham (2024). ISBN 978-3-031-47100-1.
- [11] BOOTH, H. National Vulnerability Database, National Institute of Standards and Technology (2015). (Dati del 2023-01-10). Disponibile su: <https://nvd.nist.gov/>.
- [12] BRIZINOV, S., MOSHE, N., AND GOLDSCHMIDT, T. Pwn2Own: WAN-to-LAN Exploit Showcase, Part 1 (2024). Disponibile su: <https://claroty.com/team82/research/pwn2own-wan-to-lan-exploit-showcase>.
- [13] CASADEI, M. Pmi, sull'Italia pesano gap di produttività e bassa scalabilità. *Il Sole 24 Ore*, (2024). Disponibile su: <https://www.ilsole24ore.com/art/pmi-sull-italia-pesano-gap-produttivita-e-bassa-scalabilita-AGxlyyQ>.
- [14] CASTIGLI, M. Poste Italiane a 360 gradi: le 4 direttive della sua cyber difesa (2023). Disponibile su: <https://www.cybersecurity360.it/outlook/poste-italiane-a-360-gradi-le-4-direttive-per-protettgere-i-suoi-servizi/>.
- [15] Certificazioni del Gruppo Poste Italiane. Disponibile su: <https://www.posteitaliane.it/it/certificazioni-del-gruppo.html>.
- [16] CHAMKAR, A. S., MALEH, Y., AND GHERABI, N. Security operation center. *The Art of Cyber Defense: From Risk Assessment to Threat Intelligence*, (2024), 271.
- [17] CHAN, M.-Y. AND CHEUNG, S.-C. Applying white box testing to database applications. *Hong Kong University of Science and Technology, Department of Computer Science, Tech. Rep*, (1999).
- [18] CHIDUKWANI, A., ZANDER, S., AND KOUTSAKIS, P. A Survey on the Cyber Security of Small-to-Medium Businesses: Challenges, Research Focus and Recommendations. *IEEE Access*, **10** (2022), 85701. DOI:10.1109/ACCESS.2022.3197899.
- [19] CHO, S., HAN, I., JEONG, H., KIM, J., KOO, S., OH, H., AND PARK, M. Cyber Kill Chain based Threat Taxonomy and its Application on Cyber Common Operational Picture. In *2018 International Conference On Cyber Situational Awareness, Data Analytics And Assessment (Cyber SA)*, pp. 1–8 (2018). DOI:10.1109/CyberSA.2018.8551383.
- [20] What Is a CISO? (2024). Disponibile su: <https://www.cisco.com/c/en/us/products/security/what-is-ciso.html>.
- [21] The MITRE Corporation. Disponibile su: <https://cve.mitre.org/>.
- [22] The MITRE Corporation. Disponibile su: <https://cwe.mitre.org/>.

- [23] CYBERNEWS TEAM. We hijacked 28,000 unsecured printers to raise awareness of printer security issues. *Cybernews*, (2022). Disponibile su: <https://cybernews.com/security/we-hacked-28000-unsecured-printers-to-raise-awareness-of-printer-security-issues/>.
- [24] CYBERSECURITY AND INFRASTRUCTURE SECURITY AGENCY. Cybersecurity Advisories (2023). Disponibile su: https://www.cisa.gov/news-events/cybersecurity-advisories?f%5B0%5D=advisory_type%3A94 [citata 2023-10-01].
- [25] DAMEFF, C., TULLY, J., CHAN, T. C., CASTILLO, E. M., SAVAGE, S., MAYSENT, P., HEMMEN, T. M., CLAY, B. J., AND LONGHURST, C. A. Ransomware Attack Associated With Disruptions at Adjacent Emergency Departments in the US. *JAMA Network Open*, **6** (2023), e2312270. Disponibile su: <https://doi.org/10.1001/jamanetworkopen.2023.12270>, arXiv: <https://jamanetwork.com/journals/jamanetworkopen/articlepdf/2804585/dameff_2023_oi_230381_1682948883.13075.pdf>, DOI: [10.1001/jamanetworkopen.2023.12270](https://doi.org/10.1001/jamanetworkopen.2023.12270).
- [26] DAR, A. The Modern SOC – Time to Look Beyond Automation. Disponibile su: <https://www.cyberbit.com/soc-operations/modern-soc-time-to-look-beyond-automation/>.
- [27] DAVID FERRAIOLI, N. L., DENNIS GILBERT. An Examination of Federal and Commercial Access Control Policy Needs. Rep. Tec. 16th National Computer Security Conference, National Institute of Standards and Technology, Gaithersburg, MD (1993).
- [28] ESFAHANI, N., KACEM, T., MIRZAEI, N., MALEK, S., AND STAVROU, A. A whitebox approach for automated security testing of Android applications on the cloud. *7th International Workshop on Automation of Software Test (AST)*, (2012). DOI: [10.1109/IWAST.2012.6228986](https://doi.org/10.1109/IWAST.2012.6228986).
- [29] FEDERMEIER, K. D. Thinking ahead: The role and roots of prediction in language comprehension. *Psychophysiology*, **44** (2007), 491. Disponibile su: <https://onlinelibrary.wiley.com/doi/abs/10.1111/j.1469-8986.2007.00531.x>, arXiv: <https://onlinelibrary.wiley.com/doi/pdf/10.1111/j.1469-8986.2007.00531.x>, DOI: <https://doi.org/10.1111/j.1469-8986.2007.00531.x>.
- [30] What Is The COBIT Framework? (2023). Disponibile su: <https://www.fortinet.com/resources/cyberglossary/what-is-cobit>.
- [31] FRANKE, U. AND BRYNIELSSON, J. Cyber situational awareness – A systematic review of the literature. *Computers & Security*, **46** (2014), 18. Disponibile su: <https://www.sciencedirect.com/science/article/pii/S0167404814001011>, DOI: <https://doi.org/10.1016/j.cose.2014.06.008>.
- [32] GAGLIARDI, T. User Access Reviews: A Step-by-Step Guide + Checklist. *Drata*, (2024). Disponibile su: <https://drata.com/blog/user-access-review>.

- [33] GREIG, J. Nearly 400 US healthcare institutions hit with ransomware over last year, Microsoft says. *The Record from Recorded Future News*, (2024). Disponibile su: <https://therecord.media/ransomware-healthcare-microsoft-last-year>.
- [34] HASHIM, W. AND HUSSEIN, N. A.-H. K. Securing Cloud Computing Environments: An Analysis of Multi-Tenancy Vulnerabilities and Countermeasures. *SHIFRA*, **2024** (2024), 8–16. Disponibile su: <https://peninsula-press.ae/Journals/index.php/SHIFRA/article/view/47>, DOI:10.70470/SHIFRA/2024/002.
- [35] IBM. Cos'è la gestione delle patch? Disponibile su: <https://www.ibm.com/it-it/topics/patch-management>.
- [36] IBM. What is backup and disaster recovery? Disponibile su: <https://www.ibm.com/think/topics/backup-disaster-recovery#:~:text=The%20sub%20processes%E2%80%94'backup',IT%20resources%20after%20an%20outage>.
- [37] JACK, B., DAVID, B., ZACH, F., AND SUMAN, B. A Review of Colonial Pipeline Ransomware Attack. In *2023 IEEE/ACM 23rd International Symposium on Cluster, Cloud and Internet Computing Workshops (CCGridW)*, pp. 8–15 (2023). DOI:10.1109/CCGridW59191.2023.00017.
- [38] KB, S. K. NIST vs. ISO 27001: Choosing the Right Cybersecurity Framework. *LinkedIn*, (2023). Disponibile su: <https://www.linkedin.com/pulse/nist-vs-iso-27001-choosing-right-cybersecurity-framework-kb/>.
- [39] KHAN, M. E. AND KHAN, F. A comparative study of white box, black box and grey box testing techniques. *International Journal of Advanced Computer Science and Applications*, **3** (2012).
- [40] KHOTANZAD, A. AND SADEK, N. Multi-scale high-speed network traffic prediction using combination of neural networks. In *Proceedings of the International Joint Conference on Neural Networks, 2003.*, vol. 2, pp. 1071–1075 vol.2 (2003). DOI:10.1109/IJCNN.2003.1223839.
- [41] KISIELIUS, J. Automated Incident Response Explained (2020). Disponibile su: <https://levelblue.com/blogs/security-essentials/automated-incident-response-in-action-7-killer-use-cases>.
- [42] KWON, R., ASHLEY, T., CASTLEBERRY, J., MCKENZIE, P., AND GUPTA GOURISETTI, S. N. Cyber Threat Dictionary Using MITRE ATT&CK Matrix and NIST Cybersecurity Framework Mapping. In *2020 Resilience Week (RWS)*, pp. 106–112 (2020). DOI:10.1109/RWS50334.2020.9241271.
- [43] LAKSHMANAN, R. Cisco Patches Critical ISE Vulnerabilities Enabling Root CmdExec and PrivEsc. *The Hacker News*, (2025). Disponibile su: <https://thehackernews.com/2025/02/cisco-patches-critical-ise.html>.

- [44] LAKSHMANAN, R. Microsoft's Patch Tuesday Fixes 63 Flaws, Including Two Under Active Exploitation. *The Hacker News*, (2025). Disponibile su: <https://thehackernews.com/2025/02/microsofts-patch-tuesday-fixes-63-flaws.html>.
- [45] LAMBERTI, A. A Guide to Different Types of Network Monitoring Tools: Unveiling the Superheroes (2023). Disponibile su: <https://obkio.com/blog/types-of-network-monitoring-tools/>.
- [46] LEHNER, P., SEYED-SOLORFOROUGH, M.-M., O'CONNOR, M., SAK, S., AND MULLIN, T. Cognitive biases and time stress in team decision making. *IEEE Transactions on Systems, Man, and Cybernetics - Part A: Systems and Humans*, **27** (1997), 698. DOI:10.1109/3468.618269.
- [47] LENTEPUBBLICA.IT. Un attacco cyber ad AWS ripropone la fragilità dei dati sensibili. *lentepubblica.it*, (2024). Disponibile su: <https://lentepubblica.it/cittadini-e-imprese/attacco-cyber-aws-dati-sensibili/>.
- [48] LI, J.-H. Cyber security meets artificial intelligence: a survey. *Frontiers of Information Technology & Electronic Engineering*, **19** (2018), 1462. Disponibile su: <https://doi.org/10.1631/FITEE.1800573>, DOI:10.1631/FITEE.1800573.
- [49] LIAO, F. Analysis of Computer Network Security Problems and Countermeasures. In *Proceedings of the 2017 7th International Conference on Social Network, Communication and Education (SNCE 2017)*, pp. 905–908. Atlantis Press (2017/07). ISBN 978-94-6252-386-9. Disponibile su: <https://doi.org/10.2991/snce-17.2017.186>, DOI:10.2991/snce-17.2017.186.
- [50] LIN, H., YAN, Z., CHEN, Y., AND ZHANG, L. A Survey on Network Security-Related Data Collection Technologies. *IEEE Access*, **6** (2018), 18345. DOI: 10.1109/ACCESS.2018.2817921.
- [51] LIU, B., SHI, L., CAI, Z., AND LI, M. Software Vulnerability Discovery Techniques: A Survey. In *2012 Fourth International Conference on Multimedia Information Networking and Security*, pp. 152–156 (2012). DOI:10.1109/MINES.2012.202.
- [52] LIU, H. AND LANG, B. Machine Learning and Deep Learning Methods for Intrusion Detection Systems: A Survey. *Applied Sciences*, **9** (2019). Disponibile su: <https://www.mdpi.com/2076-3417/9/20/4396>, DOI:10.3390/app9204396.
- [53] LLC, P. I. Improving the Effectiveness of the Security Operations Center. *Ponemon Institute LLC*, (2019).
- [54] LUNTOVSKYY, A. *Advanced Networking and Cybersecurity Approaches*, pp. 79–98. Springer Nature Switzerland, Cham (2023). ISBN 978-3-031-40997-4. Disponibile su: https://doi.org/10.1007/978-3-031-40997-4_6, DOI: 10.1007/978-3-031-40997-4_6.
- [55] MACEDO, I., WANOUS, S., OLIVEIRA, N., SOUSA, O., AND PRAÇA, I. A Tool to Support the Investigation and Visualization of Cyber and/or Physical

- Incidents. In *Trends and Applications in Information Systems and Technologies* (edited by Á. Rocha, H. Adeli, G. Dzemyda, F. Moreira, and A. M. Rama-lho Correia), pp. 130–140. Springer International Publishing, Cham (2021). ISBN 978-3-030-72654-6.
- [56] MAIL, I. The future of SIEM in a machine learning-driven cybersecurity landscape. *Turkish Journal of Computer and Mathematics Education Vol*, **14** (2023), 1309.
- [57] MARKOWSKY, G. AND MARKOWSKY, L. Visualizing cybersecurity events. In *Proceedings of the International Conference on Security and Management (SAM)*, p. 1. The Steering Committee of The World Congress in Computer Science, Computer ... (2013).
- [58] MATHEW, S. AND VARIA, J. Overview of amazon web services. *Amazon Whitepapers*, **105** (2014), 22.
- [59] MAYUKHA, S. AND VADIVEL, R. Reconnaissance for Penetration Testing Using Active Scanning of MITRE ATT&CK. In *Information and Communication Technology for Competitive Strategies (ICTCS 2021)* (edited by M. S. Kaiser, J. Xie, and V. S. Rathore), pp. 693–705. Springer Nature Singapore, Singapore (2023). ISBN 978-981-19-0098-3.
- [60] McAFFEE AND INTEL SECURITY. Network Performance and Security. *Intel Security*, (2014). Disponibile su: <https://www.webtutorials.com/main/resource/papers/McAfee/paper41/network-performance-security-trade-off.pdf>.
- [61] MEHRI, V. A., ARLOS, P., AND CASALICCHIO, E. Automated Patch Management: An Empirical Evaluation Study. In *2023 IEEE International Conference on Cyber Security and Resilience (CSR)*, pp. 321–328 (2023). DOI:10.1109/CSR57506.2023.10224970.
- [62] NAZARIO, J. DDoS attack evolution. *Network Security*, **2008** (2008), 7. Disponibile su: <https://www.sciencedirect.com/science/article/pii/S1353485808700862>, DOI:[https://doi.org/10.1016/S1353-4858\(08\)70086-2](https://doi.org/10.1016/S1353-4858(08)70086-2).
- [63] NEWS, T. H. Microsoft Patches Critical Azure AI Face Service Vulnerability with CVSS 9.9 Score. *The Hacker News*, (2025). Disponibile su: <https://thehackernews.com/2025/02/microsoft-patches-critical-azure-ai.html>.
- [64] NSA and CISA Red and Blue Teams Share Top Ten Cybersecurity Misconfigurations. Rep. tec., NSA, CISA (2023). Disponibile su: <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-278a>.
- [65] NWAKEZE, O. THE ROLE OF NETWORK MONITORING AND ANALYSIS IN ENSURING OPTIMAL NETWORK PERFORMANCE. *IRJMETS*, **6** (2024), 3009. DOI:10.56726/IRJMETS59269.

- [66] PATEL, A. Network performance without compromising security. *Network Security*, **2015** (2015), 9. Disponibile su: <https://www.sciencedirect.com/science/article/pii/S1353485815700085>, DOI:[https://doi.org/10.1016/S1353-4858\(15\)70008-5](https://doi.org/10.1016/S1353-4858(15)70008-5).
- [67] Cyber Security Manager e CISO: quali competenze servono (2024). Disponibile su: <https://www.gsom.polimi.it/knowledge/cyber-security-manager-e-ciso-quali-competenze-servono/>.
- [68] POSTE ITALIANE. Cyber Security. Disponibile su: <https://www.posteitaliane.it/it/cyber-security-sostenibilita.html>.
- [69] PROTOCOL, A. AND FEDERAL, W. I. N. Security Automation. *Citeseer*, (2010).
- [70] RANDY FRANKLIN SMITH, D. K., BRIAN COULSON. Using MITRE ATT&CK in Threat Hunting and Detection. *LogRhythm*, (2022).
- [71] RIEGLER, A. The role of anticipation in cognition. *AIP Conference Proceedings*, **573** (2001), 534. Disponibile su: <https://doi.org/10.1063/1.1388719>, arXiv:<https://pubs.aip.org/aip/acp/article-pdf/573/1/534/12023736/534\1\online.pdf>, DOI:10.1063/1.1388719.
- [72] ROGERS, R., MARCUS K.; HEROLD. *Encyclopedia of information assurance. 4 Volume Set*. CRC Press/Taylor & Francis (2011). ISBN 9781420067385; 1420067389.
- [73] ROY, P. P. A High-Level Comparison between the NIST Cyber Security Framework and the ISO 27001 Information Security Standard. In *2020 National Conference on Emerging Trends on Sustainable Technology and Engineering Applications (NCETSEA)*, pp. 1–3 (2020). DOI:10.1109/NCETSEA48365.2020.9119914.
- [74] RUBEL, A. The Black Box Society: The Secret Algorithms that Control Money and Information, by Frank Pasquale. Cambridge: Harvard University Press, 2015. 320 pp. ISBN 978-0674368279. *Business Ethics Quarterly*, **26** (2016), 568–571. DOI:10.1017/beq.2016.50.
- [75] RUCINSKI, T. American Airlines adds stops to two flights after pipeline outage (2021). Disponibile su: <https://www.reuters.com/business/energy/american-airlines-adds-fuel-stops-two-flights-after-pipeline-outage-2021-05-11/>.
- [76] SANDHU, R. AND SAMARATI, P. Access control: principle and practice. *IEEE Communications Magazine*, **32** (1994), 40. DOI:10.1109/35.312842.
- [77] SHAH, S. AND MEHTRE, B. M. An overview of vulnerability assessment and penetration testing techniques. *Journal of Computer Virology and Hacking Techniques*, **11** (2015), 27. Disponibile su: <https://doi.org/10.1007/s11416-014-0231-x>, DOI:10.1007/s11416-014-0231-x.

- [78] SHINDE, P. S. AND ARDHAPURKAR, S. B. Cyber security analysis using vulnerability assessment and penetration testing. In *2016 World Conference on Futuristic Trends in Research and Innovation for Social Welfare (Startup Conclave)*, pp. 1–5 (2016). DOI:10.1109/STARTUP.2016.7583912.
- [79] SOPHOS. The State of Ransomware 2024. *Sophos*, (2024). Disponibile su: <https://www.sophos.com/en-us/content/state-of-ransomware>.
- [80] SOUPPAYA, M. AND SCARFONE, K. NIST Special Publication 800-40 Revision 3, Guide to Enterprise Patch Management Technologies. Rep. tec., U.S. Department of Commerce (2013). DOI:10.6028/NIST.SP.800-40r3.
- [81] STAFFORD, V. Zero trust architecture. *NIST special publication*, **800** (2020), 800.
- [82] STEINBERG, S., STEPAN, A., AND NEARY, K. Target Cyber Attack: A Columbia University Case Study. *Picker Center Digital Education Group at Columbia's School of International and Public Affairs (SIPA)*, (2021).
- [83] SULISTYOWATI, D., HANDAYANI, F., AND SURYANTO, Y. Comparative Analysis and Design of Cybersecurity Maturity Assessment Methodology Using NIST CSF, COBIT, ISO/IEC 27002 and PCI DSS. *JOIV : International Journal on Informatics Visualization*, **4** (2020). DOI:10.30630/joiv.4.4.482.
- [84] TEN, C.-W., LIU, C.-C., AND MANIMARAN, G. Vulnerability Assessment of Cybersecurity for SCADA Systems. *IEEE Transactions on Power Systems*, **23** (2008), 1836. DOI:10.1109/TPWRS.2008.2002298.
- [85] UFFICIO DELLE PUBBLICAZIONI DELL'UNIONE EUROPEA. Piccole e medie imprese (2022). Disponibile su: <https://eur-lex.europa.eu/legal-content/IT/ALL/?uri=LEGISSUM:sme>.
- [86] WIKIPEDIA. Colonial Pipeline — Wikipedia, L'enciclopedia libera (2012). Online; controllata il 22-Giugno-2024. Disponibile su: https://en.wikipedia.org/wiki/Colonial_Pipeline.
- [87] WIKIPEDIA CONTRIBUTORS. EternalBlue — Wikipedia, The Free Encyclopedia (2024). Disponibile su: <https://it.wikipedia.org/wiki/EternalBlue>.

Ringraziamenti

La redazione di questo elaborato è frutto di un percorso accademico, simbolo della sua conclusione, reso possibile grazie al mio impegno ma anche al supporto, all'incoraggiamento e alla vicinanza di molte persone che voglio ringraziare.

Ai miei genitori, senza i quali questo cammino non sarebbe stato possibile. Questo percorso è anche il loro, emblema del vostro sostegno nella mia vita, dato in silenzio e senza battere ciglio. Grazie per aver sempre creduto in me. Sarete sempre un luogo sicuro per me, a voi devo tutto, soprattutto la persona che sono oggi e non ci sono parole per esprimere a pieno la mia profonda gratitudine per voi.

A mia sorella, per avermi sopportato e avermi ascoltato con i dubbi più grandi. Sappi che anche se non te lo dico, ti voglio bene.

A mia nonna, che si è sempre interessata alla mia vita, a te che hai sempre cercato di spronarmi a fare meglio, a non abbandonare e a non farmi abbattere.

Ai miei amici, quelli di sempre e quelli incontrati nel cammino, ma anche a tutte le persone a me vicine. Un grazie profondo a tutte quelle chiacchierate, di pochi minuti o di qualche ora, che mi hanno ricordato la persona che sono e mi hanno motivato e aiutato a non mollare. Al tempo passato insieme e alle esperienze vissute, che hanno contribuito alla nostra crescita e a parte del nostro legame, ma soprattutto al nostro rapporto. A voi che avete sempre il consiglio giusto per me e siete sempre stati dalla mia parte.

Un ringraziamento va anche ai miei colleghi, compagni di viaggio con i quali ho condiviso molto e in cui ho trovato un appoggio, ma soprattutto un'amicizia.

Questa tesi è frutto di un mio impegno e sacrificio, che senza la vostra presenza non sarebbe stato possibile.