Università degli Studi di Padova

Corso di Laurea in Informatica

Analisi criticità e risoluzione di problematiche di rete e sicurezza in un contesto aziendale

Relatore
Prof. Claudio Palazzi

Candidato
Marco Marangon
1171128

Anno Accademico 2021–2022

Indice

Capitolo 1

Introduzione

Lo scopo di questo documento è presentare, in sintesi, il lavoro svolto presso l'azienda San Marco Informatica S.p.A. Inizialmente verrà presentata l'azienda ed, in generale, i campi di cui essa si occupa. Verrà poi introdotta la BU (Business Unit) presso cui ho svolto lo stage e di cosa si occupa, nonchè le attività svolte nello stage stesso. Verranno trattati diverse tipi di problematiche incontrate durante l'intero percorso

1.1 Individuazione e gestione criticità

I problemi che si presentano durante il ciclo di vita di un progetto sono più che problemi comuni. Si tratta infatti di situazioni che presentano una precisa caratterizzazione. Le gestione delle criticità nel project management fa riferimento a problemi formalmente definiti che ostacolano l'avanzamento dei lavori e che generalmente non possono essere risolti solo con il contributo del project manager e del team di progetto. Le procedure per la gestione delle issues, in particolare per i progetti più grandi e complessi, prevedono infatti di coinvolgere il management nel processo decisionale e richiederne le necessarie autorizzazioni.

I problemi che si presentano in maniera più o meno costante, in circostanze o per cause (seppur in gran numero) più o meno simili, a seconda della loro gravità non sono assolutamente ignorabili. Tenendo conto che diverse problematiche aventi un risultato uguale, possono avere origini molto diverse fra loro.

1.2 L'azienda

San Marco Informatica S.p.A. è un'azienda che da più di quarant'anni si occupa di sviluppo software, principalmente gestionali, e consulenza digitale. Garantisce assistenza a circa 2000 aziende diverse ed ha un capitale umano di circa 500 dipendenti. Fornisce soluzioni avanzate (di cui si occupa degli interi processi di sviluppo, distribuzione ed implementazione) per accelerare i processi interni, rendere più sicura l'infrastruttura informatica delle aziendi clienti e gestire al meglio e monitorare i flussi aziendali. L'azienda ha molteplici partner e sei diverse sedi,

delle quali le tre principali si trovano in Veneto, a Vicenza e provincia, le altre tre sono a Udine, Vimarcate e Reggio Emilia. Due delle sedi di Vicenza si trovano a Grisignano di Zocco (VI). Villa Romanelli, una villa veneta settecentesca restaurata è la sede principale ed ospita l'assistenza, SMITech ed il SOC (Security Operation Council, di cui si parlerà più in dettaglio nel corso dell'elaborato). Il Centro di Ricerca e Sviluppo si trova a pochi minuti dalla Villa in zona produttiva in un fabbricato moderno più grande dove diverse Business Unit lavorano per produrre soluzioni software gestionali, WebApp e molto altro. La terza sede, il Centro per la Formazione, si trova, invece nel territorio comunale di Vicenza, seppur non molto lontana dalle altre due sedi.

Figura 1.1: Villa Romanelli (Sec. XVIII e sec. XX)

Figura 1.2: Logo ufficiale SMI: San Marco Informatica

1.3 Struttura e suddivisione interna

L'azienda è suddivisa internamente in più subunità, dette Businness Unit (BU). Ciascuna di queste ha il proprio scopo e spettro d'interesse, il proprio personale

specializzato e la strumentazione adeguata. Le BU all'interno di San Marco Informatica sono nove:

- **JGalileo**: Software Gestionale ERP
- **NextBi**: Analisi dei dati e consulenza digitale
- **4Words**: Ecommerce, sviluppo Web, App, CRM
- **Discovery Quality**: Qualità e governance aziendale
- **ECM**: Documentazione digitale
- **SMITech**: Protezione dei dati aziendali
- **JPA**: Process Management
- **Factory**: Operations and Supply Chain
- **JPC**: Project Management

1.4 SMITech

La BU, presso cui ho svolto lo stage, è la SMITech, dedicata a migliorare la sicurezza e l'efficienza digitale dei clienti dell'azienda tramite la realizzazione di progetti di infrastrutture IT e la realizzazione di servizi gestiti di CyberSecurity. I compiti della SMITech vanno dalla consulenza IT alla realizzazione di progetti di infrastruttura, fino allo sviluppo e all'erogazione di servizi gestiti. SMITech ofrre soluzioni IBM Power, architetture IT, sicurezza informatica e GDPR e privacy.

1.5 SOC

Con l'obiettivo di fornire servizi gestiti per la sicurezza informatica ed offrire attività di monitoraggio e controllo, così da elevare il livello di sicurezza informatica dei sistemi informativi dei propri clienti, l'azienda ha costituito un proprio SOC (Security Of Council), una sub-unità all'interno della SMITech con l'importante compito di adempiere alle attività sopra citate, sia esternamente, dai clienti, che internamente all'azienda.

1.6 Tecnologie Utilizzate

Di seguito, vengono elencati e brevemente introdotti spiegando la loro funzione i vari software e tecnologie utilizzate durante il percorso di stage (tutti quanti verranno comunque approfonditi nel corso dei prossimi capitoli):

- **BKSMI**: soluzione integrata nei Power IBM delle varie aziende. L'utente BKSMI ha i privilegi di amministratore. E' utilizzato per la gestione giornaliera di errori hardware ed errori di backup, nonchè per l'installazione di dispositivi di rete (come stampanti) ed altro. Ha, inoltre, un servizio di reportistica integrato.

Figura 1.3: Menù iniziale (dopo login) di BKSMI, le operazioni possibili sono elencate numericamente

- **OpenVPN**: alcuni (non tutti) i clienti hanno un collegamento VPN diretto, realizzato tramite schede RaspBerry e Soekris e da alcuni tool e script sviluppati da alcuni operatori.Tramite il collegamento diretto è possibile collegarsi da remoto alle macchine IBM AS400 dei clienti tramite la sessione 5250, senza dover ogni volta chiamare il cliente ed avviare la sessione da un computer della sua rete aziendale avente installato il Client Access per accedere all'utility BKSMI.
- **AnyDesk e LiveCare**: software per il collegamento remoto. Sono tra i principali strumenti utilizzati per la connessione remota ai computer dei clienti quando sono necessarie manutenzioni a quella specifica postazione o se il cliente non è provvisto di un collegamento diretto con San Marco Informatica.
- **Connessione Desktop Remoto**; utilizzato per gli stessi motivi di AnyDesk, LiveCare, TeamViewer, ecc. ma, in questo caso, anche per interfacciarsi a macchine aziendali interne. Ad esempio una tramite la quale,

Figura 1.4: Logo OpenVPN

Figura 1.5: Logo AnyDesk

Figura 1.6: Logo LiveCare

mediante QLik Sense, il SOC tiene traccia dei backup di giornalieri e di sistema, segnalando eventuali errori, quali errori di tipo FTP, dovuti soprattutto a spazi pieni e connessione non riuscite, errori sul backup di alcuni oggetti (o librerie), principalmente a causa di backup mal schedulati, ad esempio in orario lavorativo, quando molti o alcuni oggetti e librerie sono ancora in utilizzo. Tutti questi errori sono possibili, ovviamente, anche nei casi dei backup settimanali e nei backup di sistema. Nel caso di questi ultimi, è necessaria un'azione tepestativa e, soprattutto, esaustiva, per arginare il problema fin da subito. Tutto ciò verrà visto più in dettaglio meglio errori hardware ed errori backup (errori HW ed errori BK rispettivamente).

- **3CX**: applicazione VoIP mobile e per Desktop. Molto utilizzata dai dipendenti di San Marco Informatica per chiamare i clienti esterni, qualora si fosse sprovvisti di un'eventuale SIM aziendale (ma anche nel caso in cui ce la si avesse a disposizione. E' usata anche per chiamare i colleghi all'interno dell'azienda e può svolgere la funzione di telefono aziendale interno. Per esempio, una persona esterna chiama il numero fisso dell'assistenza dell'azienda per parlare con uno dei tecnici del SOC, in quanto

Figura 1.7: Logo 3CX

non è a conoscenza del numero personale (aziendale) del tecnico. Tramite l'assistenza, la chiamata è inoltrata al numero del tecnico, tutto tramite 3CX. L'uso di quest'applicazione può però, talvolta, risultare fastidioso, soprattutto se si utilizzano i dati mobili, in quanto, in quest'ultimo caso in particolare, la connessione può essere più instabile, garantendo una conversazione non sempre fluida perchè avviene tramite una linea che può essere potenzialmente instabile in determinate circostanze.

1.7 Ticketing

I ticket sono, sostanzialmente, dei problemi di cui, le persone che li aprono, non conoscono la soluzione e non c'è qualcuno a loro disposizione che sappia risolverli, oppure, anche se hanno un'idea di come potrebbe essere affrontato e risolto il problema, non si applicano per timore di provocare ulteriori problematiche o, addirittura, danni (reversibili ed irreversibili). A questo proposito nascono i sistemi di ticketing. Le aziende clienti di San Marco Informatica possono disporre di tale servizio per presentare le problematiche ai tecnici. SMITech e SOC dispongono di una piattaforma su cui è possibile vedere i ticket assegnati ad esse.

1.8 Gestione clienti

Il rapporto con i clienti è stato un aspetto importante durante il corso dell'esperienza di stage. I ticket aperti, molto spesso con problematiche totalmente differenti tra loro, si svolgevano seguendo una prassi comune: chiamare il cliente tramite il contatto fornito nel ticket e farsi spiegare dettagliatamente il problema. Se il problema riguardava il Power IBM, e l'azienda coinvolta aveva il collegamento diretto tramite VPN con San Marco Informatica, si poteva evitare di contattare il cliente, interfacciandosi direttamente alla macchina e risolvendo il problema nel caso fosse di tipo già conosciuto ed affrontato più volte. Se invece si

trattava di una problematica più complessa o rara si ricercavano i tecnici aziendali preposti alla risoluzione specifica. Nel caso vi fosse la richiesta di risolvere un problema fisico, in alcuni casi si risolveva direttamente da remoto, oppure si istruiva il personale tecnico dell'azienda cliente sulle operazioni da compiere. In caso di gravi problemi alla macchina si apriva una chiamata dal sito IBM, chiedendo una possibile soluzione, o, nel caso dovesse essere sostituito/acquistato un componente, si procedeva richiedendo un preventivo ed attendendo l'accettazione da parte del cliente. Durante le chiamate, si richiedeva, preferibilmente, di parlare con l'addeto all'IT dell'azienda.

Capitolo 2

Percorso dello stage

Come già accennato , il percorso di stage è stato elaborato anche come se fosse una formazione professionale. Mediante l'utilizzo di software dell'azienda, è stato possibile imparare ad eseguire attività di monitoraggio e manutenzione.

2.1 BKSMI

Un utility molto importante nei problemi che si riscontrano giornalmente è BKSMI. Avendo i privilegi di amministratore è possibile, appunto, fare determinate operazioni di manutenzione. Tramite il servizio di reportistica, gli operatori del SOC sono aggiornati in tempo reale sulle criticità che si presentano sulle macchine dei vari clienti dell'azienda. Ossia, gli errori vengono segnalati automaticamente dai Power dei clienti tramite mail e ticket su una piattaforma ad uso interno. In questo modo, è possibile agire velocemente individuando la natura dell'errore e le cause. Per qualsiasi operazione su un Power, che non si tratti di un'installazione fisica di un componente, ad esempio una nuova NAS o rimpiazzare una vecchia batteria Cache con una nuova, è necessario interfacciarsi alla console.

2.2 SOC

Con l'obiettivo di fornire servizi gestiti per la sicurezza informatica ed offrire attività di monitoraggio e controllo, così da elevare il livello di sicurezza informatica dei sistemi informativi dei propri clienti, l'azienda ha costituito un proprio SOC (Security Of Council), una sub-unità all'interno della SMITech con l'importante compito di adempiere alle attività sopra citate, sia esternamente, dai clienti, che internamente all'azienda.

2.3 Ticket SOC: Criticità a livello Power IBM

Queste problematiche sono spesso relative all'hardware di un Power o al software di BKSMI. I ticket di competenza del SOC non sono solo relative alle aziende

clienti esterne, ma vi è anche l'apposita unità interna che si occupa dell'installazione, manutenzione e, se necessaria, rimozione, dei dispositivi interni a San Marco Informatica S.p.A. Il setup e la manutenzione dei PC (Personal Computer) dei dipendenti è di loro responsabilità, cos Gli errori, a livello Power sono molto comuni, sono presenti giornalmente e se non sono trattati con il dovuto riguardo in tempi più o meno ragionevoli, possono portare a serie problematiche, di integrità e di sicurezza, all'interno dell'azienda il/i cui Power IBM sta/stanno riscontrando criticità. Le problematiche hardware possono essere visualizzate tramite il comando *WRKPRB*. Per praticità, nell'iTech, vengono composte, e salvate, delle query, il cui compito è selezionare tutti i ticket che, sodisfano determinati requisiti nei loro attribbuti. Possono chiaramente essere aggiunte nuove query, salvate o essere usate temporaneamente, queste ultime chiaramente sono "volatili". in quanto ad ogni refresh vengono perse.

2.3.1 Errori Hardware (Errori HW)

Queste anomalie riguardano tutti i componenti hardware della macchina. Tali errori sono segnalati, come già detto, all'assistenza ITech. Talvolta, se l'errore è grave o non lo è ancora ma rischia di portare gravi conseguenze (come errori sui dischi o su componenti hardware fondamentali). Gli errori HW possono essere dovuti a moltissime cause. Alcune di queste sono:

Anomalie della corrente elettrica

Fra gli errori più comuni vi si trovano gli errori dovuti ad interruzioni e sbalzi di corrente, come gli errori SRC110000AC e SRC11001510 (in generale, gli errori che iniziano con 110 vengono segnalati come anomalie dovute a sbalzi/perdita di corrente.

La segnalazione viene poi chiusa. A seconda del tipo di errore e della gravità, si decide se sia opportuno segnalare il problema al cliente o meno. Queste anomalie vengono segnalate anche dal Power tramite il LED SST, ossia un LED arancione, che si accende quando ci sono anomalie dovute alla corrente. In seguito, la prassi è chiudere le nuove segnalazioni e premere il tasto F6 "Acknowledge all errors". Successivamente, il LED SST si spegne. Spesso questo tipo di problema non è causa di forti preoccupazioni, ma se continua a ripresentarsi viene aperta una chiamata IBM tramite il sito *https://www.ibm.com/mysupport/*, dove si riporta il codice SRC dell'errore e l'unità della macchina coinvolta, descrivendo brevemente ma in modo incisivo il problema che è stato riscontrato. Si lasciano un contatto di chi ha aperto la chiamata e del cliente. Quest'ultimo viene in seguito informato dell'apertura della chiamata tramite telefonata o mail, in modo da informarlo che verrà contattato dal supporto IBM in futuro.

Anomalie della temperatura

Un altro errore comune che viene segnalato si ha quando il power rileva delle temperature superiori ad una certa soglia.

Errori relativi alla linea

Questo tipo di segnalazione di errore hardware fa riferimento ad uno scollegamento dalla rete. Un comune codice d'errore è SRCB025A6E3. Spesso, la causa è un semplice distacco dalla rete. Spesso, la causa è attribuita al sol distacco dei cavi Ethernet, ma la segnalazione può presentarsi anche dopo un distacco dalla rete dovuto a problemi di connessione non relatvi all'azienda. La causa descritta nella segnalazione del problema è, però, la stessa. La descrizione della problematica contiene il messaggio:
Problema = xxxxxxxxxx *La linea ETHLINE è in errore. Avviato il*
automatico. Solitamente basta chiudere la segnalazione del problema tramite il comando *WRKPRB*, in quanto la linea si riattiverà automaticamente nella maggior parte dei casi.

Errori relativi agli utenti

Errore che viene segnalato quando un utente sbaglia troppe volte le credenziali d'accesso. La correttezza delle parole d'ordine è verificata tramite collegamenti a dei server (ad esempio a dei server FTP) e delle chiamate API quali QSYGETPH (Get Profile Handle). Qualora l'utente aabbia effettivamente sbagliato le credenziali troppe volte, questi viene disabilitato, chiedendo, nella segnalazione d'errore al SOC, un ripristino dello stato dell'utente. Per riabilitare l'utente si usa il comando CHGUSRPRF, ed in seguito si setta ad *ENABLED l'attributo STATUS.

2.3.2 Errori Backup (Errori BK)

I backup sono il più delle volte programmati per essere giornalieri, settimanali e di sistema. I backup di sistema sono più pesanti e lunghi e talvolta li si imposta perchè avvengano su nastro. Uno degli aspetti più importanti dell'impostazione dei backup è la schedulazione di quando questi avvengono, cioè in che orario e, nel caso del backup settimanale e di sistema, in che giorno. I backup di sistema vengono talvolta salvati in una Nas apposita, raggiungibile tramite un server ftp. Alcuni errori backup sono dovuti al fatto che la Nash sia piena, in tal caso si avvisa il cliente del fatto e gli si propone una soluzione. Gli errori backup vengono segnalati quando una o più librerie od oggetti non vengono salvati correttamente. Anche qui, i motivi del salvataggio fallito possono essere molteplici, la maggior parte si possono raggruppare in:

Oggetti in utilizzo durante il salvataggio

Si tratta di un errore che capita quando alcuni oggetti e/o librerie sono ancora in utilizzo durante la fase di backup. Questo, come già precedentemente acceennato, è semplicemente dovuto a personale che non rispetta i tempi di schedulazione del backup del Power.

Backup fallito per spegnimento Power

Questo tipo di errore deriva dal fatto che il Power è programmato per spegnersi durante il backup, quindi si tratta di un errore umano di malconfigurazione.

Spazio insufficiente

Chiaramente, se lo spazio è insufficiente il backup non viene completato e le librerie non sono salvate o lo sono solo parzialmente.

Backup schedulato durante spegnimento Power

Questo errore è dovuto principalmente alla disattenzione. Il salvataggio è schedulato per un orario in cui il Power viene spento, di conseguenza, il salvataggio non avverrà o si fermerà al punto dove era arrivato prima dello spegnimento.

Errore FTP

Questo tipo di errori accade quando c'è un tentativo di connessione verso il server ftp dove verrebbero salvati in esterno le librerie, ma per diversi motivi il server non può essere raggiunto.

2.4 Ticket Itech (Help-Desk Itech): Criticità a livello software

I ticket ricevuti dall'Itech riguardano principalmente problematiche riguardanti i prodotti software di San Marco Informatica e richieste di aiuto per la risoluzione di problematiche legate a dispositivi hardware (stampanti soprattutto) o ad altri software. Un altro gran numero di ticket ITech riguarda interventi di manutenzione, modifiche ad alcuni parametri, aggiornamenti e risoluzione di problematiche normalmente presenti nei ticket SOC HW e BK. Più in dettaglio, si possono suddividere una notevole parte di ticket trattati durante il mio percorso di stage, nei seguenti gruppi:

Supporto per installazione Client Access per utilizzo VPN diretta

Per poter utilizzare la VPN diretta con S. Marco Informatica è necessario che vi sia un preventivo per l'installazione di alcune schede RaspBerry o Soekris e poi i tecnici dell'Itech installino il Client Access cosìcchè in futuro, se si presentano problematiche per cui bisogna accedere al Power, non sarà necessario chiamare il cliente per farsi interfacciare al un computer con la sessione 5250 installata, ma si potrà accedere direttamente da remoto a tale terminale.

Problematiche relative a stampanti

Le stampanti sono i dispositivi più comunemente oggetto di ticket Itech, talvolta si tratta di richieste d'installare i dispositivi nel Power aziendale, come sessione di stampa e anche come stampanti di rete, altre volte di risolvere alcuni problemi. Diversi ticket infatti sono dovuti a richieste di aiuto per stampanti che eseguono la stampa in modo anomalo (es. stampa di barcode in modo incompleto, stampa impossibile da eseguire e altre problematiche simili).

Problematiche relative a Power

Le problematiche relative al Power sono criticità segnalate sia tramite i ticket SOC che all'Itech, questo perchè al tecnico aziendale sembrano problemi gravi. Talvolta si tratta di questioni di semplice risoluzione (es. spegnimento di led SST, risoluzione tramite comandi specifici e altri problemi che potevano essere indirizzati al SOC anzichè all'Itech).

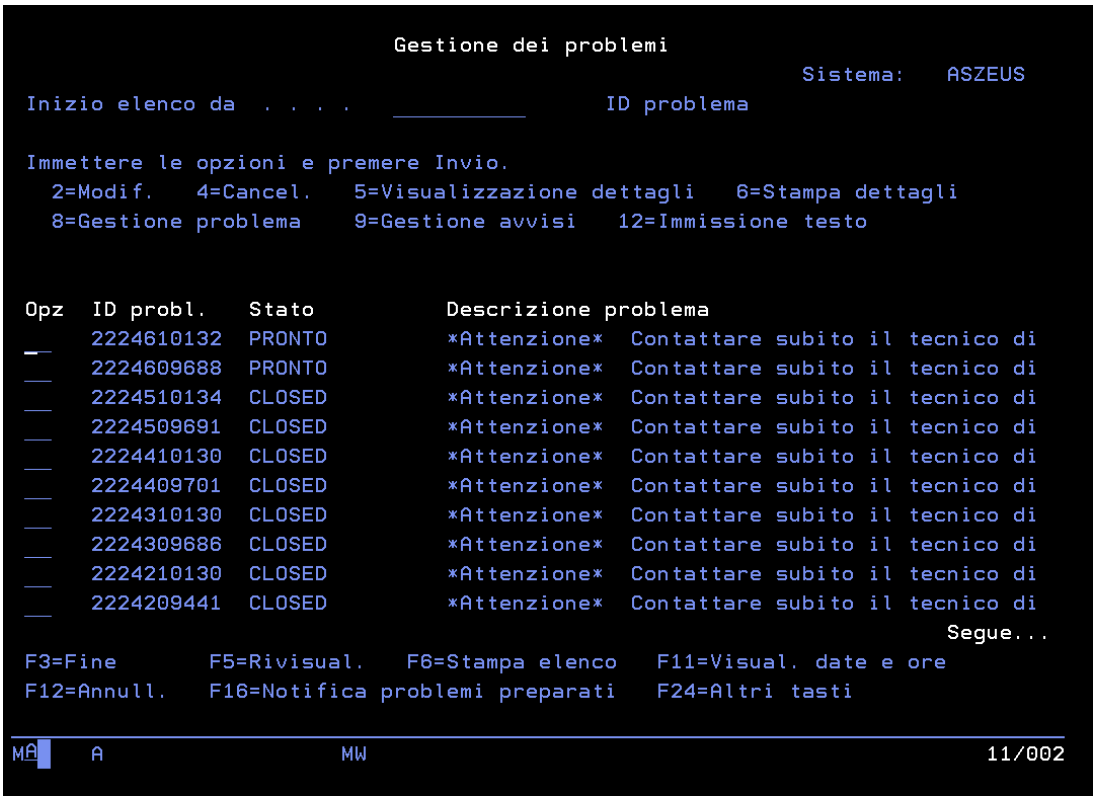


Figura 2.1: Contenuto visibile dopo l'esecuzione del comando WRKPRB in un Power IBM tramite BKSMI, con descrizione del problema

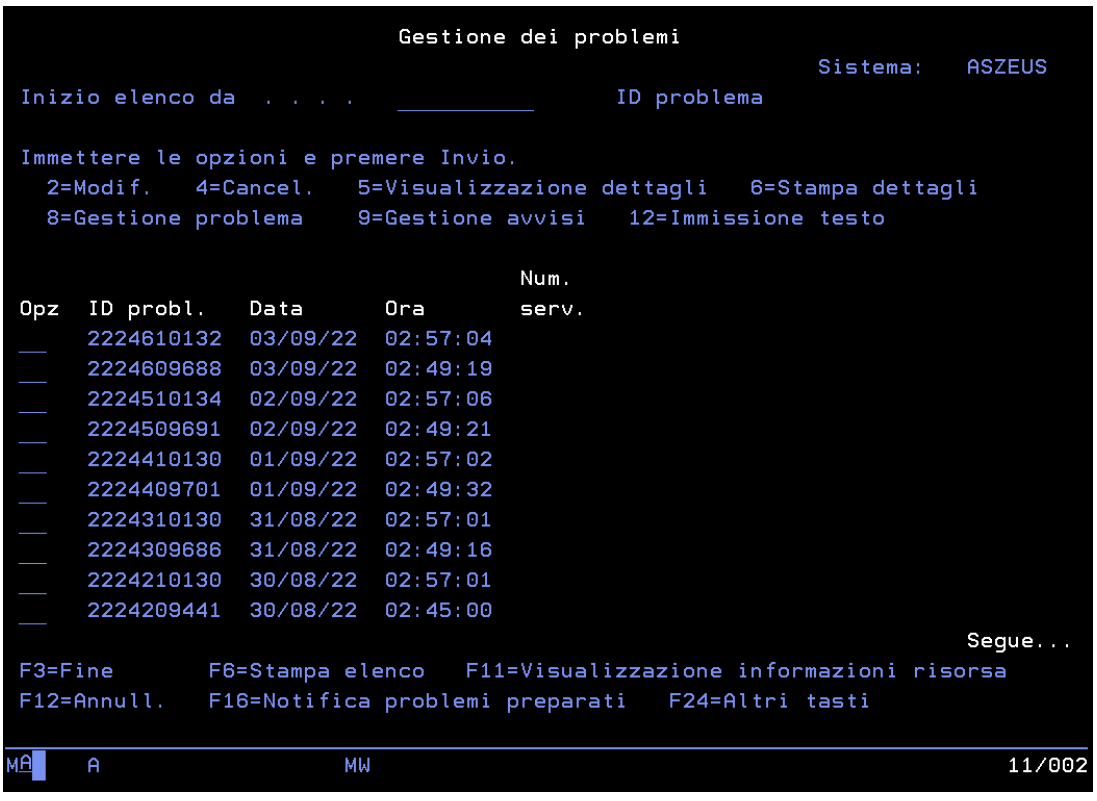


Figura 2.2: Cliccando F11 una prima volta, nella schermata compaiono la data e l'ora in cui si è verificato il problema, al posto della descrizione

Figura 2.3: Cliccando F11 una seconda volta, nella schermata compare la SRC del problema che si è verificato, sempre a fianco dell'ID del problema, ed anche l'identificativo della risorsa coinvolta, se per caso la problematica riiguarda una particolare unità. Con le SRC, i tecnici controllano, tramite il sito e la documentazione IBM, il significato ed eventualmente la procedura risolutiva del problema

Capitolo 3

Problematiche di rete

3.1 Sicurezza infrastruttura di rete

3.1.1 Definizione

La sicurezza di un'infrastruttura di rete dipende da tutte le tecnologie e soluzioni utilizzate. Quando reti e sistemi informativi non sono protetti in modo idoneo, dati e informazioni sensibili rischiano di essere esposti al rischio di attacchi. Per tale motivo, è fondamentale comprendere appieno che cosa davvero significhi Network Security, a quali concetti rimanda e quali sono le misure che le aziende possono adottare per una puntuale strategia di sicurezza. Tali soluzioni, nell'attuale panorama di minacce informatiche, diventano preziose per fare fronte alle vulnerabilità che ogni organizzazione, indipendentemente da dimensioni, settore di appartenenza e tipologia di infrastruttura adottata, presenta. Pratiche e processi adottati per prevenire, rilevare e monitorare gli accessi non autorizzati e l'uso improprio di una rete di computer – sia pubblica che privata – e delle risorse accessibili dalla rete, sono indispensabili per garantire un grado soddisfacente di sicurezza ed un flusso tranquillo delle operazioni aziendali. Inoltre, due fattori esterni hanno influenzato molto l'atteggiamento sulla sicurezza: l'avvento del GDPR nel 2018, che ha imposto determinati adempimenti allo scopo di accrescere la consapevolezza sull'importanza strategica della sicurezza delle reti e della protezione di dati (di cui si parlerà nel prossimo capitolo), e l'avvento dello Smart Working dovuto alla pandemia che, dato il maggior tempo nel quale i dispositivi sono connessi ed anche l'aumento del numero di persone che utilizzano tali dispositivi.

3.1.2 Esempi di criticità e problematiche

Nel corso del percorso formativo è stato possibile risolvere molteplici tipi di problematiche in seguito a tickets di segnalazione e, talvolta, anche individuarne qualcuna e segnalarla alla persona/reparto competente. Fra questi, problemi sulla configurazione del firewall aziendale, sui criteri antivirus

3.1.3 Alcune soluzioni

Una rete cui si vuole dare l'appellativo di sicura, dovrebbe, innanzitutto, considerare una "buona norma", ossia la suddivisione in "strati" (o *layers*) di una rete. Una possibile suddivisione può essere:

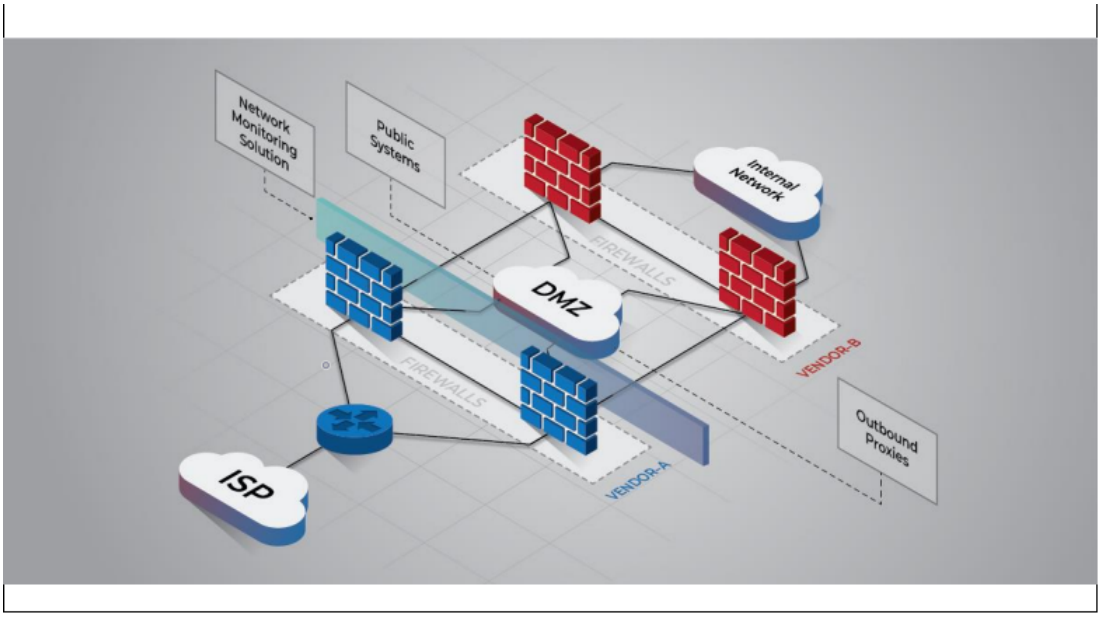
- ***Sicurezza fisica di una rete***: l'obiettivo è prevenire l'accesso ai dispositivi fisici di un'azienda, dalle fonti di corrente ai dispositivi, come switch e router ma anche ai singoli computer.
- ***Sicurezza tecnica di una rete***: ha a che fare con i dispositivi facenti parte della rete ed i dati già memorizzati in essi o i dati che lo saranno nel breve e/o lungo termine. Ha il compito di prevenire l'accesso a tali dispositivi/dati da parte di utenti non autorizzati/malintenzionati, interni od esterni all'azienda.
- ***Sicurezza amministrativa di una rete***: si occupa di definire delle polizze ed alcune norme di comportamento sul comportamento dell'utente mentre utilizza un dispositivo connesso alla rete.

Ciascuno di questi strati dovrebbe mettere in campo alcune precauzioni ed implementare soluzioni atte a prevenire l'accesso ai dati da persone/utenti non autorizzati. Per quanto riguarda la *Sicurezza fisica*, le misure da adottare devono quindi prevenire l'accesso fisico, ciò può richiedere l'utilizzo di più risorse umane o di utilizzare i dati personali degli utenti autorizzati all'accesso. Alcune di queste misure sono:

- **Personale di sicurezza**.
- **Blocchi fisici** come, ad esempio, serrature aventi una chiave che solo alcuni individui possiedono, e serrature magnetiche che richiedono un badge o altre misure per aprirsi.
- **Utilizzo di dati biometrici** (come ID magnetiche (o in alcuni casi non, in caso l'accesso sia regolato solamente da personale), scansione facciale, dell'impronta digitale, della retina e diverse altre).

Per garantire il più possibile la *Sicurezza tecnica* di una rete, è fondamentale applicare i giusti accorgimenti durante il suo design e progettazione. Come già accennato, è molto utile progettare la rete in modo che sia multistrato, ossia con molteplici strati disicurezza. Per la protezione da minacce esterne è consigliabile limitare il traffico inbound ed outbound della rete. L'installazione e configurazione di dispositivi e software di sicurezza come router aggiuntivi, più layers di firewall hardware e/o software per il nel perimetro della rete. E' consigliabile che ogni layer utilizzi soluzioni di vendor differenti, così da prevenire che vengano utilizzati eventuali exploit che mirano a sfruttare vecchie versioni non ancora patchate o vulnerabilità Zero-Day siano sfruttate, vanificando la suddivisione in layers. Non meno importante è l'utilizzo di subnet DMZs (De-Militarized Zones), in modo che l'accesso possa essere adeguatamente controllato

fra i dispositivi esterni, i dispositivi DMZ ed i sistemi interni, creando dunque una zona intermedia. L'implementazione di soluzioni *NIDS (Network Intrusion Detection System)* per monitorare il traffico inbound ed outbound che producano log in particolari server dedicati (uno o più a seconda del livello di sicurezza che si desidera ed anche dall'intensità del traffico) controllando così eventuali movimenti laterali e permettendo la correlazione di attività fra i dispositivi è un'altra azione consiglisata, così come l'aggiunta di dispositivi di ridondanza in alcune aree chiavi della rete in modo da assicurare la disponibilità di tutti o determinati servizi, diminuire la latenza ed aumentare il throughput di rete.



Network perimeter with firewalls and a DMZ

Sistemi simili dovrebbero essere logicamente raggruppati assieme. Questo perchè un presunto attaccante, tendenzialmente, prende di mira dispositivi che può facilmente sfruttare (come le stampanti), tramite exploit, per avere accesso poi agli altri sistemi. Come detto sopra, una buona pratica è raggruppare simili sottosistemi in gruppi logici separati. In questo modo sarà anche più semplice implementare differenti restrizioni d'accesso per differenti sottosistemi della rete, oltre che rendere più facile la loro gestione, il controllo ed il monitoraggio. Per dividere la rete in sottosistemi si ricorre all'uso di sottoreti o di VLANs (Virtual Local Area Networks) oppure separare fisicamenti tali sottositemi tramite firewall o router secondari con azione di "filtraggio". Workstation, server, stampanti, tecnologia operativa e sistemi di telecomunicazione dovrebbero essere raggruppati in sottosistemi differenti. In un modello di architettura di rete incentrata sulla sicurezza importantissimi sono i router perimetrali. Questi implementano degli ACL (Access Control List, servono a regolare il traffico in ingresso e in uscita) con un set di regole specificamente configurato per permettere solo sistemi e servizi necessari alla rete aziendale. Un buon approccio è quello che in inglese si dice *deny by default, allow by exception.* Tale approccio viene applicato prestando particolare attenzione quali connessioni permettere e, di conseguenza, creare un set di regole che permetta automaticamente lo stabilire queste connessioni.

Qualora la rete ziendale sia stata architettata ed implementata in precedenza, i controlli e gli eventuali aggiustamenti da apporre per garantire la sicurezza della rete non vanno sottovalutati. Alcune buone pratiche possono essere:

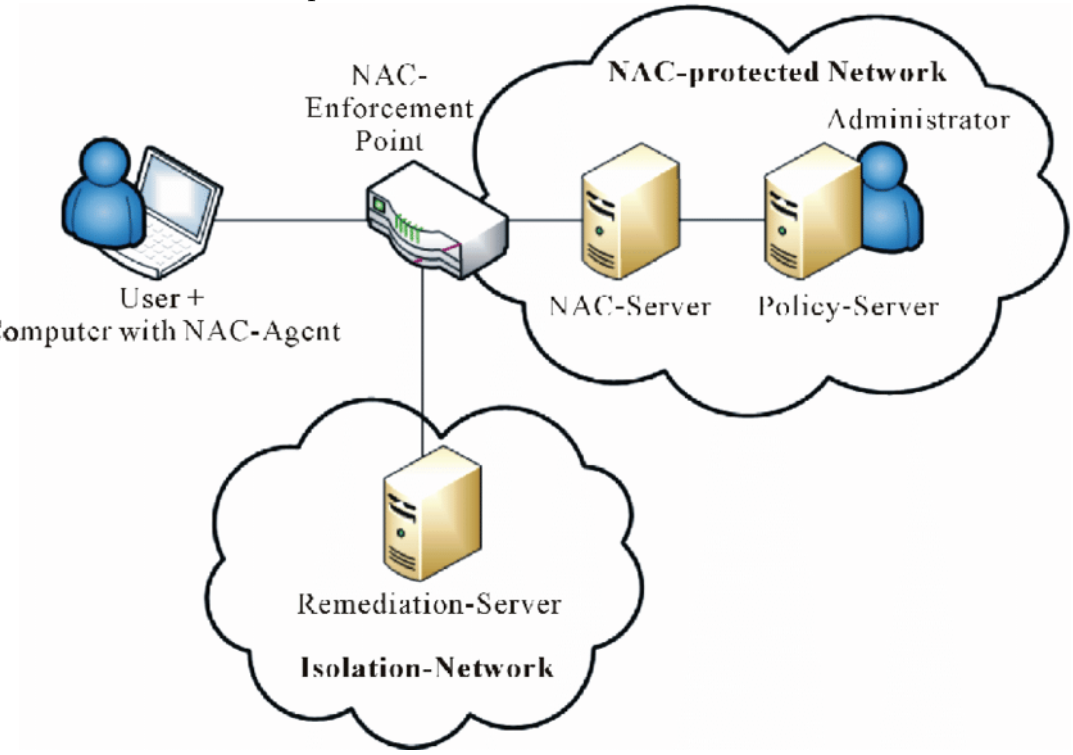
- *Network Audit*: è il primo step da fare per identificare eventuali debolezze della rete. Una Network Audit identifica la presenza di eventuali vulnerabilità nella rete, controlla se vi sono applicazioni non necessarie o inutilizzate, la presenza di porte aperte, controlla la presenza di Anti-Virus/Anti-Malware e di backup. Inoltre, un Software Audit sui software di terze parti è utile per verificare l'esistenza di altre vulnerabilità.
- *Utilizzare soluzioni per la sicurezza della rete*: l'uso di firewall e WAF (Web Application Firewall) sono estremamente consigliate per la protezione del sito web aziendale da attacchi, così da garantire una memorizzazione sicura dei dati. Per mantenere alto il livello di sicurezza, la messa in campo di misure quali sistemi di rilevamento e prevenzione delle intrusioni (IDS, Intrusion Detection System e IPS, Intrusion Prevention System)
- *Disabilitare la condivisione di file*: è consigliabile usare questa funzione solo su determinati server privati ed indipendenti. Nonostante sia spesso attivata, la condivisione di file dovrebbe essere disabilitata nei computer dei dipendenti, se non in particolari occasioni.
- *Software Anti-Virus ed Anti-Malware sempre aggiornati*: le macchine dei dipendenti, una volta acquistate, contengono già questi software, spesso però non vengono tenuti aggiornati. Si dovrebbe dunque avere questi programmi sempre aggiornati con gli ultimi fix usciti ed aggiornamenti di sicurezza.
- *Prestare attenzione alla sicurezza del router*: per evitare che avvenga una potenziale manomissione fisica del router (ex. spegnendolo), che può causare enormi danni al"azienda, è consigliabile tenere i dispositivi più importanti in stanze separate ed accessibili solo da determinato personale autoriizzato. La sorveglianza delle stanze è altrettanto consigliabile. Inoltre, andrebbero cambiate le password ed il nome di default delle reti. In tal modo, lo sforzo per provare ad indovinare le credenziali tramite brute-force è molto ridotto. L'ideale sarebbe avere i router in una o più stanze accessibili solo da personale autorizzato e/o strumenti di sorveglianza come telecamere che monitorano il flusso di persone ed eventi così che gli operatori possano agire tempestivamente e/o abbiano prove su come si è svolto un determinato evento. Talvolta, viene impiegato anche personale speciale, come guardie di sicurezza. Queste misure però, in particolare l'ultima citata, si impiegano "efficientemente" e quando fortemente necessarie. Ad esempio, i sistemi di controllo delle tecnologie operative industriali dovrebbero essere separati dagli altri sottosistemi dell'azienda, ed in paticolar modo da potenziali vettori di minacce, come Internet. Inoltre, vengono impiegati a seconda dell'importanza che l'azienda attribuisce alle proprie macchine ed i dati in essi (diverse aziende si dimostrano negligenti in quest'ambito ed in altri) e, sempre in primo piano, alla grandezza e fatturato dell'azienda. Gli

ultimi metodi sopra descritti, infatti, sono tipicamente limitati ad aziende molto grandi, con molti dipendenti e con un fatturato non indifferente.

- *Utilizzare IP privati*: ai server ed ai dispositivi più importanti nella rete aziendale, dovrebbero essere assegnati IP privati. Questo permette all'amministratore dell'IT di tenere traccia di tutti i tentativi di connessione non autorizzati da parte di determinati dispositivi (quindi, ovviamente, dautenti). Questo gli permette di analizzare i log e tutte le informazioni a disposizione per comprendere di che tipo attività si trattano ed agire nel modo più adatto. Per quanto riguarda la CyberSecurity, concernente Internet soprattutto, utilizzare IP privati è più sicuro che utilizzare IP pubblici, in quanto gli IP privati non sono direttamente visibili da Internet e si trovano oltre la NAT, che assicura ..... Usando un IP pubblico per i dispositivi sensibili appena citati
- *Istituire un sistema di gestione, controllo e manutenzione della sicurezza di una rete*: ad esempio un sistema che svolge automaticamente, tramite scripts o applicazioni con schedulazioni apposite. L'utente viene avvisato con adeguato anticipo, della programmazione di ogni quanto cambiare credenziali l'aggiornamento dei software (gli aggiornamenti dell'OS e delle applicazioni native di Windows, ad esempio, vengono schedulati automaticamente da Microsoft) i backup dei dati dei server, dei computer, ecc, come BKSMI, tramite cui si controlla e si programma i backup dei power IBM delle aziende clienti di San Marco Informatica S.p.A. di cui si è parlato nel capitolo stage. L'importanza del mantenere aggiornati i sistemi operativi ed i software di manutenzione (così come Anti-Virus ed Anti-Malware) è dunque, ancora una volta, ribadita, in quanto un attaccante può sfruttare qualsiasi vecchio bug non patchato e prendere il controllo del dispositivo introducendo software malevolo, eseguendo il proprio codice tramite caricandolo ed eseguendolo tramite gli esegubili già in memoria (è il caso delle Shellcode o di attacchi con DLL Injection) o addirittura modificando il file-system ed il bootloader del dispositivo (dunque con modifiche a livello kernel), ottenendo così il totale controllo del device.
- *Segmentazione di una rete*: suddividere la rete in molteplici sottoreti rende più facile e rapida la loro manutenzione e la loro analisi sulla sicurezza. In caso di criticità, ad esempio un tentativo di intrusione, ci si può concentrare solo sul sottosistema che presenta il problema, in quanto questo è isolato e l'impatto che l'episodio può avere sull'intera rete aziendale è ridotto, così come i rischi di un'intrusione in altri sottosistemi e su larga scala, in quanto l'attaccante dovrebbe fare molti più sforzi.
- *Educazione del personale (anche non specializzato) sul tema della CyberSecurity*: un particolare spesso trascurato, ma non per nulla di secondo piano, è l'educazione del personale, soprattutto quello non competenti in materia/non specializzati. Se sprovvisti dellla minima conoscenza tecnica e non a conoscenza delle basilari buone norme di condotta in materia di cyber sicurezza, i normali utenti di un'azienda possono andare incontro a serie minnacce per i loro dati personali e per quelli dell'azienda. Pos-

sono, inoltre, essere delle minacce a loro volta. Si pensi, ad esempio, ad un utente, dunque molto probabilmente un dipendente dell'azienda stessa, che, nonostante le raccomandazioni di non eseguire il download di nessun allegato da una mail sospetta e, oltretutto, nonostante l'AntiVirus avvisi l'utente della possibile pericolosità del file allegato, l'utente persiste nel download e, una volta completato, apre il file, che risulta essere un malware trojan, con capacità di worm e che sfrutta uno o più exploit 0-day (ossia un exploit, o vulnerabilità, non ancora documentato), ad esempio uno sulle funzionalità di file sharing di Windows. Dopo un episodio come questo, la sicurezza della rete è compromessa. Nonostante l'esempio sia un caso abbastanza estremo, dimostra come l'errore umano, dovuto alla negligenza/scarsa conoscenza, possa portare a condizioni molto serie, pericolose e compromettenti.

- *Implementare soluzioni NAC (Network Access Control)*: in sostanza, una soluzione NAC usa un insieme di protocolli che definiscono e implementano delle politiche che descrivono come effettuare un accesso sicuro ai nodi della rete da parte dei dispositivi, quando questi tentano di accedere alla rete. Ha lo scopo di controllare l'accesso a una rete con policies, inclusi i controlli dei criteri di sicurezza dell'endpoint pre-ammissione e controlli post-ammissione su dove utenti e dispositivi possono andare su una rete e cosa possono fare. Una NAC previene connessioni fisiche non autorizzate in una rete e monitora quelle autorizzate.



L'implementazione di un'adeguata soluzione NAC che identifichi e autentichi unici dispositivi alla rete, affiancata ad una funzionalità di Port Security, implemenetata negli Switch ed utilizzata per controllare, tramite gli inidi-

rizzi MAC (Media Access Control) dei vari dispositivi (ogni dispositivo ne ha uno unico ed immutabile), qualora ve ne siano di connessi alla rete ma non autorizzati. La Port Security, pur essendo un buon metodo, presenta anche degli inconvenienti, primo su tutti la difficoltà nella gestione, che può comportare disagi di varia natura. Fra questi, ad esempio, aumenta il rischio di incontrare difficoltà nella semplice navigazione a causa di possibili porte necessarie bloccate o "trafficate" per varie valide ragioni. Ad esempio, le sale conferenze potrebbero ospitare dispositivi che stabiliscono la loro connessione su porte comunemente usate, dunque può risultare che non si riesca a stabilire nuove connessioni su queste porte, oppure, situazione più probabile, che queste abbiano già un gran flusso di dati che passi da loro e che dunque il traffico risulti più rallentato. Problemi come questo e simili, comportano un aumento del flusso di ticket assistenziali che chiedono, appunto, un rapido ripristino delle "condizioni di traffico" precedenti. Episodi come questo, cioè l'aumento del flusso di ticket di questo tipo, sono fenomeni ordinari a San Marco Informatica S.p.A., e spesso vengono reindirizzati al SOC o allo SMITech come ticket SOC o ticket SMITech, di cui si è, per l'appunto, discusso nel capitolo iniziale. Un'altra "pecca" di un meccanismo di Port Security mal implementato è che, se un attaccante è in grado di portare a compimento con successo la tecnica dello *MAC Spoofing* (in cui, in parole povere, un attaccante è in grado di "mascherare", a livello software, l'indirizzo MAC che, come già accennato, non è modificabile in alcun modo), allora esso è potenzialmente in grado di bypassare anche il meccanismo di Port Security. Unq soluzione più robusta utilizza il protocollo IEEE 802.1x, basato sul controllo d'accesso delle porte MAN e WAN. I dispoositivi sono autenticati utilizzando un certificato digitale riconosciuto, intallato con il device

- *Limitare l'utilizzo di VPNs (Virtual Private Networks*: un tunnel VPN viene stabilito fra due endpoint per garantire un canale di comunicazione criptato utilizzando una rete, ossia un canale criptato all'interno di una rete. invece che imporre un divieto, completo o parziale, delle VPN, come fanno diversi governi ultra-autoritari, che spesso sono molto utili, se non estremamente consigliate in alcune occasioni, ironia della sorte, proprio se, per qualsiasi motivo si ha a che fare con determinati governi o organizzazioni come appena accennato. Dunque, la scelta di utilizzare una VPN è dovuta dalla necessità di avere garanzia della confidenzialità e dell'integrità del traffico, qualora non vi siano altre strategie che garantiscano la stessa sicurezza ed affidabilità. Non è da sottovalutare il fatto che i gateway VPN sono accessibili da Internet, dunque suscettibili a Network Scanning, attacchi brute force sulle credenziali. Inoltre, fattore spesso trascurato ma che può rivelarsi fonte di grandi criticità: essendo le VPN, molto spesso, dei software di terze parti, essi possono anche essere frutto di una società malintenzionata che all'interno del codice del Client VPN da loro prodotto e distribuito/venduto può avere introdotto una BackDoor (la storia dell'informatica contemporanea annovera più di una di queste imprese) con l'in-

teresse di carpire i dati personali degli utenti dove viene installato il Client e usarli per gli scopi più disparati, a seconda dalla quantità e dall'entità dei dati raccolti. Possono essere usati per fare Carding ossia utilizzare dati delle carte di credito altrui per fare acquisti seguendo diversi schemi per non essere rintracciati, o anche per fare Doxxing, cioè pubblicare informazioni sensibili su di un individuo, ente, attività o altro, dalle generalità ed indirizzo di residenza/domicilio, all'indirizzo IP, ecc. (talvolta il doxxing può essere usato anche per scopi ricattativi/vendicativi). Un'altra legittima preoccupazione per la sicurezza della rete aziendale, quando si installano Client VPN, come già accennato in altre parti del capitolo, è che essi siano vulnerabili ad attacchi di tipo 0-day. Da questi ultimi non ci si può difendere a meno che non siano stati scoperti da noi stessi o da un dipendente dell'azienda, che ha prontamente o sviluppato un aggiornamento (patch o fix) che sistemi la problematica, tamponando o sistemando la vulnerabilità o informando tempestivamente la casa produttrice. Un caso del genere è più unico che raro, a meno che l'azienda che abbia installato il client VPN vulnerabile non si tratti di un'attività specializzata in ingegneria riversa, analisi e debugging. Per prevenire eventualità come quelle descritte finora e mitigare più debolezze possibili, innanzitutto, come già ribadito, si mantengono aggiornati il più possibile il Sistema Operativo e le applicazioni (in particolar modo Anti-Virus e Anti-Malware e Client VPN), si disabilitano tutte le funzionalità non strettamente necessarie nei Gateway VPN e si implementano regole di filtraggio del traffico di rete. Se possibile, queste regole di filtraggio, che valgono per tutto il traffico di rete, andrebbero accoppiate a misure che restringono quanto può passare tramite proxy o VPN, come limitare l'accesso al gateway VPN a sole determinate porte (ad esempio la porta UDP 500). Se possibile, inoltre, limitare il traffico accettato verso gli IP di Provider VPN.

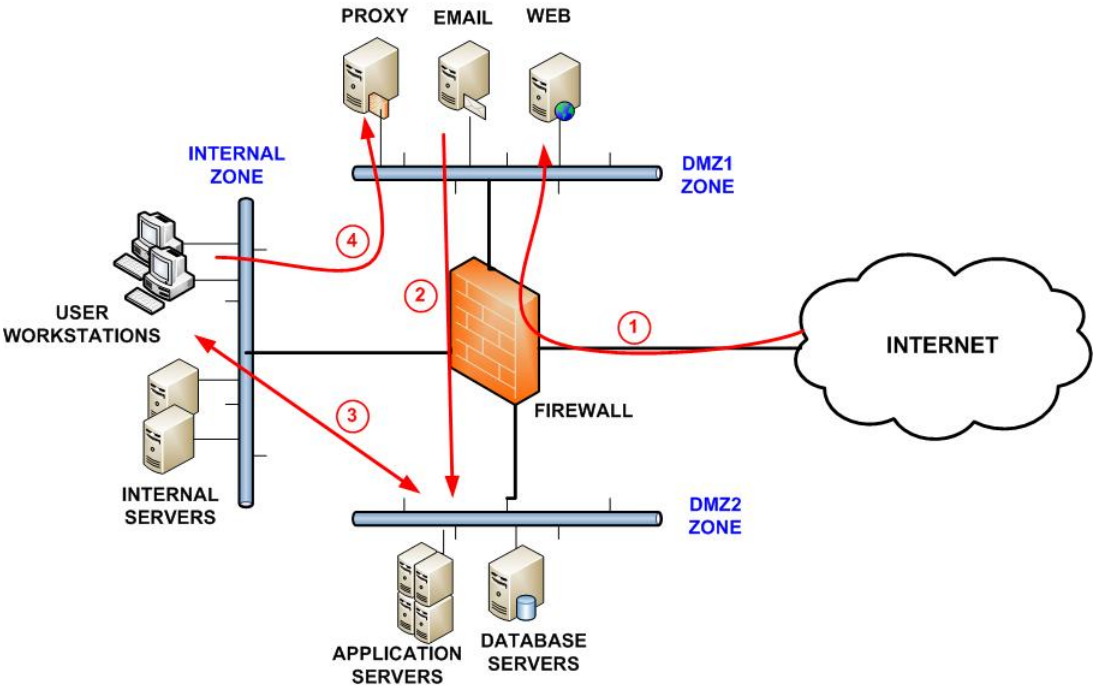


Figura 3.1: Schema di una rete avente una soluzione NAC implementata, con schema di autenticazione da parte di un utente esterno

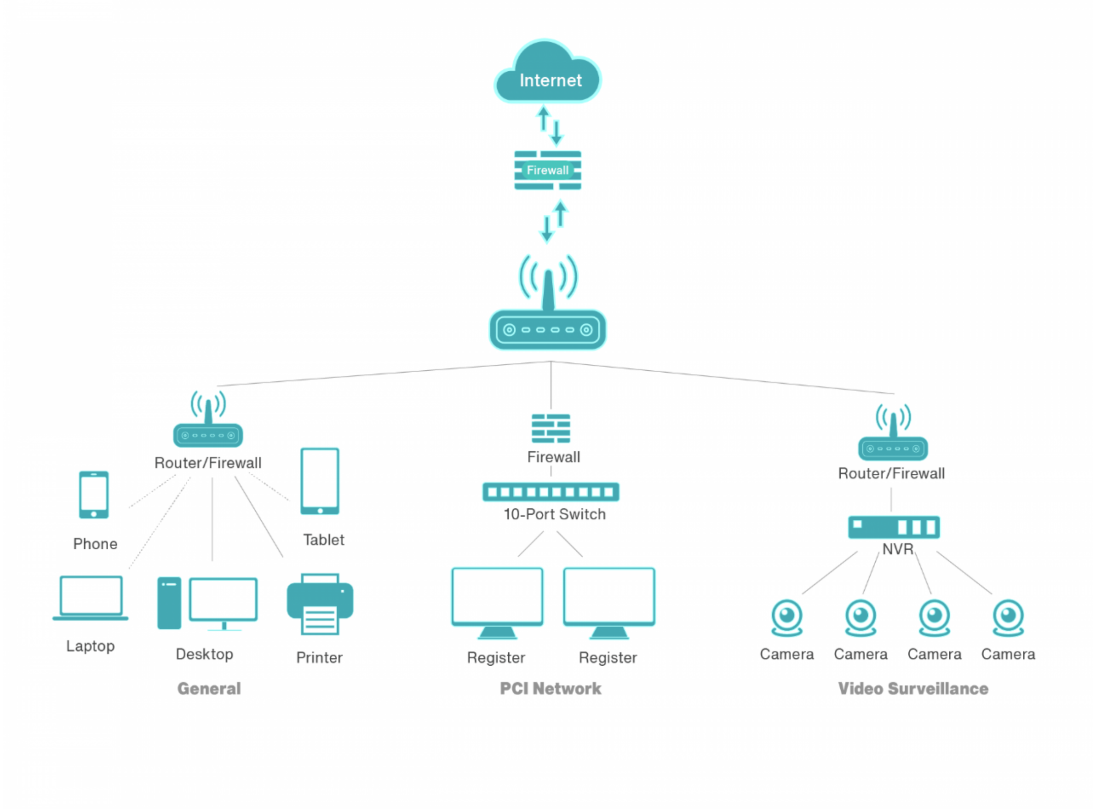


Figura 3.2: Esempio di rete *"ad architettura piatta"*. E' così chiamata in quanto non vi è nessun firewall o separazione logica fra i dispositivi della rete, questi possono comunicare liberamente fra loro. Questo tipo di architettura era diffuso negli anni '90 e primi 2000 quando pochissimi telefoni mobili possedevano un browser e tutte le funzionalità necessarie per navigare in Internet ed usufruire di tale browser. Inoltre, non c'erano router WiFi e l'IoT ed i dispositivi connessi.

Capitolo 4

Sicurezza aziendale

4.1 Sicurezza dei dati

4.1.1 Definizione

Per sicurezza aziendale non si intende solo la protezione da fattori esterni quali attacchi informatici, malware, ransomware, furti, ecc, ma anche perdite e/o problemi dovuti ad errori umani, come l'impropria gestione dei salvataggi, backup ed anche negligenza nel controllare lo stato delle macchine.

4.1.2 Esempi di criticità e problematiche

I dati sono una realtà fondamentale ed essenziale per una qualsiasi attvità, chiaramente anche in base alla loro natura ed entità. Al giorno d'oggi, gli attacchi si fanno di giorno in giorno molto più sofisticati. Ad esempio, un gruppo di attaccanti con intenzioni malevole nei confronti di una grossa compagnia, possono ottenere una lista delle aziende clienti, controllare i rapporti che hanno con l'azienda obiettivo e ispezionare la loro rete, i loro dati e le loro misure di sicurezza in generale alla ricerca di vulnerabilità da sfruttare e guadagnare l'accesso a ciò che di sensibile la grossa azienda obiettivo condivide con l'attività più piccola, in modo da pianificare futuri attacchi in modo più mirato, se necessario. Un episodio del genere è successo all'azienda statunitense Target, i cui sistemi sono stati oggetto di intrusione e alcuni dati rubati. Ciò è avvenuto in seguito all'introduzione di un malware POS (Point-Of-Sale malware, installati nei sistemi POS per memorizzare i dati digitati nel dispositivo, ed inviarli poi ad un server esterno. Si pensa che tramite l'uso di questo sistema, gli attaccanti abbiano ottenuto le credenziali di accesso ai sistemi dell'azienda HVAC System, sempre statunitense, produttrice ed installatrice di impianti di refrigerazione. Pare che Target avesse condiviso le credenziali delle propria rete interna con HVAC, per cui i malintenzionati hanno avuto facile accesso in seguito. Una falla così può essere assolutamente evitata.

4.1.3 Alcune soluzioni

E' necessario, dunque, apprestarsi a prendere precauzioni il prima possibile, l'ideale sarebbe in concomitanza o subito dopo la realizzazione dell'infrastruttura di rete, così da avere fin da subito, una volta avviate le attività aziendali, un'infrastruttura all'avanguardia che offre un buon grado di sicurezza e privacy ai dispositivi, ai dati ed agli utenti. Alcune soluzioni per avvicinarsi il più possibile a tale obiettivo sono:

- *Protezione dei Dati*: usare la crittografia sia per la trasmissione che per lo storage di dati e assegnare i permessi in modo che solo determinati utenti possano leggere, aggiungere, cambiare o eliminare dati, questo è riferito ai dati sensibili. Sarebbe opportuno considerare anche strumenti di prevenzione della perdita di dati in modo da monitorare il flusso di dati e bloccare quelli non autorizzati.

- *Rinforzare la sicurezza all'accesso*: utilizzare password complesse e l'autenticazione a due fattori.

- *Formare il personale*: stabilire delle linee guida basiche per il personale ai lavori non addetto alla sicurezza e organizzare una formazione periodica degli addetti ai lavori con corsi di aggiornamento e stimolandoli a proporre delle soluzioni.

- *Sicurezza fisica*: isolare i server, i data center e in generali i dispositivi più importanti in modo che solo personale qualificato e autorizzato possa accedervi.

- *Utilizzo del cloud*: utilizzare il cloud permette di ridurre il numero di data center o server, ciò comporta un vantaggio considerevole soprattutto per le grandi aziende. Tuttavia possono esserci dei rischi per la sicurezza se il cloud non è gestito e mantenuto all'interno dell'azienda stessa. Infatti è consigliato utilizare strumenti di sicurezza del cloud per criptare i dati prima che questi vengano caricati nel cloud, proteggere, monitorare endpoints, classificare i dati in base al livello di rishio e tracciarne i movimenti all'interno del cloud.

- *Rendere sicuri gli Access Points e WiFi*: impiegare i migliori algoritmi di sicurezza per router WiFi, come il WPA (WiFi Protector Access) di cui l'ultima versione è il 3 (WPA3).

- *Pianificare backup regolari*: prestare particolare attenzione alla schedulazione del backup in modo che non coincidano con altre operazioni o con lo spegnimento del/dei server e/o data center.

- *Classificare i dati in base alla loro importanza*: classificare è utile in quanto si riesce a distinguere quali dati meritano priorità di protezione rispetto ad altri, al fine di utilizzare al meglio lo spazio di salvataggio.

- *Proteggere dai Cyber Attacks*: configurare appropriatamente e mantenere aggiornati i software di sicurezza (es. Firewall, Anti-Virus/Anti-Malware) e applicare dei filtri per la navigazione web e le e-mail. Inoltre un'opzione che viene ultimamente considerata è lo spostare applicazioni molto importanti per il business, come servizi e.mail e finanziari, a servizi cloud-based, per una migliore sicurezza.

Capitolo 5

Considerazioni finali

S. Marco Informatica S.P.A. è una realtà costituita da un gran numero di figure professionali occupate in diverse sezioni aziendali, spesso interfacciate tra loro. Durante il periodo di stage ho avuto modo di verificare i rapporti tra le diverse unità aziendali, le gerarchie professionali interne, le procedure da rispettare. L'Azienda si è comunque dimostrata molto flessibile prevedendo anche giorni lavorativi da remoto (smart working) utilizzando un computer aziendale. L'aspetto più complicato è stato rapportarmi direttamente con i clienti e acquisire fin da subito capacità e linguaggi appropriati, meno complesso è stato imparare a utilizzare in poco tempo alcuni software. Molto importanti sono state le comunicazioni con il tutor aziendale, anche se spesso oberato d'impegni per l'assenza di alcuni colleghi esperti. I programmi dei corsi di Sistemi Operativi e Reti e Sicurezza sono stati una buona preparazione, utile ad affrontare questa prima esperienza lavorativa. L'esperienza vissuta durante lo stage è stata positiva, ma molto intensa. Ho avuto la conferma del diverso approccio alle questioni tecniche fra il mondo accademico e quello aziendale, ma soprattuto ho vissuto in diretta la molteplicità di criticità non affrontate durante il percorso universitario. L'inserimento nel gruppo di lavoro è stato positivo e da subito inclusivo, benchè fossimo operatori provenienti da percorsi di formazione diversi. L'Azienda ha valutato positivamente il mio operato, benchè fossi privo di qualunque esperienza specifica, tant'è che mi ha proposto di continuare a lavorare con loro. Il proseguimento lavorativo all'interno dell'azienda ospitante lo stage è una opportunità abbastanza diffusa tra noi studenti d'Informatica, questo prova che lo stage curriculare, seppur molto impegnativo per numero di ore richieste, è un buon modo per inserirsi nell'ambito lavoro.

Bibliografia e Sitografia

5.1 Bibliografia

- *A. S. Tenenbaum, D. J. Wetherall, Reti di calcolatori, Ed. Pearson, 2015*
- *A. S. Tenenbaum, H. Bos, I moderni sistemi operativi, Ed. Pearson, 2018*

5.2 Sitografia

- *https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/*
- *https://resources.infosecinstitute.com/topic/9-best-practices-for-network-security/*
- *https://www.ibm.com/docs/en/addi/5.0.4?topic=guide-error-codes*
- *https://www.sanmarcoinformatica.com/*
- *https://media.defense.gov/2022/Jun/15/2003018261/-1/-1/0/CTR$_N$SA$_N$ETWORK$_I$NFR*