UNIVERSITÀ DI PISA

DIPARTIMENTO DI INGEGNERIA DELL'ENERGIA DEI SISTEMI DEL TERRITORIO E DELLE COSTRUZIONI

RELAZIONE PER IL CONSEGUIMENTO DELLA LAUREA MAGISTRALE IN INGEGNERIA GESTIONALE

Information Risk Management in un istituto di credito: Network & Data Security

SINTESI

RELATORI

Prof. Ing. Riccardo Dulmin
Dipartimento di Ingegneria dell'Energia, dei Sistemi, del Territorio e delle Costruzioni

Dott. Giovanni Lelli
IT Advisory

IL CANDIDATO

Marco Moretti

marco.moretti.995@gmail.com

Sessione di Laurea Magistrale del 30/09/2020
Consultazione NON Consentita

Information Risk Management in un istituto di credito: Network & Data Security
Marco Moretti

Sommario

L'elaborato di tesi delinea il percorso formativo intrapreso presso una società di consulenza e in particolare nel team che supporta le imprese nella gestione dei rischi a livello IT e nella protezione del patrimonio informativo aziendale. Il progetto di tirocinio ha riguardato quindi lo svolgimento di consulenza manageriale in ambito IT risk di supporto ad un istituto di credito italiano (di seguito "La Società"), facente parte di un Gruppo internazionale che ha scelto di adottare il framework di cybersecurity del *National Institute of Standards and Technology (NIST)* per tutte le proprie *Entity*. In particolare, il tirocinante è stato inserito nel cantiere progettuale riguardante la messa in sicurezza delle reti e salvaguardia dell'integrità e confidenzialità dei dati. Il lavoro è consistito nell'assessment della situazione As-Is dei requisiti del framework al fine di rilevare le non conformità e supportare il cliente, attraverso costanti meeting, nelle azioni di miglioramento attraverso la progettazione di metodi, processi e procedure al fine di disegnare una situazione To-Be conforme al NIST e atta a ridurre il rischio IT.

Abstract

The thesis work defines the training journey which has been carried out at a consulting firm and in particular in the service line that supports companies managing IT level risks at and protecting the company's information assets. The internship project involved the provision of IT risk management consulting to an Italian credit institution that is part of an international Group, which has chosen to adopt the cybersecurity framework of the *National Institute of Standards and Technology (NIST)* for all its *Entities*. In particular, the intern has been included in the project regarding the security of networks and safeguard of data integrity and confidentiality. The work consisted in the assessment of the As-Is situation for the framework requirements in order to detect non-compliances and support the client, through constant meetings, in improvement actions through the design of methods, processes and procedures in order to design a To-Be situation that is compliant with NIST and suitable to reduce IT risk.

1. Introduzione e Contesto di Lavoro

Il tema della *cybersecurity* risulta in forte crescita espansiva in termini sia di impatti sul business che di conseguenti investimenti da parte delle imprese a difesa delle proprie infrastrutture IT sia a livello hardware che software al fine di ridurre gli impatti dei cyberattacchi in aumento. La gestione del rischio IT risulta, all'interno del contesto finanziario e in particolar modo di quello bancario, sempre più attuale e rilevante in quanto gli istituti di credito costituiscono uno dei principali target di attacchi informatici ma anche di frodi provenienti dall'interno, ovvero compiute da dipendenti della Società. Il contesto operativo che vede la digitalizzazione sempre più crescente dei processi di business ha richiesto un'attenzione particolare nell'implementazione dei requisiti di sicurezza IT del *cybersecurity framework del NIST* per la Società.

2. Attori in Gioco e Problema Affrontato

Il cliente è un istituto di credito italiano specializzato nel credito al consumo, cioè nel credito alle famiglie per l'acquisto di beni e servizi ad uso privato ed è parte di un gruppo internazionale. Al fine di rafforzare le misure di sicurezza informatica delle proprie Entity, il Gruppo ha scelto di adottare il framework di cybersecurity del NIST.

La società di consulenza offre ai propri clienti servizi di consulenza in vari ambiti. In particolare, il progetto è supportato dalla linea di servizi di relativa alle tematiche di sicurezza informatica, che ha lo scopo di supportare le imprese nella gestione dei rischi a livello IT e nella protezione del patrimonio informativo aziendale. Il Gruppo ha scelto questa società di consulenza per la continuità di assistenza e in quanto main partner per i servizi di IT risk management & cybersecurity. Il ruolo della società di consulenza è quello di offrire un supporto operativo nell'analisi e definizione dei processi impattati dalle nuove misure di sicurezza, nel coordinamento con altre attività del cantiere progettuale.

Il framework NIST si inserisce nell'ambito del programma pluriennale di incremento della sicurezza dell'infrastruttura IT delle proprie Entity, avviato dal Gruppo e finalizzato al miglioramento e all'implementazione di misure di sicurezza aggiuntive su specifiche tematiche di cybersecurity. Il framework si compone di *varie Security Card* relative a specifiche tematiche cyber, ognuna delle quali è declinata in una serie di requisiti, afferenti ad un criterio di valutazione e specifici per ognuno dei Security Level. In particolare, l'obiettivo prefissato è quello di incrementare il livello di sicurezza della Società per le Security Card in scope. Il livello di maturità *Repeatable* si raggiunge se "sono messe in atto a

livello aziendale politiche formali e programmi per i processi di gestione dei rischi, con parziale collaborazione esterna".

In particolare, la figura del candidato è stata inserita a supporto della *Sicurezza delle reti wireless e VPN* e della *Sicurezza dei dati*.

3. Approccio Metodologico

Di seguito vengono riportati gli step dell'approccio metodologico seguito alla base della gestione delle attività progettuali.

1. *Assessment dei requisiti NIST:* lo step prevede l'identificazione del perimetro relativo al progetto NIST e la raccolta e l'analisi dei requisiti per i Topic in scope;
2. *Gap Analysis:* il secondo step prevede un'analisi del contesto As-Is della Società al fine di identificare gli scostamenti rispetto ai requisiti richiesti. È necessaria inoltre l'analisi e la progettazione delle attuali soluzioni IT a supporto del raggiungimento degli obiettivi di ogni Security Card;
3. *Identificazione della soluzione To-Be e stima dell'effort:* il terzo step prevede l'identificazione delle soluzioni tecnologiche da integrare e/o acquistare al fine di raggiungere il livello di sicurezza prefissato. È necessaria inoltre una stima delle attività da avviare, dei tempi di esecuzione, delle interdipendenze con altri progetti, dell'effort e dei costi;
4. *Definizione del piano delle attività:* il quarto step prevede la definizione del piano di progetto atto a raggiungere gli obiettivi prefissati che deve essere quindi condiviso con tutte le strutture coinvolte nel piano delle attività e successivamente validato dalle stesse;
5. *Implementazione:* l'ultimo step prevede la realizzazione del piano di progetto condiviso e approvato e la realizzazione della documentazione di progetto relativa a processi, metodologie e soluzioni tecnologiche To-Be implementate.

L'approccio prevede inoltre attività di *project management* lungo tutta la durata del progetto al fine di pianificare, monitorare e controllare il piano di progetto annuale. A tal fine sono stati predisposti strumenti di supporto per il monitoraggio e fissati SAL bisettimanali sia interni con il team di progetto che con la società di consulenza. Tale approccio di lavoro persegue l'obiettivo di identificare e anticipare eventuali criticità che potrebbero rallentare il raggiungimento degli obiettivi prefissati.

4. Lavoro Svolto

In particolare, il ruolo del candidato è stato quello di supporto nelle seguenti attività e relativi deliverable:

- Partecipazione alle riunioni con il cliente al fine di identificare le opportunità di miglioramento e condividere le attività svolte e i next step necessari al conseguimento della conformità ai requisiti;
- Predisposizione di documenti che riassumano in modo chiaro e completo quanto emerso nel corso degli incontri svolti con il cliente;
- Predisposizione di documentazione di supporto per il cliente quali presentazioni in PowerPoint e fogli Excel al fine di delineare in modo efficace ed efficiente le attività e le tempistiche del cantiere progettuale in linea con l'analisi e la definizione dei processi impattati, supportando il cliente nel processo decisionale delle migliori soluzioni da implementare al fine di minimizzare l'impatto sul business e sugli utenti coinvolti nei processi IT;
- Supporto nella revisione delle metodologie e delle politiche a supporto dei processi impattati dal progetto nell'ottica di raggiungere la conformità documentale ai requisiti richiesti dal framework.

4.1. Sicurezza delle Reti Wireless e VPN

Di seguito in *Figura 1* viene riportato il diagramma di Gantt della attività relative alla messa in sicurezza delle reti wireless e VPN necessarie al fine di raggiungere la conformità ai requisiti. Le attività includono l'installazione delle sonde NIPS e l'implementazione di ulteriori misure di sicurezza per quanto riguarda le reti VPN e Wifi.

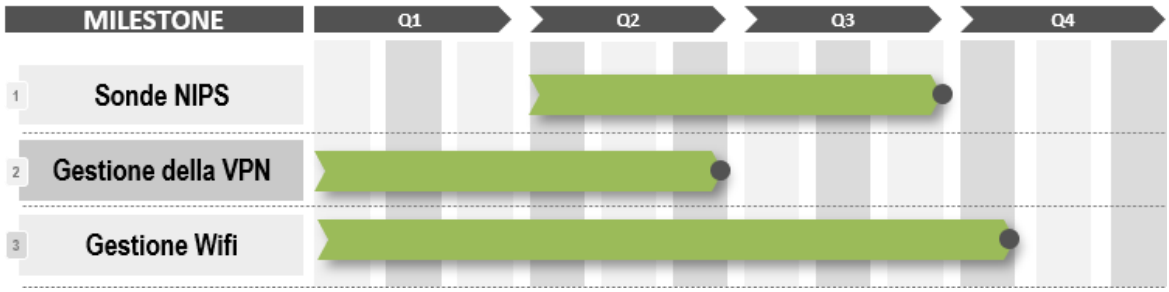

Figura 1: Diagramma di Gantt della attività relative alla Sicurezza delle reti

L'iniziale assessment svolto sui requisiti richiesti ha dato buoni risultati in quanto più del 50% dei requisiti sono risultati conformi sia per quanto riguarda le reti wireless che l'infrastruttura VPN, delineando già un elevato grado di maturità della Società per quanto riguarda la sicurezza delle reti. In particolare, lo svolgimento di Vulnerability Scan e

Penetration Test è stato pianificato da un fornitore esterno al fine di programmare piani di intervento per appianarle. Per quanto riguarda le reti wireless, esse sono già rese sicure dal fatto che possano essere considerate come hotspot in quanto non permettono, come già evidenziato, l'accesso alla intranet aziendale ma solo ad internet. La conformità ai restanti requisiti protegge l'infrastruttura da attacchi esterni sia sull'interfaccia amministrativa che sulle risorse che comunicano con l'esterno. La milestone che ha richiesto più sforzo è stata quella relativa all'infrastruttura VPN, a cui di fatto il framework dedica più requisiti. Le azioni di miglioramento hanno riguardato soprattutto la progettazione di processi conformi ai requisiti per quanto riguarda la gestione dell'accesso remoto che deve avvenire attraverso un meccanismo di autenticazione forte ed essere sottoposto a revisione periodica. Il candidato è stato quindi coinvolto nel processo di progettazione dei seguenti processi in base ai feedback del cliente ricevuti nelle riunioni svolte.

L'abilitazione all'accesso da remoto viene gestita attraverso lo strumento di ticketing aziendale, ovvero un sistema informatizzato che permette di risolvere in maniera rapida il problema attraverso l'apertura di un ticket e la successiva chiusura, una volta risolto il problema.

Per quanto riguarda il processo di acceso remoto da estendere a tutti gli utenti interni, esso inizia con l'utente che apre un ticket "Accesso remoto tramite VPN per utente interno" attraverso lo strumento di ticketing aziendale. La richiesta viene approvata o meno da parte del Responsabile Gerarchico dell'utente interno e in seguito validata da parte di HR. Sicurezza IT provvede ad assegnare l'utente al Gruppo Reperibile per accedere in VPN. Infine, Servizi provvede alla configurazione dell'OTP (*One-Time Password*) necessaria per effettuare l'accesso in VPN attraverso l'autenticazione multi-fattore.

Per quanto riguarda il processo To-Be per la gestione delle richieste di accesso degli utenti esterni, esso inizia con il Referente Interno apre, per conto dell'utente esterno, una service request attraverso lo strumento di ticketing aziendale. La richiesta è inoltrata al Responsabile Gerarchico dell'utente esterno che approva o meno la richiesta. Se la richiesta viene approvata, questa passa al secondo livello di approvazione da parte di Sicurezza IT. Quest'ultimo, dopo aver valutato ed eventualmente approvato la richiesta, assegna il gruppo AD per l'accesso in VPN all'utente esterno. A questo punto Servizi provvedere a concedere all'utente il token per l'autenticazione multi-fattore necessaria per l'accesso in VPN. Servizi procede con la chiusura della service request attraverso lo strumento di ticketing aziendale. Il processo termina quindi con l'accesso ai sistemi della Società da parte dell'utente.

In *Figura 2* è riportata la matrice RACI relativa al processo di gestione delle utenze esterne.

Attività	Referente interno	Responsabile gerarchico	Sicurezza IT	Sistemi	Utente
Apertura della richiesta mediante Ticket	R	I A			C
Approvazione della richiesta		A R	I		
Secondo livello di approvazione			A R		
Assegnazione gruppo AD per accesso in VPN			A R	I	
Concessione Token per autenticazione MFA				A R	
Chiusura service request				A R	I
Accesso ai sistemi	I	A	I	I	R

Figura 2: RACI Matrix del processo To-Be di gestione delle utenze esterne

4.2. Sicurezza dei Dati

Di seguito in *Figura 3* viene riportato il diagramma di Gantt della attività relative alla messa in sicurezza dei dati e necessarie al fine di raggiungere la conformità ai requisiti. Le attività includono l'implementazione dei tool di data discovery & classification e Digital Rights Management, il potenziamento della cifratura dei dati, la revisione del processo del DLP e la revisione dei flussi verso l'esterno.

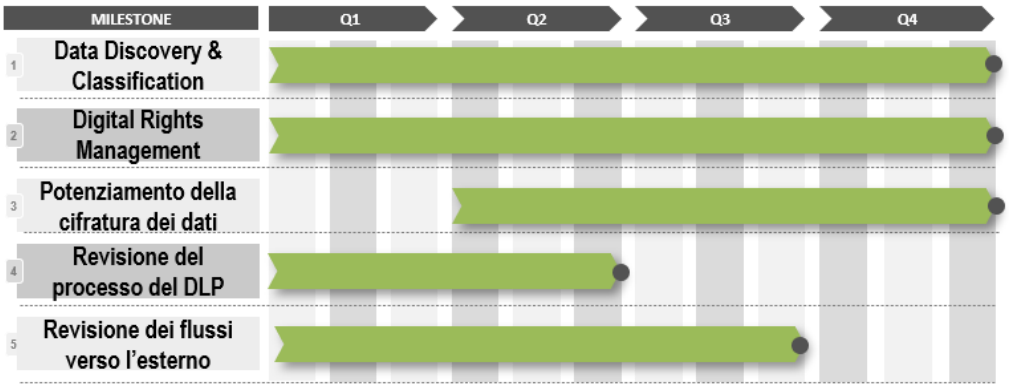

Figura 3: Diagramma di Gantt della attività relative a Data Security

Al fine di raggiungere la conformità ai requisiti ed evitare il data leakage, si è resa necessaria il supporto al cliente per l'adozione di specifici tool ovvero:

- tool di *data discovery e data classification* sui dati strutturati;
- tool di *data discovery e data classification* sui dati non strutturati (il tool risulta già acquistato e implementato);
- tool di *data encryption* per i dati strutturati;
- tool di *Digital Rights Management* (DRM) per i dati non strutturati;
- tool di *Data Loss Prevention* (DLP) (il tool è già presente a livello di endpoint).

In particolare, il ruolo del candidato è stato quello della predisposizione di presentazioni, al fine di esplicare alle funzioni coinvolte il ruolo e le funzionalità dei tool, ed inoltre di workflow e modelli di controllo per i processi in cui essi sono coinvolti.

In *Figura 4* viene mostrata l'integrazione tra i tool di data classification, Digital Rights Management e Data Loss Prevention (DLP).

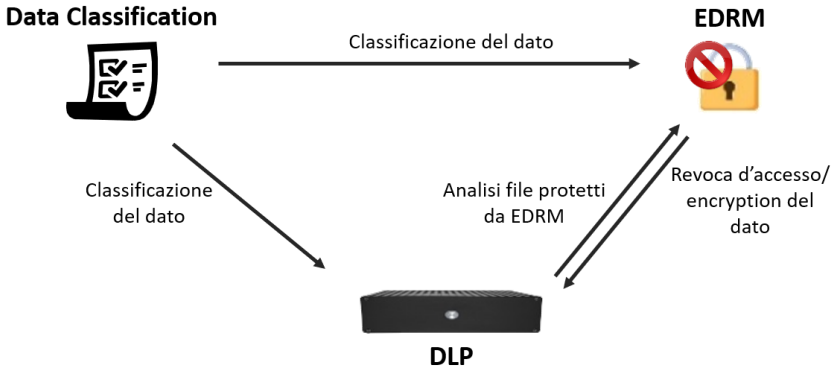

Figura 4: Schematizzazione della comunicazione tra i tool

A valle della classificazione dei dati in accordo con la *Politica di Data Classification* della Società, il DLP monitora i dati scambiati con l'esterno via web e mail ed eventualmente ne blocca l'invio. Anche il tool di DRM permette di monitorare chi accede al dato e in caso di revocare l'accesso agli utenti non autorizzati.

Il DLP consente di definire specifiche regole tramite tecniche di pattern matching e di finger printing, volte ad individuare un determinato dato. Il DLP invia quindi degli alert ogni volta che le regole definite vengono violate, al fine di registrare l'evento per un successivo monitoraggio da parte dell'utente, oppure può andare a bloccare direttamente il flusso in uscita. Tali log possono essere inviati alla piattaforma SIEM dove vengono raccolti e analizzati.

Dato che il DLP implementato dalla Società non permette di attivare le regole di quarantena, si è reso necessario lo svolgimento, da parte del candidato, dell'analisi dell'impatto dell'attivazione delle regole di quarantena in modalità di blocco. Una delle due analisi svolte è stata quella per direzioni impattate dalle regole di blocco implementate per i dati inviati via mail e web. Come risultato dell'analisi è stata pianificata l'implementazione delle regole del DLP a perimetri crescenti che sono costituiti dalle direzioni impattate. Il diagramma di Gantt è riportato in *Figura 5*.

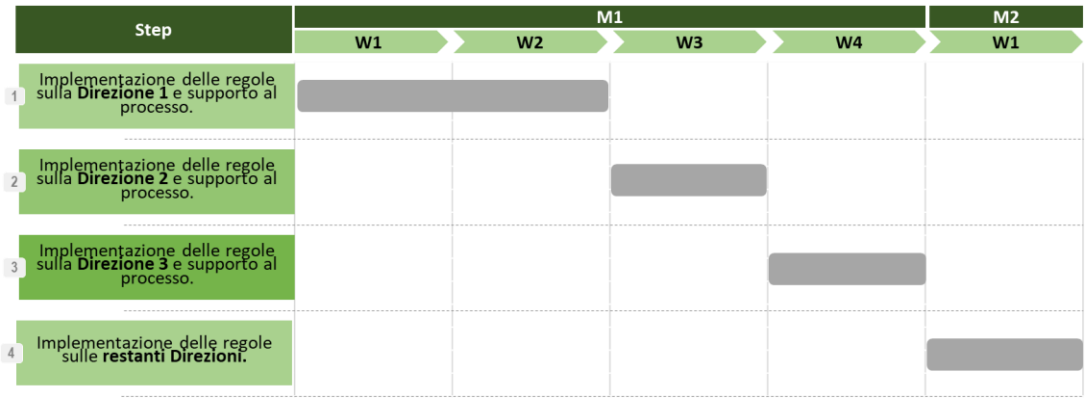

Figura 5: Pianificazione dell'implementazione delle regole per direzioni

L'implementazione prevede prima il deployment sulla Direzione 1 e sulla Direzione 2 in quanto sono le direzioni a maggiore impatto. Successivamente segue il deployment sulla Direzione 3 e sulle restanti direzioni. Il punto di forza di questa proposta è il ridotto effort di Sicurezza IT per quanto riguarda la gestione delle utenze mentre il punto di debolezza è l'effort di Sicurezza IT elevato per la difficoltà di implementazione.

L'implementazione del DLP a livello gateway permette anche la messa in sicurezza dei dati scambiati attraverso gli *Unified Communication Channels* (es. Skype, Microsoft Teams, etc.). In questo modo, qualsiasi documento che viene inviato all'esterno del dominio di Gruppo viene analizzato dal tool e bloccato, qualora violi le regole implementate. Lo schema della soluzione è riportato in *Figura 6*.

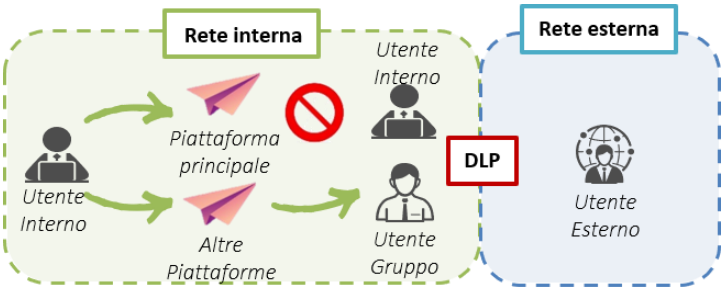

Figura 6: Attivazione del DLP a livello gateway

Attraverso la configurazione e l'implementazione del DLP, tutti i documenti che vengono inviati attraverso i canali di comunicazioni unificati vengono analizzati dal DLP installato sul gateway che procede a bloccare tutti gli invii che violino le regole definite. Il rischio risulta essere completamente mitigato in quanto i flussi verso l'esterno sono monitorati dal DLP.

Al fine di incrementare la sicurezza dei dati at rest, il candidato è stato coinvolto inoltre nell'analisi funzionale del tool di data encryption. Il vantaggio della *Transparent Data Encryption* (TDE) sta proprio nell'impatto limitato sulle performance, poiché essa è completamente trasparente per utenti ed applicativi. Questo tipo di encryption mitiga il

rischio di furto dei dati, sia esso causato dalla perdita di uno o più dischi fisici o di un file di export/backup del database. In *Figura 7* si riporta lo schema funzionale predisposto per il tool di data encryption.

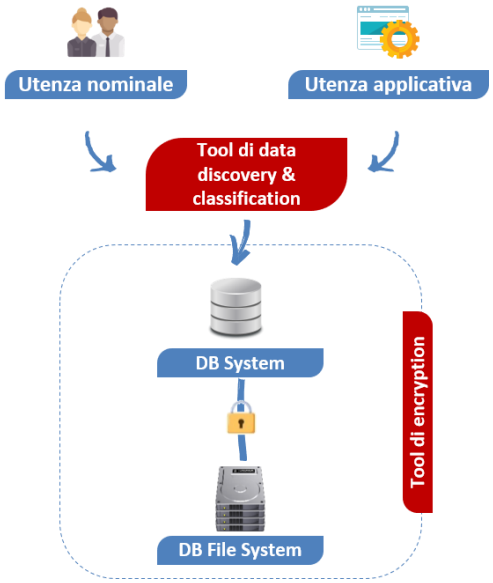

Figura 7: Schema funzionale della TDE

Le utenze nominali o applicative accedono agli ambienti dei database per svolgere le operazioni di gestione ordinaria. Gli accessi e le attività vengono monitorati attraverso le funzionalità messe a disposizione dal tool di data discovery & classification. I dati contenuti all'interno dei database sono cifrati a livello di *file system*.

Il candidato è stato inoltre coinvolto nello svolgimento dell'analisi della cifratura dei flussi esterni. Questi flussi sono quelli che contengono dati che dalla Società vengono trasmessi esternamente alla rete interna, tramite la rete pubblica. In *Figura 8* è riportato lo schema funzionale.

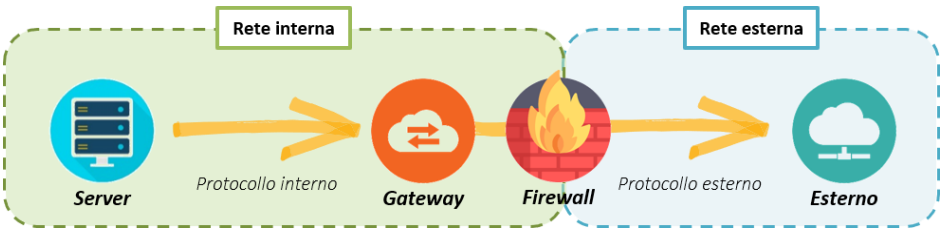

Figura 8: Schema funzionale della rete e dei protocolli usati

In particolare, è stata effettuata l'analisi dei flussi aperti verso l'esterno ed il loro livello crittografico. I risultati dell'analisi svolta sui flussi indica la tipologia di protocollo utilizzata e la tipologia di dati scambiata. Un protocollo non cifrato è considerato come non conforme. Tali protocolli potrebbero essere utilizzati per lo scambio di file sulla base di un sistema client-server pertanto essi non sono protocolli sicuri in quanto non prevedono la cifratura e

quindi effettuano lo scambio di dati in chiaro, permettendone ad un esterno la lettura. A valle della validazione finale dell'analisi, qualora vengano rilevati flussi non conformi, è necessario contattare l'owner del flusso e richiedere che il flusso venga dismesso o migrato su un protocollo cifrato.

5. Risultati ottenuti

Per quanto riguarda la messa in sicurezza delle reti wireless e VPN lo svolgimento di Vulnerability Scan e Penetration Test sulle reti permette alla Società una maggiore conoscenza delle proprie vulnerabilità al fine di programmare piani di intervento per appianarle. Per le reti wireless, esse sono già rese sicure dal fatto che esse possano essere considerate come hotspot in quanto non permettono l'accesso alla intranet aziendale ma solo ad internet. La conformità ai restanti requisiti protegge l'infrastruttura da attacchi esterni sia sull'interfaccia amministrativa che sulle risorse che comunicano con l'esterno. Relativamente all'infrastruttura VPN, la Società risulta avere un'infrastruttura di accesso remoto già abbastanza sicura per lo standard NIST dal punto di vista crittografico, delle misure di sicurezza e procedurale. Le azioni di miglioramento hanno riguardato soprattutto la progettazione di processi conformi ai requisiti per quanto riguarda la gestione dell'accesso remoto e il processo di revisione periodica degli accessi rende la struttura VPN più sicura allontanando il rischio di accessi non autorizzati.

Per quanto riguarda la sicurezza dei dati, l'implementazione di tool di data discovery e data classification sia su dati strutturati che non strutturati consente alla Società la conoscenza delle proprie banche dati. Inoltre, in un'ottica di integrazione con i tool di DLP e DRM, ciò permette da un lato di prevenire la fuoriuscita di dati sensibili e dall'altro di revocare i diritti di utilizzo ai file in qualunque sistema essi siano contenuti.

L'encryption a livello di dato proteggere dati sensibili e segreti da potenziali attacchi malevoli sia esso causato dalla perdita di uno o più dischi fisici o di un file di export/backup del DB. In particolare, la TDE permette, rispetto ad altre crittografie a livello di dato, di non avere impatti sull'operatività delle utenze che accedono ai database.

Anche le chiave crittografiche che devono essere considerate come dati critici in quanto atte a rendere illeggibili i dati. La revisione del processo di gestione dell'intero ciclo di vita della chiave permette alla Società di garantirne l'integrità e di ridurre il rischio di furto. In ultima istanza, l'analisi dei flussi di dati in uscita dalla Società ha permesso di analizzare la presenza di flussi non crittografati al fine di eliminare il rischio di eventuali intercettazioni.

6. Sviluppi Futuri e Conclusioni

Per quanto riguarda gli sviluppi futuri del progetto, si delinea che il progetto vede avviate le attività dell'anno corrente che saranno integrate dalle continue iniziative di sicurezza che saranno individuate nei prossimi anni. Per il cantiere progettuale in corso e in particolare per i Topic per cui il candidato è stato coinvolto, sono necessari, per alcuni requisiti, ulteriori step. In particolare, per la sicurezza delle reti è necessario principalmente lo svolgimento dei Penetration Test da parte del fornitore esterno, la valutazione di tempi e costi delle tre soluzioni proposte per quanto riguarda il requisito sulla DMZ dell'infrastruttura wireless e il monitoraggio dell'altro progetto sul potenziamento delle reti Wi-Fi al fine di includere le attività di administration. Il progetto risulta al momento bloccato a causa dell'emergenza Covid-19. Per la sicurezza dei dati, è necessario continuare nel supporto all'implementazione dei tool di data discovery & classification, Digital Rights Management e del DLP a livello gateway e raccogliere le informazioni necessarie all'interno di una metodologia che supporterà la Società in tutte le operazioni in cui i tool sono richiesti. Si rende inoltre necessaria l'integrazione tra i tool e anche con il SIEM della Società, al fine di gestire in maniera unificata i log generati dalle operazioni compiute. È necessario inoltre procedere con l'implementazione delle regole di blocco del DLP e, per quanto riguarda la gestione delle chiavi crittografiche, il proseguimento delle interviste ai key custodian con il fine di validare i processi del ciclo di vita delle chiavi. Infine, a valle dell'analisi dei flussi effettuata, è necessaria la validazione che i flussi individuati siano effettivamente non conformi e provvedere all'eliminazione o migrazione di tali flussi.

L'esperienza professionale ha permesso al candidato l'utilizzo delle proprie conoscenze di project management e dell'approccio per processi apprese durante il corso di studi e l'apprendimento di concetti della sicurezza dei sistemi ICT nel settore finanziario. Infine, il lavoro svolto ha permesso lo sviluppo di capacità non meno importanti come le soft skills quali team working, problem solving e ascolto del cliente che costituiscono qualità imprescindibili per poter affrontare l'ambiente di lavoro in cui opera una società di consulenza. È stato possibile per il candidato inoltre potenziare la propria capacità di stesura di deliverable quali presentazioni PowerPoint e documenti Word di supporto al cliente.

L'esperienza è stata maturata in un contesto reale e stimolante, benché la quasi totalità delle giornate lavorative sia stata svolta da remoto a causa dell'emergenza Covid-19. Nonostante ciò, la crescita professionale è stata maturata soprattutto grazie al costante contatto tra il candidato e le esperte figure professionali del team.