White Paper.

Lesson 2: Protezione della posta elettronica e applicazioni core

La posta elettronica nelle Aziende

Il massiccio uso di Internet e della posta elettronica, in particolare, oltre a facilitare enormemente lo scambio di dati tra soggetti diversi, realizza di fatto una maggiore esposizione delle aziende verso l'esterno.

Questi strumenti elettronici ormai divenuti indispensabili per il flusso di documenti e di informazioni digitali, scambiate sia all'interno dell'impresa sia all'esterno con altre realtà, (aziende, enti, istituti di credito, ecc.) presentano però vantaggi e svantaggi. Mentre i vantaggi sono facilmente intuibili, vedi la riduzione dei tempi ed il conseguente abbattimento dei costi, gli svantaggi sono invece sostanzialmente legati al rischio di diventare vittima di attacchi informatici che insidiano la sicurezza dei dati e del business aziendale. In tale contesto, diventa indispensabile dotarsi di un piano di protezione, ovvero:

- adottare misure necessarie a bloccare i tentativi di intrusione da parte di soggetti, siano essi esterni o interni, non autorizzati nei propri sistemi;
- proteggere i dati in modo che le informazioni siano ben custodite e non corrano il rischio di andare perdute;
- evitare possibili danneggiamenti causati da una scarsa consapevolezza, sensibilità e formazione sul tema della sicurezza aziendale da parte del personale interno.

Nella lezione precedente abbiamo visto come la tipologia di attacco, che va sotto il nome di "man-in-the-middle", consente di dirottare il traffico generato durante la comunicazione tra due host verso un terzo host (attaccante), il quale fingerà di essere l'end-point legittimo della comunicazione. Questa attività presenta un elevato grado di pericolosità se applicata ad esempio alla posta elettronica o ad applicazioni core erogate in modo non conforme.

Per comprendere appieno come il servizio di posta elettronica possa divenire per un'azienda fonte di perdita o danneggiamento dei propri dati, è bene considerare che attraverso la mail passa ormai quasi il 100% delle informazioni aziendali. E' evidente quindi la centralità di tale servizio e di come sia importante proteggerlo. Per poter proteggere tale servizio è innanzitutto necessario capire come funziona.

Come viene erogato il servizio

Il primo passo per definire una strategia di protezione è la scelta di un servizio di posta elettronica, che può essere erogato in differenti modalità. Di seguito ne analizziamo le possibili alternative:

- a) scegliendo un provider esterno all'azienda che offra tale servizio;
- b) installando un proprio server presso una server farm di un provider;
- c) installando un proprio server nella propria server farm.

A) Affidando il servizio di posta elettronica completamente all'esterno, si decide di non applicare in autonomia nessuna policy di sicurezza, password escluse. Di conseguenza si sceglie di seguire il piano di sicurezza previsto dal provider per il servizio erogato. Oltre a questo, le modalità di recovery o di archiviazione della posta spesso non sono contemplate perché lo stesso provider non ha interesse ad implementarle.

B) Nel caso in cui si decida di installare un proprio server di posta elettronica in modalità Hosting, presso un provider, si avrà la possibilità di controllare l'intero iter di erogazione del servizio, comprese le policy di sicurezza. Per quanto riguarda l'archiviazione ed il recovery sarà necessario installare presso il provider o presso la propria organizzazione, dei server appositamente strutturati con un conseguente costo economico.

C) Installare il server di posta elettronica all'interno dell'azienda è sicuramente la soluzione migliore. Questa scelta comporta l'organizzazione di una struttura IT interna con persone dedicate. Nella propria server farm è possibile avviare i servizi sopra citati anche condividendo risorse già presenti e attive, rimane da affrontare solo il problema del "Disaster recovery", che qui accenniamo soltanto in quanto non oggetto della presente.

Ma vediamo ora come funziona la posta elettronica!

I protocolli di messaggeria (SMTP, POP3, IMAP4)

La posta elettronica è il servizio più usato su internet. Quindi la serie di protocolli TCP/IP utilizzati per l'erogazione del servizio offre una panoplia di protocolli che permettono di gestire facilmente l'instradamento (routing) della posta sulla rete. Il servizio di posta elettronica può essere realizzato tramite l'utilizzo di protocolli sicuri o non sicuri.

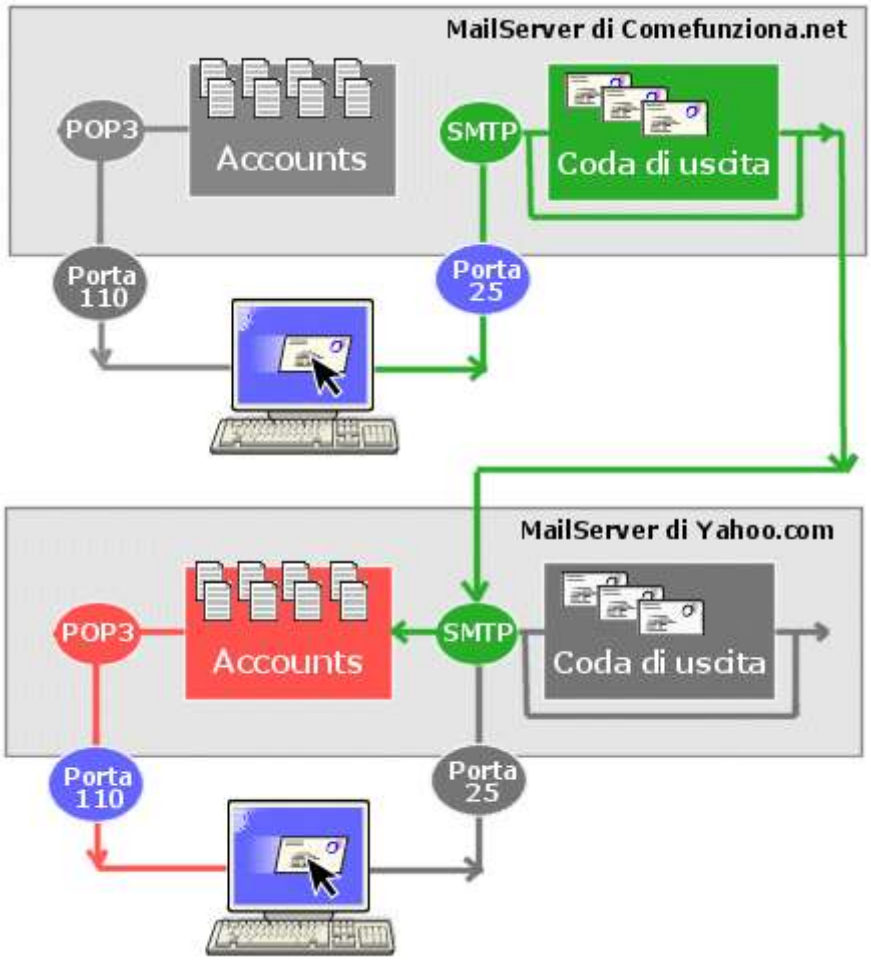
Protocolli insicuri:

- http,
- POP (porta TCP:110),
- IMAP (TCP:143),
- SMTP (TCP:25).

Protocolli sicuri:

- HTTP abbinato ad SSL,
- POP + SSL (porta TCP:995),
- IMAP + SSL (TCP:993),
- SMTP + SSL (TCP:465).

La prima considerazione da fare è quindi quella che diventa fondamentale per qualsiasi azienda, indipendentemente da come intenda erogare il servizio, e cioè analizzare quali protocolli sono o saranno utilizzati nel proprio servizio di posta elettronica.



Un disegno riasuntivo del viaggio compiuto dalla nostra eMail

Il protocollo SMTP

Il **protocollo SMTP** (*Simple Mail Transfer Protocol*, tradotto *Protocollo Semplice di* Trasferimento della Posta) è il protocollo standard che permette di trasferire la posta da un server ad un altro con una connessione point to point.

Si tratta di un protocollo funzionante in modalità connessa, incapsulato in una trama TCP/IP. La posta è consegnata direttamente al server di posta del destinatario. Il protocollo SMTP funziona grazie a dei comandi testuali inviati al server SMTP (per default sulla porta 25). Ogni uno dei comandi inviati dal client è seguito da una risposta del server SMTP composta da un numero e da un messaggio descrittivo.

Ecco uno scenario di richiesta di invio di mail ad un server SMTP:

- All'apertura della sessione SMTP, il primo comando da inviare è "*HELO" (oppure EHLO)* seguito da uno spazio e dal nome del dominio del vostro terminale (come dire "buongiorno sono il tal terminale"), poi validare con invio;
- Il secondo comando è "*MAIL FROM:*" seguito dall'indirizzo e-mail del mittente. Se il comando è accettato il server rinvia il messaggio "*250 OK*";
- Il comando seguente è"*RCPT TO:*" seguito dall'indirizzo e-mail del destinatario. Se il

comando è accettato il server rinvia il messaggio "*250 OK*";

- Il comando "*DATA*" è la terza tappa dell'invio. Esso annuncia l'inizio del corpo del messaggio. Se il comando è accettato il server rinvia un messaggio intermedio numerato "*354*" che indica che l'invio del corpo della mail può cominciare e considera l'insieme delle linee seguenti fino alla fine del messaggio individuata da una linea contenente unicamente un punto.

All'interno del corpo della mail ci sono poi altre informazioni contenute in campi appositi formattati in maniera diversa a seconda del client di posta utilizzato. Tali informazioni sono le seguenti:

- Date
- Subject
- Cc
- Bcc
- From

Se il comando è accettato il server rinvia il messaggio"*250 OK*".

E' possibile inviare una mail grazie ad un semplice telnet sulla porta 25 del server SMTP es: telnet smtp.pippo.net 25.

Il protocollo POP3

Il **protocollo POP** (*Post Office Protocol* tradotto con "*protocollo dell'ufficio postale*") permette, come indicato dal suo nome, di andare a recuperare la propria posta giacente su un server remoto (server POP). E' necessario a tutti quegli utenti che, non essendo connessi in permanenza ad internet, devono consultare le proprie mail off-line.

Esistono due versioni principali di questo protocollo, POP2 e POP3, alle quali sono attribuite rispettivamente le porte 109 e 110 e che funzionano attraverso dei comandi testuali radicalmente diversi.

Esattamente come nel caso del protocollo SMTP, il protocollo POP (POP2 e POP3) funziona grazie a dei comandi testuali inviati al server POP. Ciascuno dei comandi inviati dal client è composto da una parola-chiave, eventualmente accompagnata da uno o più argomenti ed è seguito da una risposta del server POP composta da un numero e da un messaggio descrittivo.

Comandi POP2

HELLO	Identificazione attraverso l'indirizzo IP del computer mittente.
FOLDER	Nome della casella da consultare.
READ	Numero del messaggio da leggere.
RETRIEVE	Numero del messaggio da recuperare.
SAVE	Numero del messaggio da salvare.
DELETE	Numero del messaggio da cancellare.
QUIT	Uscita del server POP2.

Comandi POP3

USER identificativo	Questo comando permette di autentificarsi. Esso deve essere seguito dal nome dell'utente; cioè da una stringa di caratteri che identificano l'utente sul server. Il comando USER deve precedere il comando *PASS.*
PASS password	Il comando *PASS* permette di indicare la password dell'utente il cui nome è specificato da un comando *User* precedente.
STAT	Informazione sui messaggi contenuti sul server.
RETR	Numero di messaggi da recuperare.
DELE	Numero di messaggi da cancellare.
LIST [msg]	Numero di messaggi da visualizzare.
NOOP	Permette di mantenere le connessioni aperte in caso di inattività.
TOP <messageID> <n>	Comando che visualizza *n* linee di messaggio, il cui numero è dato in argomento. In caso di risposta positiva da parte del server, questo rinvia le intestazioni del messaggio, poi una linea vuota e infine le *n* prime linee del messaggio.
UIDL [msg]	Richiesta al server di rinviare una linea contenente delle informazioni sul messaggio eventualmente dato in argomento. Questa linea contiene una stringa di caratteri, detta *listing d'identificatore unico*, che permette di identificare in modo univoco il messaggio sul server, indipendentemente dalla sessione. L'argomento opzionale è un numero corrispondente ad un messaggio esistente sul server POP, cioè un messaggio non cancellato.
QUIT	Il comando *QUIT* chiede l'uscita del server POP3. Esso implica la cancellazione di tutti i messaggi segnati come eliminati e rinvia lo stato di questa azione.

Risulta a questo punto evidente che il protocollo POP3 gestisce l'autentificazione tramite il nome utente e la password. Questa modalità di autenticazione **non è sicura** in quanto, come la mail, anche nome utente e password sono in chiaro (in modo non cifrato) e quindi facilmente intercettabili. Così come è possibile inviare una mail grazie a telnet, si può anche accedere alla propria posta grazie ad un semplice telnet sulla porta del server POP (110 per default):

Es:"telnet mail.pippo.net 110"

Immaginate a questo punto un malintenzionato venuto in possesso della vostra username e password… cosa può fare se il vostro sistema di posta utilizza i protocolli sopra descritti?

Il protocollo IMAP

Il protocollo **IMAP** (*Internet Message Access Protocol*) è un protocollo alternativo al protocollo POP3 ma che offre molte più possibilità:

- IMAP permette di gestire più accessi simultanei.
- IMAP permette di gestire più caselle postali.
- IMAP permette di smistare la posta secondo più criteri.
- IMAP **permette di criptare le password**.

Al di là delle caratteristiche del protocollo è subito evidente che il dato più eclatante è appunto quello di impedire il transito in chiaro delle password in modo da rendere inutile l'operazione di monitoraggio "Sniffer" da parte dei malintenzionati.

Le applicazioni Core

Quanto espresso per il servizio di posta elettronica è purtroppo valido anche per tutti gli accessi ad applicazioni e servizi pubblicati in modalità non sicura spesso necessari se non addirittura vitali per le aziende. A questo punto dare l'accesso a portali WEB, permettere lo scambio di informazioni via internet, consentire l'accesso remoto, utilizzare sistemi di messaggistica (facebook etc…), ci consente di stare tranquilli? Per le applicazioni diverse dalla posta elettronica che protocolli si usano? Che grado di sicurezza hanno?

Proviamo a fare un po' di chiarezza. Anche in questi casi i protocolli maggiormente utilizzati dalle aziende per accedere a determinate applicazioni sono da suddividere in sicuri e non sicuri.

Protocolli insicuri:

- http,
- FTP,
- Telnet,
- PPTP,
- VPN,
- ICQ,
- SNMP ver.1 e 2

Protocolli sicuri:

- HTTP abbinato ad SSL,
- FTPS o SFTP,
- SSH (non basato su SSL ma concettualmente similare),
- PPTP su SSTP VPN,
- Client di messaggistica istantanea configurati per l'uso di SSL,
- Skype (uso di PKI proprietario),
- Uso di SSL-VPN,

- L2TP (impiego di certificati digitali lato server e lato client),
- IPSEC (certificati digitali lato server e lato client oppure utilizzo di chiavi scambiate inizialmente),
- tunneling SSH VPN.
- SNMP ver.3

Il furto di credenziali

Utilizzando i protocolli non sicuri appena menzionati, sia per le applicazioni di posta elettronica che per quelle Core, è possibile con azioni di tipo "man in the middle" (descritte nella lezione 1) acquisire le credenziali dall'interno o dall'esterno della rete da cui l'utente si connette alla propria casella di posta elettronica o ai propri server applicativi.

Durante gli audit eseguiti anche in organizzazioni di rilievo, ci siamo trovati sovente di fronte a realtà molto diverse tra loro. Alcuni provider ad esempio Aruba, qui citato solo in quanto molte aziende gli affidano il proprio servizio di posta elettronica, non offrono un servizio di **secure mail**. Tutto il traffico viene infatti fatto transitare in chiaro inclusa la posta elettronica esponendo i propri utenti al rischio sopra citato.

La stessa cosa accade per il traffico dei dati contenuto sui server posti in hosting all'interno della server farm (Web Server). A seguito di un'analisi fatta il traffico da e verso tali web server è in **http**. Lo stesso Facebook non supporta appieno tutti i protocolli di sicurezza e si corre il rischio di farsi intercettare le proprie credenziali. Anche in questo caso la citazione è fatta solo perché molto utilizzato all'interno delle aziende.

Molti portali aziendali consentono l'accesso ai propri utenti o ai clienti in modalità non protetta. Se i dati a cui si accede sono importanti o addirittura fondamentali (pubblicazioni di listini, acquisizione ordini, etc…), sarebbe buona norma proteggerli. In moltissimi casi però, non solo sono completamente privi di protezione ma addirittura le persone preposte alle strutture informatiche non sono a conoscenza delle falle e della legislazione in materia.
Rendere sicuri i dati genera un'immagine più sicura della propria azienda a tutti gli utenti fruitori dei servizi oltre a preservare i responsabili da pesanti azioni penali.

E' bene riflettere che permettere di entrare in possesso di username e password può purtroppo rappresentare per il malintenzionato la possibilità concreta di avere in un solo colpo l'accesso a tutti i servizi dell'azienda, in quanto è diffusissima la pratica di usare una sola password in modo da non dimenticarla. **Pessima abitudine……!!!!!!!!!!**

Un altro servizio diffusissimo in tutte le organizzazioni è quello rappresentato dal server FTP. Questo servizio viene implementato per consentire lo scambio di file tra organizzazioni diverse, tra utenti della stessa organizzazione e in generale tutte quelle volte in cui sia necessario spostare grosse quantità di dati, che con la posta elettronica non è consigliato inviare. L'accesso a tali server avviene spesso in modalità non protetta, correndo il rischio di facilitare l'acquisizione di dati e delle relative credenziali di autenticazione. Questo processo è alla base del furto o del danneggiamento delle informazioni contenute nei server.

Cos'è l'FTP e come funziona

L'FTP (File Transfer Protocol) è un sistema di comunicazione datato, estremamente semplice da implementare e per questo molto usato da parte degli utenti. Questa combinazione lo rende preferibile ad altri sistemi più avanzati ma sicuramente più complessi. La struttura del protocollo consta di pochissimi comandi attraverso i quali è possibile impostare permessi, eliminare o spostare file, caricare o scaricare dati, mostrare il contenuto di cartelle e directory e via dicendo.

Trattandosi di un sistema ormai datato presenta alcuni problemi, il più grande dei quali è rimasto il sistema di trasferimento dei dati, tra il client ed il server. Il protocollo utilizza due distinti canali di comunicazione, il primo per lo scambio dei comandi che viene aperto alla connessione, ed il secondo invece viene utilizzato per lo scambio dei file che viene aperto e richiuso durante lo scambio dei dati. Avere due canali di comunicazione aperti contemporaneamente genera problemi di sicurezza e di trasmissione in quanto è possibile dare altre istruzioni mentre il trasferimento dati è in corso, con il rischio di perdita dei dati ed in alcuni casi la loro corruzione fino alla perdita totale. Per impedire questo problema è stato implementato **il supporto per le connessioni passive**. Queste connessioni vengono avviate dal client e non più dal server in modo da evitare anche i problemi legati a firewall, router o all'architettura della rete dell'utente finale.

A differenza però di quelle attive, le connessioni passive si portano in dote **notevoli problemi di sicurezza.** Una su tutte è quella dovuta al fatto che quando il server apre la connessione verso il client, non viene fatto più nessun controllo in quanto il software dà per scontato che dall'altra parte ci sia l'utente. Utilizzando invece l'altra connessione questa sicurezza non c'è più in quanto al posto del client ci potrebbe essere qualche software malevolo pronto a intercettare la comunicazione. Tra le altre debolezze c'è anche il fatto che la porta di connessione utilizzata in queste transizioni è casuale; per cui se si voleva utilizzare tale servizio è gioco forza aprire tutte le porte dei propri server per permettere il servizio stesso. **Una catena di punti deboli**. Buona norma è quella di non usare il protocollo FTP ma utilizzare l'**SFTP** che risulta integralmente cifrato e quindi sicuro.

Esistono poi soluzioni più o meno efficaci. Utilizzando ad esempio dei firewall in modalità Stateful Inspection è possibile risolvere molte delle problematiche legate alla sicurezza. Questi

software, estremamente avanzati, leggono il contenuto di una sequenza di pacchetti e agiscono mettendo in campo azioni preordinate. Nel caso dell'FTP aprono la porta solo quando è necessario per eseguire la connessione passiva richiesta dal client e bloccano una connessione passiva qualora questa provenga da un IP diverso da quello della connessione principale.

Per l'utilizzo invece dei protocolli di comunicazione "**sicuri**", è necessario usare (lato server) i cosiddetti "certificati digitali firmati" riconosciuti da parte di Certification Autority. L'uso di certificati creati autonomamente oppure già scaduti è assolutamente sconsigliabile in quanto induce negli utenti la pratica pericolosa che è quella, purtroppo diffusa, di ignorare da parte dell'utente i messaggi d'allerta restituiti, ad esempio, dal browser.

La possibilità di usare SSL per la ricezione e l'invio della posta elettronica o per l'accesso a portali sicuri, dipende dalla configurazione del server utilizzato in quel momento (sempre consigliabile il suo utilizzo). Nel caso in cui si usi la posta elettronica o altre applicazioni WEB erogate da provider esterni, è possibile attivare entrambe le modalità di sicurezza. E' invece fortemente criticabile il fatto che venga impiegato in modo predefinito il protocollo http e non https. **Mai trasmettere informazioni in chiaro!!!!**

Per concludere ricordiamo che l'utilizzo di un protocollo di posta non sicuro consente ad un malintenzionato di:

- assumere l'identità di un'altra persona,
- di leggere le e-mail di un altro utente,
- di carpire i dati personali memorizzati sui server di posta,
- di inviare posta elettronica per conto dell'ignaro utente.

Solo un'idonea formazione può evidenziare questo pericolo, ma è un argomento sottovalutato in quanto assorbe tempo e risorse rendendo improduttive le persone durante tale periodo, ma……. è davvero tempo perso?

Il Tuo
EterNet Team