FOCUS
SUI RANSOMWARE

Novembre 2021

A cura di Luigi Zampetti e Sergio Spera

SOMMARIO

1. COSA SONO I RANSOMWARE.

Il ransomware è un tipo di malware [1] che limita l'accesso degli utenti al dispositivo che infetta, richiedendo all'azienda un riscatto (ransom in inglese) da pagare per rimuovere la limitazione.

Ad esempio alcune forme di ransomware bloccano il sistema e intimano l'utente a pagare per sbloccare il sistema, altri invece cifrano i file dell'utente chiedendo di pagare per riportare i file cifrati in chiaro. [2]

Dal 1989, data di realizzazione del primo ransomware, il PC Cyborg o trojan AIDS, ne sono stati prodotti e immessi nella rete Internet decine di diverse "famiglie" ognuna con migliaia di varianti.

Sotto il profilo tecnico, i ransomware sono dei "trojan horse crittografici" e si caratterizzano perché si rivelano in un tempo brevissimo, a differenza, ad esempio, degli APT (Advanced Persistent Threat) che hanno per obiettivo di restare nel sistema il più a lungo possibile.

I ransomware più famosi sono stati in ordine cronologico:

- 2013 - Cryptolocker
- 2014 – CryptoWall, CTB-Locker, TorrentLocker
- 2015 - Ransom32, TeslaCrypt
- 2016 – Locky, CryptXXX, Petya, Petya-GoldenEye, Cerber, PokemonGo, Popcorn
- 2017 – WannaCry, NotPetya, Bad Rabbit
- 2018 - GandCrab, Ryuk
- 2019 – LockerGoga, Anatova, MegaCortex, Maze.

[1] Un programma/codice dannoso che mette a rischio un sistema
[2] Fonte: https://it.wikipedia.org/wiki/Ransomware

2. QUALI DANNI PROVOCANO.

I ransomware possono provocare danni di entità crescente: questa minaccia serve ad aumentare la pressione sull'azienda vittima dell'infezione e convincerla a pagare il riscatto richiesto.

Nella tabella che segue sono incrociate le minacce con i tipi di attacchi.

	blocco del sistema	cifratura dei dati	furto dei dati con minaccia di pubblicazione	attacchi DDoS	pubblicizzazione del ricatto in corso
estorsione	X	X			
doppia estorsione	X	X	X		
tripla estorsione	X	X	X	X	
quadrupla estorsione	X	X	X	X	X

Da sottolineare che il blocco del sistema avviene in genere cifrando la Master Boot Record (MBR) del disco, rendendo quindi impossibile anche l'avvio del computer.

3. PROBLEMATICHE LEGALI IN CASO DI PAGAMENTO.

Il pagamento del riscatto, sconsigliato da tutte le aziende di sicurezza informatica per l'incertezza del risultato atteso (lo sblocco del sistema o la decifrazione dei dati), pone altresì problemi di legittimità all'azienda vittima dell'infezione e al soggetto (hacker) a cui affluisce:

- reato di riciclaggio
- reato di favoreggiamento per l'aiuto dato all'hacker nell'assicurargli il profitto di un reato
- reato tributario
- reato di false comunicazioni sociali
- reato di autoriciclaggio se utilizzati fondi "neri".

4. COME AVVIENE E COME PREVENIRE L'INFEZIONE.

Nel corso del tempo sono stati individuate le vulnerabilità che consentono ai ransomware di infettare i sistemi, vulnerabilità che corrispondono anche alle azioni da eseguire o meno per prevenire l'infezione.

Oltre alle azioni di contrasto illustrate nelle tabelle che seguono, e che da sole rappresentano la quasi totalità delle contromisure più efficaci, l'azienda può e deve utilizzare i software antivirus/antimalware presenti sul mercato, sia gratuiti che a pagamento, tenendoli costantemente aggiornati.

	Cause / veicoli di infezione più diffuse	Azioni di contrasto
1	**Indirizzi di email** dai quali il mittente è potenzialmente riconoscibile, in quanto possono essere falsi anche SE quasi identici a quelli veri. Ad esempio, mario.rossi@azienda.it invece di mario.rossi@azienda.com	A. Porre SEMPRE la massima attenzione agli indirizzi di email dei mittenti, anche quelli con i quali abitualmente si scambiano email. B. NON aprire le email false. C. Le email sconosciute vanno Cancellare dalla cartella "Posta in arrivo" le email false e subito dopo dalla cartella Trash.
2	**Indirizzi di email** delle quali il mittente è da tempo conosciuto (ad esempio un cliente o un fornitore abituale), in quanto possono essere stati hackerati secondo una modalità di falsificazione nota come "spoofing".	A. Porre la massima attenzione ANCHE a questi indirizzi. B. In caso di dubbio, inviare una email di risposta chiedendo conferma dell'invio.
3	**Email da spamming**: messaggi ripetuti ad alta frequenza o a carattere di monotematicità, in genere di carattere commerciale.	A. Installare servizi Antispam che implementino i protocolli SPF, DKIM e DMARC, che bloccano quasi tutte le email di phishing, veicolo di ransomware. B. NON rispondere mai alle email di spamming. C. Controllare la casella di posta "Junk" dove confluiscono email di fonti ritenute incerte e pericolose dal sistema. D. Impostare la non-archiviazione nella cartella degli elementi pervenuti. E. Le email sconosciute vanno cancellate dalla cartella Junk e subito dopo dalla cartella Trash. F. Spostare le email che sono confluite per errore nella cartella Junk nella cartella "Posta in arrivo".

	Cause / veicoli di infezione più diffuse	Azioni di contrasto
4	**Email da phishing**: messaggi fraudolenti creati in modo da sembrare autentici, che in genere richiedono di fornire informazioni personali sensibili (password, PIN, IBAN, ecc) in vari modi: conferma di una iscrizione, ricezione di bonus e rimborsi, conferme di ordini, riattivazione dell'account, ecc.	A. Controllare la correttezza dell'indirizzo della email. B. Controllare l'autenticità del logo. C. Controllare la URL del link che si è invitati a cliccare per fornire le informazioni richieste: fare clic con il pulsante destro del mouse sul link, quindi copiare e incollare l'URL in un testo, esaminare il link, individuare eventuali errori grammaticali o di ortografia, evitando il rischio di aprire una pagina Web potenzialmente dannosa. Valgono anche le azioni di contrasto 3B, 3E ,3F.
5	**Allegati di email** delle quali il mittente non è assolutamente certo.	A. NON aprire gli allegati. B. Inviare una email di risposta chiedendo chiarimenti sulla identità del mittente e il motivo dell'invio della email e degli allegati.
6	**Cliccare su banner** (o finestre pop-up) pubblicitarie.	A. Evitare accuratamente di cliccare su banner o finestre pop-up di siti Web di cui non si è assolutamente certi (modalità di attacco "*drive-by download*").
7	**Esecuzione di macro** da parte di componenti Office (Word, Excel, PowerPoint).	A. Disabilitare l'esecuzione automatica, ove non assolutamente necessaria.
8	**Estensione dei file** allegati (esempio: *.doc, *.ppt, *.xls, *.pdf, ecc.), sapendo che i file più pericolosi hanno estensione *.exe, *.zip, *.js, *.jar, *.scr.	A. Abilitare l'opzione "Mostra estensioni nomi file" nelle impostazioni di Windows per riconoscere quelle potenzialmente più pericolose.
9	Collegamento di **supporti di memoria** esterni come chiavette USB, CD/DVD	A. Evitare di collegarli se la provenienza non è certa. B. Disabilitare la riproduzione automatica o "autorun" (modalità di attacco "baiting") di fiale *.exe. C. Adottare policy restrittive, che consentono l'utilizzo delle porte USB dei computer in dotazione agli utenti per collegare SOLO mouse, o smartphone, disabilitandone altri utilizzi.

	Cause / veicoli di infezione più diffuse	Azioni di contrasto
10	Utilizzo di siti e applicazioni consentono la **condivisione di file** con altri utenti.	A. Evitare di usare soluzioni gratuite e comunque di cui non si è assolutamente certi.
11	Sistemi operativi e browser.	A. Installare le "patch" (gli aggiornamenti) di sicurezza APPENA sono proposti e resi disponibili dai produttori del software.
12	Utilizzo di **account CON diritti** da amministratore.	A. Utilizzare SOLO account (UserID e password) con privilegi ed accessi di utente non-amministratore.
13	Utilizzo di **Remote Desktop Protocol** (RDP) che rappresenta in genere la porta 3389 esposta in rete.	A. Chiuderla SE non necessaria. B. Proteggere l'accesso con password forti. C. Proteggere l'accesso con doppia autenticazione (PIN inviato tramite SMS).
14	Utilizzo dei **plugin** di Java, HTML, Adobe, ecc.	A. Installare le "patch" (gli aggiornamenti) di sicurezza APPENA sono proposti e resi disponibili dai produttori dei plug in.
15	Utilizzo di **Adobe Flash Player**.	A. Disabilitarlo (abbandonato da Adobe a fine 2020).
16	Utilizzo di **software "craccati"**.	A. Evitare accuratamente di usare questi software e videogiochi non regolarmente acquistati o gratuiti erogati da siti Web di cui non si è assolutamente certi.
17	**Eventi "anomali"**: traffico dati superiore alla media, accesso ad indirizzi IP classificati come malevoli, accesso e scrittura in cartelle di sistema che non dovrebbero essere utilizzate.	A. Monitoraggio e protezione della rete aziendale con soluzioni di tipo "User Behavior Analytics" (UBA): Intrusion Detection System (IDS), Intrusion Prevention System (IPS), Endpoint Detection & Response (EDR), Sandboxing.
18	**Vulnerabilità** di soluzioni industriali (es. Windows Server Message Block versione 1.0, Microsoft Exchange Server.	A. Installare le "patch" (gli aggiornamenti) di sicurezza APPENA sono proposti e resi disponibili dai produttori delle soluzioni. B. Aggiornamento del browser utilizzato. C. Attivazione e aggiornamento della funzione di "Sicurezza di Windows". D. Installazione di Microsoft Defender Firewall.

5. COME ACCORGERSI E REAGIRE ALL'INFEZIONE.

Una volta installato, il malware può:

1. bloccare il funzionamento del sistema
2. iniziare a cifrare i file del disco rigido e delle condivisioni di rete mappate localmente con la chiave pubblica e salvare ogni file cifrato in una chiave di registro

La seconda azione (cifrare i dati) produce:

- il rallentamento del funzionamento del sistema, sia nell'utilizzo delle applicazioni che nella navigazione su Internet
- la perdita di spazio su disco
- la chiusura del sistema accompagnata da messaggi (schermata blu di errore (BSOD), segnalazione di un errore irreversibile Windows)
- il cambiamento della homepage, della toolbar, delle estensioni e plug-in del browser
- la comparsa di pop-up e link indirizzano a pagine web indesiderate
- il blocco del software antivirus installato nel computer.

In entrambi i casi, può comparire il messaggio che informa l'utente di aver preso possesso del computer o dei suoi dati, chiedendo un riscatto per la restituzione dela operatività (sblocco, decifrazione).

Se si sospetta che il computer sia stato contaminato da un ransomware che cifra i dati, occorre:

A. disconnettere immediatamente il PC dalla rete locale LAN
B. disattivare il WiFi
C. disconnettere dalla rete locale LAN eventuali server utilizzati per memorizzare copie di sicurezza dei dati (backup).

Se invece si è certi che il PC sia stato infettato o è bloccato, sapendo che il risultato non è assicurato, l'azienda:

I. può utilizzare software di de-criptaggio disponibili sia gratuitamente che a pagamento
II. può incaricare un'azienda specializzata nella cybersecurity
III. mette in atto le contromisure predisposte.

6. CONTROMISURE DA PREDISPORRE.

La difesa efficace dai ransomware richiede alcune contromisure che, va sottolineato, sono valide per qualunque azione accidentale o intenzionale, proveniente dall'interno o dall'esterno all'organizzazione, che sia stata o sia in grado di procurare danni all'attività aziendale, attraverso un incidente ai sistemi e/o ai dati.

	Contromisura e benefici	**Dettagli**
A	**Classificare i dati in base alla loro criticità.**	La criticità dei dati aziendali si identifica: • nella capacità di assicurare la continuità operativa dell'organizzazione (es. ricezione ordini, bollettazione, fatturazione, ecc) • nella possibilità di provocare danni patrimoniali (costi di ripristino dei servizi) e di immagine (reputazione presso i clienti) • nella possibilità di violare le norme applicabili (privacy) • nella difficoltà di reperire per reinserire i dati nei sistemi partendo da fonti attendibili (es. documenti cartacei, data base di altri soggetti).
B	**Individuare i sistemi che ospitano i dati critici.**	Un sistema, inteso sia come PC e server che come applicazione software, che gestisce dati critici è definibile un sistema critico.
	Il beneficio delle contromisure A e B è la possibilità per l'azienda di modulare gli investimenti a partire dalla protezione dei dati e dei sistemi critici che li gestiscono.	

	Contromisura e benefici	Dettagli
C	**Proteggere i sistemi**	Le azioni di protezione raccomandate e prescritte dagli standard sono: 1. l'isolamento dei sistemi collegati alla rete Internet (mail server, Web server, FTP server) 2. l'utilizzo per l'accesso solo di account-utente e non di account con privilegi di amministratore 3. la determinazione del tempo massimo di blocco operativo di ogni sistema critico (e quindi il tempo di ripristino in funzione degli stessi, **RTO o Recovery Time Objective**). In base a quanto lungo è il periodo di blocco che l'azienda definisce che possa sopportare, si appronta la soluzione per tamponare l'emergenza: 4. duplicazione dei sistema hardware che ospita applicazioni e dati critici 5. virtualizzazione dei server in un ambiente cloud (che è naturalmente ridondato).
	Il beneficio della disponibilità di un'infrastruttura ridondata è la possibilità per l'azienda di ripristinare la situazione di normalità superando in un tempo molto breve (basso RTO) gli effetti dell'infezione dei sistemi critici.	
D	**Proteggere le applicazioni software**	Le azioni di protezione raccomandate dagli standard sono: 1. produrre una copia del software applicativo in uso, che spesso è stato personalizzato per l'azienda 2. in alternativa, prevedere, nel contratto di manutenzione e assistenza stipulato con il fornitore del software applicativo, la fornitura in tempi ridottissimi di una copia anche in download dell'applicazione in uso 3. produrre una copia dell'ambiente software (Sistema Operativo, tool a corredo, ecc) che ospita il software applicativo, indispensabile per la corretta e rapida re-installazione del software applicativo in un nuovo computer/server (*vedi backup totale*). Le reazioni all'infezione sono: 4. il ripristino del sistema operativo sui sistemi infettati per tornare all'ultima configurazione non infettata 5. meglio ancora, la formattazione completa delle macchine infettate 6. l'installazione dell'ambiente e del software applicativo.
	Il beneficio della disponibilità di una copia dell'ambiente e del software applicativo è la possibilità per l'azienda di ripristinare la situazione di normalità di funzionamento superando gli effetti dell'infezione dei sistemi critici.	

	Contromisura e benefici	Dettagli

E	**Proteggere i dati**	Premesso che i dati critici possono essere sia dati strutturati (i record di un data base) che dati discreti (file PDF o di altro formato), l'altra **azione di protezione principale dall'infezione da ransomware**, oltre alla disponibilità del software applicativo, è la produzione di copie aggiornate dei dati utilizzati (backup). L'indice che l'azienda deve considerare per valutare le soluzioni di backup da adottare è l'**RPO o Recovery Point Objective**, che rappresenta la quantità di dati prodotti, memorizzati sui sistemi ma NON ancora sincronizzati su una copia di sicurezza. L'RPO indica il tempo che l'azienda ha definito che intercorra tra la generazione di un'informazione e la produzione della sua copia: di converso fornisce la quantità di dati che il sistema potrebbe perdere a causa di evento negativo (guasto, violazione).
E1	**Tipi di backup**	È possibile eseguire queste tipologie di backup: • backup totale o snapshot (sistema operativo, applicazioni software, settaggi e di tutti i dati in uso) • backup completo (tutti i dati in uso) • backup differenziale (tutti i dati diversi dall'ultimo backup completo) • backup incrementale (solo i dati in uso diversi da quelli dell'ultimo backup completo). La tipologia più efficace è il backup incrementale, che segue un ciclo di N esecuzioni: al termine del ciclo il primo backup incrementale del nuovo ciclo ricopre il primo backup incrementale del ciclo precedente. Va sottolineato che, al termine del ciclo di backup incrementale, va sempre eseguito il backup completo. Il backup totale risponde all'esigenza di proteggere le risorse software utilizzate per gestire i dati critici.
E2	**Le copie di backup**	Le copie di backup dovrebbero essere tre, secondo la regola 3-2-1, ovvero: • due copie "**on-site**" (nel sito aziendale) su storage differenti (Hard Disk, NAS, Cloud ecc.) • una copia "**off-site**" (in sito remoto) su Cloud o memorie rimovibili (USB memory card, nastri).

7. ORGANIZZAZIONE DEL BACKUP.

Ci sono due semplici regole che permettono di ottimizzazione la gestione del backup:

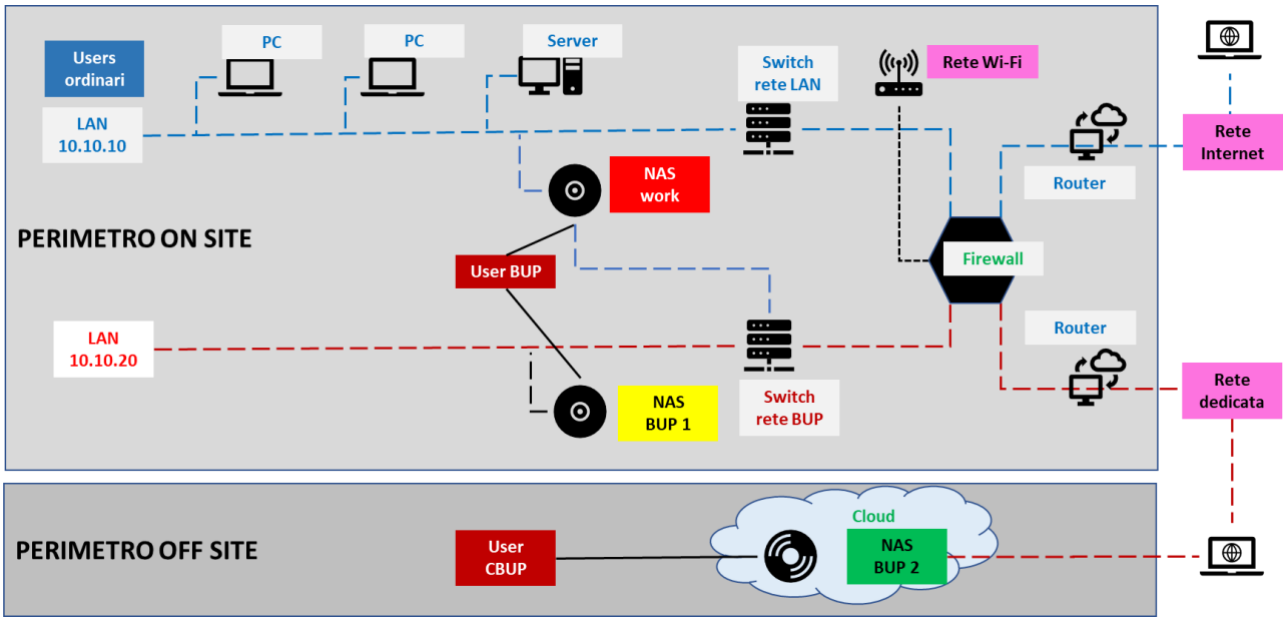
- organizzare il backup dei dati strutturati (record di data base) separatamente dalla produzione della copia di sicurezza dei file (dati discreti), in quanto le dimensioni ed il livello di aggiornamento delle informazioni dei due formati sono generalmente diverse;
- verificare periodicamente la capacità di ripristino del backup che prevedono il restore, essendo un'operazione più critica della semplice replica.

Ma l'obiettivo più importante nella gestione del backup è contrastare la capacità dei malware di propagarsi nelle reti aziendali, riuscendo così a bloccare non solo tutti i PC e i server collegati, ma anche le macchine dedicate a memorizzare le copie di sicurezza dei dati (backup).

Il contrasto a questa eventualità, che è diffusissima in tutte le dimensioni delle aziende, richiede di predisporre una rete aziendale che rispetti determinate accortezze in grado di minimizzare i rischi di diffusione del malware:

I. ridondanza del backup
II. segregazione di una copia di backup on site
III. allocazione di una copia off site.

Nella figura che segue è rappresentata una ipotetica rete aziendale in grado di minimizzare i rischi di diffusione del malware.



L'infrastruttura prevede questi elementi:

1. la realizzazione della rete LAN principale
2. l'attestazione del "NAS work" sulla rete principale sulla quale sono già collegati PC e server
3. lo switch che collega la LAN principale al Firewall
4. il Firewall multicanale che filtra il traffico verso la rete Internet sul canale ordinario
5. la realizzazione della rete LAN secondaria
6. l'attestazione del "NAS di backup 1" sulla rete secondaria
7. lo switch della rete di backup che collega la LAN secondaria al Firewall
8. il Firewall multicanale che filtra il traffico verso la rete Internet sul canale dedicato
9. l'attestazione del "NAS di backup 2" su una infrastruttura cloud
10. l'abilitazione di "Users ordinari" che possono lavorare solo sulle risorse IT collegate alla rete LAN principale
11. l'abilitazione di uno "User di backup", l'unico ad autorizzare l'esecuzione della memorizzazione dei dati registrati nel "NAS di backup 1" prendendoli dal "NAS work"
12. l'abilitazione di uno "User di Cloud backup", l'unico ad avere accesso ai dati memorizzati nel "NAS di backup 2" ospitati nel cloud, che sono la replica dei dai memorizzati nel "NAS di backup 1".

7.1 Il rapporto costi-benefici.

La realizzazione di una infrastruttura ICT come quella rappresentata può comportare costi anche elevati.

La valutazione sull'opportunità di sostenerli deve considerare da un lato la complessità del sistema informativo dell'organizzazione e dall'altra la dimensione dei dati e dei sistemi critici: in ultima analisi i rischi aziendali.

D'latra parte, **l'infrastruttura ICT** in figura **garantisce un livello molto elevato di sicurezza tecnica e la minimizzazione dei rischi legati ai diversi tipi di minacce** in grado di procurare danni all'attività aziendale, attraverso un incidente ai sistemi e/o ai dati:

A. azioni accidentali provenienti dall'interno dell'organizzazione (errori involontari di dipendenti e collaboratori, carenze tecniche e organizzative dell'azienda)
B. azioni accidentali provenienti dall'esterno dell'organizzazione (eventi naturali disastrosi)
C. azioni intenzionali provenienti dall'interno dell'organizzazione (azioni dolose di dipendenti e collaboratori)
D. azioni intenzionali provenienti dall'esterno dell'organizzazione (azioni dolose di hacker, ladri).

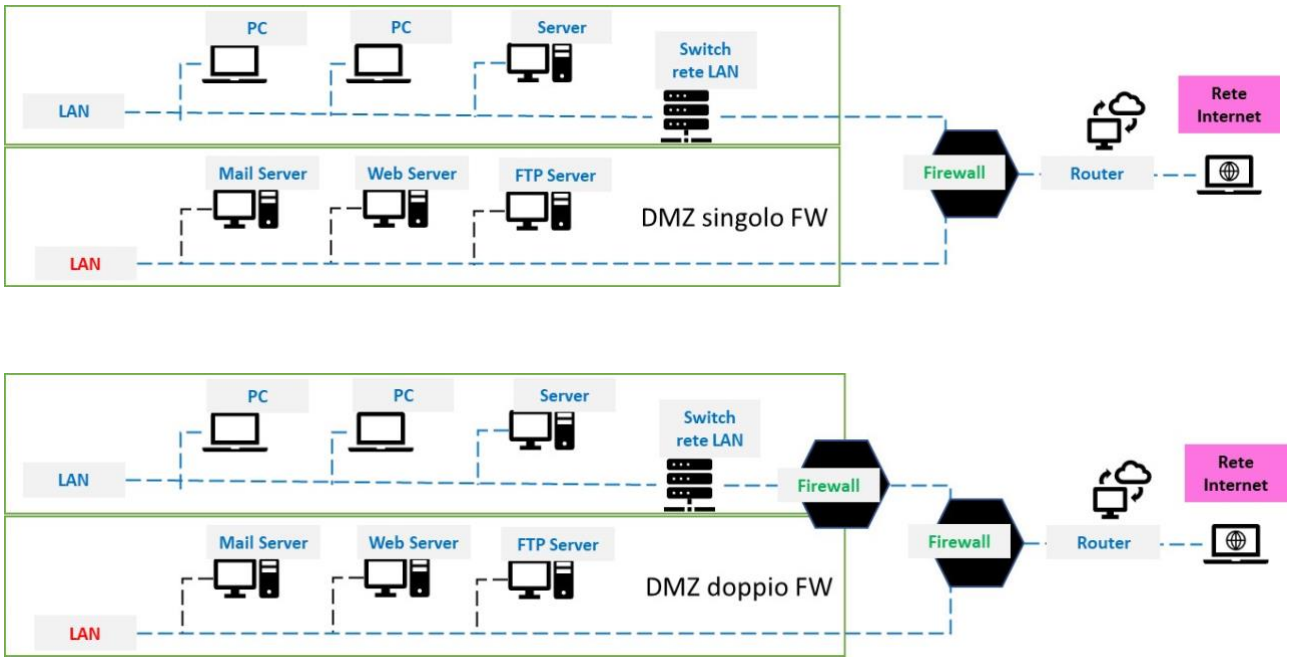
7.2 L'opzione DMZ.

La sempre maggiore digitalizzazione dei processi aziendali e l'utilizzo intensivo della rete Internet per abilitare numerosi servizi utilizzati da utenti interni all'organizzazione (dipendenti) ed esterni (prospect, clienti, fornitori), espongono le aziende agli attacchi che sfruttano questo canale di trasmissione.

L'infrastruttura ICT deve tenere conto di questa evidenza segregando i sistemi che sono esposti alla rete Internet in una sottorete fisica o logica, detta zona demilitarizzata (DeMilitarized Zone o DMZ), per proteggere la rete LAN ed i sistemi ad essa connessi.

I più comuni sistemi che erogano servizi basati su Internet sono email server (posta elettronica), Web server (presenza sul Web), FTP server (scambio di file).

Nelle figure che seguono sono rappresentate due tipi di DMZ, realizzate utilizzando uno o due Firewall, uno a difesa della LAN e uno per creare la zona demilitarizzata.



8. LA SCELTA DEI SERVIZI CLOUD.

La crescita del mercato del cloud computing dimostra la tendenza delle aziende a sostituiscono le proprie infrastrutture on site con i servizi cloud.

L'affermazione di questa dinamica è dovuta ad una serie di fattori: riduzione degli investimenti, spalmatura dei costi, maggiore indipendenza dalle competenze tecniche specifiche: in sintesi, la affermata comodità nell'ICT del "buy" sul "make".

In questo contesto, ad esempio, l'outsourcing di servizi di email e Web presence rende inutile la realizzazione di DMZ oltre a delegare la sicurezza ad operatori in genere estremamente affidabili.

Parimenti, la copia di backup ospitata in una infrastruttura cloud piuttosto che l'acquisto di software applicativo in versione SaaS o l'hosting dei server più critici sono scelte tecniche e imprenditoriali che agevolano il raggiungimento di un livello di sicurezza sempre più adeguato alle sfide poste dall'evoluzione delle tecnologie e delle minacce.