File Transfer (FTP) 21:

La porta in questione consente la condivisione, upload e download tra il client e il server.

Seppur semplice nelle sue funzionalità il protocollo è spovvisto di crittografia i dati sono

suscettibili a sniffing e attacchi MITM.

Un'alternativa più sicura sarebbe FTPS che ha le stesse funzionalità ma è affidabile

nella criptazione di dati sensibili.

SSH Remote Login Protocol 22:

SSH è un protocollo di rete crittografato utilizzato per operazioni sicure su reti non sicure.

Permette anche di accedere in remoto a un dispositivo e di trasferire file tra di essi.

Mantere aggiornato il software SSH e implementare sistemi di auntenticazione forti

usando le giuste configurazioni eviterà molti degli attachi informatici possibili.

Si consiglia anche di monitorare gli accessi del log per eventuali intrusioni.

TELNET 23:

Telnet fa si che ci sia una comunicazione bidirezionale tra due macchine su rete TCP/IP,

permette anche di accedere in remoto su un computer e di esegurie comandi come se si fosse

collegati localmente.

Non ha nessuna crittografia rendendolo vulnerabile a intercettazione e MITM, per questa ragione

se necessarie le funzione elencate soprastanti si consiglia di chiudere la porta e passare a SSH.

Simple Mail Transfer 25 (SMTP):

SMTP è un protocollo standard per l'invio di di email attraverso le reti IP dal client al server di posta

notificando eventuali errori nel processo.

Per evitare problemi di spam e abusi è necessario prevenire l'accesso non autorizzato usando meccanismi

di autenticazione forte.

Per impedire sniffing e MITM bisogna crittografare le comunicazioni usando SSL/TLS.

Domain Name Server 53 (DNS):

Essenziale per la risoluzione dei nomi di dominio va comunque configurata e calibrata correttamente

usando firewall e autenticazioni per impedire eventuali attacchi.

Nonostante le utilità il DNS non è necessaria al dispositivo del web server creando vulnerabilità facilmente evitabili.

World Wide Web HTTP 80:

Il protocollo in questione ha molte vulnerabilità ed è fortemente consigliato di evitare molte complicazioni

passando ad usare HTTPS che mantiene i dati integri usando un servizio di hashting.

La sostituzione proposta si aprirebbe sulla porta 443 consentendo anche la crittografia dei dati tramite SSL/TLS,

il server viene anche autentificato tramite certificati digitali.

SUN Remote Procedure Call 111:

Remote Procedure Call consente di invocare una determinata funzione sul web server in remoto da un'altro dispositivo.

Lasciare la porta aperta crea delle vulnerabilità ampliamente conosciute ad eventuali attaccanti quindi se non è necessaria

al server è preferibile bloccare la porta 111.

NETBIOS Session Service 139:

NetBIOS è solitamente usato su windows per condividere file e stampanti in rete locale, in poche parole permette

comunicazione tra i computer.

Essendo un protocollo datato ha varie vulnerabilità, come esporre i pc in comunicazione tra di loro e rendendono le

sessioni vulnerabili a spoofing.

Se la sua funzione rimane necessaria all'azienda si consiglia di usare TCP/IP o DNS che risultano

simili ma con sistemi di sicurezza più robusti.

Microsoft-DS 445:

La porta in questione è una delle più vulnerabili essendo spesso soggetto di attacchi informatici, il protocollo è pensato unicamente

per la condivisione di file e stampanti tramite pc con diversi OS senza imporre nessun sistema di sicurezza.

Per farne uso è cruciale implementare autenticazioni forti, crittografie, controllo degli accessi e isolare le rete a questa

funzone solo dove necessario.

Per evitare molte problematiche è preferibile chiudere la porta.

Remote process execution 512:

Come altri protocolli permette di eseguire comandi da remoto sul server, utile per amministratori e sviluppatori per gestire

il web dell'azienda.

Nonostante ciò comporta delle problematiche di sicurezza come un'autenticazione debole e una mancanza di cifratura,

l'alternativa migliore sarebe usare SSH.

Remote Login 513:

Il servizio Remote Login permette l'accesso in remoto al server usando una connessione TCP così da poter eseguire comandi

e accedere i file da altri dispositivi esterni.

Per queste stesse ragioni va strettamente monitorata e configurata per impedire qualsiasi abuso, ha anche gravi problemi

come una mancanza di cifratura e di autenticazione forte.

Come la precedente è meglio passare a SSH che mantiene la stesse funzioni.

REMOTE SHELL 514:

Problematica: permette a utenti esterni di eseguire comandi sulla macchina del server in remoto senza la necessità di autorizzazioni,

anche usare semplicemente Remote Shell senza aggiunte di sicurezza può comportare a una intercetazzione dei dati che sono pericolosamente non criptati.

Implementare sistemi di autenticazione e criptazione è essenziale per mantenere l'integrità del server anche come riconfigurare correttamente il firewall.

RMI REGISTRY 1099:

Questa funzione di Java permette di registrare in una sorta di rubrica tutti i dispositivi collegati in remoto facilitandone la connessione.

Non essendo provvisto di metodo di autenticazione e crittografia chiunque può modificare i registri creando connessioni non sicure o collegamenti Man-In-The-Middle.

Altri rischi sono di andare incontro ad attachi DOS (Denial of service) e RCE (Remote code execution).

Configurare il registro con autenticazione e criptazioni delle connessioni può evitare molte di queste problematiche.

INGRES /DTSPCD 1524:

Ingres permette la gestione e archiviazione dei dati nel database del server, bisogna assicurarsi che sia aggiornato per evitare vulnerabilità nel server.

Il DTSPCD comporta dei rischi nella manipolazione dei dati e la porta è consigliato chiuderla per evitare che attaccanti esterni possano accedere sul server con privilegi Root e mantenendosi collegati con una backdoor.

NETWORK FILE SYSTEM 2049:

Permette la condivisione efficiente dei file sulla rete di un server.

Per rendere sicura questa funzione bisogna implementare un servizio di autenticazione o limitare con il firewall l'accesso ad utenti esterni non riconosciuti.

Non avendo le funzioni capaci di criptare i dati si consiglia di implementarne per evitare vulnerabilità come SNIFFING e MITM.

CCProxy FTP / SCIENTIA-SSDB 2121:

CCProxy è un software che permette la gestione di dati attraverso il protocollo FTP e all'uso del servizio di SCIENTIA-SSDB.

La porta se lasciata aperta mette in rischio il server a uso di codici in remoto, senza autenticazione e lettura dei dati non criptati adeguatamente.

Si consiglia vivamente di chiudere la porta se non necessaria o affidarsi a FTPS invece di FTP avendo delle funzionalità molto più sicure per gli standard di oggi.

MySQL 3306:

Questo sistema permette la gestione dei database ed è utile per il supporto di applicazioni web dinamiche.

Per evitare accessi non autorizzati si consiglia di configurare il firewall consentendo l'accesso solo agli ip di rete fidati della rete interna.

Implementare un sistema di autenticazione a due fattori e mantenere aggiornato il software sono cruciali per mantenere la sicurezza del server.

POSTGRES DATABASE SERVER (PostgresSQL) 5432:

Utile per stabilire connessioni tra il client e il server capace di inviare query SQL al server per eseguire operazioni CRUD.

Limitare l'accesso con l'uso di firewall e autenticazioni sicure può limitare l'area di attacco del server.

Aggiornare e configurare il software sono elementi cruciali per mantenerne la sicurezza.

VNC Virtual Network Computing 5900:

La porta in questione permette l'accesso in remoto al server potendo così di mantenere aggiornato e risolvere eventuali problemi senza dover essere fisicamente presenti.

Come le precedenti, seguire gli stessi passagi di configurazione per il software e il firewall limitando gli ip a quelli aziendali.

L'implementazione di un sistema di autenticazione per l'uso in remoto è necessario per evitare che esterni sfruttino le funzioni del VNC.

X-Windows / W32.LoveGate.ak virus 6000:

Questa porta presenta già delle vulnerabilità ed è da chiudere immediatamente essa sfrutta X-Windows per accedere

alla grafica del web server, va scansionata la rete per eventuali virus già presenti.

IRC (Internet Relay Chat) 6667 :

Permette la discussione attraverso una chat tra i dispositivi client e il server.

Spesso trojan e backdoors sfruttano la porta per mantenere l'accesso al server, ormai in declino questo protocollo

è preferibile evitarlo per non andare incontro a svariate exploit.

Chiudere la porta e usare un sistema di comunicazione in tempo reale alternativo è la scelta preferita, in poche parole

è meglio chiudere la porta.

Apache JServ Protocol 8009:

L'ultima porta aperta nella lista è usata per le comunicazioni tra Apache e l'applicazione del server in maniera efficiente alleggerendo il traffico di rete.

Se le funzioni non sono necessarie è meglio chiudere la porta per evitare gravi danni all'integrità del web aziendale.

Configurare con autenticazioni e crittografie i datiche vengono inviati è necessario per assicurare la sicurezza del protocollo.