UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII
Dipartimento di Ingegneria
dell'Informazione

unIMC

Case study
Rool out ERP: considerazioni relative alla sicurezza

Lorenzo Bossoletti

lorenzo.bossoletti@gmail.com

Martedì 19 Luglio 2022

Corso di Perfezionamento in Cybersecurity, Cyber Risk and Data Protection

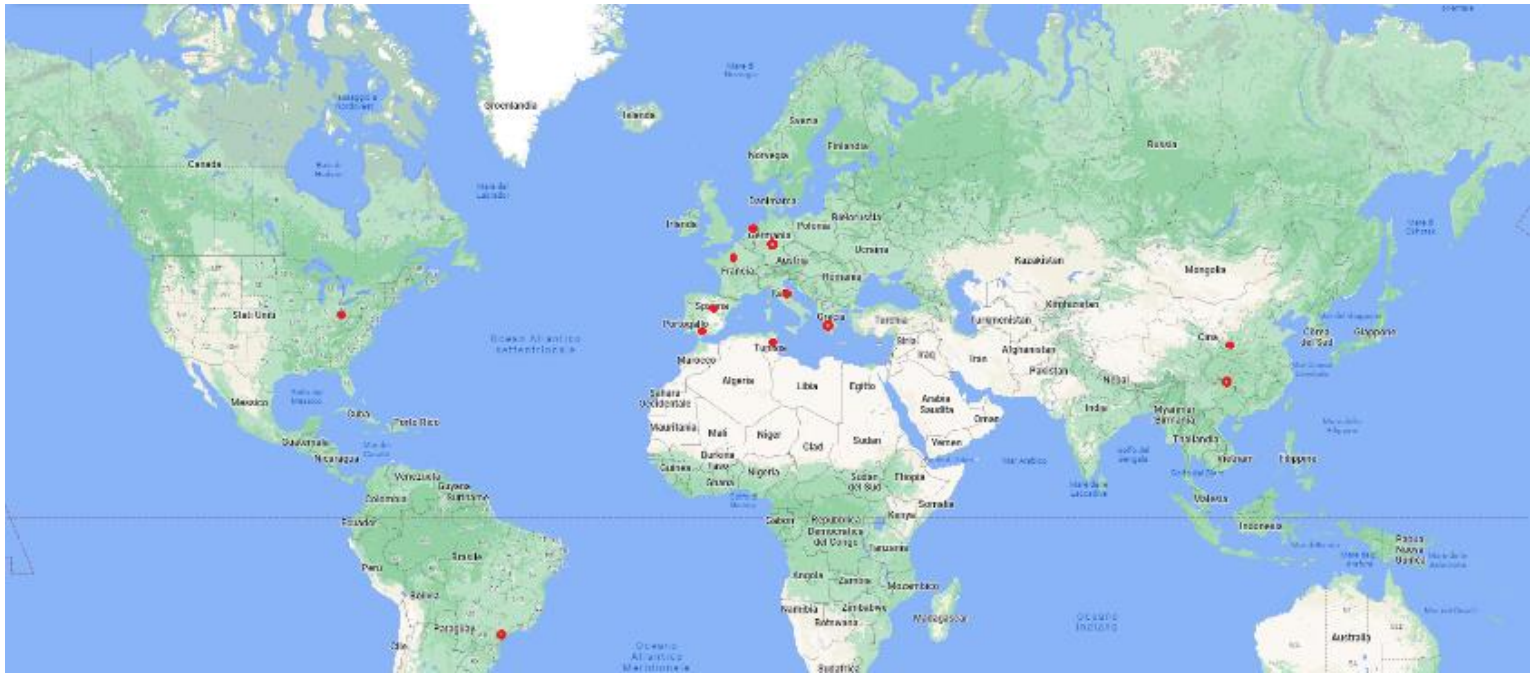
Introduzione del progetto

Introduzione del progetto

- ERP (Enterprise resource planning): Applicazione che le organizzazioni utilizzano per la gestione quotidiane del business.
- Sono applicazioni modulari:
  - Accounting
  - Procurement
  - Sales
  - Warehouse
  - Project management
  - Operations
  - Quality management system
  - After sales
- Elaborazione dati on line / Real Time
- Architettura client / server

Introduzione del progetto

- Gruppo che produce impianti e macchine industriali Fatt. 120 Mil
  - Sede Italiana HQ Ancona: 100 utenti
  - Spagna: 40 utenti
  - Germania/Olanda: 30 utenti
  - Francia: 2 utenti
  - Grecia: 10 utenti
  - USA: 10 utenti
  - Tunisia: 15 utenti
  - Brasile: 25 utenti



Come esporre il servizio

Come esporre il servizio

- Soluzione ERP nata per un utilizzo solo nella sede Italia, in LAN, autenticazione con SSO (single sign on)
- Come renderle disponibile il servizio all’estero
- Tema Sicurezza: quali sono le soluzioni disponibili e quali sono quelle maggiormente adatte al contesto del Gruppo

Soluzione disponibili

- PPTP VPN
  - Utilizzo adatto per uso domestico o small business o comunque limitato a brevi periodi. Accesso tramite programma VPN, autenticazione in genere avviene con utente e password (Point to Point Tunneling Protocol)

- STS VPN
  - In questo caso gli apparati di rete alle due estremità si occupano di realizzare la virtual private network e quindi la gestione del traffico e della crittografia. Viene creato un tunnel sicuro per garantire le comunicazioni all'interno di una rete. I metodi di funzionamento di IPSec sono due: "tunnel" e "trasport". In modalità tunnel tutto il pacchetto dati, indirizzo IP incluso, viene crittografato mentre in modalità trasport vengono crittografati solo i dati scambiati. Richiede l'installazione e la configurazione dei client prima dell'utilizzo. (Site to Site VPN)

Soluzione disponibili

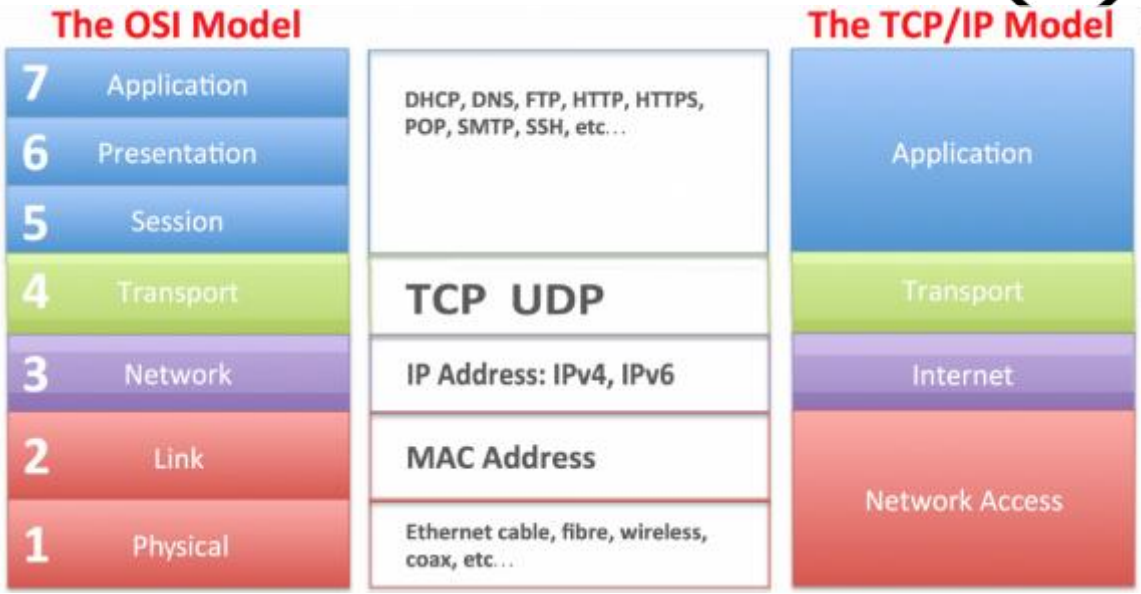
- SSL / TSL
  - In questo caso la connessione VPN è limitata alle applicazioni specifiche e non a tutta la rete. Inizialmente utilizzati principalmente per gli acquisti e per servizi sul web. Forniscono una connessione sicura tra il browser client e il server dell'applicazione, grazie alla crittografia. (Secure Socket Layer, Transport Layer Security)

- MPLS VPN
  - E' una tecnologia di data forwarding che controlla il flusso del traffico di rete e ne aumenta la velocita. Ogni MPLS indirizza i dati in un percorso tramite etichette (label) invece di richiedere complesse ricerche in una tabelle ai routing ad ogni fermata. (Multi protocol Label Switching)

Soluzioni approfondite

Soluzioni: SSL/TSL

- Soluzione SSL / TSL (protocotto HTTPS): sono protocolli crittografici di presentazione, permettono una comunicazione sicura end to end. Fornendo autenticazione, integrità dei dati confidenzialità.
- Il funzionamento del protocollo TLS è suddiviso in tre fasi:
  - Negoziazione fra le parti dell'algoritmo da utilizzare
  - Scambio delle chiavi e autenticazione
  - Cifratura simmetrica e autenticazione dei messaggi
- SSL/TLS crittografa i dati delle connessioni di rete a livello di applicazione, il protocollo è inizializzato nel livello 5 (livello di sessione) e reso funzionante nel ***livello 6*** (livello di presentazione).

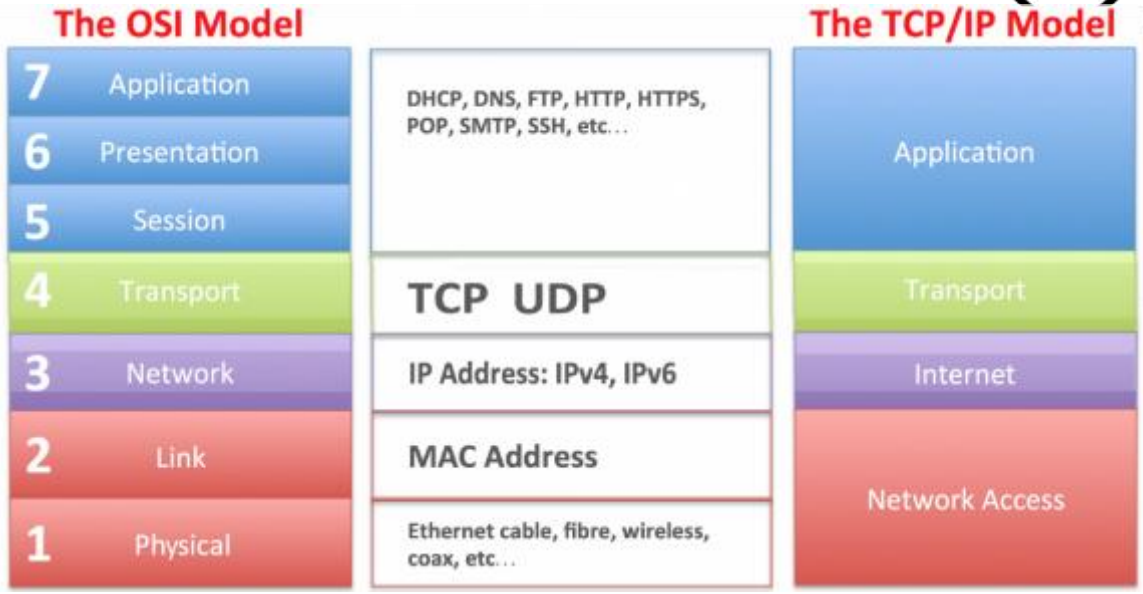


- Vantaggi:
  - Costi ridotti certificato,
  - Connessione client server
  - Relativa semplicità di configurazione
  - Non richiede hardware aggiuntivo
- Punti di attenzione:
  - Limitata alle applicazioni SSL, non a tutta la rete.
  - Il servizio è esposto nel web

Soluzioni: VPN Site to Site

- VPN Site-To-Site ci consente di instaurare un tunnel sicuro che passa tra diversi router e provider, rimanendo completamente trasparente ai client

- IPsec è un protocollo che opera a ***livello 3*** del modello ISO/OSI, rimanendo trasparente alle applicazioni che non devono avere nessun particolare prerequisito per interoperare.



- Vantaggi:
  - Sfruttamento delle risorse gia presenti, linee di connessione internet
  - Massima flessibilità di accesso alle risorse aziendali
  - Architettura facilmente scalabile

- Punto di attenzione:
  - Richiede hardware aggiuntivo, costi più elevati

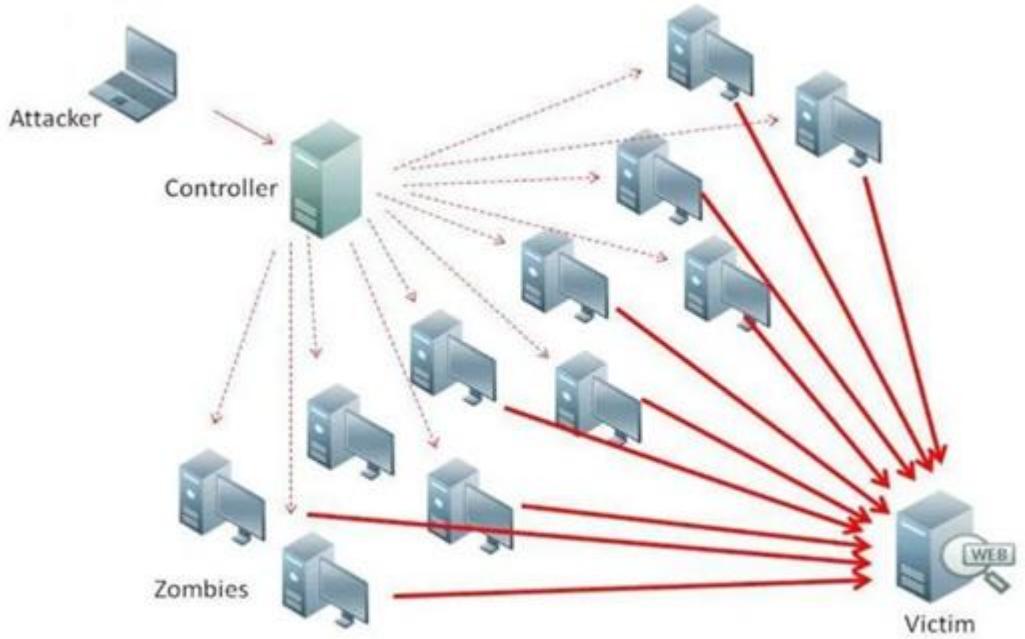
Scenari di attacco

Scenari di attacco: DDoS Attack

- Un attacco DDoS (*Distributed Denial of Service*) è un tipo di attacco che viene condotto ai danni di un server con l'obiettivo di compromettere la sua operatività.
- Un DDoS prevede la creazione di una enorme quantità di connessioni HTTPS dirette simultaneamente verso il server bersaglio, allo scopo di saturare le sue capacità di gestione delle stesse, impedendo così ai client "legittimi" di utilizzare il servizio.

- Se il servizio Https è esposto verso internet e quindi potenzialmente più soggetto a questa tipologia di attacco poiché il domino di attacco è esteso a tutto il web.

- I servizi che invece sono protetti da VPN site to site risultano meno esposti, poiché sono visibili solo agli utenti presenti nei siti interconnessi



Scenari di attacco: Ransomware

- Un ransomware è un tipo di virus che prende il controllo dei computer di un utente ed esegue la crittografia dei dati e quindi chiede un riscatto per ripristinare il normale funzionamento.
- Si diffonde generalmente mediante attacchi di phishing o clickjacking
- Una volta entrato nella rete, il virus è in grado di muoversi e diffondersi lateralmente su tutti i dispositivi.

- Quindi una volta entrato in una rete con n connessioni VPN site to site questo è potenzialmente libero di diffondersi in ogni dispositivo

- Nel caso di connessioni SSL TSL il client viene compromesso, ma questo non accedendo alla rete non compromette la rete interna

Considerazioni Finali

Considerazioni Finali

- Il rischio zero non esiste

- Prevenzione:
  1. Analisi rischi
  2. Piani di mitigazione
  3. Compliance GDPR
  4. Formazione del personale (pillole periodiche/questionari/sessioni asincrone)
  5. Redazione/Aggiornamento procedure (27001 / 27701)
  6. Assessment e test
  7. Audit, Vulnerability test
  8. Ripartire dal punto 1

Considerazioni Finali

- La scelta della soluzione richiede un’attenta valutazione dei pro e dei contro dei diversi tipi di VPN. E’ strettamente connessa con le specifiche esigenze di ogni singolo progetto:
  - Livello di sicurezza richiesto
  - Numero di servizi/applicazioni che a tendere si vorranno esporre
  - Numero utenti per ogni singola filiale
  - Analisi costi / benefici

Considerazioni Finali

- Nel nostro caso la scelta è stata quella di dotarsi di connessioni VPN site to site con le consociate (security appliance Cisco Meraki MX series: 64/100/250 fault tolerance)

- Sebbene i costi (investimenti) siano più elevati ha pesato nella scelta:
  - gli aspetti relativa la sicurezza
  - maggiore affidabilità del servizio
  - la possibilità di esporre un maggior numero di servizi
  - l'adozione di una architettura unificata completa (unica dashboard in cloud per la gestione)

Considerazioni Finali: effetti positivi

- Domini:
  1. Federazione domini esistenti
  2. Unico dominio on premise (Group Policy)
  3. Migrazione Azure (multi factor authentication)

- Armonizzazione delle applicazioni:
  1. Exchange locali → unico Exhange
  2. soluzione unica per cad / plm
  3. Unificazione dei processi aziendali
  4. Armonizzazione dei dati

- Approccio globale al tema della sicurezza

Grazie

Lorenzo Bossoletti

lorenzo.bossoletti@gmail.com