wallix

bjosora
Operational Technologies

Proteggere gli ambienti OT nell'era della trasformazione digitale:

approfondimenti da un esperto del settore

Agenda del Webinar

1. 10:00 Introduzione [Wallix]

- Benvenuto ai partecipanti e presentazione del tema del webinar
- Breve introduzione di Federico e del suo background (evidenziare la sua esperienza in ENEL e la sua competenza in ICS/OT)
- Definire le aspettative per il webinar (ad esempio, "Questa sarà una sessione interattiva focalizzata su approfondimenti pratici e sfide reali nella cybersecurity OT")

2. 10:10 Presentazione [Bjosora]

- ➢ Il panorama delle minacce in evoluzione negli ambienti OT:
  - Come le minacce informatiche stanno cambiando nel settore delle infrastrutture critiche e industriali.
  - Esempi reali di incidenti informatici OT (ad esempio, ransomware, attacchi alla catena di approvvigionamento).
- ➢ Le principali sfide nella protezione degli ambienti OT:
  - Sistemi legacy e le loro vulnerabilità.
  - La convergenza tra IT e OT e le sue implicazioni per la sicurezza.
  - L'importanza di proteggere l'accesso remoto e i fornitori terzi.
- ➢ Best practice per la cybersecurity OT:
  - Il ruolo del Privileged Access Management (PAM) negli ambienti OT.
  - Come bilanciare sicurezza ed efficienza operativa.
  - L'importanza dei principi zero-trust in OT.
- ➢ Il futuro della sicurezza OT:
  - Tecnologie e tendenze emergenti (ad esempio, AI, IoT, integrazione cloud).
  - Come le organizzazioni possono prepararsi per la prossima ondata di minacce.

3. 10:40 Domande e risposte [Parte interattiva]

2.1 Il panorama delle minacce in ambiente OT: la storia

Premessa:

- è la storia vista dal mio personale punto di vista, di chi non si è mai occupato di IT o ICT, ma solo di **OT** (come si dice oggi, all'inizio era telecontrollo tanto e automazione poca per arrivare ai giorni nostri a tantissima automazione);
- l'IT è sempre stato affianco perché le dotazioni che l'azienda mi ha dotato erano fornite dall'IT.

2.1 Il panorama delle minacce in ambiente OT: la storia

Anni ‘80 del 20° sec.

- OT: mini computer DEC, 16 bit, MMU, real time OS, multitasking, multi user e logica cablata assai diffusa; RTU su tech. discreta, rete dati analogica;
- IT: mainframe IBM, sistemi di fatturazione e paghe;
- Tech.: appaiono i microprocessori 8080 - 8086; gli inverter di potenza
- Realizzazione del primo EMS;
- Nessuna manutenzione remota, solo in sito;
- investimenti in OT stimati oltre 500M€.

Anni ‘90 del 20° sec.

- OT: mini computer DEC a 16 bit su LSI in LAN, MMU real time OS, multitasking e logica cablata assai diffusa; RTU su tech CMOS, rete dati analogica;
- IT: mainframe IBM per sistemi di fatturazione e paghe; distribuzione massiva di PC; LAN scarse;
- Tech.: appaiono il processori 64bit RISC; nascono i microcontrollori;
- Messa in servizio sistematico di sistemi SCADA;
- Primi sistemi di manutenzione remota basare su terminal server (veri) e multiplex (4-8 porte RS232);
- investimenti stimati in OT oltre 230M €.

Anni ‘00 del 21° sec.

- OT: PC su architettura x86 32bit in LAN, MMU, no-real time, multitasking solo a divisione di tempo, multiuser abbozzato; rete dati basata su TCP/IP; RTU embedded con protocollo standard IEC;
- IT: si concentra su pochi datacenter su mainframe; distribuzione massiva di PC; LAN con cablaggio strutturato di palazzo; posta elettronica; introd. antivirus;
- Nuova generazione SCADA; primi usi di PLC e microcontrollori per automazione; completiamo il decennio con STUXNET;
- Sistemi di manutenzione remota basati su RAS (call back); cellulare e satellitare dal Millenium bug (ipotetico); uso dei notebook;
- investimenti stimati in OT non più di 35M €.

2.1 Il panorama delle minacce in ambiente OT: la storia

Anni 2011 - 2015.

- OT: server su architettura AMD64 64bit in LAN, MMU, no-real time, 32bit, multitasking solo a divisione di tempo, multiuser; rete dati TCP/IP, RTU embedded protocollo IEC;
- IT: si concentra su pochissimi datacenter su mainframe e server distribuiti; distribuzione massiva di NB; LAN con cablaggio strutturato e WiFi; posta elettronica e siti WEB aziendali; admin-to-user,
- Introduzione del Dominio di Autenticazione OT; segmentazione della rete IP; patching, antivirus, whitelisting; prime automazioni interamente a PLC, microcontrollore; soft PLC su RTU;
- Manutenzione remota in VPN anche mobile;

Anni 2016 - 2020

- OT: sistemi virtualizzati su multiprocessore a 64bit, no-real time, 32bit, multitasking solo a divisione di tempo, multiuser; rete TCP/IP; compresenza IT-OT in impianto; RTU embedded con prot. IEC, potenz. soft PLC;
- IT: smantellamento dei datacenter migrazione in cloud; diffusione smartphone come strum. lavorativo;
- Segmentazione rigorosa della rete OT; introduzione di firewall d'impianto; introduzione massiva automazione basata su microcontrollore e PLC; introduzione del monitoraggio di processo e IDS; primo tentativo di introduzione di protocolli basati IEC 62351; automazioni su soft-PLC sempre più potenti;
- manutenzione da remoto in VPN con IAM con MFA;
- investimenti stimati in OT nel decennio 201x ca. 65M€.

Anni 2021 - 2025

- OT: diffusione della virtualizzazione nei Control Center tanto quanto negli impianti; diffusione di embedded, le RTU diventano puri gateway; appare l'impiego di servizi cloud;
- IT: solo cloud, SAAS; smart working - smart office; CERT;
- Diffusione a tutti i livelli di segmentazione, dominio di autenticazione, patching, antivirus, monitoraggio, IDS/IPS con largo uso di AI; anomaly detection;
- operazione quasi esclusivamente da remoto adozione di sistemi di separazione e monitoraggio dell'attività da remoto (adozione di sistemi IAM e PAM combinati);

2.1 Esempi di attacchi in ambito OT

Da cosa va protetto un sistema OT?

- Sabotaggio ai sistemi di telecomunicazioni (non dimentichiamo la sicurezza fisica);
- l'accesso per vie "legali" guadagnato per via "illegale" (leggi furto di credenziali);
- l'abbiamo già citato l'invenzione di software capace di replicarsi, all'inizio era solo un gioco (i virus attaccano popolazioni con lo stesso DNA);
- anche STUXNET l'abbiamo già citato, un virus classico capace di modificare moduli di automazione industriale;
- gli attacchi coordinati sfruttando macchine compromesse di ignari proprietari (Botnet);
- l'attacco alla rete di distribuzione in Ucraina, dall'email all'intrusione nei sistemi OT;
- La comparsa dei ransomware con ondate potenti spinti dai facili guadagni;
- La combinazione ransomware (o altro virus aggressivo) VPN.

2.2 Le principali sfide nella protezione degli ambienti OT

- Garantire un accesso sicuro localmente e remotamente (monitoraggio delle attività, log riservati all'audit, identificazione sicura, concessione dei privilegi minimi per quello che devi fare)
- Gestione di sistemi con ambienti che vanno da Win NT 4.1 a Linux di ultima generazione, passando per i firmware di decine e decine di sistemi embedded che anch'essi sono vulnerabili (dispositivi di rete, molti funzioni di automazione, ecc.);
- Qualcuno pensa che la convergenza IT - OT sia il superamento delle differenze fra i due mondi invece …. non è così
- In termini IEC 62351 si chiama NSM (Network Management System), sistema di controllo del sistema di controllo, indipendente, con banda riservata con accesso PAM rigidamente esclusivamente riservato alle funzioni di Operation chiave. Non esiste nessun sistema di rete sicuro se non lo è anche il suo sistema di controllo.
- backup delle configurazione certo, sicuro e immodificabile;
- ciclo di vista di applicazioni e/o relativi firmware ben definito organizzativamente.

2.3 Best practice per la cybersecurity OT

1. La protezione del perimetro fisico
2. La segmentazione geografica e locale delle reti (sono ammesse solo le rotte strettamente necessarie, fuori e dentro l'impianto OT)
3. Funzioni di monitoraggio che alimentano IDS/IPS su tutti di "varchi" di segmentazione;
4. Autenticazione degli operatori mediante IAM e autorizzati ad operare mediante PAM nel modo più capillare possibile;
5. Patching di OS, software e firmware ad ogni livello basati su VA certe e sistematiche;
6. Protezione dei dispositivi tramite EDR (comprendo qui antivirus evoluti, whitelisting, anomaly detection, ecc.); dopo un attento hardening se si parte da OS general purpose;
7. Uso di applicazioni sviluppate con un sano concetto RBAC (a minimo privilegio per quello che devi fare);
8. Backup a tutti i livelli (versioni fw, os, applicativo, di configurazione, ecc.) certi, non alterabili e memorizzati in un luogo sicuro;
9. Riconoscimento di ciascun dispositivo e operatore tramite un certificato in modo da consentire la sicurezza E2E, ma anche l'approccio zero-trust; inserimento nel sistema di una PKI OT;
10. Impiego di soli protocolli (OT) sicuri, cioè garantito da scambio iniziali di certificati, da cifratura del canale e mutua autenticazione applicativa per E2E security.

2.4 Il futuro della sicurezza OT

- Adottare quella che fin dal 2010 definimmo nel mio gruppo “Smart authentication” basata su riconoscimento via certificato di manutentori/operatori associato in modo sicuro (certificato in smartphone presentato dopo riconoscimento biometrico);
- Lo stesso deve valere per i dispositivi che possono essere tutti dotati di un certificato che li identifica univocamente;
- Questo richiede l’adozione di nuove tecnologie che rendano “trasparenti” oggetti e meccanismi complessi come quelli legati alle CA.

Grazie per la vostra attenzione

- 250 bis, rue du Faubourg Saint-Honoré
  75008 Paris, France
- +33 1 53 42 12 81
- info@wallix.com

- via Guecello Tempesta, 59
  30033 Noale, Città Metropolitana di Venezia, Italia
- +39 041 82 21 386
- info@bjosora.com