Diodo dati - Laboratorio Industria 4.0

Scenario

Le reti tecnologiche all'interno di infrastrutture industriali critiche possono costituire la spina dorsale di un'impresa. Ogni nuova connessione di rete, dal monitoraggio del sistema di controllo industriale ai dispositivi intelligenti, introduce un nuovo vettore per gli attacchi informatici e, di conseguenza, rappresenta un aumento della superficie per eventuali vulnerabilità. Per questo motivo vi è un'urgente necessità globale di strumenti più efficaci per combattere le minacce informatiche e proteggere queste reti da attacchi che potrebbero causare gravi danni fisici, personali o finanziari. Le migliori pratiche per la protezione di queste reti implicano la semplificazione, la riduzione e l'isolamento delle connessioni di rete, inclusa la segmentazione delle reti l'una dall'altra creando una separazione virtuale o fisica tra di esse. Tuttavia, la separazione fisica o virtuale può impedire alle informazioni e ai dati di raggiungere gli utenti autorizzati e queste reti spesso contengono una grande quantità di informazioni che sono troppo preziose per essere semplicemente scartate.

I sistemi di trasferimento dati unidirezionali, chiamati genericamente "diodi dati", sono stati progettati specificamente per affrontare questo problema di sicurezza fornendo una difesa di rete rafforzata e condividendo in modo sicuro i dati. I diodi dati rappresentano una prima linea di difesa, isolando e proteggendo le reti dalle minacce informatiche esterne, consentendo a queste reti di importare o esportare dati in modo altamente controllato e deterministico. I diodi dati, in combinazione con altri strumenti, dispositivi, software e best practice di sicurezza informatica, aiutano gli utenti, gli operatori e i professionisti della sicurezza a ridurre i rischi per proteggere le proprie reti e i dati dalle minacce informatiche.

Realizzazione

Per la realizzazione di questo progetto si ipotizza di collegare fra loro due reti (visibili in Figura 1): una sicura (IT Network) e una non sicura (External Network). Questo collegamento avverrà tramite un diodo dati realizzato attraverso due Raspberry Pi o Arduino collegati in tre diverse modalità:

1. via cavo seriale;
2. via cavo Ethernet (eventualmente da modificare fisicamente affinché sia realizzata una vera comunicazione unidirezionale e non simulata);
3. tramite comunicazione a infrarossi.

Per la comunicazione tra le due Raspberry Pi si ipotizza di realizzare la comunicazione tramite due servizi/processi realizzabili con il linguaggio di programmazione desiderato (ad esempio Python).

Rasp-A rappresenta un collettore dati che ha il compito di ricevere tutte le informazioni dalle diverse macchine all'interno della rete "IT Network" e di inoltrarle alla rete non sicura "External Network" tramite comunicazione unidirezionale. Per la raccolta di informazioni e delle metriche di tutti gli host e macchinari presenti nella rete IT Network, è possibile utilizzare diverse soluzioni come ad esempio Zabbix (software Open Source per il monitoraggio di reti e dei sistemi informatici) o similari. Questi strumenti saranno installati all'interno di Rasp-A, che, a intervalli regolari, avrà il compito di trasmettere i dati verso Rasp-B.

Come anticipato, questa comunicazione avverrà tramite una delle tre tipologie di diodi e il processo sulla Rasp-A dovrà aprire la comunicazione in sola scrittura, mentre il servizio situato su Rasp-B in sola lettura. Ricevute le metriche sarà necessario salvare queste informazioni all'interno di un database e visualizzarle tramite delle dashboard. L'interfaccia di visualizzazione all'interno della Rasp-B può essere realizzata tramite diverse soluzioni software, ad esempio Grafana o Thingsboard.

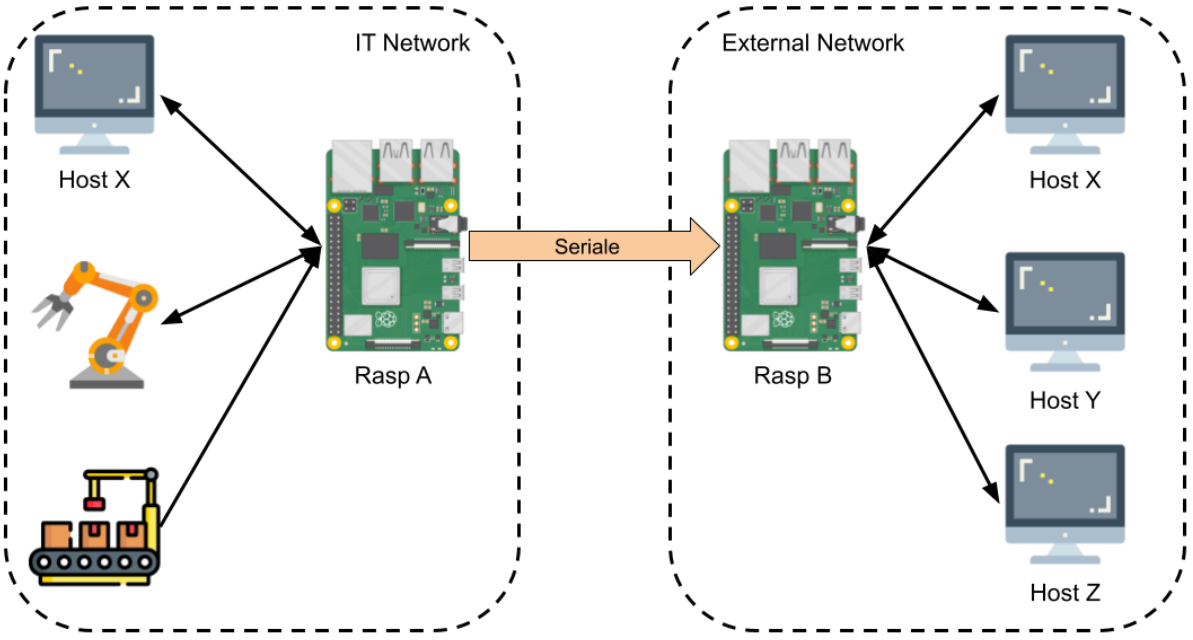

Figura 1. Esempio schema architetturale

Realizzare infine un bot Telegram da posizionare sulla Rasp-B che permetta di ricevere dei messaggi in caso di allarmi o di visualizzare alcune tipologie di metriche delle macchine monitorate.

In dettaglio per la sezione degli allarmi si richiede di:

- Creare una catalogazione degli allarmi su una scala di tre livelli. Livello 1 - Grave; Livello 2 - Medio; Livello 3 - Basso.
- Se viene ricevuto un allarme di livello 1, il bot invia subito il messaggio a chi deve essere informato.
- Se viene ricevuto un allarme di livello 2, il bot attende di ricevere 3 messaggi uguali (di seguito oppure anche a distanza o con altri messaggi fra loro) e invia il messaggio a chi deve essere informato.
- Se viene ricevuto un allarme di livello 3, il bot non invia il messaggio, ma tiene in memoria gli ultimi 100; quando chi deve essere informato li richiede, viene inviata la lista memorizzata.
- Fra le funzioni del bot è anche possibile richiedere di inviare lo storico degli ultimi 100 messaggi di livello 1, 100 messaggi di livello 2, gli ultimi 300 messaggi di qualsiasi livello. Tutti i messaggi sono ordinati temporalmente.
- Oltre a queste funzioni, quando richiesto, il bot invia le metriche di alcuni macchinari monitorati dalla Rasp-A sulla rete sicura. Prevedere per questo step una procedura di autenticazione.