ORGANIZZA LA TUA CYBERSECURITY: GUIDA PER L'USO

diginnova
sharing the future

DIGINNOVA.IT

1 /7 NETWORK ASSESSMENT: PARTIRE DALLA MAPPA DEL RISCHIO

Il Network Assessment è il punto di partenza imprescindibile. Significa fotografare in modo dettagliato l'infrastruttura esistente, mappare asset, dispositivi connessi, protocolli utilizzati e flussi di dati.

Molte aziende non hanno nemmeno un inventario completo delle proprie risorse OT e IT: senza questa conoscenza, difendersi diventa impossibile. L'assessment consente di:

> Identificare le vulnerabilità più critiche.
> Evidenziare connessioni superflue o rischiose.
> Definire priorità di intervento in base all'impatto sul business.

2 /7 SEGMENTAZIONE DELLA RETE: ISOLARE PER PROTEGGERE

La segmentazione è uno dei principi cardine della sicurezza. Separare i sistemi critici OT dalle reti IT aziendali riduce drasticamente la superficie d'attacco.

In questo modo, anche se un malware penetra nella rete amministrativa, non può propagarsi facilmente agli impianti di produzione.

3 /7 FIREWALL INDUSTRIALI, IDS E IPS: MONITORARE E BLOCCARE LE INTRUSIONI

Oltre ai firewall tradizionali, oggi le aziende hanno a disposizione sistemi di Intrusion Detection System (IDS) e Intrusion Prevention System (IPS) specifici per ambienti industriali, uniti a soluzioni di protezione endopoint specifiche e testate per il mondo OT. Questi strumenti consentono di:

> Monitorare il traffico in tempo reale
> Rilevare anomalie rispetto al comportamento normale dei sistemi
> Bloccare tentativi di intrusione prima che compromettano la produzione
> Garantire sicurezza senza generare impatti sulla produzione

4 /7 ZERO TRUST ARCHITECTURE: CONTROLLARE OGNI ACCESSO

Il paradigma della Zero Trust Architecture parte da un principio semplice: non fidarsi mai, verificare sempre. Ogni accesso, interno o esterno, deve essere autenticato e autorizzato. Non esistono più zone "fidate": anche un dipendente o un fornitore devono passare controlli multipli.

Questo approccio è fondamentale in contesti industriali dove spesso convivono sistemi moderni e legacy, e dove l'errore umano può aprire porte pericolose.

5 /7 SOC OT E MONITORAGGIO CONTINUO: UNA DIFESA SEMPRE EFFICACE

Un Security Operations Center (SOC) dedicato agli ambienti OT rappresenta il cuore pulsante della difesa. Attraverso sistemi di threat intelligence e correlazione dei log, il SOC può:

- Identificare rapidamente comportamenti sospetti.
- Coordinare la risposta a incidenti.
- Fornire report utili al management per decisioni strategiche.

Sempre più aziende scelgono di affidarsi a SOC esterni specializzati, capaci di garantire copertura H24 e competenze verticali sugli ambienti industriali.

6 /7 FORMAZIONE DEL PERSONALE: DA RISCHIO A RISORSA

Il fattore umano resta la principale superficie di attacco. Phishing, password deboli, comportamenti inconsapevoli sono spesso l'innesco di incidenti cyber. La formazione non è opzionale, e può comprendere diverse azioni:

- Corsi periodici per aggiornare il personale
- Simulazioni di attacco per testare le reazioni
- Best practice operative integrate nei processi quotidiani

Quando le persone comprendono il proprio ruolo nella sicurezza, diventano il primo baluardo di difesa, non l'anello debole della catena.verticali sugli ambienti industriali.

7 /7 PROCEDURE DI INCIDENT RESPONSE: COSA FARE IN CASO DI ATTACCO

Nessun sistema è infallibile. È quindi cruciale avere un piano di risposta agli incidenti ben definito: chi deve fare cosa, quali sistemi devono essere isolati, come comunicare internamente ed esternamente.

Un'azienda preparata può ridurre drasticamente l'impatto di un attacco e ripristinare la continuità in tempi molto più rapidi.