Industrial Cybersecurity: Gli attacchi più diffusi e le contromisure

Le vulnerabilità non sono isolate ma correlate tra di loro; ed esistono tipiche sequenze del loro sfruttamento per portare a compimento degli attacchi. Certamente avere barriere al confine tra parte IT e parte OT, così come adeguate policy di sicurezza, sono sfide ancora da vincere.

Boundary Protection: il confine tra le reti IT e OT in CPS sta svanendo a causa della maggiore connettività. I confini deboli rappresentano un grande rischio, come si è visto negli incidenti informatici del passato. Stabilire una DMZ che contenga meccanismi di protezione, incluso un firewall, è il primo passo per rafforzare questi confini. Tuttavia, anche la stessa DMZ può essere soggetta ad attacchi e deve essere attentamente progettata e implementata.

Least Functionality: la rete industriale eterogenea interconnessa contiene una varietà di potenziali punti di accesso (ad es. porta, protocollo, servizi) e non è necessario mantenerli tutti attivi. La Least Functionality si riferisce al divieto e alla limitazione dell'uso di questi per prevenire potenziali abusi: tenere "aperti" solo i punti di accesso strettamente necessari. Le aziende tendono a sottovalutare o addirittura ignorare la sicurezza perché si concentrano sulla riduzione dei costi, con conseguente presenza di vulnerabilità legate alla mancata implementazione di tale policy, che effettivamente ha un costo: ridurre al minimo necessario le funzionalità di un sistema, spegnendo quelle non necessarie, richiede un'analisi attenta e costante delle sue necessità, funzionalità e prestazioni. Costa meno lasciare i dispositivi configurati così come vengono forniti dal venditore, anziché entrare nel merito dell'uso che se ne farà una volta

installati.

Identification & Authentication: l'applicazione di adeguati meccanismi di autenticazione in un ambiente industriale impedisce l'accesso non autorizzato a dispositivi e informazioni. L'autenticazione delle comunicazioni uomo-macchina o macchina-macchina (M2M) richiede l'identificazione preventiva. Alle entità non identificate in tali ambienti dev'essere proibito di agire. Un avversario che riesca a inserirsi in una comunicazione non autenticata può danneggiare il CPS modificando, da un lato, i valori comunicati dai sensori e/o agli attuatori nonché, al contempo, impedire il rilevamento dell'intrusione stessa.

Physical Access Control: l'accesso alle strutture industriali avviene tramite chiavi, schede elettroniche e tecnologie mobili. Mentre le chiavi fisiche sono soggette a furto, le carte elettroniche e le tecnologie mobili non sono inviolabili. Disporre quindi di sistemi di verifica continua degli accessi a tutti i livelli consente di prevenire eventuali abusi.

Audit Review and Analysis: le organizzazioni dovrebbero adottare il sistema ISM (Information Security Management) come meccanismo operativo di monitoraggio e analisi degli eventi in tempo reale, nonché tracciamento e registrazione dei dati di sicurezza per scopi di conformità o di auditing. Naturalmente il sistema ISM stesso dev'essere protetto perché, se manipolato da un attaccante, costui potrebbe renderlo inefficace, e non consentire l'individuazione degli abusi commessi.

Authentication Management: tre principi essenziali che devono essere regolati dai criteri di applicazione della password sono la modifica, la rimozione e la crittografia delle password.

1. Password Change: i dispositivi COTS (Commercial Off-the-

Shelf) per CPS, come i PLC, vengono forniti con una password predefinita assegnata dal fornitore. Ciò (vedi Stuxnet) rappresenta un grande rischio, pertanto dovrebbe essere impostata una nuova password prima della messa in funzione del dispositivo, cambiandola con frequenza regolare.
2. Password Removal: questo è, più in generale, il tema delle credenziali che devono essere rimosse dal sistema e rese inattive per tutti quei soggetti che, a vario titolo, non hanno più necessità od obbligo di usarle. Anche questa attività richiede un'attenzione continua al controllo degli accessi. Anche gli eventuali repository di credenziali devono essere protetti.
3. Password Encryption: è necessario applicare meccanismi di crittografia avanzata per proteggere le password a partire dalla fase di autenticazione. Se la password viene trasmessa o conservata come testo in chiaro, un malintenzionato può accedervi in caso di intrusione.

Least Privilege: il NIST suggerisce di applicare il principio del privilegio minimo come parte della strategia di difesa in profondità per il CPS. In base a tale principio, si fornisce un accesso minimo a un software/utente per attività essenziali e solo quando necessario, mentre il numero di attività viene mantenuto al minimo. Ciò determina sistemi facili da analizzare, con una maggiore sicurezza complessiva. Il privilegio minimo può essere fornito tramite l'applicazione del controllo degli accessi in base al ruolo (RBAC) che assegna ben precisi diritti di accesso a specifici ruoli.

Allocation of Resources: a causa della crescente interconnettività, fornire un ambiente sicuro per i CPS richiede sempre più risorse. Questo problema dev'essere affrontato anche a livello di management, per orientare anche verso la sicurezza gli investimenti da effettuare.

Account Management: gli account aggiuntivi nelle reti dei CPS vengono utilizzati in situazioni eccezionali (ad esempio,

prima messa in funzione da parte del venditore/installatore). Questi account temporanei/di emergenza hanno in genere elevati privilegi di accesso Pertanto, devono essere rimossi/disabilitati una volta completato il loro utilizzo. Tale azione dovrebbe essere regolata da una rigorosa politica di controllo degli accessi.



Figura 7: Linee di difesa

Remote Access: la possibilità di accedere remotamente ai CPS ne aumenta indubbiamente la superficie di attacco; anche perché ormai l'accesso remoto non solo è utilizzato in modo passivo per scopi di monitoraggio, ma si vuole che consenta di operare sul sistema e i suoi dispositivi esattamente come se si fosse fisicamente presenti nell'impianto. A fronte di un'indubbia comodità in tal senso, una politica forte di controllo degli accessi a tutti i livelli, compreso quello remoto, è allora necessaria. I principali modelli di controllo degli accessi implementati negli ambienti industriali sono il DAC (Discretionary Access Control), MAC (Mandatory Access Control), RBAC (Role Based Access Control) e ABAC (Attribute Based Access Control). Ulteriori modelli sono stati sviluppati per l'IIoT e il Cloud.

I pilastri della sicurezza

Gli attacchi informatici più sofisticati della storia (ad es. Stuxnet, TRITON) prendono di mira i sistemi di controllo gestiti da CPS. Pertanto, il concetto di difesa in profondità deve essere applicato a tutti gli elementi del CPS. La difesa in profondità può essere fornita stabilendo diversi livelli di difesa in cui ogni livello ha un determinato scopo, mentre l'obiettivo comune è fornire un ambiente sicuro. Questi livelli possono differire per le risorse tecniche (ad es. hardware, software) pur mostrando somiglianze in termini di personale e procedure. Un ambiente industriale sicuro, progettato sulla base di un approccio di difesa in profondità,

dovrebbe contenere le tre linee di difesa schematizzate in Figura 7.

In particolare, la prevention si basa su meccanismi capaci di impedire il successo di eventuali attacchi, quindi renderli inoffensivi. D'altro canto non è possibile poter sempre prevenire tutto ciò che è indesiderato, compreso ciò che ancora non si conosce; inoltre, in ambito cyber, la ricerca e lo sviluppo di nuove tecniche di attacco corrono persino più velocemente dell'attività opposta, sul fronte della difesa. Quindi, accanto alla prevention, occorre disporre di sistemi di detection che, utilizzando informazioni fornite dal monitoring, identifichi con la maggiore tempestività possibile i potenziali attacchi.

In che modo? Ad esempio riconoscendo deviazioni rispetto al comportamento atteso o agli standard del sistema. A quale livello? Tutti: dall'analisi del traffico di rete a livello di singolo pacchetto, ad anomalie nel consumo di energia da parte di attuatori in tempo reale, ma anche offline, ad esempio con la verifica di corretta implementazione nel sistema di determinate policy di sicurezza, o con l'analisi di prestazioni dei dispositivi impiegati per la sicurezza per accertare che siano compatibili coi requisiti prestazionali del sistema. La detection dunque prevede di disporre di una sorta di riferimento, che può anche essere un modello, rispetto al quale valutare il comportamento e/o la configurazione effettiva del sistema. In questo tipo di attività, oggi trovano largo impiego tecniche basate sull'intelligenza artificiale. La reaction rappresenta l'applicazione dei correttivi necessari a contrastare e possibilmente inibire quanto di (potenzialmente) malevolo o rischioso è stato individuato dalla detection, parallelamente all'eventuale ripristino delle funzionalità e prestazioni eventualmente già affette dall'attacco stesso. Chiaramente, detection e reaction sono attività che si possono sviluppare su tempi anche lunghi: ad esempio sequenze storiche che vanno

molto indietro nel tempo per la detection, mentre la reaction, soprattutto quando non può essere totalmente automatica e richiede quindi un intervento umano, può portare a tempi assai lunghi per il recupero totale delle funzionalità e prestazioni del sistema attaccato, oltre al suo irrobustimento nei confronti delle criticità identificate.

Come appare quindi evidente, la sicurezza dei sistemi in generale è un processo sempre attivo, in continua esecuzione ed evoluzione, che può essere schematizzato come ISM (Information Security Management) in Figura 8, secondo i principali documenti sul tema che adottano modelli concettuali simili basati sui passaggi logici e temporali rappresentati nella parte sinistra della figura. Gli eventi che compaiono nella parte destra dell'immagine, invece, sono i responsabili del (ri)avvio e dell'iterazione del processo ISM fino al raggiungimento di una situazione soddisfacente e confermata dalla fase di validazione. La convalida ha lo scopo di dimostrare che il rischio complessivo è stato abbassato al di sotto di una soglia accettabile e di solito comporta sia attività offline (ovvero nuove sessioni di valutazione del rischio) che run-time (ovvero monitoraggio e misurazioni).



Figura 8: Information Security Management (ISM)

L'intera sequenza di passaggi viene quindi ripetuta ogni volta che:

1. i risultati verificati in fase di validazione non corrispondono alle aspettative (riduzione del rischio inadeguata);
2. vengono introdotte modifiche in qualsiasi parte/componente del sistema generale, comprese apparecchiature, policy, livelli di rischio, requisiti aziendali, normativi o legali, minacce o vulnerabilità scoperte di recente e così via;
3. le attività di monitoring e detection in fase di

esecuzione rilevano un incidente di sicurezza con conseguenze superiori alla soglia di gravità accettabile (le conseguenze stimate fanno parte dei risultati prodotti durante la valutazione del rischio).

In sostanza, dunque, l'ISM riguarda l'intera organizzazione di una società, includendo i seguenti elementi:

- formazione e impegno dei dipendenti e dei dirigenti;
- rapporti con partner, fornitori e clienti;
- business continuity;
- requisiti legali e contrattuali;
- rispetto delle politiche e degli standard di sicurezza;
- conformità tecnica;
- gestione delle risorse;
- access control;
- gestione delle comunicazioni e delle operazioni;
- sicurezza fisica e ambientale.

Si noti che tutti gli aspetti sopra elencati sono strettamente correlati: ad esempio, l'impegno del management garantisce le risorse e gli investimenti necessari (formazione, attrezzature e audit), mentre la formazione dei dipendenti consente la comprensione di meccanismi e tecniche di sicurezza, così come la corretta attuazione delle policy e delle procedure.

Questo articolo è stato estratto dal white paper "Industrial Cybersecurity" disponibile in maniera gratuita al seguente link: https://www.ictsecuritymagazine.com/pubblicazioni/industrial-cybersecurity/

Articolo a cura di **Luca Durante**

Profilo Autore

Luca Durante è Primo Ricercatore presso l'Istituto di

Elettronica e Ingegneria dell'Informazione e delle Telecomunicazioni del Consiglio Nazionale delle Ricerche (CNR-IEIIT) di Torino.
Nel 1996 ha conseguito il Dottorato di Ricerca in Ingegneria Informatica presso il Politecnico di Torino, è autore di oltre 70 articoli per riviste e conferenze internazionali, ed è stato ed è tuttora Responsabile Scientifico per il CNR in Progetti Europei e in contratti di ricerca con aziende.
È stato inoltre general co-chair, program co-chair e membro del comitato di
programma di conferenze internazionali, associate editor di IEEE Transactions on Industrial Informaatics e revisore per riviste internazionali.
Gli interessi di ricerca vertono principalmente sulle tematiche di sicurezza
informatica, attualmente declinati sulle policy di sicurezza per il controllo di accessi e la sicurezza dei sistemi cyber-fisici.

Condividi sui Social Network:
https://www.ictsecuritymagazine.com/articoli/industrial-cybersecurity-gli-attacchi-piu-diffusi-e-le-contromisure/