Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze
Segreteria generale

Centro nazionale per la cibersicurezza NCSC
www.ncsc.admin.ch

NCSC

Lista di controllo e guida
Misure di protezione dei sistemi di controllo industriali (ICS)

Indice

1 Introduzione

I sistemi di controllo e di gestione consistono in uno o più dispositivi che gestiscono, regolano e/o sorvegliano il comportamento di altri dispositivi o sistemi. Nella produzione industriale il concetto di «sistemi di controllo industriali» («industrial control systems», ICS) è consolidato. Da tempo i sistemi di controllo e di gestione industriali si ritrovano anche all'infuori dell'industria di produzione, ad esempio nella domotica o nella regolazione del traffico. Di principio, ogni sistema che regola e/o sorveglia un processo fisico è un sistema di controllo industriale. La maggior parte delle regole di base per la protezione di simili sistemi si applica anche all'infuori della produzione industriale. Per questo motivo nel presente testo i sistemi di controllo industriali sono indicati come «ICS».

SANS[1], un istituto di sicurezza degli USA, ha pubblicato 20 elementi chiave[2] che generalmente permettono di proteggere le infrastrutture IT e possono in parte essere applicati anche agli ICS. Ulteriori raccomandazioni sono emesse dall'«US Industrial Control Systems Cyber Emergency Response Team» (ICS-CERT[3]) e dal «National Institute of Standards and Technology» (NIST[4]).

Le raccomandazioni qui appresso poggiano su questi documenti.

2 In breve

La guida dettagliata si trova più avanti nel presente documento.

11 Misure di protezione dei sistemi di controllo industriali (ICS)
1. Allestire e curare una banca dati Asset per tutti i dispositivi
2. Predisporre una gestione del ciclo di vita e dei patch per software
3. Definire e utilizzare configurazioni sicure
4. Pianificare ed edificare architetture di rete robuste
5. Implementare una protezione da malware a più livelli
6. Autenticare e autorizzare
7. Pianificare una valutazione centrale dei log
8. Garantire la protezione fisica
9. Eseguire e testare regolarmente backup e recovery
10. Predisporre ed eseguire processi di security incident management
11. Sviluppare una cultura della sicurezza

1 SANS: http://www.sans.org

2 SANS Top 20 Critical Security Controls: http://www.sans.org/critical-security-controls/

3 ICS CERT: http://ics-cert.us-cert.gov/

4 NIST: http://csrc.nist.gov/publications/nistpubs/800-82/SP800-82-final.pdf

3 Misure di protezione degli ICS

Le misure indicate dovrebbero essere integrate in un processo di sicurezza sovraordinato che garantisca l'applicazione, la regolare verifica e il costante miglioramento delle misure. Inoltre, l'operatore dell'impianto dovrebbe conoscere le minacce attuali e far confluire gli insegnamenti nell'implementazione e nel miglioramento delle misure di sicurezza. A tale scopo è molto importante che vi sia una stretta collaborazione tra gestione dei rischi, engineering ed esercizio.

Nella maggior parte dei casi la sicurezza non aumenta con una sola azione. Si tratta di un processo costante che non dovrebbe mai finire. Stabilite obiettivi realistici e raggiungibili ed eseguite dapprima i punti che consentono di elevare sensibilmente la sicurezza con relativamente poco sforzo. Ad esempio potete iniziare modificando tutte le password predefinite. In tal modo proteggete le interfacce di gestione raggiungibili dall'esterno.

3.1 Banca dati Asset per dispositivi

Misura	Tenete una banca dati di tutte le componenti di gestione, dei sistemi periferici e anche dei «normali» dispositivi finali.
Motivazione	Una protezione effettiva ed efficace è impossibile senza sapere quali elementi devono essere protetti e quali elementi sono degni di fiducia.
Indicazioni per l'implementazione	Esistono diversi strumenti ausiliari tecnici per raggiungere questo obiettivo. Con uno strumento di inventario basato su rete è possibile avere una prima visione d'insieme. Nel caso di una scansione attiva occorre tuttavia procedere con grande prudenza. Molti ICS non sono predisposti per ricevere un traffico di rete inaspettato che può portare a un messaggio di errore. I dispositivi sconosciuti che si collegano per la prima volta alla rete dovrebbero fare scattare un allarme, basato ad esempio sull'indirizzo MAC. Sebbene un indirizzo MAC possa essere facilmente falsificato, questa misura svolge già un grande effetto di rilevamento.

3.2 Gestione dei software

Misura	Tenete una banca dati di tutti gli elementi di software. Vi servirà anche come base per la buona gestione dei patch, dei release e della gestione del ciclo di vita. Se possibile usate una whitelist, in particolare per tutti i dispositivi critici, in modo che vengano eseguiti soltanto i software conosciuti.

Motivazione	La banca dati Asset dei software è la base per la gestione dei patch, dei release e del change management. Molti attacchi, in particolare quelli mirati, sono perpetrati attraverso sistemi con diritti elevati poco protetti, come ad esempio i dispositivi dedicati all'amministrazione o degli sviluppatori. Rendendo meno accessibili questi sistemi, gli attacchi diventeranno molto più impegnativi per gli aggressori. Considerata la grande longevità degli ICS, la gestione del loro ciclo di vita è generalmente di grande importanza.
Indicazioni per l'implementazione	L'allestimento iniziale della banca dati può essere agevolato da strumenti ausiliari tecnici («software inventory tools»). La gestione dei patch è molto delicata in ambito di ICS e spesso (per motivi di garanzia) può in genere essere effettuata soltanto in collaborazione con i fornitori. Ciò significa che di norma esistono finestre temporali durante le quali il sistema è vulnerabile agli attacchi. Il rischio può essere ridotto mediante una whitelist delle applicazioni eseguibili. Quasi tutti gli attacchi richiedono l'esecuzione di un software sul dispositivo preso di mira. L'obiettivo della whitelist è fare in modo che possano essere eseguiti soltanto i programmi autorizzati.

3.3 Configurazioni sicure

Misura	Configurazioni sicure
Motivazione	Spesso gli aggressori sfruttano password deboli o password standard.
Indicazioni per l'implementazione	I livelli di amministrazione non dovrebbero mai essere raggiungibili direttamente via Internet. All'occorrenza si deve introdurre una limitazione che consenta l'accesso solo agli indirizzi IP autorizzati. Le direttive in materia di sicurezza e di durezza ("hardening") del produttore devono essere imperativamente osservate. Se l'ICS offre la possibilità di firmare il software e di attivare un allarme in caso di modifica del software utilizzato, questa opportunità va assolutamente utilizzata. Le configurazioni devono anche garantire che non vengano usate password deboli o standard.

3.4 Architettura di rete robusta

Misura	Architettura di rete robusta con zone di rete separate le une dalle altre
Motivazione	Gli ICS dovrebbero essere gestiti nella misura del possibile su reti separate senza accesso diretto a Internet. Questo riduce la superficie vulnerabile e rende la vita più difficile agli aggressori. La rete d'ufficio e la rete degli ICS dovrebbero essere completamente separate. Se ciò non fosse possibile, deve essere predisposto un concetto di zone che gestisca la comunicazione fra di loro.
Indicazioni per l'implementazione	L'accesso va protetto in modo particolare se gli elementi devono essere raggiungibili via Internet. Raccomandiamo il ricorso a tecnologie VPN con un'autenticazione a due fattori (ad es. con un OTP Token e un PIN). Ai fini della manutenzione si dovrebbero inoltre sbloccare in maniera mirata soltanto singoli indirizzi IP. Il medesimo principio si applica anche alla segmentazione interna: se è necessario un accesso alla rete ICS dalla rete «normale», tale accesso deve essere effettuato attraverso un punto dedicato, dove vengono eseguiti un'autenticazione e un monitoraggio. Le reti dovrebbero essere sorvegliate con sistemi dedicati di «intrusion detection» (IDS) basati sulle reti e specializzati su protocolli ICS. I protocolli di rete dovrebbero essere redatti in forma cifrata. Se non esiste una variante corrispondente di protocollo il traffico di rete può essere impacchettato in un tunnel. Si dovrebbe sempre utilizzare SSL/TLS, specialmente in caso di accesso a un'interfaccia di amministrazione basata sul web. Se devono essere trasmessi regolarmente dati dall'ambiente produttivo alla rete d'ufficio (ad es. a fini statistici), tali dati possono essere estratti attraverso un isolatore ottico di dati («data diode») che autorizza la comunicazione in una sola direzione. In questo modo si impedisce che un codice nocivo in provenienza dalla rete d'ufficio raggiunga i sistemi di controllo attraverso questa linea.

3.5 Protezione contro i malware a più livelli

Misura	Protezione contro i malware a più livelli
Motivazione	Gli ICS basati su sistemi operativi ad uso commerciale sono esposti ai malware, in particolare perché (a causa delle prescrizioni del produttore, per motivi di validazione o di sicurezza di produzione) devono sovente essere mantenuti a un vecchio livello di patch. Spesso i malware vengono utilizzati per assumere il controllo di sistemi ausiliari, dispositivi di amministrazione o server di banche dati collegati agli ICS. Le vecchie piattaforme di ICS che poggiano su sistemi operativi basati su Windows sono particolarmente minacciate da attacchi malware.
Indicazioni per l'implementazione	In genere una buona protezione contro i malware è essenziale per il corretto funzionamento di ogni ICS. Spesso non è né possibile né opportuno installare soluzioni di protezione contro i malware su ICS critici. I dispositivi di amministrazione e i server Windows «normali» dovrebbero tuttavia essere provvisti di una soluzione di protezione antivirus aggiornata. La protezione contro i malware dovrebbe essere effettuata a più livelli in maniera tale che i software nocivi non rilevati a un determinato livello possano essere individuati a un altro livello. La rete dovrebbe inoltre essere sorvegliata per rilevare la presenza di flussi di dati che suggeriscono infezioni malware. È più che mai opportuno che nessuno dei sistemi partecipanti possa collegarsi direttamente a Internet, ma che vengano autorizzati unicamente collegamenti limitati da punto a punto attraverso un server Proxy.

3.6 Autenticazione e autorizzazione

Misura	Autenticazione sicura e autorizzazione di tutte le persone e i sistemi partecipanti
Motivazione	Occorre attribuire grande importanza all'autenticazione e all'assegnazione dei diritti, perché le lacune in questo ambito possono essere sfruttate in maniera molto rapida e semplice dagli aggressori.

Indicazioni per l'implementazione	Se possibile occorre richiedere un'autenticazione e dare l'autorizzazione secondo il principio dell'attribuzione di diritti minima. Diversi ICS e/o protocolli ICS non supportano alcuna autenticazione o solo un'autenticazione rudimentale. In questo caso si devono adottare misure compensatorie, come ad esempio un'autenticazione al limite tra rete e ICS. Verificate che non vi siano account utente standard con password predefinite. Tutte le password devono essere complesse e per le superfici di amministrazione deve essere utilizzata un'autenticazione a due fattori. Agli utenti – in particolare anche alle imprese che si occupano della manutenzione – devono essere assegnati unicamente i diritti effettivamente necessari all'esecuzione dei propri compiti.

3.7 Valutazione centrale dei log

Misura	I log di tutti i sistemi devono essere raccolti, valutati e conservati a livello centrale.
Motivazione	Riunire tutti i log è l'unico modo per comprendere le interazioni dei singoli eventi e individuare gli attacchi.
Indicazioni per l'implementazione	Per ogni classe di sistema occorre stabilire quali eventi devono essere registrati, che si tratti di ICS, di un dispositivo di amministrazione o di un sistema periferico. I dati registrati devono essere conservati il più a lungo possibile, perché a volte gli attacchi vengono scoperti dopo mesi o anni e possono essere ricostruiti solo analizzando i log. Si dovrebbero definire degli eventi di riferimento che rappresentano un funzionamento normale e senza guasti. Le anomalie, gli errori e i comportamenti inaspettati devono sempre essere analizzati.

3.8 Protezione fisica

Misura	Gli ICS e i sistemi periferici collegati direttamente o indirettamente devono essere protetti da accessi fisici non autorizzati.
Motivazione	In genere il grado di protezione di accesso fisico agli ICS è molto elevato. Vanno tuttavia presi in considerazione anche i sistemi periferici e le postazioni di manutenzione a distanza, nonché gli impianti dismessi e comandati da remoto. L'accesso fisico a un collegamento permette di eludere perlopiù le misure di sicurezza a livello di rete.

Indicazioni per l'implementazione	Estendete la ricerca di vulnerabilità della protezione fisica ai sistemi periferici e di amministrazione, nonché a eventuali sistemi situati fuori sede. Ogni interfaccia fisica offre un accesso agevolato alla rete.

3.9 Procedure di backup e recovery

Misura	Le procedure di backup e recovery devono essere definite e testate regolarmente. Ciò si applica sia agli ICS veri e propri, sia ai sistemi periferici collegati. L'integrità dei file di backup deve essere verificata regolarmente.
Motivazione	Spesso i backup non vengono testati. In caso di crisi sono disponibili file di backup che, secondo le circostanze, non possono però essere letti o eseguiti.
Indicazioni per l'implementazione	I dati di backup devono essere archiviati in un luogo sicuro, a una certa distanza dal sistema protetto. I backup non dovrebbero contenere solo dati, ma anche file di configurazione. Il ripristino di backup deve essere effettuato almeno una volta all'anno, idealmente due. L'integrità dei file di backup deve essere verificata regolarmente. A tale scopo occorre calcolare e conservare valori hash crittografici di tutti i file di backup.

3.10 Processi di security incident management

Misura	In caso di incidente sono definiti processi pronti e testati. Ciò comprende la prevenzione, l'individuazione e la reazione.
Motivazione	Reagire in modo corretto e deciso in caso di incidente in genere può ridurre sensibilmente i danni.
Indicazioni per l'implementazione	Gli ICS devono essere integrati nel normale processo di gestione degli incidenti di sicurezza. Gli incidenti di sicurezza non sono sempre immediatamente riconoscibili. Per questo motivo i comportamenti anomali di un ICS devono sempre essere analizzati e chiariti. Dopo un incidente di sicurezza deve sempre essere eseguita un'analisi delle cause e si devono definire misure per evitare incidenti in futuro. Ciò permette di ottenere un miglioramento continuo.

3.11 Sviluppare una cultura della sicurezza

Misura	Sviluppare una cultura della sicurezza con responsabilità e procedure che includano esplicitamente anche gli ICS.
Motivazione	La sicurezza deve essere parte di tutti i processi aziendali. Le misure necessarie e il contesto di rischio dovrebbero poter essere comunicati direttamente e inalterati alla direzione attraverso un sistema di controllo interno. La direzione deve essere informata sui rischi e sulle caratteristiche particolari degli ICS.
Indicazioni per l'implementazione	I processi di sicurezza dovrebbero essere integrati nei normali processi aziendali e circuiti di controllo. Il funzionamento e il raggiungimento degli obiettivi devono essere verificati regolarmente a livello tecnico e organizzativo e vanno pianificati e attuati miglioramenti laddove necessario. L'esecuzione delle verifiche e la comunicazione dei risultati alla direzione devono essere trasferite a una persona con un ruolo specifico possibilmente indipendente che disponga delle risorse e delle competenze necessarie. La responsabilità compete sempre alla direzione.