

IEC 62443-4-1:2018 Ciclo di vita di sviluppo sicuro dei prodotti per l'automazione industriale

Ciclo di vita di sviluppo sicuro, otto pratiche

47 requisiti. Questa norma è certificabile da un organismo accreditato. Versione di 07/2026.

La norma IEC 62443-4-1 ammette la certificazione, ma l'oggetto è insolito: ciò che viene certificato è il processo di sviluppo di un'organizzazione di sviluppo nominata, cioè una versione documentata e concreta del ciclo di vita sicuro. Non viene certificato né un prodotto né una persona. I percorsi sono ISASecure SDLA e lo IECCEB Scheme. Allo stato attuale, un simile certificato non genera una presunzione di conformità con il Regolamento sulla Ciberresilienza dell'UE (Cyber Resilience Act). Da non confondere con la IEC 62443-4-2, che pone requisiti sul componente stesso. Questo elenco è un supporto di lavoro per l'autovalutazione, non una prova.

Azienda	Data	Redatto da
---------	------	------------

5 Pratica 1: Gestione della sicurezza (SM)13

SM-1

Esiste un ciclo di vita di sviluppo del prodotto definito che porta la sicurezza attraverso ogni fase, dal concetto iniziale fino alla dismissione del prodotto, e questo ciclo di vita è quello effettivamente seguito nella pratica.

Documento

Come si dimostra: Descrizione del processo o istruzione di lavoro che elenca le fasi, i deliverable per fase e i punti di passaggio di consegne, insieme a evidenze di un progetto in corso che dimostrino che le fasi sono state effettivamente percorse. Una piccola organizzazione può bastare con una pagina per fase più una lista di controllo nel sistema di ticket; ciò che conta è che il processo documentato e la prassi quotidiana coincidano.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SM-2

Ogni attività del ciclo di vita di sviluppo sicuro ha un responsabile assegnato, e questa assegnazione è nota alle persone coinvolte.

Documento

Come si dimostra: Matrice dei ruoli e delle responsabilità che assegna ogni fase del processo a un ruolo nominato, integrata dall'attuale copertura di quei ruoli. Con solo poche persone è sufficiente una tabella con ruolo, attività e persona; la parte importante è la regola di sostituzione per ferie e malattie.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SM-3

È definito in modo tracciabile quali prodotti, varianti, versioni e componenti rientrano nel ciclo di vita di sviluppo sicuro e quali no.

Documento

Come si dimostra: Elenco dei prodotti e degli stati di versione inclusi nell'ambito con la motivazione delle inclusioni ed esclusioni, aggiornato a ogni nuova versione. In pratica funziona bene una colonna nella panoramica prodotti, con un sì o un no per riga più una frase di motivazione.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SM-4

Le persone che si assumono compiti di sicurezza possiedono la competenza tecnica richiesta, e tale competenza viene costruita e aggiornata in modo deliberato.

Come si dimostra: Profilo di competenza per ruolo di sicurezza, registrazioni delle qualifiche, piano di formazione e registri di partecipazione, integrati da una panoramica delle lacune. Le organizzazioni piccole lo documentano tramite certificati, partecipazione a conferenze o webinar e una breve revisione annuale su chi colma quale lacuna entro quando, ricorrendo a competenze esterne dove necessario.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SM-5	L'ambito del ciclo di vita di sviluppo sicuro è delimitato e indica le sedi, le unità organizzative, i contributi dei fornitori e gli ambienti di sviluppo coinvolti, insieme ai confini di tale ambito.				Documento
	Come si dimostra: Dichiarazione di ambito che copre sedi, team, parti esternalizzate e sistemi, più uno schema delle interfacce esterne. Chi sviluppa in una singola sede lo documenta in poche frasi e indica esplicitamente ciò che ne resta fuori, come assieme sviluppati esternamente o hosting presso terzi.				
	Aperto	In corso	Soddisfatto	Non applicabile	
Evidenza / motivazione					
SM-6	Per ogni elemento consegnato agli utenti, software, firmware, configurazioni e file di accompagnamento, è possibile un controllo di integrità, in modo che i destinatari possano rilevare una modifica non avvertita.				
	Come si dimostra: Firme o checksum pubblicati per ogni pacchetto di consegna, una descrizione del metodo e un esempio tratto da una versione reale, insieme a istruzioni per il cliente su come eseguire il controllo. Per i team piccoli è sufficiente un file di checksum firmato accanto al download più un paragrafo nelle note di versione.				
	Aperto	In corso	Soddisfatto	Non applicabile	
Evidenza / motivazione					
SM-7	Gli ambienti utilizzati per sviluppo, build e test sono protetti da accessi non autorizzati e da manomissioni del codice sorgente, degli strumenti di build e degli artefatti.				
	Come si dimostra: Concetto di controllo degli accessi per repository, server di build e sistemi di test, elenchi di accesso con la data dell'ultima revisione, registrazioni delle modifiche rilevanti per la sicurezza ed evidenza che l'accesso di produzione e quello di sviluppo sono separati. Senza un reparto IT interno, bastano l'accesso a due fattori, un ramo principale protetto con revisione obbligatoria e una revisione semestrale di chi ha ancora accesso.				
	Aperto	In corso	Soddisfatto	Non applicabile	
Evidenza / motivazione					
SM-8	Le chiavi private utilizzate per firmare le consegne sono protette da divulgazione e uso improprio, e il loro utilizzo è limitato a persone e sistemi autorizzati.				
	Come si dimostra: Descrizione della conservazione, dell'accesso, del rinnovo e della revoca delle chiavi, evidenza di una conservazione protetta come un token hardware o un servizio di gestione delle chiavi, più registrazioni delle operazioni di firma. Una piccola organizzazione conserva la chiave di firma su un token hardware, documenta le due persone con accesso e tiene pronta una procedura per il caso di smarrimento.				
	Aperto	In corso	Soddisfatto	Non applicabile	
Evidenza / motivazione					
SM-9	Per i componenti acquistati o adottati, incluso il software open source, le aspettative di sicurezza poste al fornitore sono definite e vengono applicate durante la selezione.				Documento
	Come si dimostra: Requisiti di sicurezza nelle specifiche o nei contratti con i fornitori, criteri di selezione per i componenti di terze parti, un inventario di tutti i componenti di terze parti con versione e origine, più la valutazione se il fornitore soddisfa le aspettative. Senza un ufficio acquisti, è sufficiente un elenco di componenti aggiornato con una colonna che registri se sono stati verificati gli aggiornamenti di sicurezza e i canali di segnalazione del fornitore.				
	Aperto	In corso	Soddisfatto	Non applicabile	
Evidenza / motivazione					
SM-10	I componenti sviluppati su commissione da terzi sono soggetti agli stessi requisiti di sicurezza dello sviluppo interno, e il rispetto di tali requisiti viene verificato.				
	Come si dimostra: Ordine di acquisto o documenti contrattuali che indicano gli obblighi di sicurezza richiesti, evidenza da parte del fornitore di servizi sulle pratiche applicate, registrazioni di accettazione e risultati dei propri controlli sul lavoro consegnato. Senza un budget per audit, sono sufficienti una garanzia contrattuale, la consegna dei risultati di test del fornitore e un controllo a campione proprio prima dell'accettazione.				
	Aperto	In corso	Soddisfatto	Non applicabile	
Evidenza / motivazione					

SM-11

I riscontri relativi alla sicurezza provenienti da tutte le fonti, test, revisioni, segnalazioni degli utenti e notifiche di terzi, vengono registrati, valutati nel loro impatto, assegnati a un responsabile con una scadenza, e seguiti fino alla chiusura.

[Documento](#)

Come si dimostra: Sistema di difetti o ticket con un contrassegno dedicato per i temi di sicurezza, e per ogni voce la valutazione dell'impatto, il responsabile, la scadenza e la nota di chiusura, più un report sui punti aperti. Un piccolo team utilizza un'etichetta nel sistema di ticket esistente e un punto fisso all'ordine del giorno della riunione settimanale.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SM-12

Prima che un prodotto venga rilasciato si verifica e si documenta che le fasi previste del ciclo di vita di sviluppo sicuro sono state effettivamente svolte e che le relative registrazioni sono state prodotte.

[Documento](#)

Come si dimostra: Revisione di rilascio per ogni versione, confrontata con le fasi del processo, riferimenti alle rispettive registrazioni e una decisione di rilascio documentata con data e firma. In pratica funziona bene una lista di controllo di rilascio che non consente la spedizione senza tutte le caselle spuntate; i punti aperti vengono motivati e dotati di una data.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SM-13

Il ciclo di vita di sviluppo sicuro stesso viene regolarmente messo in discussione e migliorato, attingendo alle conoscenze derivanti da incidenti, risultati dei test, riscontri dei clienti e dall'evoluzione del panorama delle minacce.

Come si dimostra: Registrazioni della revisione del processo, ad esempio un riesame di direzione o una retrospettiva, con le modifiche di processo innescate, il loro stato di attuazione e un riferimento alla causa radice. Chi utilizza i livelli di maturità della norma registra lo stato attuale e l'obiettivo per ogni pratica; il livello di maturità 4 richiede esattamente questa evidenza di miglioramento continuo. Per una piccola organizzazione basta una riunione all'anno con verbale e tre miglioramenti concreti.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

6 Pratica 2: Specifica dei requisiti di sicurezza (SR)

5

SR-1

Viene descritto il contesto d'uso previsto del prodotto: ambiente operativo atteso, misure di sicurezza che si presume siano fornite da tale ambiente, gruppi di utenti e ruoli previsti, confini di fiducia assunti, e gli usi per i quali il prodotto è esplicitamente non destinato.

[Documento](#)

Come si dimostra: Una descrizione del contesto di sicurezza del prodotto, come documento a sé stante o come sezione fissa della specifica di prodotto, che copra l'ambiente di rete, le protezioni esterne assunte come un firewall o un controllo di accesso fisico, un elenco dei ruoli e un elenco esplicito degli usi fuori ambito. Una piccola organizzazione la limita a due pagine, aggiunge uno schema semplice dell'ambiente di impianto e la fa datare e approvare dal responsabile di prodotto.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR-2

Esiste un modello delle minacce per il prodotto che rappresenta i flussi di dati, le interfacce, i confini di fiducia e i percorsi di attacco, indica le minacce risultanti e il loro possibile impatto, e assegna le contromisure. Viene rivisto e aggiornato in caso di modifiche rilevanti e almeno una volta per ogni versione del prodotto, e i punti aperti vengono seguiti fino alla chiusura.

[Documento](#)

Come si dimostra: Modello delle minacce con un diagramma dei flussi di dati, un elenco delle minacce per ogni interfaccia, le contromisure assegnate e lo stato dei punti aperti, più uno storico delle revisioni con data e autore. Una piccola organizzazione può lavorare con una tabella per interfaccia, con colonne per cosa potrebbe andare storto, quanto sarebbe grave, cosa si fa al riguardo e chi la rivede.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR-3

I requisiti di sicurezza del prodotto sono definiti e documentati. Coprono i risultati del modello delle minacce, il contesto di sicurezza del prodotto descritto, gli obblighi legali e contrattuali applicabili e il livello di sicurezza target, e includono le capacità di sicurezza che il prodotto stesso deve fornire.

[Documento](#)

Come si dimostra: Elenco dei requisiti o strumento di gestione dei requisiti con un identificativo univoco per ogni requisito, l'origine di ciascuna voce, come una minaccia, un contratto con il cliente o un obbligo legale, e il livello di sicurezza target. Una piccola organizzazione lo gestisce come un'unica tabella con una colonna ID fissa a cui successivamente si agganciano verifica e test.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR-4

Ogni singolo requisito di sicurezza è formulato in modo inequivocabile, privo di contraddizioni, verificabile e tracciabile fino a una specifica funzione o interfaccia del prodotto, e contiene le informazioni necessarie per verificarlo in seguito senza ulteriori chiarimenti.

Come si dimostra: Un campione dell'elenco dei requisiti che mostri, per ogni requisito, un criterio di accettazione misurabile e la funzione o interfaccia interessata, insieme alla corrispondenza tra requisito e caso di test. Una piccola organizzazione lo verifica con un modello di formulazione fisso e la domanda di controllo se sia possibile scrivere un caso di test a partire dal requisito senza dover chiedere chiarimenti.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR-5

I requisiti di sicurezza vengono rivisti prima di essere utilizzati nella progettazione e nell'implementazione, con il coinvolgimento delle parti interessate, come sviluppo, test, responsabile di prodotto e, dove utile, vendite o il cliente. La revisione copre la completezza rispetto al modello delle minacce e al contesto di sicurezza del prodotto, la correttezza e la verificabilità. I riscontri vengono registrati e seguiti fino alla chiusura.

Come si dimostra: Registrazione della revisione con data, partecipanti e relativi ruoli, la versione dei requisiti sottoposta a revisione, un elenco dei riscontri con responsabile e stato di chiusura, e una nota di approvazione. Una piccola organizzazione lo gestisce come una revisione a due persone tra sviluppo e test, con una breve registrazione e una riga di approvazione nell'elenco dei requisiti.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

7 Pratica 3: Sicurezza fin dalla progettazione (SD)

4

SD-1

Ogni prodotto dispone di una descrizione di progettazione che coglie gli aspetti rilevanti per la sicurezza dell'architettura: quali componenti esistono, come comunicano tra loro, dove corrono i confini di fiducia, quali interfacce esterne sono esposte e con quali meccanismi i requisiti di sicurezza definiti in precedenza vengono realizzati nella progettazione.

[Documento](#)

Come si dimostra: Documento di architettura o specifica di progettazione contenente un diagramma che mostri i componenti, i flussi di dati e i confini di fiducia, più una tabella di corrispondenza tra ogni requisito di sicurezza e l'elemento di progettazione che lo implementa. Un piccolo fornitore si accontenta di un diagramma mantenuto aggiornato più due o tre pagine di spiegazione; ciò che conta è che sia sotto controllo di versione nel repository e aggiornato ogni volta che l'architettura cambia.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SD-2

La progettazione viene analizzata sistematicamente alla ricerca di minacce. L'analisi indica gli obiettivi dell'attaccante, i confini di fiducia e le interfacce interessate, le minacce risultanti insieme alla loro valutazione, e le contromisure adottate nella progettazione. Viene ripetuta ogni volta che l'architettura o l'ambiente cambiano in modo sostanziale, e le minacce individuate vengono seguite finché non è stata presa una decisione su ciascuna di esse.

[Documento](#)

Come si dimostra: Modello delle minacce per prodotto o per ogni versione principale, ad esempio una tabella con colonne per minaccia, interfaccia interessata, valutazione, contromisura e stato, insieme al verbale della sessione di modellazione con partecipanti e data. Un piccolo team modella in modo pragmatico in un workshop di due o tre ore seguendo il diagramma di architettura e registra i punti aperti come ticket, in modo che l'evidenza del monitoraggio venga prodotta senza sforzo aggiuntivo.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SD-3 La progettazione segue in modo dimostrabile principi di progettazione sicura riconosciuti, tra cui il privilegio minimo, la superficie di attacco minima, la difesa in profondità, le impostazioni predefinite sicure, il comportamento sicuro in caso di guasto e meccanismi di sicurezza il più possibile semplici e verificabili. L'applicazione di questi principi è visibile nella progettazione ed è motivata.

Come si dimostra: Una sezione nella descrizione di progettazione o una linea guida di progettazione interna che indichi i principi, più evidenze concrete per ogni principio nel prodotto, come la matrice dei privilegi dei servizi, l'elenco delle porte aperte con relativa motivazione, le impostazioni predefinite di consegna o il comportamento documentato di gestione degli errori. Un piccolo fornitore utilizza una breve lista di controllo di questi principi come voce fissa nella revisione di progettazione e archivia il foglio compilato insieme alla progettazione.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SD-4 La progettazione viene rivista da pari qualificati prima dell'inizio dell'implementazione. La revisione copre la completezza rispetto ai requisiti di sicurezza, la correttezza e l'efficacia dei meccanismi di sicurezza e i risultati dell'analisi delle minacce. Partecipano persone con competenza di sicurezza sufficiente, i riscontri vengono registrati e seguiti fino alla chiusura. [Documento](#)

Come si dimostra: Registrazione della revisione con data, elemento sottoposto a revisione con relativa versione, partecipanti e ruoli, elenco dei riscontri con stato e decisione di rilascio. Un piccolo team allega la revisione alla pull request dei documenti di progettazione e lascia i riscontri come commenti con una nota di chiusura, il che documenta il monitoraggio senza strumenti aggiuntivi. Dove manca la competenza di sicurezza interna, coinvolgere un revisore esterno a ore per le progettazioni critiche è la via pragmatica.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

8 Pratica 4: Implementazione sicura (SI)

2

SI-1 Esiste un processo definito per verificare l'implementazione effettiva rispetto alla progettazione sicura: la revisione conferma che le misure di protezione previste nella progettazione sono effettivamente presenti ed efficaci nel codice, che la difesa in profondità è preservata, e che non sono state introdotte nuove vulnerabilità durante l'implementazione. La revisione viene svolta da personale adeguatamente qualificato, e ogni scostamento riscontrato viene registrato e seguito fino alla chiusura.

Come si dimostra: Una procedura scritta per la revisione dell'implementazione insieme a registrazioni di revisione per componente o versione: il modulo rivisto, il riferimento al documento di progettazione, la data, il revisore, i riscontri e il loro stato di risoluzione. Come evidenza adeguata servono le revisioni delle pull request con una lista di controllo di sicurezza obbligatoria, i risultati dell'analisi statica del codice con una valutazione documentata di ogni segnalazione, e i verbali delle sessioni di revisione. Un piccolo team copre questo aspetto con il principio dei quattro occhi, un modello di revisione conservato nel repository in cui ogni misura di progettazione viene spuntata singolarmente, e un ticket per ogni riscontro aperto. Il punto essenziale è che l'autore del codice non sia mai il revisore dello stesso codice.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SI-2 Regole vincolanti di codifica sicura si applicano a tutto il lavoro di sviluppo rilevante per la sicurezza e coprono almeno l'evitare costrutti e funzioni insicuri noti, la gestione degli input e degli errori, la gestione della memoria e delle risorse, e l'uso di codice di sicurezza collaudato invece di implementazioni proprie. Le regole si applicano per ogni linguaggio di programmazione utilizzato, sono note a tutti gli sviluppatori, e vengono aggiornate quando necessario, ad esempio quando emergono nuovi schemi di attacco o nuovi strumenti. [Documento](#)

Come si dimostra: Uno standard di codifica sicura approvato con stato di versione, ambito per linguaggio e data di approvazione, integrato da evidenza che venga applicato nel lavoro quotidiano: la configurazione di linter e strumenti di analisi nel repository, una regola di build che segnali le violazioni, e l'elenco delle presenze al briefing. Le organizzazioni piccole non scrivono uno standard da zero; dichiarano vincolante un insieme di regole pubbliche già affermato, aggiungono un breve elenco di regole proprie supplementari, e ancorano il controllo nella pipeline in modo che il rispetto venga dimostrato automaticamente.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

9 Pratica 5: Verifica e validazione della sicurezza mediante test (SVV)

5

SVV-1

Ogni requisito di prodotto rilevante per la sicurezza ha assegnato almeno un caso di test, che dimostra che la funzione di protezione funziona come previsto durante il funzionamento normale, che si comporta come specificato in presenza di input non validi o di uso improprio, e che le impostazioni predefinite di consegna del prodotto corrispondono allo stato sicuro. L'esecuzione e l'esito vengono registrati per ogni versione software testata.

[Documento](#)

Come si dimostra: Una matrice di tracciabilità che collega requisito, caso di test e risultato, più registrazioni di test che mostrino la data, la versione o build testata, e il nome della persona che ha eseguito il test. Un piccolo fornitore aggiunge semplicemente una colonna con l'ID del caso di test al proprio elenco di requisiti e archivia il log di output dell'esecuzione automatica dei test dalla pipeline di build come file allegato alla rispettiva versione.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SVV-2

Le contromisure derivate dal modello delle minacce vengono testate specificamente per confermare che chiudono effettivamente il percorso di attacco assunto. I test vengono eseguiti a fronte delle minacce individuate, non solo a fronte di un uso conforme, e i punti aperti vengono inseriti nel processo di gestione dei difetti.

Come si dimostra: Casi di test che fanno riferimento direttamente alle voci del modello delle minacce, ad esempio un caso di abuso per ogni ID di minaccia con il comportamento difensivo atteso, insieme alle registrazioni di tali esecuzioni. Senza macchinari pesanti è sufficiente aggiungere al modello delle minacce una colonna che faccia riferimento al caso di test e alla data dell'ultimo controllo riuscito.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SVV-3

Il prodotto viene esaminato sistematicamente alla ricerca di vulnerabilità prima del rilascio. L'ambito copre almeno: l'esame delle interfacce e dei servizi raggiungibili dall'esterno, i test con input malformati e mutati in modo casuale, la revisione dei componenti di terze parti utilizzati rispetto alle vulnerabilità note e segnalate, e una verifica delle classi di debolezza note nel codice proprio del fornitore. I riscontri vengono registrati insieme alla loro valutazione.

[Documento](#)

Come si dimostra: Report degli strumenti utilizzati, che indicano nome dello strumento, versione e lo stato dei dati del database delle vulnerabilità, registrazioni di fuzzing, un elenco dei componenti di terze parti con la data dell'ultimo confronto, e l'elenco dei riscontri con valutazione e decisione. Un piccolo fornitore combina strumenti standard gratuiti, una scansione delle dipendenze e una scansione di porte e servizi sul prodotto installato, e archivia gli output per ogni versione in una cartella.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SVV-4

Il candidato al rilascio viene sottoposto a un tentativo di attacco in condizioni realistiche che cerca attivamente di aggirare i meccanismi di protezione, anziché limitarsi a interrogarli. Ambito, condizioni al contorno e limiti del test vengono concordati in anticipo, e le debolezze riscontrate vengono gestite e seguite come difetti.

Come si dimostra: L'incarico o l'ordine di test che indica ambito e ambiente di test, un report che copre l'approccio, le debolezze sfruttate e la loro valutazione, più le voci nel sistema di difetti o ticket con evidenza della correzione o di un'accettazione motivata del rischio. I piccoli fornitori acquistano tipicamente questo test esternamente con un budget di tempo delimitato, oppure lo fanno eseguire da una persona che non ha sviluppato il prodotto.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SVV-5

L'indipendenza del personale addetto ai test è definita ed è adeguata al livello di maturità previsto. Chi ha sviluppato un componente non lo rilascia basandosi unicamente sui propri test, e con l'aumentare del livello di maturità i test sono di competenza di un'unità organizzativamente separata o di terzi esterni. L'assegnazione effettiva è tracciabile per ogni test.

Come si dimostra: Una definizione dei ruoli all'interno del processo di sviluppo che mostri la separazione tra creazione e test, più, per ogni esecuzione o report di test, il nome e il ruolo registrati della persona che ha eseguito il test. Un'attività a conduzione di due persone gestisce questo aspetto attraverso una revisione reciproca con una nota documentata a quattro occhi, e coinvolge una persona esterna per i test di sicurezza approfonditi.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

10 Pratica 6: Gestione dei difetti di sicurezza (DM)

6

DM-1

Esiste un canale definito attraverso il quale vengono ricevute e registrate le segnalazioni di debolezze di sicurezza nel prodotto da ogni direzione: dal team di sviluppo stesso, da test e revisioni, da clienti e integratori, da segnalatori esterni, e da avvisi su componenti di terze parti e open source utilizzati. Il canale di segnalazione è individuabile da parte di terzi, e ogni segnalazione viene registrata con la relativa data di ricezione e la sua origine.

[Documento](#)

Come si dimostra: Una descrizione del canale di segnalazione, il punto di contatto pubblicamente raggiungibile (una pagina di sicurezza, un file security.txt, o una casella come security@), e il registro di ingresso con data, origine e una breve descrizione per ogni segnalazione. Una piccola organizzazione può lavorare con una casella condivisa e un unico foglio di calcolo o etichetta di ticket, purché ogni segnalazione vi confluisca, incluse quelle sollevate nella chat interna degli sviluppatori.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

DM-2

Ogni segnalazione in arrivo viene classificata ed esaminata per determinare se è rilevante per la sicurezza e quali prodotti, versioni e componenti riguarda. Anche le segnalazioni che risultano non rilevanti per la sicurezza, o non applicabili, vengono chiuse indicando un motivo, anziché essere scartate silenziosamente.

Come si dimostra: Una nota di classificazione per ogni segnalazione che indichi l'esito (rilevante per la sicurezza sì o no), le versioni interessate, e il motivo del rifiuto dove applicabile, visibile nel ticket o nell'elenco di ingresso. I team con un basso volume di segnalazioni possono svolgere la classificazione in una breve sessione periodica e registrare l'esito in due frasi per ogni voce.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

DM-3

I difetti di sicurezza confermati vengono valutati con un metodo coerente: causa radice, versioni e configurazioni interessate, potenziale impatto sull'operatività e sulla sicurezza, sfruttabilità e gravità rispetto a una scala definita. Il risultato della valutazione viene registrato ed è tracciabile.

[Documento](#)

Come si dimostra: Una registrazione di valutazione o un insieme di campi del ticket per ogni difetto che copra la causa radice, la gravità e la scala applicata (ad esempio un sistema di valutazione comune con un vettore documentato), insieme all'elenco delle versioni interessate. I piccoli team possono affidarsi a un modello di campi fisso nel sistema di ticket più mezza pagina che descriva la scala e le soglie che innescano un'azione immediata.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

DM-4

Per ogni difetto di sicurezza valutato viene presa una decisione su come verrà gestito: correzione, misura compensativa, o un'accettazione motivata del rischio. La decisione deriva dalla gravità, viene assegnata a una persona responsabile e a una scadenza, e il difetto viene seguito fino alla chiusura.

[Documento](#)

Come si dimostra: Un elenco di azioni o lo stato del ticket che mostri responsabile, data obiettivo, tipo di misura, e una nota di chiusura, collegato alla baseline di codice o alla versione in cui la correzione diventa effettiva. I rischi residui accettati necessitano di una breve motivazione scritta approvata dal responsabile di prodotto. Una piccola organizzazione può gestire questo aspetto in una bacheca di ticket con scadenze, senza strumenti aggiuntivi.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

DM-5

Gli utenti interessati, gli integratori e le altre parti interessate vengono informati sui difetti di sicurezza non appena la valutazione lo richiede, indicando le versioni interessate, l'impatto e la correzione o misura compensativa disponibile. Le tempistiche e l'ambito dei destinatari di tale divulgazione sono definiti in anticipo, così come l'approccio alle segnalazioni di terzi che arrivano con una propria scadenza di divulgazione.

Come si dimostra: Avvisi o bollettini di sicurezza pubblicati con data e riferimento di versione, l'elenco di distribuzione o il canale di iscrizione, e la regola scritta su tempistiche e divulgazione coordinata. I fornitori con pochi clienti possono utilizzare un unico invio a un elenco clienti aggiornato più una pagina di avvisi datata le cui modifiche sono versionate.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

DM-6

La gestione dei difetti di sicurezza viene rivista a intervalli fissi. La revisione esamina i casi aperti e scaduti, il tempo trascorso dalla segnalazione alla correzione, le cause radice ricorrenti e l'efficacia delle misure adottate. I miglioramenti al processo derivanti dalla revisione vengono attuati e la loro attuazione viene seguita.

[Documento](#)

Come si dimostra: Verbale della revisione periodica con data, partecipanti, dati sui casi aperti e scaduti, e un elenco dei miglioramenti concordati con responsabile e scadenza. Una piccola organizzazione può aggiungere questo punto a una riunione trimestrale già esistente e mantenere i dati e le decisioni su una sola pagina.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

11 Pratica 7: Gestione degli aggiornamenti di sicurezza (SUM)

5

SUM-1

Ogni aggiornamento di sicurezza del prodotto viene verificato rispetto alle versioni di prodotto e agli ambienti operativi supportati prima di essere rilasciato ai clienti, ed esiste una registrazione che dimostra che l'aggiornamento chiude la vulnerabilità senza compromettere la funzione prevista del prodotto.

[Documento](#)

Come si dimostra: Registrazione di test per ogni patch che copra la versione di prodotto testata, la piattaforma, i casi di test (efficacia contro la vulnerabilità più la regressione delle funzioni principali) e l'approvazione del rilascio. Un piccolo fornitore può lavorare con una breve voce di approvazione della patch nel ticket: ID ticket, verificato da, verificato il, risultato, con il log dell'esecuzione automatica dei test allegato.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SUM-2

Per tutti i componenti di prodotto non sviluppati internamente (librerie di terze parti, sistema operativo, ambienti di runtime), è definito e documentato come vengono valutati i rispettivi aggiornamenti di sicurezza e come vengono adottati nel prodotto oppure respinti con una motivazione documentata.

[Documento](#)

Come si dimostra: Inventario dei componenti delle parti di terze parti con versione e origine, più una voce di valutazione per ogni vulnerabilità di terze parti segnalata, indicando la decisione (adottare, non interessato, coperto da una misura compensativa) e la motivazione. I piccoli team eseguono una scansione automatica delle dipendenze nella build e mantengono le decisioni come commenti sul risultato della scansione o in un semplice elenco di eccezioni.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SUM-3

Per ogni aggiornamento di sicurezza distribuito, gli utenti ricevono informazioni di accompagnamento comprensibili: quali versioni di prodotto sono interessate, quale vulnerabilità viene corretta, quanto è grave, se occorre tenere conto di effetti collaterali o misure compensative, e come si installa l'aggiornamento.

[Documento](#)

Come si dimostra: Avvisi di sicurezza o note di versione pubblicati che indicano l'identificativo della vulnerabilità, le versioni interessate, la valutazione di gravità, i passaggi di installazione e le indicazioni per tornare allo stato precedente. I piccoli fornitori mantengono un'unica pagina pubblica con un elenco cronologico degli avvisi di sicurezza e vi rimandano dall'interno del prodotto.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SUM-4

Esiste un percorso definito e protetto da manomissioni attraverso il quale gli utenti ottengono gli aggiornamenti di sicurezza, e l'autenticità e l'integrità di un aggiornamento possono essere verificate lato utente prima dell'installazione.

Come si dimostra: Descrizione del canale di distribuzione (area di download, server di aggiornamento, supporto fisico) insieme alle relative misure di protezione, più la firma digitale o il checksum per ogni pacchetto e istruzioni che indichino all'utente come verificarlo. I piccoli fornitori raggiungono questo obiettivo firmando sul server di build, pubblicando il checksum accanto al download e indicando un unico luogo chiaro in cui è conservata la chiave pubblica.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SUM-5

Esistono obiettivi di tempo definiti per la disponibilità degli aggiornamenti di sicurezza, graduati in base alla gravità della vulnerabilità; i tempi effettivamente raggiunti vengono monitorati, e ogni obiettivo mancato viene motivato e supportato da una misura provvisoria per gli utenti.

[Documento](#)

Come si dimostra: Specifica interna con una finestra temporale per categoria di gravità (ad esempio critica <= 30 giorni, alta <= 90 giorni) e una valutazione per ogni vulnerabilità: data di segnalazione, data di rilascio della patch, giorni trascorsi, motivo dello scostamento. I piccoli fornitori mantengono questo aspetto come due campi data nel ticket della vulnerabilità e rivedono l'elenco una volta al trimestre invece di allestire un sistema di metriche dedicato.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

12 Pratica 8: Linee guida di sicurezza per l'implementazione e l'esercizio del prodotto (SG)

7

SG-1

Ogni prodotto è accompagnato da una descrizione della propria strategia di difesa in profondità: indica i livelli di protezione integrati nel prodotto stesso, li collega alle minacce che contrastano, e mostra quale effetto protettivo emerge solo dall'interazione di più livelli.

[Documento](#)

Come si dimostra: Una sezione nella documentazione di prodotto consegnata, o un concetto di sicurezza separato, che indichi per ogni livello di protezione il meccanismo, la minaccia coperta e i limiti del suo effetto. Una piccola organizzazione mantiene questo come una tabella di due pagine: colonna livello di protezione, colonna minaccia tratta dal proprio modello delle minacce, colonna rischio residuo. È sufficiente un riferimento incrociato al modello delle minacce di SR-2, il contenuto non deve essere mantenuto due volte.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SG-2

La documentazione indica le misure di sicurezza che il prodotto non fornisce da sé ma che si attende dall'ambiente di implementazione, ad esempio la segmentazione di rete, firewall a monte, il controllo di accesso fisico o un servizio orario esterno, e chiarisce che il livello di sicurezza garantito non viene raggiunto senza tali misure.

[Documento](#)

Come si dimostra: Un capitolo sui prerequisiti di implementazione nel manuale, o uno schema di architettura di riferimento con zone e condotti in cui vengono contrassegnate esplicitamente le misure da fornire a cura del proprietario dell'asset. Nella pratica si è dimostrato utile un elenco di assunzioni sull'ambiente, derivato direttamente dal contesto di sicurezza del prodotto e riletto a ogni versione del prodotto.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SG-3

Esiste una guida alla configurazione di base sicura che elenca tutte le impostazioni, i servizi, le porte e le interfacce rilevanti per la sicurezza, indica lo stato di consegna raccomandato e descrive l'impatto di uno scostamento da tale raccomandazione.

[Documento](#)

Come si dimostra: Guida all'hardening con una tabella delle impostazioni: parametro, valore raccomandato, effetto, effetto collaterale in caso di scostamento. Più l'elenco dei servizi e delle porte attivi nella configurazione predefinita con la motivazione del perché restano abilitati. Un piccolo team mantiene questa tabella proprio accanto al file di configurazione nel repository e la esporta nella documentazione di consegna, in modo che resti allineata al prodotto.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SG-4

Per l'esercizio continuativo esiste una guida che descrive come il prodotto viene gestito in modo sicuro, monitorato e mantenuto nel suo stato sicuro, incluso backup e ripristino, registrazione degli eventi e la gestione dei messaggi di evento rilevanti per la sicurezza.

[Documento](#)

Come si dimostra: Guida operativa con sezioni su registrazione degli eventi, backup, riavvio e messaggi di evento. Come evidenza aggiuntiva, un elenco dei messaggi rilevanti per la sicurezza emessi dal prodotto, ciascuno con una breve azione raccomandata, in modo che il proprietario dell'asset non debba interpretarli da solo.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SG-5	La documentazione spiega come vengono impostati e mantenuti gli account utente, i ruoli e i permessi del prodotto, in particolare la separazione dei ruoli, la modifica delle credenziali predefinite e la rimozione degli account non più necessari.				Documento
	Come si dimostra: Un capitolo di gestione degli account con una panoramica dei ruoli e dei diritti assegnati a ciascun ruolo, più una nota esplicita sulle credenziali predefinite e sulla loro modifica in fase di messa in servizio. Nella pratica funziona bene una breve lista di controllo di messa in servizio nel manuale, che il proprietario dell'asset possa spuntare e archiviare.				
	Aperto	In corso	Soddisfatto	Non applicabile	
Evidenza / motivazione					
SG-6	Esiste una guida per la dismissione sicura che descrive la rimozione completa dei dati sensibili dal prodotto, come credenziali, chiavi, dati di configurazione e log, prima che il dispositivo venga ceduto, riutilizzato o smaltito.				Documento
	Come si dimostra: Una sezione di dismissione che elenchi ogni ubicazione di archiviazione di dati sensibili all'interno del prodotto e la relativa procedura di cancellazione, compresi i casi in cui la cancellazione è tecnicamente impossibile e l'hardware deve essere distrutto fisicamente. Qui aiuta un elenco della memoria persistente tratto dalla descrizione dell'architettura, che evita che un'ubicazione di archiviazione venga dimenticata.				
	Aperto	In corso	Soddisfatto	Non applicabile	
Evidenza / motivazione					
SG-7	La documentazione di sicurezza consegnata agli utenti viene rivista prima del rilascio: è tecnicamente corretta, coerente con la versione di prodotto consegnata, completa rispetto al contenuto previsto e comprensibile per il pubblico a cui è destinata, e viene aggiornata ogni volta che il prodotto cambia.				
	Come si dimostra: Una registrazione di revisione per ogni documento e versione di prodotto con revisore, data, riscontri e la loro chiusura, collegata all'approvazione del rilascio. Una piccola organizzazione risolve questo aspetto con il principio dei quattro occhi nella pull request della documentazione: uno sviluppatore verifica il contenuto tecnico, una seconda persona verifica la comprensibilità, e l'approvazione viene registrata nel ticket. Una versione è distribuibile solo una volta documentata la revisione.				
	Aperto	In corso	Soddisfatto	Non applicabile	
Evidenza / motivazione					

IEC 62443-3-3:2013 Requisiti di sicurezza di sistema per l'automazione industriale

Sette requisiti fondamentali, 51 requisiti di sistema

100 requisiti. Questa norma è certificabile da un organismo accreditato. Versione di 07/2026.

La norma IEC 62443-3-3 è certificabile, e ciò che viene certificato è un sistema, non un'organizzazione né una persona. Le vie sono ISASecure SSA e lo IECCEB Scheme. Chi vuole certificare l'organizzazione ha bisogno della 62443-2-1 o della 2-4, chi intende il componente ha bisogno della 62443-4-2. Questo elenco contiene i 51 requisiti di sistema e i 49 miglioramenti di requisito. Quali di essi si applicano dipende dal livello di sicurezza a cui si punta: 38 da SL 1, 60 da SL 2, 90 da SL 3, tutti i 100 a SL 4. Nessun miglioramento si applica già a SL 1. Questo elenco è uno strumento di lavoro per l'autovalutazione, non una prova.

Azienda

Data

Redatto da

5 FR 1: Chi o cosa richiede l'accesso, ed è davvero chi dichiara di essere

24

SR 1.1 Gli utenti umani vengono identificati e la loro identità è verificata prima che ottengano l'accesso, in ogni punto in cui possono operare o configurare il sistema di automazione. Questo include i pannelli operatore sulla macchina, l'accesso di ingegneria e i servizi di rete.

Come si dimostra: Inventario di tutti i punti di accesso del sistema, cioè HMI, sala controllo, accesso di programmazione PLC, switch, VPN e client di manutenzione remota, ciascuno con il meccanismo di autenticazione utilizzato in quel punto. Aggiungere un estratto di configurazione o una schermata della maschera di accesso per ogni classe di dispositivo. Una piccola realtà parte con una tabella per dispositivo, colonne: dispositivo, interfaccia, autenticazione presente sì o no, giustificazione se no. Richiesto da SL 1 in poi.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 1.1 RE 1 Ogni utente umano lavora con un identificativo individuale assegnato esclusivamente a quella persona. Gli account condivisi e di turno sono disabilitati, le eccezioni residue sono giustificate caso per caso e supportate da misure aggiuntive.

Come si dimostra: Esportazione degli account per sistema che associa l'identificativo alla persona, elenco delle eccezioni con giustificazione e misura compensativa, per esempio una telecamera o un registro presenze alla postazione operatore. Questa riga è un miglioramento del requisito e quindi non è mai obbligatoria a SL 1, è richiesta da SL 2 in poi.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 1.1 RE 2 Chi accede da una rete non affidabile, per esempio da internet o tramite una connessione di manutenzione remota, dimostra la propria identità utilizzando almeno due fattori indipendenti.

Come si dimostra: Configurazione dell'accesso remoto con il secondo fattore attivato, un esempio di registrazione di accesso che mostri entrambi i fattori, e l'elenco di rilascio di token o registrazioni delle app. Una piccola realtà utilizza il secondo fattore del gateway VPN esistente o un'app di autenticazione, il che non comporta costi oltre al tempo di configurazione. Miglioramento del requisito, richiesto da SL 3 in poi, non a SL 1.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 1.1 RE 3 La verifica tramite due fattori indipendenti si applica non solo all'accesso dall'esterno, ma a ogni accesso di un utente umano, compresi gli accessi all'interno della rete classificata come affidabile.

Come si dimostra: Estratto della policy del servizio centrale di autenticazione che mostri che il secondo fattore è applicato senza alcuna eccezione di rete, più esempi di registrazioni di accesso dalla sala controllo e dal pannello operatore. Miglioramento del requisito, richiesto solo da SL 4 in poi.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 1.2 Non solo le persone, ma anche i processi software e i dispositivi si autenticano presso il sistema prima che sia loro consentito scambiare dati o utilizzare servizi. Questo include gli accoppiamenti tra controllori, i collegamenti dati verso sistemi di livello superiore e gli strumenti diagnostici.

Come si dimostra: Elenco delle connessioni macchina a macchina con origine, destinazione, protocollo e la credenziale utilizzata in ciascun caso, per esempio certificato, account di servizio o chiave precondivisa. Aggiungere un estratto di configurazione di un accoppiamento che renda visibile l'autenticazione. Richiesto da SL 2 in poi, non richiesto a SL 1.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 1.2 RE 1 Ogni processo software e ogni dispositivo presenta un proprio identificativo univoco. Non sono ammessi account di servizio condivisi né un'unica chiave utilizzata a livello di sistema da più dispositivi.[Documento](#)

Come si dimostra: Mappatura dispositivo-identificativo o numero di serie del certificato che dimostri che nessun identificativo compare due volte. Miglioramento del requisito, richiesto da SL 3 in poi e quindi non parte di SL 1.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 1.3 Gli account sono gestiti lungo l'intero ciclo di vita: creazione, modifica dei privilegi, disabilitazione all'uscita e rimozione sono disciplinate da regole e supportate dai sistemi coinvolti. Questo copre account utente, account di servizio e account di emergenza.[Documento](#)

Come si dimostra: Registro degli account con tipo, titolare, scopo e stato, più evidenza per assunzioni e cessazioni, per esempio un passaggio di consegne firmato o un ticket che mostri la disabilitazione con la relativa data. È consigliabile una revisione periodica degli account, e in una piccola realtà è sufficiente una riconciliazione annuale dell'elenco account con l'elenco del personale. Richiesto da SL 1 in poi.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 1.3 RE 1 La gestione degli account è unificata su tutti i componenti del sistema, in modo che disabilitare un account in un punto non resti senza effetto su singoli dispositivi.

Come si dimostra: Evidenza dell'integrazione con la directory centrale, per esempio servizio di directory o RADIUS, con un elenco dei componenti collegati e un elenco esplicito dei dispositivi che non possono essere collegati insieme alla relativa procedura alternativa. Verbale di test di una disabilitazione che ha effetto su tutti i sistemi collegati. Miglioramento del requisito, richiesto da SL 3 in poi.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 1.4 Gli identificativi sono rilasciati secondo regole fisse, assegnati in modo univoco a una persona, un dispositivo o un ruolo, ritirati quando non più utilizzati e mai riassegnati in seguito a un titolare diverso.

Come si dimostra: Regola di denominazione degli identificativi, per esempio cognome più iniziale oppure codice impianto più numero, più lo storico degli identificativi ritirati che dimostri che non vengono riutilizzati. Una piccola realtà mantiene un unico elenco progressivo con data di rilascio e data di ritiro. Richiesto da SL 1 in poi.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 1.5 Gli autenticatori come password, chiavi, certificati e token sono rilasciati in modo ordinato, cambiati quando si sospetta una divulgazione e revocati quando necessario. Gli account predefiniti e le password di fabbrica come consegnate vengono cambiati prima della messa in servizio.

Come si dimostra: Elenco di rilascio di token e certificati con destinatario e data, evidenza di cambi e revoche, più una checklist di messa in servizio per dispositivo con la voce password di fabbrica cambiata, firmata. Richiesto da SL 1 in poi.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 1.5 RE 1 Le credenziali dei processi software non sono memorizzate come file leggibile sul supporto di memorizzazione, ma in una memoria protetta da hardware che impedisce la lettura della parte segreta.

Come si dimostra: Evidenza del tipo di componente di sicurezza utilizzato, per esempio TPM, elemento sicuro o HSM, con un estratto di configurazione che dimostri che la chiave è memorizzata all'interno del componente. Una registrazione d'acquisto o una scheda tecnica sono sufficienti come evidenza di tipo. Miglioramento del requisito, richiesto da SL 3 in poi, non richiesto a SL 1 e SL 2.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 1.6 L'accesso wireless al sistema, per esempio WLAN, radiocomandi o diagnostica Bluetooth, è utilizzabile solo dopo l'identificazione e l'autenticazione sia dell'utente sia del dispositivo, ed è gestito in modo consapevole.

Come si dimostra: Inventario di tutti i collegamenti wireless con scopo, portata e metodo di cifratura, estratto di configurazione del punto di accesso e l'elenco dei dispositivi finali approvati. Una piccola realtà documenta inoltre quali interfacce wireless dei dispositivi sono state deliberatamente disattivate. Richiesto da SL 1 in poi.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 1.6 RE 1 Ogni accesso wireless deve poter essere attribuito a uno specifico utente o a uno specifico dispositivo, una chiave di rete condivisa da tutti i partecipanti non è sufficiente.

Come si dimostra: Evidenza di un metodo con credenziali individuali, per esempio autenticazione WLAN enterprise verso una directory oppure certificati per dispositivo, più un registro di connessione che mostri l'identificativo individuale. Miglioramento del requisito, richiesto da SL 2 in poi e quindi non a SL 1.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 1.7 Ovunque siano utilizzate password, la loro robustezza minima è configurabile, per esempio lunghezza minima e tipi di carattere richiesti, e i valori configurati hanno effetto su tutti gli account interessati.

Come si dimostra: Estratto di configurazione della policy password per sistema con i valori effettivamente impostati, per esempio lunghezza ≥ 10 caratteri e almeno tre tipi di carattere, più un elenco dei sistemi che non possono tecnicamente supportare questa impostazione insieme alla relativa misura compensativa. Richiesto da SL 1 in poi.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 1.7 RE 1 Per gli utenti umani valgono regole aggiuntive sulla generazione e sulla durata delle password: il riutilizzo di password precedenti è impedito e la validità è limitata nel tempo.

Come si dimostra: Estratto di configurazione che mostri lo storico delle password, per esempio blocco del riutilizzo delle ultime cinque password, e la validità massima configurata. Miglioramento del requisito, richiesto da SL 3 in poi.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 1.7 RE 2 Il limite sulla durata della password si applica non solo alle persone, ma a tutti gli account, compresi quelli di servizio, di manutenzione e di dispositivo.

Come si dimostra: Piano di rotazione per gli account tecnici con data dell'ultimo e del prossimo cambio per account, più evidenza dei cambi effettuati, per esempio un verbale di modifica o un ticket. Miglioramento del requisito, richiesto solo da SL 4 in poi.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 1.8 Ovunque siano utilizzati certificati, essi provengono da una gestione ordinata dei certificati con regole definite per richiesta, emissione, periodo di validità, rinnovo e revoca.

[Documento](#)

Come si dimostra: Policy dei certificati o una breve regola scritta che indichi responsabilità, periodi di validità e il percorso di revoca, più un inventario dei certificati emessi con le relative scadenze. Una piccola realtà mantiene una tabella con certificato, dispositivo, data di scadenza e data di promemoria, il che evita fermi impianto silenziosi causati da certificati scaduti. Richiesto da SL 2 in poi.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 1.9 Quando vengono utilizzate coppie di chiavi per l'autenticazione, il sistema convalida il certificato in modo completo: catena di fiducia, periodo di validità, stato di revoca e prova che la controparte possieda effettivamente la chiave privata. Il legame tra certificato e account è univoco.

Come si dimostra: Estratto di configurazione con il controllo di revoca attivato, per esempio CRL o OCSP, verbale di test di un accesso rifiutato con un certificato scaduto o revocato, più la tabella di corrispondenza certificato-account. Richiesto da SL 3 in poi, non richiesto a SL 1 e SL 2.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 1.9 RE 1 Le chiavi private risiedono esclusivamente in una memoria protetta da hardware dalla quale non possono essere lette, e vengono utilizzate anche all'interno di quella memoria.

Come si dimostra: Scheda tecnica o evidenza di certificazione del componente di sicurezza utilizzato e un estratto di configurazione che dimostri che la chiave viene generata all'interno del componente, così che la chiave privata non lo lasci mai. Miglioramento del requisito, richiesto solo da SL 4 in poi.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 1.10 Durante l'accesso il sistema non rivela alcuna informazione che possa essere sfruttata. Le password inserite sono oscurate e i messaggi di errore non rivelano se era errato l'identificativo o la password.

Come si dimostra: Schermata della maschera di accesso con l'input mascherato e una schermata del messaggio di errore dopo un tentativo fallito. Per i dispositivi che tecnicamente non lo consentono, per esempio pannelli operatore datati, aggiungere una breve nota sulla misura compensativa, per esempio accesso fisico limitato al luogo dell'installazione. Richiesto da SL 1 in poi.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 1.11 Il numero di tentativi di accesso falliti consecutivi è limitato e la risposta è configurabile, per esempio un blocco temporaneo. La risposta scelta non ostacola il funzionamento della pianta legato alla sicurezza.

Come si dimostra: Estratto di configurazione con la soglia, per esempio blocco dopo ≤ 5 tentativi falliti, e la durata del blocco, più una breve valutazione del perché il blocco non impedisce l'operatività di emergenza o un arresto sicuro dell'impianto. Nelle postazioni operatore con funzione di sicurezza, un blocco temporizzato è preferibile a un blocco permanente dell'account. Richiesto da SL 1 in poi.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 1.12 Prima dell'accesso può essere visualizzato un avviso d'uso, che rimanda alle regole d'uso e di monitoraggio del sistema. Il testo e la visualizzazione sono configurabili dal proprietario dell'impianto.

Come si dimostra: Schermata del testo dell'avviso visualizzato e della formulazione approvata con la data di approvazione. Le piccole realtà concordano la formulazione brevemente con la rappresentanza dei lavoratori o con la direzione, un paragrafo è sufficiente. Richiesto da SL 1 in poi.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 1.13 L'accesso da reti non affidabili, per esempio la manutenzione remota da parte di fornitori, è limitato a percorsi definiti, è monitorato e può essere interrotto in qualsiasi momento.

Come si dimostra: Inventario dei percorsi di accesso remoto con scopo, controparte remota, persona di contatto e il percorso utilizzato, più registri di connessione ed evidenza della possibilità di disconnessione, per esempio un interruttore a chiave, una regola del firewall o un router di manutenzione remota disattivabile. Richiesto da SL 1 in poi.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 1.13 RE 1 Ogni singola sessione da una rete non affidabile viene approvata esplicitamente da una persona responsabile prima che la connessione venga stabilita, una connessione permanentemente aperta non è sufficiente.

Come si dimostra: Verbali di approvazione per sessione di manutenzione remota con ora, motivo, persona che approva e durata, tecnicamente per esempio tramite un interruttore a chiave sul router di accesso o tramite un portale di approvazione. In una piccola realtà è sufficiente un registro di manutenzione remota nell'armadio di controllo, firmato dal tecnico di manutenzione per ogni sessione. Miglioramento del requisito, richiesto da SL 2 in poi e quindi mai a SL 1.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

6 FR 2: Controllo dell'uso (privilegi, sessioni, registri di audit)

24

SR 2.1 Il sistema applica tecnicamente i privilegi che sono stati concessi: ogni persona connessa, ogni dispositivo e ogni processo software riceve esattamente l'accesso assegnato, e ogni tentativo che va oltre viene respinto.

Come si dimostra: Un concetto di privilegi che associ gli account ai permessi, più una schermata o un estratto di configurazione per sistema di controllo, HMI e postazione di ingegneria che mostri i privilegi attivi. Inoltre, un verbale di test in cui un account con privilegi ridotti tenta un'azione bloccata e viene respinto. Richiesto da SL 1. Una piccola realtà si gestisce con due o tre ruoli, per esempio operare, mantenere, progettare, e li documenta in una singola pagina.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.1 RE 1 L'applicazione dei privilegi riguarda non solo gli operatori umani ma allo stesso modo i processi software e i dispositivi che accedono al sistema in autonomia.

Come si dimostra: Un elenco di account tecnici e di servizio, per esempio client OPC UA, connessioni historian, servizi di backup, ciascuno con il proprio insieme di privilegi assegnato. Un estratto della gestione privilegi che mostri che questi account non operano con diritti di amministratore. Miglioramento del requisito, richiesto da SL 2, non a SL 1.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.1 RE 2 I privilegi non vengono concessi alle singole persone una per una, ma tramite ruoli, e la corrispondenza tra ruolo e azioni consentite è registrata in modo tracciabile.

[Documento](#)

Come si dimostra: Una matrice ruoli-privilegi in forma di tabella: le righe sono i ruoli, le colonne le azioni come modificare un setpoint, scaricare un programma, riconoscere un allarme, creare un account. Più l'elenco di corrispondenza tra persona e ruolo. Miglioramento del requisito, richiesto da SL 2. Un foglio di calcolo mantenuto e con data di modifica è un'evidenza pienamente sufficiente.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.1 RE 3 Per casi eccezionali definiti in modo ristretto, un supervisore autorizzato può revocare temporaneamente una restrizione di privilegio per un periodo limitato, e ogni deroga di questo tipo è registrata nella traccia di audit.

Come si dimostra: Una descrizione della procedura di approvazione delle eccezioni che indichi chi può concederla e per quanto tempo resta valida, più i registri di audit delle deroghe già concesse, tratti dal log di sistema. Miglioramento del requisito, richiesto da SL 3.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.1 RE 4 Gli interventi particolarmente critici richiedono l'approvazione di due persone autorizzate indipendenti prima che l'azione venga eseguita.

Come si dimostra: Un elenco delle azioni soggette a doppia approvazione, per esempio la modifica di parametri di sicurezza o il download di un nuovo programma di controllo, insieme all'evidenza di configurazione e ai registri di audit che indicano entrambi gli approvatori. Miglioramento del requisito, richiesto solo da SL 4.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.2 L'uso di connessioni wireless nella rete di automazione è vincolato a un'autorizzazione esplicita, e solo i partecipanti approvati possono scambiare dati o intervenire per via radio.

Come si dimostra: Un inventario di tutti i collegamenti wireless, per esempio access point WLAN, associazioni Bluetooth, router cellulari, ciascuno con il proprio scopo e i propri partecipanti approvati. Più la configurazione del controllo accessi sull'access point. Richiesto da SL 1. Chi non gestisce alcun collegamento wireless nella rete di processo lo dichiara esattamente per iscritto e lo supporta con una vista di configurazione che mostri il wireless disattivato.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.2 RE 1 I dispositivi wireless non autorizzati nelle vicinanze della rete di automazione vengono rilevati e segnalati.

Come si dimostra: Un verbale del monitoraggio wireless o di una scansione wireless periodica con data, elenco dei risultati e una nota per ogni dispositivo sconosciuto. Viene indicato il percorso di segnalazione verso la funzione responsabile. Miglioramento del requisito, richiesto da SL 2, non a SL 1. Una piccola realtà può eseguire una scansione trimestrale con un notebook e archiviare il risultato come verbale.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.3 L'uso di dispositivi portatili e mobili sul sistema, per esempio notebook di servizio, memorie USB o tablet, è disciplinato da regole e tecnicamente limitato a dispositivi esplicitamente approvati.

Come si dimostra: Il regolamento per l'uso dei dispositivi, un elenco dei dispositivi di servizio approvati con i relativi identificativi, ed evidenza della limitazione tecnica, per esempio porte USB su HMI e postazione di ingegneria disabilitate o limitate a dispositivi specifici. Richiesto da SL 1. Una piccola realtà lavora con due chiavette di servizio etichettate che vengono scritte solo su un'unica postazione di trasferimento.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.3 RE 1 Prima del collegamento viene verificato lo stato di sicurezza di un dispositivo portatile o mobile, e ai dispositivi che non soddisfano i requisiti viene impedito l'accesso.

Come si dimostra: I criteri di verifica dello stato del dispositivo, per esempio protezione antimalware aggiornata e livello delle patch, più verbali di verifica per dispositivo di servizio ed evidenza dell'applicazione tecnica, per esempio tramite una postazione di trasferimento o un controllo di accesso alla rete. Miglioramento del requisito, richiesto da SL 3.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.4 Per il codice mobile eseguito sul sistema, per esempio script nelle interfacce operatore o contenuto attivo nei report, è definito quali tipi sono ammessi, e ai tipi non ammessi è impedita l'esecuzione.[Documento](#)

Come si dimostra: Una definizione di quale codice mobile è ammesso su quali sistemi, più evidenza di configurazione della limitazione, per esempio esecuzione di script nel browser HMI disabilitata, macro nei file di valutazione bloccate. Richiesto da SL 1. Una definizione di una pagina che copra i tre o quattro casi effettivamente presenti è sufficiente.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.4 RE 1 Prima che il codice mobile venga eseguito, si verifica che provenga dalla fonte prevista e che non sia stato alterato.

Come si dimostra: Evidenza di configurazione della verifica della firma o del controllo checksum, più un verbale di test in cui il codice manipolato o non firmato viene respinto. Miglioramento del requisito, richiesto da SL 3.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.5 Una sessione viene bloccata dopo un periodo definito senza azione dell'operatore ed è rilasciata nuovamente solo dopo una nuova autenticazione, senza perdere la visualizzazione delle informazioni di processo rilevanti per la sicurezza.

Come si dimostra: Un estratto di configurazione con il tempo di blocco configurato per postazione di lavoro, più una giustificazione per le postazioni in sale controllo presidiate in modo permanente dove il blocco è impostato deliberatamente in modo diverso. Richiesto da SL 1. Evidenza visiva: una schermata della schermata di blocco con la riga allarmi ancora visibile.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.6 Le sessioni remote vengono terminate dopo un periodo definito senza attività o su richiesta dell'operatore, in modo che non resti aperta e incustodita alcuna connessione remota.

Come si dimostra: La configurazione dell'accesso remoto con il relativo limite di tempo di inattività, i registri di audit delle sessioni remote terminate, e una descrizione di come l'operatore possa disconnettere immediatamente una sessione di manutenzione remota in corso, per esempio tramite un interruttore a chiave o un rilascio per sessione. Richiesto da SL 2, non a SL 1.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.7 Il numero di sessioni contemporanee per account o ruolo è limitato, e i tentativi di accesso oltre tale limite vengono respinti.

Come si dimostra: Un estratto di configurazione con il limite superiore definito per ruolo, per esempio ≤ 1 sessione contemporanea per gli account di ingegneria, più un verbale di test del secondo tentativo di accesso respinto. Richiesto da SL 3.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.8 Gli eventi rilevanti per la sicurezza vengono registrati, e ogni voce indica almeno l'ora, l'origine, l'account che l'ha innescato, il tipo di evento e l'esito.

[Documento](#)

Come si dimostra: Una definizione dei tipi di evento da registrare, per esempio accesso, accesso fallito, cambio di privilegi, modifica di programma, modifica di configurazione, più un estratto reale del registro di audit che mostri i campi indicati. Richiesto da SL 1. Una piccola realtà raccoglie i log di sistema di controllo, HMI e firewall in un'unica cartella con un periodo di conservazione fisso.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.8 RE 1 I registri di audit dei singoli componenti vengono riuniti in un punto centrale e formano un unico registro a livello di sistema che può essere valutato nel suo insieme.

Come si dimostra: Uno schema architetturale della raccolta log che mostri tutte le fonti collegate, più una valutazione che collochi eventi di almeno due componenti su un'unica linea temporale. Miglioramento del requisito, richiesto da SL 3.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.9 Viene fornito spazio di archiviazione sufficiente per i registri di audit, in modo che gli eventi siano conservati per il periodo di conservazione definito e non vengano sovrascritti involontariamente.

Come si dimostra: Un calcolo o una stima del fabbisogno di spazio a partire dal volume giornaliero di log moltiplicato per il periodo di conservazione, più la dimensione di archiviazione configurata e la regola di archiviazione. Richiesto da SL 1. In pratica è sufficiente una copia giornaliera su una posizione di archiviazione separata con un periodo di conservazione documentato.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.9 RE 1 Quando viene raggiunta una soglia definita di livello di riempimento dello spazio di archiviazione di audit, viene emesso un avviso alla funzione responsabile prima che la capacità di archiviazione sia completamente esaurita.

Come si dimostra: Un estratto di configurazione della soglia, per esempio un avviso a partire da ≥ 80 percento di utilizzo, più un esempio della notifica generata e l'elenco dei destinatari. Miglioramento del requisito, richiesto da SL 3.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.10 Se la registrazione di audit fallisce o lo spazio di archiviazione di audit si riempie, il sistema reagisce in un modo definito in precedenza e la funzione responsabile viene informata, senza mettere a rischio il funzionamento sicuro dell'impianto.

Come si dimostra: La reazione definita per ciascun caso di guasto, per esempio sovrascrivere le voci più vecchie e generare una notifica invece di fermare l'impianto, con una giustificazione dal punto di vista del processo. Evidenza tramite una notifica di test generata e la corrispondente voce di audit. Richiesto da SL 1.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.11 Ogni registrazione di audit riporta una marca temporale proveniente da una fonte oraria indicata, in modo che gli eventi di componenti diversi possano essere ordinati tra loro.

Come si dimostra: Un'indicazione della fonte oraria utilizzata per componente e un estratto di log con una marca temporale visibile che includa il fuso orario. Richiesto da SL 2, non a SL 1.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.11 RE 1 Gli orologi di tutti i componenti coinvolti sono sincronizzati su una fonte oraria comune in modo che lo scostamento resti entro un limite definito.

Come si dimostra: La configurazione della sincronizzazione oraria, per esempio server NTP e intervallo di sincronizzazione, più un verbale di verifica con lo scostamento misurato per componente rispetto al limite definito, per esempio ≤ 1 secondo. Miglioramento del requisito, richiesto da SL 3.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.11 RE 2 La fonte oraria stessa è protetta contro le manipolazioni, e un riferimento orario inverosimile o alterato viene rilevato e segnalato.

Come si dimostra: Una descrizione di come è protetta la fonte oraria, per esempio sincronizzazione oraria autenticata, limitazione a una fonte interna, monitoraggio dei salti temporali, più notifiche o registri di audit di uno scostamento rilevato. Miglioramento del requisito, richiesto solo da SL 4.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.12 Per azioni critiche definite si può stabilire senza dubbio a posteriori chi le ha innescate, in modo che la persona che ha agito non possa negare in modo credibile di averlo fatto.[Documento](#)

Come si dimostra: Un elenco delle azioni a cui si applica questa evidenza, per esempio modifica di ricetta, rilascio di lotto, modifica di valori limite, più i registri corrispondenti con un identificativo univoco della persona ed evidenza che gli account di gruppo sono esclusi per queste azioni. Richiesto da SL 3.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 2.12 RE 1 L'attribuzione innegabile della persona che agisce si applica non solo alle azioni critiche selezionate, ma a tutti gli utenti e a tutte le azioni che innescano.

Come si dimostra: Evidenza che ogni account è legato a un'unica persona e che non restano accessi condivisi, più un estratto di log di azioni qualsiasi in cui compare in modo coerente un identificativo univoco della persona. Miglioramento del requisito, richiesto solo da SL 4.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

7 FR 3: Integrità di sistema, protezione di dati, software e sessioni da modifiche non autorizzate

19

SR 3.1

Il sistema di controllo rileva quando un'informazione è stata alterata durante il transito su un canale di comunicazione, e lo fa sia per i dati di controllo sia per i dati di configurazione e il traffico di gestione. La protezione copre anche le connessioni che escono dal sistema o che attraversano segmenti di rete non affidabili.

Come si dimostra: Una panoramica di rete e protocolli che indichi quale canale utilizza quale meccanismo di integrità (checksum, codice di autenticazione del messaggio, telegrammi firmati), un estratto di configurazione delle impostazioni di sicurezza del bus di campo o di OPC UA, e un verbale di test che mostri che un telegramma manomesso è stato dimostrabilmente respinto. Una piccola realtà raccoglie questo in una tabella per connessione con le colonne origine, destinazione, protocollo e meccanismo di integrità, e dimostra l'efficacia una volta con una cattura di traffico. Richiesto da SL 1 in su.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 3.1 RE 1

La protezione dell'integrità in transito si basa su meccanismi crittografici, in modo che una manipolazione deliberata da parte di un attaccante con mezzi propri non possa passare inosservata. Un semplice checksum contro gli errori di trasmissione non è sufficiente in questo caso.

Come si dimostra: Un elenco dei meccanismi crittografici e delle lunghezze di chiave in uso per canale, un riferimento alla gestione delle chiavi sottostante, ed estratti di configurazione (per esempio cipher suite TLS, SecurityPolicy di OPC UA, profili IPsec). Le piccole realtà si affidano ai profili sicuri predefiniti dei propri controllori e archiviano una schermata dell'impostazione attiva. Miglioramento del requisito, richiesto da SL 3 in su.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 3.2

Sono presenti meccanismi di protezione contro il codice dannoso che impediscono l'esecuzione di codice di programma indesiderato sui componenti del sistema e che segnalano ogni rilevamento. I meccanismi sono scelti in modo da non disturbare il funzionamento previsto dell'impianto, e vengono mantenuti aggiornati.

Come si dimostra: Una panoramica per componente di quale meccanismo si applica (antivirus, whitelisting delle applicazioni, sistema operativo irrobustito senza diritti di esecuzione), evidenza che le firme o le whitelist vengono aggiornate, e allarmi dal sistema di protezione. Dove l'antivirus non è praticabile, per esempio su un controllore, la misura compensativa viene registrata con la relativa motivazione. Alle piccole realtà conviene un whitelisting sul PC operatore e una regola scritta per i supporti USB. Richiesto da SL 1 in su.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 3.2 RE 1

La protezione contro il codice dannoso ha effetto anche nei punti di ingresso e di uscita dell'impianto, dove i dati entrano o escono, e non solo sui dispositivi terminali stessi.

Come si dimostra: Un elenco di tutti i punti di ingresso e di uscita (accesso di manutenzione remota, gateway di trasferimento dati, supporti rimovibili, passaggio alla rete d'ufficio, percorso email per le versioni di programma) con il meccanismo di scansione efficace in ciascuno, più registri dei passaggi che sono stati verificati. Le piccole realtà predispongono un unico PC di passaggio con scansione antivirus come gateway e lo fissano in un'istruzione di lavoro. Miglioramento del requisito, richiesto da SL 2 in su.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 3.2 RE 2

I meccanismi di protezione contro il codice dannoso sono gestiti da un punto centrale, gli aggiornamenti sono distribuiti centralmente, e i rilevamenti sono raccolti in un unico luogo per la valutazione.

Come si dimostra: La configurazione della console di gestione centrale, un report sullo stato di aggiornamento di tutti i componenti collegati, e una valutazione dei rilevamenti segnalati nell'arco di un periodo. Miglioramento del requisito, richiesto da SL 3 in su.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 3.3

Le funzioni di sicurezza del sistema vengono verificate a intervalli pianificati e dopo le modifiche per confermare che funzionino effettivamente. I test sono programmati in modo da non mettere a rischio il funzionamento dell'impianto, e i risultati vengono registrati.

[Documento](#)

Come si dimostra: Un piano di test che indichi l'oggetto della prova, l'intervallo e la finestra temporale, insieme ai verbali di test che mostrino data, esaminatore, comportamento atteso e comportamento osservato. Test individuali utili sono: un accesso con un account disabilitato fallisce, l'antivirus reagisce a un file di prova, l'accesso di manutenzione remota è irraggiungibile senza rilascio. Le piccole realtà collegano i test al fermo di manutenzione già pianificato e lavorano con una checklist fissa. Richiesto da SL 1 in su.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 3.3 RE 1

La verifica delle funzioni di sicurezza viene eseguita con mezzi automatizzati, in modo da essere ripetibile senza sforzo manuale e da fornire un risultato coerente.

Come si dimostra: Gli script o gli strumenti di test insieme alla loro pianificazione, i relativi file di output, e un confronto tra più esecuzioni che dimostri che gli scostamenti vengono rilevati. Miglioramento del requisito, richiesto da SL 3 in su.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 3.3 RE 2

La verifica delle funzioni di sicurezza è possibile anche durante il normale funzionamento, senza dover fermare l'impianto o portarlo in uno stato speciale.

Come si dimostra: Una descrizione della procedura di test con evidenza che non ha effetti negativi sul processo, per esempio un'analisi dell'impatto sui tempi di ciclo e sul carico di rete, più verbali di test tratti dal funzionamento produttivo. Miglioramento del requisito, richiesto da SL 4 in su.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 3.4

Le modifiche non autorizzate a software, firmware e informazioni a riposo vengono rilevate. Questo vale allo stesso modo per i programmi di controllo, gli insiemi di parametri, le ricette e i file di configurazione.

Come si dimostra: Un inventario delle versioni degne di protezione con i valori di controllo o le firme memorizzati, i risultati dei confronti di integrità, e la riconciliazione documentata con la versione conservata nel controllo di versione. Le piccole realtà conservano la versione di programma rilasciata insieme al relativo checksum in una posizione protetta da scrittura e confrontano in caso di sospetto o dopo la manutenzione. Richiesto da SL 1 in su.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 3.4 RE 1

Se viene rilevata una violazione dell'integrità del software o delle informazioni, il sistema la segnala automaticamente a un punto responsabile, senza che nessuno debba cercarla attivamente.

Come si dimostra: La configurazione dei percorsi di notifica (allarme in sala controllo, email, messaggio al sistema di monitoraggio), un elenco di destinatari con le disposizioni di sostituzione, e almeno un allarme di test con un tempo di risposta documentato. Miglioramento del requisito, richiesto da SL 3 in su.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 3.5

Gli input che il sistema accetta da dati di processo, interfacce o interfacce utente vengono verificati per sintassi ammessa, intervallo di valori ammesso e lunghezza ammessa prima di essere elaborati. Gli input non validi non provocano un comportamento incontrollato.

Come si dimostra: Una specifica dei limiti e dei formati per input, estratti della logica di validazione nel controllore o nell'applicazione, e casi di test con input deliberatamente non validi (un valore troppo grande, un tipo di dato errato, una stringa di caratteri troppo lunga) insieme al comportamento documentato del sistema. Le piccole realtà registrano i limiti di plausibilità per punto di misura in una tabella e li verificano durante la messa in servizio. Richiesto da SL 1 in su.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 3.6 Per il caso di un guasto è definito quale stato assumono le uscite verso l'impianto, e il sistema assume esattamente quello stato. Lo stato definito è allineato con la sicurezza funzionale dell'impianto.

Come si dimostra: Una definizione per uscita o gruppo di uscite (mantenere il valore, valore sostitutivo definito, stato di arresto sicuro) con una motivazione derivata dalla valutazione dei rischi, un estratto di configurazione del controllore, ed evidenza di un test di guasto, per esempio un'interruzione di cavo o una perdita di comunicazione, che mostri il comportamento atteso. Richiesto da SL 1 in su.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 3.7 Il sistema gestisce le condizioni di errore in modo che il funzionamento resti sotto controllo e non venga divulgata alcuna informazione che possa aiutare un attaccante. I messaggi di errore mostrati agli operatori restano brevi, mentre i dettagli tecnici confluiscono solo nei registri interni.

Come si dimostra: Una panoramica delle classi di errore con il comportamento di sistema previsto per ciascuna, esempi dei messaggi visualizzati confrontati con le corrispondenti voci di log interne, ed evidenza di test che nessun percorso file, nome account, output di database o dettaglio di versione compaia sull'interfaccia operatore. Richiesto da SL 1 in su.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 3.8 Le sessioni attive sono protette contro il dirottamento e contro l'iniezione di messaggi estranei. Una sessione termina dopo il logout o dopo un periodo definito senza attività, e successivamente non può essere riutilizzata.

Come si dimostra: La configurazione della gestione delle sessioni con i limiti configurati per il tempo di inattività e la durata massima, evidenza del meccanismo di protezione contro la riproduzione dei messaggi, e un verbale di test in cui una sessione catturata non funziona più dopo il logout. Richiesto da SL 2 in su.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 3.8 RE 1 Gli identificativi di sessione perdono validità quando la sessione termina e non vengono più accettati dal sistema, nemmeno quando vengono ripresentati dall'esterno.

Come si dimostra: Un estratto di configurazione della gestione delle sessioni che copra l'invalidazione, più un verbale di test in cui un identificativo precedentemente valido viene inviato di nuovo dopo il logout e viene respinto dal sistema. Miglioramento del requisito, richiesto da SL 3 in su.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 3.8 RE 2 Per ogni nuova sessione viene generato un identificativo dedicato monouso. Gli identificativi non vengono riutilizzati tra sessioni, utenti o dispositivi.

Come si dimostra: Una descrizione della procedura di generazione ed evidenza dal log o da una cattura di traffico che più accessi consecutivi ricevano identificativi diversi. Miglioramento del requisito, richiesto da SL 3 in su.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 3.8 RE 3 Gli identificativi di sessione vengono generati con meccanismi casuali riconosciuti, in modo che non possano essere indovinati né derivati da identificativi precedenti.

Come si dimostra: Un'indicazione del generatore di numeri casuali utilizzato e della relativa fonte di entropia, una dichiarazione del fornitore o un rapporto di test in merito, e una valutazione statistica di un campione di identificativi generati. Miglioramento del requisito, richiesto da SL 4 in su.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 3.9

I registri relativi alla sicurezza e gli strumenti utilizzati per valutarli sono protetti contro l'accesso, la modifica e la cancellazione non autorizzati. La cerchia di persone autorizzate a modificare o rimuovere i registri è mantenuta ristretta ed è nominata.

[Documento](#)

Come si dimostra: Un concetto di autorizzazione per i dati di log con assegnazione nominale, la configurazione dell'inoltro a un sistema di logging separato, i periodi di conservazione, ed evidenza di test che un operatore ordinario non possa cancellare le voci. Le piccole realtà inoltrano i log a un dispositivo separato a cui gli operatori di impianto non hanno accesso in scrittura. Richiesto da SL 2 in su.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 3.9 RE 1

I registri relativi alla sicurezza vengono inoltre memorizzati su un supporto che esclude la sovrascrittura successiva, in modo che una voce già scritta non possa più essere alterata, nemmeno con diritti amministrativi.

[Documento](#)

Come si dimostra: Una descrizione del supporto utilizzato (supporto a scrittura unica, archivio a prova di manomissione, catena di firme continuamente estesa), evidenza di un tentativo fallito di modificare una voce, e la regola per la conservazione e il recupero dei supporti. Miglioramento del requisito, richiesto da SL 3 in su.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

8 FR 4: Riservatezza dei dati

6

SR 4.1

Il sistema di automazione protegge le informazioni riservate dalla divulgazione non autorizzata, sia durante il transito sia a riposo. È definito quali dati sono considerati riservati, per esempio ricette, insiemi di parametri, credenziali, file di configurazione o dati diagnostici con riferimento personale.

[Documento](#)

Come si dimostra: Un elenco dei tipi di dati degni di protezione, con indicazione di dove sono conservati e come vengono trasmessi, più la specifica misura di protezione per ciascuna voce, per esempio una connessione cifrata, un supporto di memorizzazione cifrato o una condivisione limitata. Una piccola realtà si gestisce con una tabella su una sola pagina: tipo di dato, dove si trova, chi può vederlo, cosa lo protegge. Richiesto da SL 1 in su.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 4.1 RE 1

Per le informazioni che viaggiano su reti non affidabili o sono memorizzate al di fuori dell'ambiente protetto, la riservatezza è imposta con mezzi tecnici e non semplicemente promessa in una regola organizzativa.

Come si dimostra: Un estratto di configurazione della cifratura di trasporto o di memorizzazione in uso, per esempio il profilo VPN per la manutenzione remota, le impostazioni TLS dell'interfaccia del sistema di controllo, o la cifratura dei supporti di backup. Una schermata datata dell'impostazione attiva è sufficiente come evidenza. Richiesto da SL 2 in su, non da SL 1, perché si tratta di un miglioramento del requisito.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 4.1 RE 2

La riservatezza è imposta anche ai confini tra le zone, in modo che l'informazione non diventi visibile in chiaro quando passa da una zona all'altra.

Come si dimostra: Un piano di zone e condotti che indichi quali attraversamenti sono cifrati, insieme alla configurazione del componente di confine come un gateway, un firewall o un diodo dati. Una cattura di traffico o un verbale di test che mostri che nessun dato in chiaro compare al confine. Richiesto da SL 4 in su.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 4.2

È definito come viene rimossa in modo affidabile l'informazione riservata quando i dispositivi vengono dismessi, cambiano proprietario, vanno in riparazione o vengono riutilizzati, in modo che non restino dati residui leggibili.

[Documento](#)

Come si dimostra: Una procedura di dismissione scritta con il metodo di bonifica per tipo di dispositivo, più registri di cancellazione con identificazione del dispositivo, data e persona che l'ha eseguita. Una piccola realtà registra questo come una riga per dispositivo in un elenco condiviso e archivia accanto i certificati dei fornitori esterni di smaltimento. Richiesto da SL 2 in su.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 4.2 RE 1 Le aree di memorizzazione condivise vengono ripulite prima di essere riassegnate a un altro utente o processo, in modo che il contenuto dell'utente precedente non possa essere letto.

Come si dimostra: Una dichiarazione del fornitore o un registro di configurazione relativo alla pulizia delle aree di memoria e buffer riutilizzate, integrato da un verbale di test tratto dal collaudo o dalla manutenzione. Dove un componente non è in grado di farlo, la misura compensativa documentata funge da evidenza, per esempio non condividere il dispositivo tra ruoli diversi. Richiesto da SL 3 in su, non da SL 1, perché si tratta di un miglioramento del requisito.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 4.3 Ovunque venga utilizzata la crittografia, gli algoritmi, le lunghezze di chiave e la gestione delle chiavi seguono le buone pratiche riconosciute, ed è definito come le chiavi vengono generate, distribuite, memorizzate, ruotate e revocate.

[Documento](#)

Come si dimostra: Una panoramica dei meccanismi utilizzati per sistema, con algoritmo, lunghezza di chiave e periodo di validità, più le regole di gestione delle chiavi e i registri delle rotazioni di chiave e dei rinnovi di certificato. Le raccomandazioni pubbliche fungono da riferimento, per esempio le linee guida tecniche del BSI tedesco. Una piccola realtà mantiene un elenco di certificati con date di scadenza e un promemoria >= 30 giorni prima della scadenza. Richiesto da SL 1 in su.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

9 FR 5: Flusso di dati limitato, zone e condotti

11

SR 5.1 Il sistema di controllo può essere suddiviso in zone separate, e il traffico tra tali zone passa solo attraverso condotti definiti. La suddivisione segue una logica spiegabile, per esempio in base all'esigenza di protezione, alla proprietà o alla funzione delle sezioni di impianto coinvolte.

[Documento](#)

Come si dimostra: Schema di rete che mostri le zone e i condotti tra di esse, un elenco di zone con la logica di ciascun confine, e la configurazione dei componenti di separazione come definizioni VLAN o interfacce firewall. Una piccola realtà si accontenta di uno schizzo su una sola pagina che mostri ufficio, rete macchine e accesso remoto come tre riquadri con i collegamenti tra loro, più una schermata della configurazione VLAN dello switch.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 5.1 RE 1 La separazione delle zone è realizzata fisicamente, cioè tramite componenti di rete dedicati e cablaggio dedicato, e non si basa unicamente sulla configurazione logica all'interno di dispositivi condivisi. Punto 9.1 di questo elenco, richiesto da SL 2 in su. I miglioramenti del requisito di questa norma non sono mai obbligatori già a SL 1.

Come si dimostra: Inventario dei componenti di rete che indichi quale switch o router serve quale zona, foto o layout dell'armadio delle distribuzioni separate, etichettatura dei cavi. Le piccole realtà dimostrano questo con due switch separati, chiaramente etichettati, invece di un unico dispositivo condiviso e una foto dell'armadio di controllo nella documentazione di impianto.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 5.1 RE 2 La rete di automazione può funzionare indipendentemente dalle reti esterne all'automazione. Se l'IT d'ufficio o un collegamento esterno si guasta, il controllo e il monitoraggio dell'impianto continuano a funzionare. Richiesto da SL 3 in su.

Come si dimostra: Elenco delle dipendenze dei servizi utilizzati all'interno della rete di automazione come server orario, risoluzione dei nomi, servizio di directory o server di licenze, con indicazione di dove ciascuno è ospitato, insieme a un verbale di test di una prova di disconnessione in cui è stato staccato il collegamento con l'IT d'ufficio. Una piccola realtà annota l'esito di tale prova nel registro di manutenzione: collegamento a monte staccato, l'impianto ha continuato a funzionare, sono mancati solo i report d'ufficio.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 5.1 RE 3 Le zone che ospitano funzioni particolarmente critiche, per esempio funzioni di sicurezza o di protezione, sono separate dalle restanti zone sia logicamente sia fisicamente. Richiesto da SL 4 in su.

Come si dimostra: Marcatura delle zone critiche nello schema delle zone con la motivazione della classificazione, evidenza di componenti di rete dedicati e cablaggio dedicato per tali zone, configurazione dei condotti con evidenza che non esiste alcun percorso condiviso.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 5.2 Ai confini di zona, il traffico viene controllato, monitorato e consentito o negato secondo regole definite. Non esiste alcun percorso tra due zone che aggiri questo punto di controllo.

Come si dimostra: Set di regole esportato del firewall o del dispositivo di confine, log delle connessioni negate e consentite, evidenza che non esistono percorsi laterali, per esempio tramite una verifica di schede di rete aggiuntive, modem o router cellulari nei computer di impianto. Una piccola realtà dimostra questo con l'esportazione delle regole del proprio unico firewall e una breve nota di sopralluogo che confermi che nessun router non pianificato si trova in alcun armadio di controllo.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 5.2 RE 1 Il set di regole al confine di zona funziona secondo il principio per cui tutto è negato a meno che non sia stato esplicitamente consentito. Ogni regola di permesso è motivata singolarmente e legata a uno scopo. Richiesto da SL 2 in su.

Come si dimostra: Set di regole con una regola finale visibile che scarta il resto, e un elenco dei permessi che indichi origine, destinazione, servizio, scopo e persona responsabile per ciascuna regola. Le piccole realtà mantengono questo elenco come tabella a cinque colonne accanto all'esportazione del firewall e lo rivedono una volta all'anno alla ricerca di regole di cui nessuno ha più bisogno.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 5.2 RE 2 La rete di automazione può essere deliberatamente isolata da tutte le connessioni esterne e mantenuta in funzione in modalità isola. L'azione può essere attivata senza dover fermare l'impianto. Richiesto da SL 3 in su.

Come si dimostra: Descrizione della procedura di isolamento che indichi chi può attivarla e come, evidenza dell'implementazione tecnica come un set di regole di emergenza o un interruttore di isolamento etichettato, più il verbale di un'esercitazione in cui l'isolamento è stato effettivamente eseguito. Una piccola realtà svolge l'esercitazione una volta all'anno durante la manutenzione e annota data, durata ed eventuali anomalie.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 5.2 RE 3 Se il dispositivo al confine di zona si guasta o perde le proprie regole, nega il traffico invece di lasciarlo passare. Un guasto non deve lasciare aperta una connessione. Richiesto da SL 4 in su.

Come si dimostra: Dichiarazione del fornitore o evidenza di configurazione su come si comporta il componente in caso di guasto e al riavvio, verbale di test di un guasto indotto deliberatamente con il risultato osservato, allineamento con la valutazione dei rischi di impianto, perché un confine che nega il traffico può a sua volta avere conseguenze a seconda del processo.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 5.3 I servizi generali di comunicazione da persona a persona come email, messaggistica o videochiamate possono essere impediti sui dispositivi di automazione e all'interno delle reti di automazione. L'estensione del blocco è definita e motivata.

Come si dimostra: Definizione di quali servizi non sono ammessi nella rete di automazione, più l'implementazione tecnica: porte e destinazioni bloccate nel set di regole, applicazioni rimosse o bloccate sulle postazioni operatore, evidenza dall'inventario software dei dispositivi. Una piccola realtà risolve questo con un blocco applicazioni sulla postazione HMI e una regola che nega il traffico email e web in uscita dalla rete macchine.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 5.3 RE 1 Tali servizi di comunicazione da persona a persona sono impediti sull'intera rete di automazione, e non semplicemente limitati in parte o ristretti a singoli dispositivi. Richiesto da SL 2 in su.

Come si dimostra: Evidenza che il blocco si applica a ogni dispositivo della zona, per esempio tramite una revisione del software installato su ogni computer della zona e un test di connessione da un computer di impianto qualsiasi. Le piccole realtà dimostrano questo con un elenco dispositivi in cui ogni riga è spuntata con la data di verifica, e una schermata del tentativo di connessione fallito.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 5.4 I dati e le funzioni applicative sono compartimentati in modo che i processi con esigenze di protezione o privilegi diversi non possano raggiungere le stesse aree. La separazione è integrata nell'architettura di sistema e non è lasciata al caso dell'installazione.

Come si dimostra: Panoramica delle applicazioni con indicazione di quali dati e servizi utilizzano e quali account vi sono dietro, configurazione di istanze, database, directory o macchine virtuali separate, e un elenco dei privilegi per area. Una piccola realtà risolve questo con account utente separati e cartelle dati separate per ingegneria e operatività, più una nota su quale applicazione accede a quale cartella.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

10 FR 6: Risposta tempestiva agli eventi

3

SR 6.1 I registri di audit raccolti nel sistema possono essere letti e valutati dalle persone e dai ruoli autorizzati a tale scopo senza disturbare il funzionamento in corso dell'impianto, e l'accesso a tali registri è a sua volta limitato agli utenti autorizzati.

Come si dimostra: Una matrice di ruoli e permessi che mostri chi può visualizzare i dati di log, più una schermata o un'esportazione di una vista di log effettivamente recuperata, con una marca temporale. Aggiungere una breve nota sul percorso utilizzato per il recupero, per esempio l'interfaccia operatore del controllore, un server di log o un'esportazione di file. Le piccole realtà si accontentano di una panoramica su una pagina per impianto: dove si trova il log, chi ha accesso in lettura, come viene recuperato. Un recupero di prova una volta all'anno, registrato nel diario di manutenzione, dimostra che il percorso funziona. Si applica da SL 1 in su per tutti i livelli di sicurezza.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 6.1 RE 1 I registri di audit possono essere recuperati tramite un'interfaccia macchina in modo che gli strumenti di analisi possano elaborarli ulteriormente senza dover essere ritrascritti manualmente, e i dati sono forniti in un formato documentato e di uso comune.

Come si dimostra: Una descrizione dell'interfaccia in uso insieme al formato, per esempio syslog, OPC UA Alarms and Conditions, una query REST o un'esportazione CSV, più un record di esempio e la configurazione del sistema ricevente. L'evidenza può essere un estratto della configurazione del SIEM o del raccogliitore di log insieme alla prova dei record in arrivo. Senza un SIEM, è sufficiente un raccogliitore di log su un semplice server che recupera i log durante la notte tramite uno script e li memorizza; lo script stesso più un elenco della directory dei file raccolti costituisce l'evidenza. Come miglioramento, questo è richiesto solo da SL 3 in su, non da SL 1.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 6.2 L'attività rilevante per la sicurezza nel sistema viene monitorata in modo continuo, il monitoraggio rileva i tentativi di attacco e gli usi impropri e li segnala tempestivamente a un punto di contatto nominato, e sono definiti gli strumenti, i percorsi di segnalazione e le responsabilità utilizzati a tale scopo.

Come si dimostra: Una panoramica degli strumenti di monitoraggio per zona, per esempio un sensore di rete, allarmi antivirus, allarmi firewall o verifica dell'integrità, con indicazione di chi riceve l'allarme ed entro quale tempo è attesa una risposta. Configurazioni di allarme, un elenco degli allarmi generati negli ultimi mesi e le relative note di gestione fungono da evidenza. Le piccole realtà non necessitano di una sala controllo attiva 24 ore su 24: una casella di posta condivisa o una coda di ticket che raggruppi gli allarmi dei sistemi esistenti, più una regola fissa secondo cui una persona nominata la controlla ogni giorno lavorativo, è sufficiente e viene dimostrata tramite lo storico della casella di posta. Richiesto da SL 2 in su.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

11 FR 7: Disponibilità delle risorse

13

SR 7.1 In caso di sovraccarico o di attacchi di inondazione deliberati, il sistema resta in uno stato operativo definito, le funzioni di controllo essenziali continuano a funzionare, e il guasto di un singolo servizio non trascina con sé l'impianto.

Come si dimostra: Configurazione dei meccanismi di protezione (limitazione della velocità, limiti di connessione, controllo delle tempeste broadcast sugli switch), dichiarazioni del fornitore sul comportamento sotto carico, più un verbale di un test di carico o di un evento reale di sovraccarico con osservazione della funzione di controllo. Richiesto da SL 1. Una piccola realtà copre questo con schermate delle impostazioni di switch e firewall e una breve nota su quale funzione ha continuato a funzionare durante un test della cella più importante.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 7.1 RE 1 Il carico di comunicazione che i singoli componenti possono immettere nella rete è limitato, in modo che un componente difettoso o compromesso non possa inondare il segmento di rete.

Come si dimostra: Limiti di banda e multicast per porta sui componenti di rete, evidenza del limite per ciascuna connessione, più una misurazione del carico di base effettivo per dispositivo. Richiesto da SL 2, non da SL 1. Senza switch gestiti questa riga non può essere dimostrata, e questo diventa quindi il punto aperto.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 7.1 RE 2 Una situazione di sovraccarico all'interno del sistema considerato non si propaga a sistemi o reti adiacenti; l'impatto verso l'esterno è tecnicamente contenuto.

Come si dimostra: Regole di segmentazione e filtraggio ai confini, evidenza che il traffico in uscita è limitato, più un verbale di test che mostri che un carico generato nella rete di cella non ha degradato la rete d'ufficio né una rete vicina. Richiesto da SL 3.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 7.2 L'uso di tempo di elaborazione, memoria, spazio di archiviazione e banda di rete è limitato in modo che un singolo processo o servizio non possa consumare le risorse necessarie per il controllo.

Come si dimostra: Configurazione dei limiti di risorse (quote, priorità di processo, limiti di memoria), valutazione del monitoraggio dell'utilizzo per un periodo rappresentativo, più le soglie a partire dalle quali viene emesso un avviso. Richiesto da SL 1. Le piccole realtà usano gli strumenti integrati del sistema operativo e un monitoraggio semplice con un avviso di spazio disco e CPU via email.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 7.3 Esistono copie di backup delle configurazioni di sistema, dei dati applicativi e delle versioni di programma; possono essere generate senza interrompere il funzionamento in corso e sono protette contro l'accesso e la modifica non autorizzati.[Documento](#)

Come si dimostra: Concetto di backup che copra ambito, frequenza e periodo di conservazione, log di backup delle esecuzioni più recenti, più evidenza della protezione degli accessi ai supporti di backup (memorizzazione separata, cifratura, permessi dedicati). Richiesto da SL 1. Una piccola realtà esegue il backup dei progetti PLC e delle versioni HMI su un supporto cifrato che viene scollegato fisicamente dopo il backup, e registra data e versione in un elenco semplice.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 7.3 RE 1 È stata verificata l'utilizzabilità dei backup; si dimostra che da essi può effettivamente essere ripristinato uno stato funzionante.

Come si dimostra: Verbale di una prova di ripristino con data, versione di backup testata, sistema di destinazione e risultato, almeno per i componenti critici. Richiesto da SL 2, non da SL 1. Le piccole realtà verificano una volta all'anno, a campione, un programma PLC e un'immagine HMI su un dispositivo di riserva e registrano il risultato in due frasi.

Aperto	In corso	Soddisfatto	Non applicabile
--------	----------	-------------	-----------------

Evidenza / motivazione

SR 7.3 RE 2 Il backup viene eseguito automaticamente secondo una pianificazione definita; un'esecuzione fallita viene rilevata e segnalata.

Come si dimostra: Pianificazione del job di backup, log di esecuzione senza lacune, più evidenza della notifica di fallimento per un'esecuzione non riuscita (allarme, ticket, email). Richiesto da SL 3.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 7.4 Dopo un disturbo, un guasto o un attacco, il sistema può essere riportato a uno stato noto e sicuro; il ripristino è stato provato e le responsabilità sono nominate.[Documento](#)

Come si dimostra: Piano di riavvio per ciascun componente critico con sequenza, supporti necessari, contatti e tempo obiettivo, insieme al verbale dell'ultima esercitazione di ripristino. Richiesto da SL 1. Una piccola realtà si accontenta di una scheda di riavvio su una pagina per linea, conservata nell'armadio di controllo e verificata ogni volta che viene sostituito un pezzo di ricambio.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 7.5 Se l'alimentazione elettrica regolare viene a mancare, il sistema passa a uno stato definito: o l'alimentazione viene mantenuta da una fonte di riserva oppure avviene uno spegnimento ordinato senza perdita dello stato sicuro.

Come si dimostra: Evidenza di dimensionamento e manutenzione del gruppo di continuità o del generatore di emergenza, verbale di test dell'ultima prova di batteria o di carico, più una descrizione del comportamento in caso di commutazione e di ripristino dell'alimentazione di rete. Richiesto da SL 1. Le piccole realtà testano l'UPS sotto carico una volta all'anno e registrano data del test, autonomia e anzianità della batteria.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 7.6 Le impostazioni di rete e di sicurezza del sistema sono fissate su uno stato obiettivo approvato, gli scostamenti da tale stato obiettivo sono rilevabili, e lo stato attuale può essere recuperato in qualsiasi momento.[Documento](#)

Come si dimostra: Configurazione obiettivo approvata per classe di dispositivo (specifica di hardening), stati di configurazione attuali dei dispositivi, più il risultato di un confronto tra stato obiettivo e stato reale con un elenco degli scostamenti e il motivo di ciascuno. Richiesto da SL 1. Una piccola realtà conserva le esportazioni di configurazione sotto controllo versione e le confronta prima e dopo ogni modifica.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 7.6 RE 1 Lo stato attuale delle impostazioni di sicurezza può essere esportato in forma leggibile da macchina in modo che possa essere verificato automaticamente rispetto allo stato obiettivo.

Come si dimostra: Output di esempio in un formato leggibile da macchina (esportazione di configurazione, file strutturato, interrogazione tramite interfaccia) e lo script o strumento che esegue il confronto rispetto allo stato obiettivo, insieme al report dei risultati di un'esecuzione. Richiesto da SL 3.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 7.7 Il sistema è limitato alle funzioni necessarie al funzionamento; servizi, porte, protocolli e interfacce non necessari sono disabilitati o rimossi.

Come si dimostra: Elenco dei servizi attivi e delle porte aperte per componente con una motivazione della necessità, evidenza che i restanti sono disabilitati (configurazione, risultato di scansione porte), più una regola per le interfacce USB e di manutenzione. Richiesto da SL 1. Le piccole realtà eseguono una semplice scansione porte per segmento e motivano ogni voce aperta in una riga.

Aperto In corso Soddisfatto Non applicabile

Evidenza / motivazione

SR 7.8

È disponibile un inventario aggiornato di tutti i componenti di sistema con produttore, tipo, versione firmware o software e indirizzo di rete, e viene mantenuto aggiornato quando si verificano modifiche.

Documento

Come si dimostra: Inventario dei componenti con data di revisione e titolare, evidenza dell'aggiornamento tramite lo storico delle modifiche, più un confronto rispetto a una scoperta di rete per individuare dispositivi non registrati. Richiesto da SL 2, non da SL 1. Una piccola realtà mantiene l'inventario come tabella e lo aggiorna come regola fissa ogni volta che un dispositivo viene sostituito e ogni volta che il firmware viene aggiornato.

Aperto

In corso

Soddisfatto

Non applicabile

Evidenza / motivazione

I requisiti sono formulati in modo autonomo e non sostituiscono il testo della norma. È vincolante soltanto la norma originale del rispettivo editore. Questo elenco è uno strumento di lavoro, non è una prova di conformità né una certificazione. Leanshift non è certificata secondo nessuna di queste norme, non è un organismo di certificazione e non ha alcun legame con ISO, IEC, DIN, IATF, IAQG o SAE. In caso di dubbio prevale la versione tedesca di questo elenco.