ServiTecno

WHITE PAPER

NIS-2

Normative più severe in materia di sicurezza informatica per la produzione

Panoramica dei requisiti della UE in materia di sicurezza informatica

AMDT

octoplant

Indice

SISTEMA INDICE

Introduzione

UNA PANORAMICA DELLE AZIONI E DELLE SOLUZIONI PER LA NUOVA DIRETTIVA UE

Dieci milioni di euro o il 2% del fatturato dell'anno precedente: la sanzione massima prevista dall'Unione Europea è finalizzata a persuadere le grandi realtà a conformarsi ai nuovi standard di sicurezza informatica. La nuova direttiva sulla sicurezza informatica mira a contrastare gli attacchi e a ridurre al minimo i danni, al fine di proteggere l'economia e la società da potenziali interruzioni dei servizi.

Le nuove norme non riguardano solo gli operatori di infrastrutture critiche, ma si estendono all'industria e aumentano indirettamente i requisiti di sicurezza di tutte le aziende che potrebbero essere oggetto di attacchi.

In sintesi: come l'Unione Europea obbliga l'industria e i fornitori ad agire

- Gestione della sicurezza preventiva obbligatoria più rigorosa e obbligo di segnalare gli incidenti di sicurezza.
- La direttiva NIS-2 riguarda tutte le imprese appartenenti a quelli che vengono definiti settori "critici" o "importanti" e che forniscono servizi o prodotti a persone e imprese nella UE, anche se il fornitore stesso ha **sede al di fuori della UE**, ad esempio negli Stati Uniti.
- Rischi: le sanzioni per la violazione delle norme possono variare da sette a dieci milioni di euro o fino al 2% del fatturato globale annuo, a seconda del settore e della gravità della violazione.

Per gli operatori di infrastrutture critiche che intendono rafforzare i propri requisiti di sicurezza in conformità con la nuova direttiva UE, queste raccomandazioni mirano a salvaguardare l'economia e la società da potenziali guasti e dalle loro ripercussioni.

Capitolo 1

Contesto: digitalizzazione e sicurezza nell'OT

Grazie alla digitalizzazione e all'automazione delle infrastrutture e della produzione, le imprese e le organizzazioni possono diventare più efficienti e sfruttare nuove potenzialità. La trasformazione dell'IT e dell'OT (Tecnologie Operative) ha subito una forte accelerazione negli ultimi tempi, anche a causa della pandemia.

Con il progredire della digitalizzazione negli ultimi anni, gli attacchi alla produzione e alle infrastrutture si sono intensificati. Ne sono esempi la manipolazione mirata di un impianto di trattamento dell'acqua potabile negli Stati Uniti e gli attacchi a parti della rete energetica in Europa.

Allo stesso tempo, gli eventi degli ultimi anni hanno messo in luce quanto possa essere profondo l'impatto dell'interruzione delle catene di approvvigionamento e del danneggiamento dei servizi di base. L'approvvigionamento energetico e sanitario e la produzione di importanti materiali di base e prodotti intermedi rappresentano insieme un pilastro fondamentale della nostra società, e ogni difetto e interruzione possono danneggiare la società nel suo complesso.

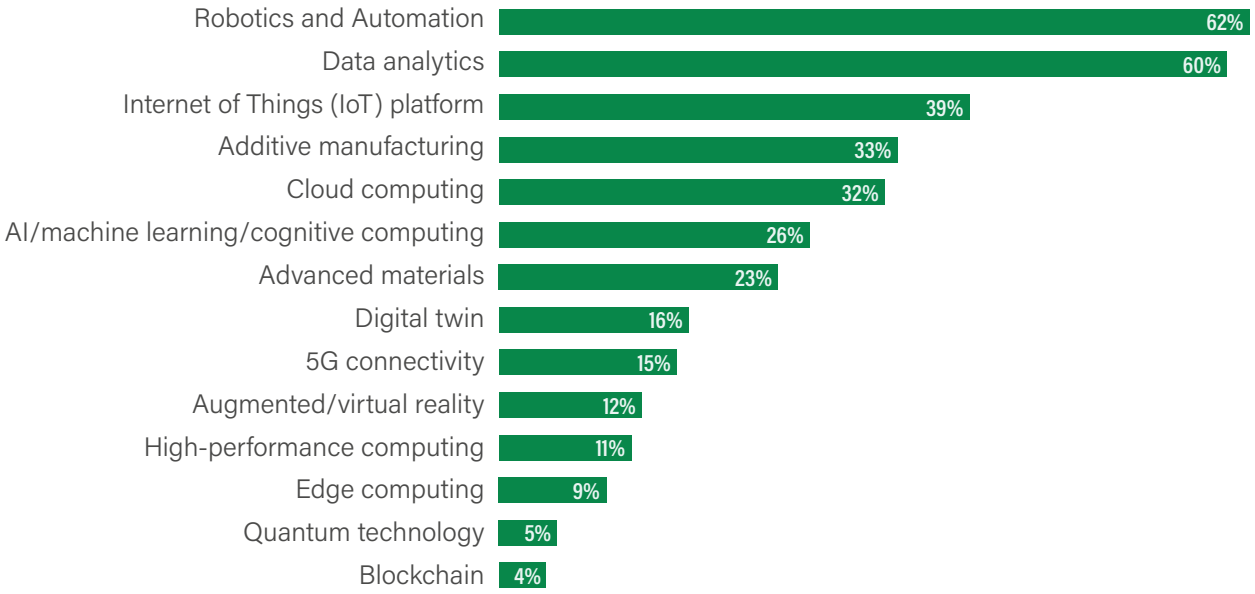


Fig.1: secondo il Manufacturing Industry Outlook 2023| Deloitte US, le aziende che adottano un livello più elevato di digitalizzazione dimostrano una maggiore resilienza. Secondo i risultati del sondaggio, gli investimenti previsti per la digitalizzazione nei prossimi 12 mesi riguarderanno l'utilizzo di una serie di tecnologie per massimizzare l'efficienza operativa. Fonte: Deloitte Manufacturing Outlook 2023.

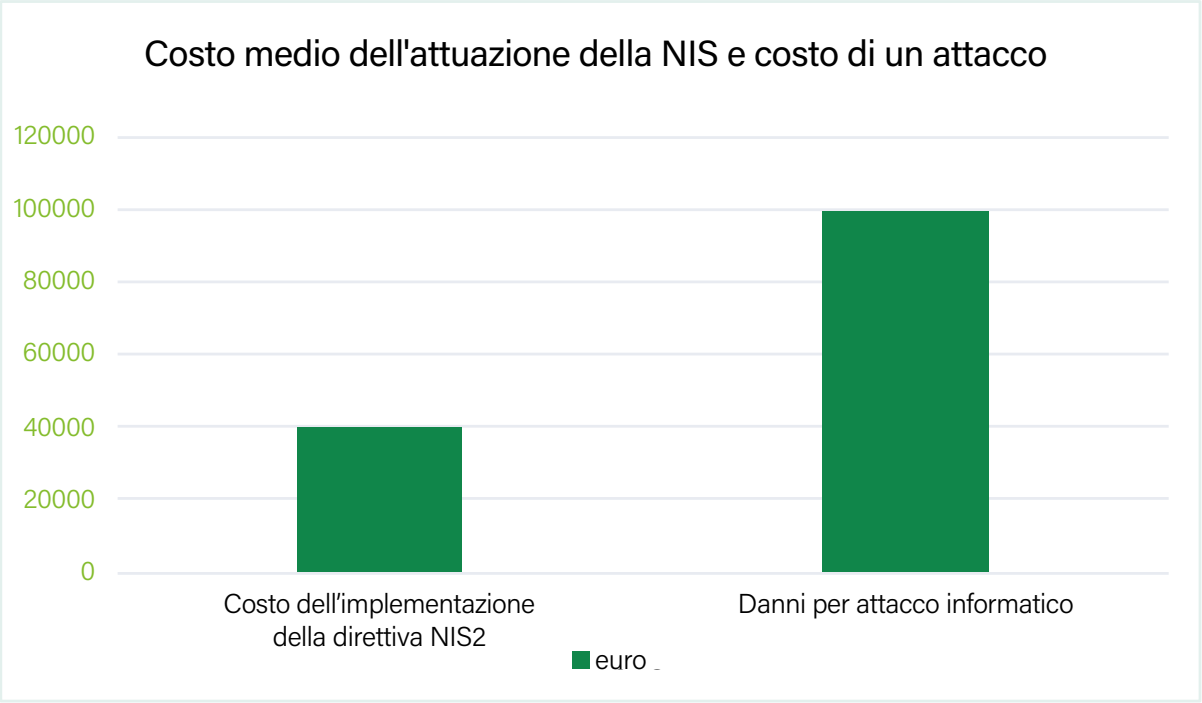
Capitolo 2

NIS e NIS-2 - la cronologia

Le aziende intervistate hanno investito in media 40.000 euro per implementare i requisiti, mentre l'Agenzia dell'Unione Europea per la Sicurezza delle Reti e dell'Informazione (ENISA) stima in 100.000 euro il costo medio di un attacco. Nel suo rapporto intitolato "The State of Ransomware in Manufacturing and Production 2021", la società di sicurezza Sophos afferma che il costo medio di un attacco alle aziende manifatturiere è pari a 1,5 milioni di dollari.

2016	2018	2020	2022	2023	2024
NIS resolution	NIS in force	NIS2 proposed	NIS2 resolution	NIS2 in force	Transposition into national law

Tre anni dopo l'entrata in vigore della NIS, **solo quattro aziende su cinque avevano soddisfatto i requisiti.**

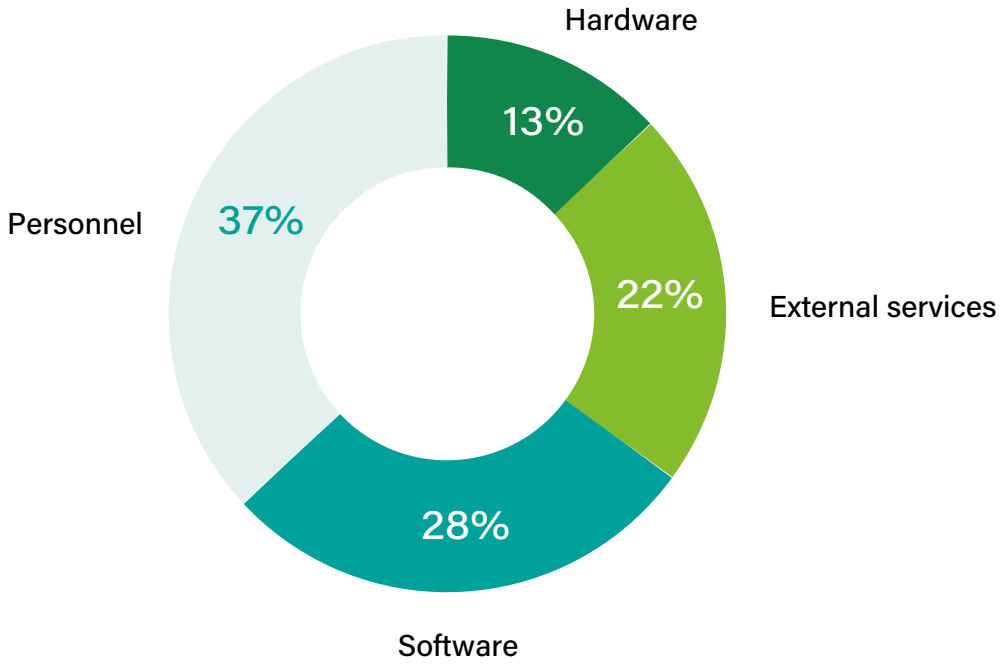


Fonti: ENISA e Sophos.

Ai sensi della direttiva NIS-2, le violazioni gravi potrebbero comportare sanzioni fino a dieci milioni di euro o al 2% del fatturato globale di un'azienda. In base alla direttiva precedente, la sanzione per le violazioni era di soli 150.000 euro. Secondo l'autorità europea per la sicurezza informatica ENISA,

solo l'82% delle aziende intervistate aveva implementato i requisiti della NIS entro la fine del 2021, nonostante la prima versione della direttiva fosse in vigore da anni.

Due terzi di esse hanno dovuto stanziare un budget aggiuntivo per l'attuazione della direttiva. **La metà delle aziende afferma che le nuove misure hanno migliorato la rilevazione delle minacce** e un quarto che, di conseguenza, sono migliorate le loro capacità di ripristino. Si tratta di un grande passo nella giusta direzione, ma c'è ancora margine di miglioramento, soprattutto nel campo del ripristino. Con l'aumento delle sanzioni in vista, gli investimenti nella sicurezza informatica sono ora distribuiti come segue:



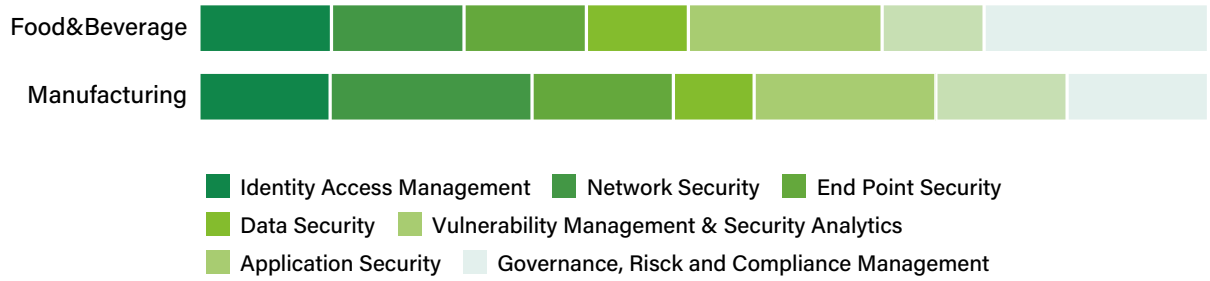


Fig.2: Distribuzione della spesa e delle misure per la sicurezza IT - dati complessivi e per settore.
Fonte: Gartner, IT Key Metrics Data 202: IT Security Measures

Capitolo 3

NIS-2 - solo per le aziende KRITIS?

A chi si applica la NIS-2 nella pratica? La sua definizione amplia il concetto di infrastruttura "critica" (NIS) della versione precedente per includere le infrastrutture "importanti", coprendo così un gran numero di settori. Finora (cioè con la prima versione della direttiva NIS), gli Stati membri dell'Unione Europea potevano decidere autonomamente quali settori e aziende classificare come infrastrutture critiche. Ora la UE sta definendo settori e criteri universalmente applicabili.

IMPORTANZA DEI SETTORI

I criteri e i settori sono simili a quelli del regolamento tedesco KRITIS, ma ora si applica la direttiva UE sulla resilienza delle entità critiche (RCE). Nella sua definizione, la UE distingue tra settori e industrie "critici" e "importanti". Undici settori rientrano nella categoria delle "infrastrutture critiche", mentre altri sette sono classificati come "infrastrutture importanti". Si tratta di un numero superiore a quello previsto dalla prima direttiva NIS in Germania. Il regolamento riguarda tutti i settori in cui un guasto potrebbe comportare un rischio per la sicurezza o la salute pubblica o rischi sistemici. **Le imprese manifatturiere** sono ora considerate "entità importanti" ai sensi della NIS-2, che le colloca nella categoria delle "imprese importanti". La direttiva NIS non copriva la **produzione** di alimenti o di prodotti industriali e chimici, ma **la NIS-2 ha un impatto diretto su di essa**.

Settori direttamente interessati dalla NIS-2:

Settori Essenziali	Sottosettori/esempi
Acque reflue e acqua potabile	-
Banche	-
Infrastrutture digitali	Fornitori, data center, registrar, ecc.
Energia	Elettricità, gas, petrolio, ecc.
Finanza	Borse, ecc.
Salute	Ricerca, dispositivi medici, fornitori di servizi sanitari, ecc
Fornitori di servizi IT	Fornitori di servizi, fornitori di sicurezza, ecc.
Aerospaziale	-
Trasporti	Ferrovie, strade, ecc.
Amministrazione	Amministrazione locale e nazionale
Settori principali	**Sottosettori/esempi**
Smaltimento dei rifiuti	
Prodotti Chimici	
Servizi Digitali	Fornitori di social media, motori di ricerca, ecc
Alimentare	
Ricerca	
Settore	Automobilistico, elettrico, informatico, ingegneria meccanica, ecc.
Post	

Fig.3: Le industrie manifatturiere sono ora coperte dalla NIS-2 e sono evidenziate qui a colori

DIMENSIONI DELL'AZIENDA

La UE opera un'ulteriore distinzione in base alle dimensioni delle imprese. Sono direttamente interessate le medie imprese (50-250 dipendenti) e le grandi imprese (> 250 dipendenti).
Sono interessate tutte le imprese che operano nel settore delle infrastrutture digitali, indipendentemente dalle loro dimensioni. Altre eccezioni: gli enti pubblici e i fornitori con un impatto transfrontaliero rientrano nella legislazione prevista, indipendentemente dalle loro dimensioni. Sono ora interessate tutte le agenzie federali e regionali. Le autorità nazionali che legiferano in materia possono decidere autonomamente se includere anche le autorità regionali e locali.

La NIS-2 non riguarda più solo le infrastrutture critiche

I settori chimico, alimentare e industriale (compresi l'ingegneria meccanica, i trasporti, l'automotive e il settore elettrico) sono tutti "settori importanti" ai sensi della NIS-2 e sono quindi direttamente interessati dalla direttiva.

La NIS e la NIS-2 hanno un impatto che va oltre i settori direttamente interessati. In primo luogo, la direttiva definisce gli standard minimi e le migliori pratiche che le imprese dei settori non essenziali devono seguire. Non perché temano violazioni della conformità o multe, ma per ragioni puramente pragmatiche. Ad esempio, i premi assicurativi contro l'interruzione dell'attività o i danni causati da attacchi informatici si basano in parte sulla presenza di misure di sicurezza, sulla probabilità di danni e sugli incidenti che si sono verificati in passato.

Inoltre, l'aumento dei livelli di protezione nei settori critici regolamentati potrebbe indurre gli autori degli attacchi a rivolgere la loro attenzione ad altri settori che considerano meno protetti e quindi più facili da colpire. Secondo l'ENISA, solo la metà delle aziende dispone attualmente di un'assicurazione contro i rischi cyber.

Capitolo 4

Cosa devono fare le aziende

I requisiti specifici della NIS-2 impongono ai fornitori di infrastrutture critiche di attuare misure efficaci di sicurezza informatica in contesti quali la gestione dei rischi. La direttiva chiarisce in modo netto che le imprese devono adottare misure strutturali. Devono valutare i rischi, stabilire norme e procedere su tale base o mettere in atto soluzioni. Ciò che viene chiesto ai policy maker è che creino una cultura della sicurezza dando l'esempio, invece di prescrivere particolari meccanismi di sicurezza, perché le soluzioni da sole aiutano solo fino a un certo punto.

Per citare un esempio, nella sua indagine sull'attuazione della NIS, l'agenzia di sicurezza ENISA ha riscontrato che le imprese sopravvalutano l'impatto della semplice presenza di soluzioni di sicurezza, sottovalutando l'effettiva efficacia di tali soluzioni come variabile.

Metà delle aziende afferma che le nuove misure (NIS) hanno migliorato la loro capacità di rilevamento delle minacce.

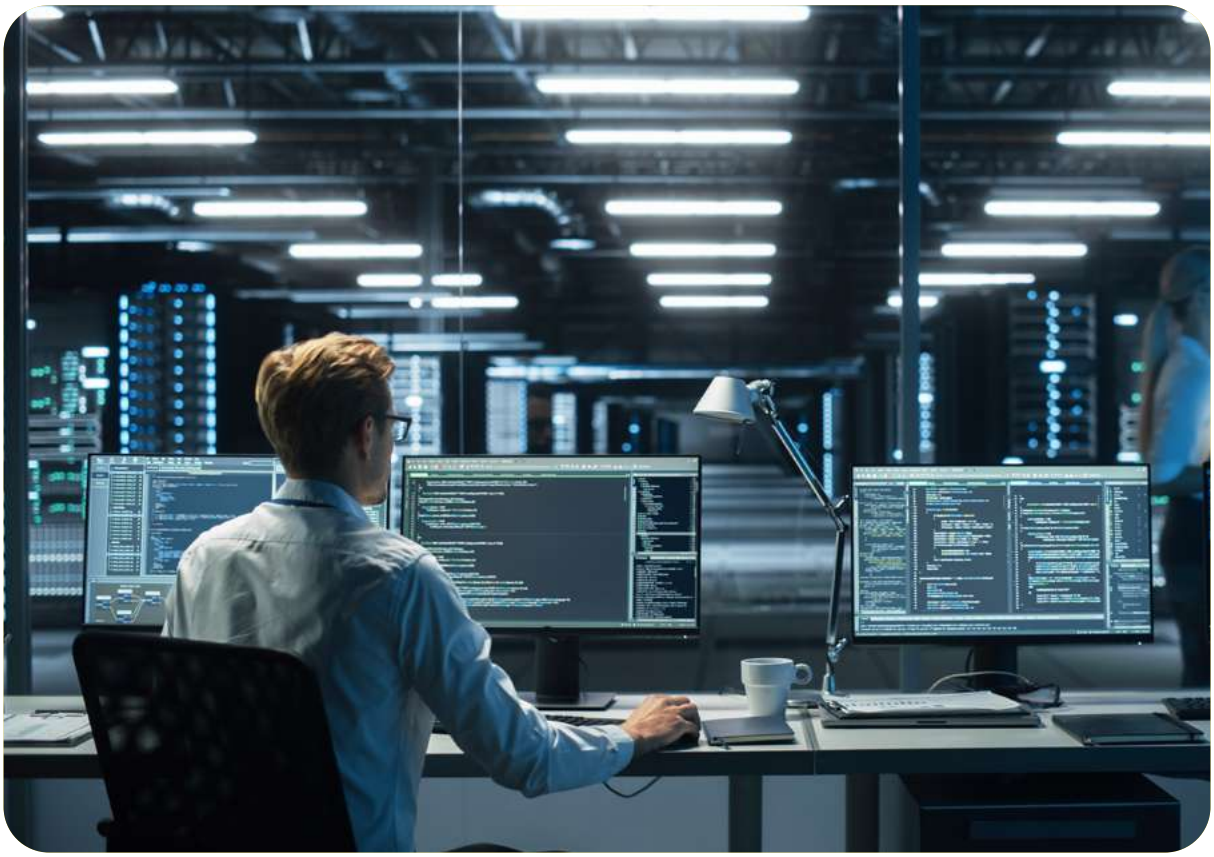
Capitolo 5

Gestione dei rischi e risposta agli incidenti nell'OT

La direttiva affronta alcuni aspetti e precauzioni relativi alla sicurezza informatica, concentrandosi principalmente su due aree: la gestione dei rischi e la risposta agli incidenti. Questi due aspetti della sicurezza informatica sono particolarmente rilevanti per i dirigenti OT.

La gestione dei rischi consiste nell'identificare le vulnerabilità e i potenziali punti di attacco prima che lo faccia qualcun altro. Comprende anche la valutazion delle potenziali conseguenze.

Fig.4: Primi passi per ottenere la conformità alla direttiva NIS-2



Capitolo 6

Cosa devono fare le aziende nella pratica

La direttiva NIS-2 obbliga oggi le aziende del settore manifatturiero che non erano contemplate dalla precedente normativa KRITIS ad attuare norme, processi e strutture adeguate per affrontare in modo sistematico i potenziali rischi per la sicurezza. Ecco una panoramica dei livelli di intervento necessari.

MANAGEMENT

I dirigenti sono responsabili della definizione delle regole e dei processi e della valutazione dell'efficacia delle misure adottate. La sicurezza informatica è ormai fondamentale per le aziende, anche per i settori non regolamentati.

GESTIONE DEI RISCHI

Le aziende devono identificare, comprendere e valutare i rischi.

ASSET MANAGEMENT

Devono essere coperti tutti i componenti necessari per eseguire i servizi elementari. Questo processo inizia con il personale, prosegue attraverso ogni dispositivo e sistema e include i dati critici.

FORMAZIONE E PERSONALE

Assumere personale specializzato in sicurezza informatica, formare i dipendenti e garantire la sicurezza nelle procedure di assunzione.

IMPLEMENTARE MISURE DI PROTEZIONE

Stabilire processi di sicurezza conformi alla norma ISO 27001/IEC 62443, come quelli descritti nel Basic IT Protection Profiles. Implementare soluzioni di monitoraggio, difesa e ripristino immediato per prevenire o ridurre al minimo i guasti.

GESTIONE DEGLI INCIDENTI

Gli incidenti devono essere prevenuti, rilevati e gestiti in modo professionale.

CRITTOGRAFIA

Le comunicazioni, i dati e i sistemi devono essere protetti con crittografia.

FORNITORI

Anche le catene di fornitura e i loro potenziali rischi per la sicurezza devono essere registrati, valutati e gestiti in conformità con la direttiva.

Capitolo 7

Implementazione attraverso la gestione dei dati e degli endpoint OT

Le aziende che rientrano nelle "aziende importanti" devono prevenire le interruzioni e, qualora si verificassero, ridurne al minimo la durata. Per farlo, hanno bisogno di soluzioni efficaci per i propri dati e strategie di backup e devono iniziare con un inventario completo dei propri endpoint.

1 In primo luogo, le aziende devono catalogare e monitorare tutte le risorse in produzione attraverso **la gestione delle risorse**. Ogni PLC, ogni componente di automazione e ogni macchina deve essere registrato

e monitorato digitalmente. Questo costituisce la base per ogni fase successiva.

2. In secondo luogo, **il controllo delle versioni** di ogni stato e modifica del software (gestione delle modifiche) fa parte di ogni strategia di sicurezza. Chi ha apportato quale modifica? Questa è anche la base su cui ripristinare l'ultimo stato funzionante dopo un errore o un attacco (recupero).
3. **Il controllo degli accessi** definisce chi è autorizzato a modificare quali dati.
4. **Il monitoraggio** di ogni sistema registrato rivela ogni modifica e deviazione dallo stato target ed è fondamentale per rispondere agli incidenti.
5. Una **strategia di backup** definisce quali dati vengono archiviati in modo ridondante, dove e per quanto tempo, in modo che sia possibile accedere in qualsiasi momento a una copia sicura di ogni programma di produzione e dello stato del software.

Adottando queste misure, le aziende manifatturiere possono creare una base da cui partire per soddisfare tutti i requisiti legali previsti dalla NIS, dalla KRITIS e da altre normative sulla sicurezza. Solo registrando e monitorando digitalmente la produzione ed eseguendo sistematicamente il backup dei dati è possibile soddisfare i requisiti più recenti e adattare i processi a requisiti ancora più severi in futuro.

Capitolo 8

Come octoplant può proteggere la vostra produzione

octoplant è una soluzione modulare per la gestione degli endpoint e dei dati in produzione che consente alle aziende di proteggere i dispositivi di automazione nella produzione dai rischi e da costosi fermi. Mantiene gli utenti aggiornati sugli ultimi progressi tecnologici e consente loro di soddisfare i requisiti di conformità. octoplant dispone di moduli progettati intorno alle necessità dell'utente:

Protezione dalle minacce

Con octoplant, le aziende possono monitorare le proprie risorse e vengono automaticamente informate in merito a vulnerabilità e rischi. Un punteggio di rischio separato per ogni risorsa rivela potenziali minacce. Altre funzionalità preventive, come il rilevamento delle modifiche e delle vulnerabilità, contribuiscono attivamente a eliminare le interruzioni. Ciò rende octoplant una componente importante dell'architettura di sicurezza nella produzione.

Protezione degli asset

In ambienti di produzione complessi, la gestione delle versioni di più progetti e delle relative modifiche può essere un'attività laboriosa e critica. La gestione delle versioni e il backup automatico di tutte le versioni e modifiche garantiscono che sia sempre in esecuzione la versione corretta. Le differenze tra gli stati dei dati possono essere visualizzate sotto forma di grafici e tabelle. I backup automatici consentono di risparmiare tempo, ridurre gli errori e rendere più affidabile la programmazione e la configurazione delle apparecchiature.

Gestione dei dispositivi

I diversi tipi di controller e soluzioni incompatibili dei produttori ostacolano l'automazione in rete e possono compromettere l'efficacia delle soluzioni di sicurezza. octoplant integra tutti i dispositivi IoT più comuni, gestisce e monitora tutti i dati di configurazione associati ai diversi produttori e individua chi ha apportato quali modifiche e quando. Questo rende octoplant la piattaforma ideale per la gestione dei dati OT.

Ripristino immediato

Se dovesse verificarsi un problema grave, il ripristino immediato consente di riportare tutti i programmi e i dati necessari allo stato più recente nel minor tempo possibile. Ciò significa che octoplant consente di ripristinare in qualsiasi momento lo stato corretto dei singoli dispositivi o dell'intero impianto di produzione. Riduce al minimo i tempi di inattività e le interruzioni e consente di annullare errori e manipolazioni.

Ottenere la conformità

octoplant offre una documentazione integrata per i processi conformi e la gestione della conformità al fine di garantire che i processi day-by-day siano conformi alla legge. Tutti i processi di produzione sono quindi completamente tracciabili in caso di audit.

Capitolo 9

Casi d’uso nella produzione e nell’approvigionamento idrico

octoplant è una soluzione modulare per la gestione degli endpoint e dei dati in produzione che consente alle aziende di proteggere i dispositivi di automazione nella produzione dai rischi e da costosi fermi. Mantiene gli utenti aggiornati sugli ultimi progressi tecnologici e consente loro di soddisfare i requisiti di conformità. octoplant dispone di moduli progettati intorno alle necessità dell’utente:

CASO D'USO - APPROVVIGIONAMENTO IDRICO

L'acqua è un servizio essenziale ed è quindi soggetta al regolamento KRITIS e ora anche alla direttiva NIS-2. Il fornitore di acqua Canal de Isabel II è l'azienda idrica centrale della regione di Madrid.
Le 600 stazioni di monitoraggio e le 250.000 variabili di misurazione di tutti i suoi impianti idrici dovevano essere consolidate in un unico sistema di monitoraggio unificato. Questa piattaforma visualizza in tempo reale le informazioni di stato relative alle stazioni, ai processi e alle apparecchiature. La gestione dei dati e degli endpoint di AMDT protegge questa rete di sistemi, gestendo i backup e ripristinando le versioni precedenti delle apparecchiature monitorate.

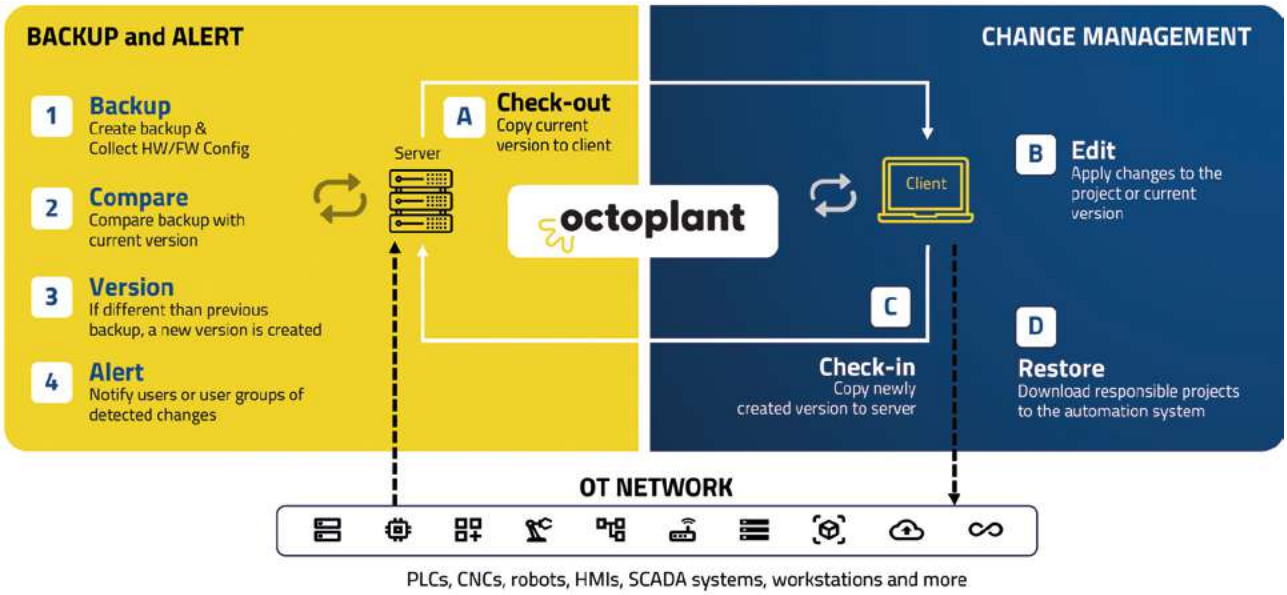
Canal de Isabel II, Spagna

CASO D'USO - PRODUZIONE

Nanostone: filtri ceramici a membrana per il trattamento dell'acqua, prodotti in uno stabilimento sempre più automatizzato in Germania. I prodotti sono utilizzati per la desalinizzazione, l'industria e l'approvvigionamento idrico pubblico. La produzione di questi filtri ceramici è altamente critica. Nanostone utilizza numerosi PLC Siemens diversi per i suoi processi di produzione. Robot, macchine CNC, laser e movimentazione nella produzione. AMDT è utilizzato dal 2018 per il controllo degli accessi e il controllo delle versioni. La sua gestione dei dati e degli endpoint amministra le versioni dei file, rende trasparenti le modifiche e salvaguarda la produzione.

L'accesso è consentito all'automazione e alla manutenzione interna C&I e a un fornitore di servizi esterno. Ciò consente all'azienda di tracciare qualsiasi modifica apportata alle versioni e alle istruzioni. Tutta la documentazione è archiviata in una cartella dedicata che funge da archivio centrale per la documentazione corrente. L'implementazione di AMDT è stata "sorprendentemente" veloce e fluida.

Nanostone Water GmbH, Germania



Capitolo 10

Conclusione: produzione sicura e conforme alla legge con octoplant

octoplant consente ai manager aziendali di monitorare e controllare l'intero processo produttivo utilizzando un'unica soluzione standard centralizzata. Gestisce centralmente tutte le risorse e i dispositivi, indipendentemente dal produttore. Il monitoraggio centralizzato dei dispositivi garantisce una visione d'insieme, mentre la protezione delle risorse tramite backup e gestione delle versioni fornisce un quadro completo di tutti i dati dell'impianto di produzione.

Inoltre, in caso di emergenza, il ripristino immediato delle versioni del software e dei dati di programma riporta tutti i dati allo stato originale. Inoltre, octoplant rileva in modo proattivo vulnerabilità, modifiche e rischi per proteggere i processi di produzione dagli attacchi ed eliminare danni e tempi di inattività.

ServiTecno

Più di 3000 clienti già si affidano alle soluzioni di AMDT per la gestione della manutenzione e della produzione

Richiedi una demo di octoplant

info@servitecno.it | +39 02 486141

AMDT

octoplant