Co-funded by
the European Union

Cyber-In

WP3- CASCADE TRAINING ITALY
PROGETTO CYBER - IN

Novembre 2025

ECOLE - AFGP PIAMARTA

Cyber-In

Sessione 2

Sicurezza Informatica Industriale

Proteggere infrastrutture critiche e processi produttivi nell'era digitale

Co-funded by
the European Union

Norme Internazionali per la Sicurezza

ISO/IEC 27001
Standard internazionale per la gestione della sicurezza delle informazioni (ISMS), base per qualsiasi strategia di protezione dei dati

ISO/IEC27019
Estensione specifica per sistemi di controllo industriale (ICS) nel settore energetico e infrastrutture critiche

IEC 62443
Serie completa dedicata alla cybersecurity dei sistemi di automazione e controllo industriale (IACS)

NIST SP 800-82
Linee guida statunitensi riconosciute globalmente per proteggere sistemi ICS/SCADA da minacce informatiche

Regolamenti Europei Vincolanti

NIS2 Directive

Rafforza requisiti di sicurezza per operatori di servizi essenziali in settori strategici: energia, trasporti, sanità e finanza. Obblighi stringenti di notifica incidenti e gestione del rischio.

GDPR

Protegge dati personali trattati anche in contesti industriali. Applicabile quando sistemi OT gestiscono informazioni su lavoratori o utenti finali.

Cyber Resilience Act

Introduce requisiti di sicurezza obbligatori per prodotti hardware e software immessi sul mercato UE, con focus su vulnerabilità e aggiornamenti.

- **Ambito di applicazione più ampio**: Include nuovi settori critici e di importanza critici, oltre a fornitori di servizi digitali come e-commerce e cloud computing.
- **Maggiore responsabilità della dirigenza**: Il management deve approvare le politiche di sicurezza, supervisionare la gestione del rischio e ricevere formazione specifica. In caso di incidenti gravi, può incorrere in sanzioni personali.
- **Requisiti di sicurezza più rigorosi**: Le aziende devono implementare politiche di gestione dei rischi, continuità operativa, gestione degli incidenti, sicurezza de ll asupply chain e sicurezza dell'acquisizione, sviluppo e manutenzione dei sistemi. È obbligatoria la crittografia dei dati sens ibi li e un controllo rigoroso degli accessi.
- **Risposta e notifica degli incidenti**: Sono previste tempistiche precise per la notifica degli incidenti significativi. Entro 24 ore dall'identificazione, deve esse re inviata una notifica iniziale al CSIRT o all'autorità competente. Entro 72 ore deve essere presentato un primo report con le contromisure , e entro un mese un report dettagliato.
- **Sicurezza della catena di approvvigionamento** (supply chain): Viene rafforzata l'attenzione sulla sicurezza dei fornitori, con la necessità di valutarne la conformità alle misure di sicurezza e di prevedere requisiti specifici nei contratti.
- **Sanzioni più severe**: Le multe possono arrivare fino al 2% del fatturato mondiale per i soggetti essenziali e fino all'1,4% per i soggetti importanti , o fino a €10 milioni e €7 milioni rispettivamente, a seconda di quale importo sia
- **Coordinamento tra gli Stati membri**: La NIS2 mira a uniformare l'attuazione della normativa tra gli Stati membri dell'UE e a potenziare la cooperazione e la capacità di risposta agli incidenti su scala europea.

Cyber-In

- **Requisiti per l'intero ciclo di vita:** I prodotti digitali devono essere sicuri fin dalla progettazione e durante tutto il loro ciclo di vita, dalla pianificazione alla manutenzione.
- **Responsabilità dei produttori:** I fabbricanti sono responsabili della conformità dei prodotti ai requisiti di sicurezza, che include la valutazione dei risch i, la dichiarazione di conformità e la gestione delle vulnerabilità.
- **Gestione delle vulnerabilità:** I produttori devono segnalare le vulnerabilità a enti come l'ENISA entro 24 ore dalla scoperta, fornendo un rapporto dettagliat entro 3 giorni.
- **Le correzioni (patch)** devono essere disponibili entro 14 giorni, e devono essere fornite patch e aggiornamenti per almeno 5 a nni
- **Gestione degli incidenti:** Le aziende devono segnalare gli incidenti di sicurezza agli utenti e alle autorità competenti. È richiesta la creazione di un te am interno dedicato alla gestione degli incidenti e delle vulnerabilità, il Product Security Incident Response Team (PSIRT).
- **Ruoli nella catena di fornitura:** Gli importatori devono verificare che i prodotti importati siano conformi al CRA e avvisare le autorità in caso di non conformità. I distributori devono garantire che i prodotti immessi sul mercato siano conformi e segnalare eventuali problemi di sicurezza.
- **Classificazione dei prodotti:**Il CRA classificherà i prodotti in base al livello di rischio (es. classe "default", "critica classe prima", "critica classe se conda") per determinare il livello di valutazione della conformità richiesto prima dell'apposizione della marcatura CE.
- **Sorveglianza del mercato**: È previsto un quadro di sorveglianza del mercato per far rispettare il regolamento e assicurare che le regole siano applicate

Attacchi Informatici: IT vs OT

Attacchi IT

WannaCry (2017)-Ransomware globale che ha cifrato file in 150 paesi, bloccando ospedali, banche e aziende con richieste di riscatto in Bitcoin.

Phishing e Social Engineering-Tecniche ingannevoli via email o messaggi per rubare credenziali e accedere a sistemi critici aziendali.

Attacchi OT

Stuxnet (2010)-Sofisticato malware che ha sabotato centrifughe nucleari iraniane manipolando PLC Siemens, primo caso documentato di cyber-arma.

Colonial Pipeline (2021)-Ransomware DarkSide ha bloccato 5.500 miglia di oleodotto USA, causando crisi energetica e pagamento di 4,4 milioni di dollari.
Triton/Trisis (2017)-Malware mirato ai Safety Instrumented Systems (SIS) con potenziale di causare danni fisici e vittime umane.

Cyber-In

WannaCry (2017)

Dettagli dell'Attacco

- **Tipo di minaccia:** WannaCry è un " cryptoworm " ransomware. Una volta infettato un computer, criptava i file dell'utente (documenti, immagini, video, ecc.), rendendoli inaccessibili, e visualizzava una richiesta di riscatto (inizialmente 300 dollari in Bitco in, poi aumentati a 600) per la loro decrittazione.

- **Modalità di diffusione:** La caratteristica più insidiosa di WannaCry era la sua capacità di auto propagarsi come un worm, senza richiedere l'interazione dell'utente (come il clic su un link o l'apertura di un allegato malevolo). Sfruttava una vulnerabilità critica del sistema operativo Microsoft Windows nota come EternalBlue

- V**ulnerabilità EternalBlue :**Questa falla, che risiedeva nel protocollo Server Message Block (SMB) di Windows, era stata originariamente scoperta dalla National Security Agency (NSA) degli Stati Uniti e successivamente rubata e pubblicata online dal gruppo di hacker "The Shadow Brokers".

- **Patch disponibile ma non applicata:** Microsoft aveva rilasciato una patch di sicurezza per la vulnerabilità EternalBlue (bollettino MS17 010) circa due mesi prima dell'attacco, nel marzo 2017. Tuttavia, molte organizzazioni e individui non avevano aggiornato i loro sistemi in tempo, o utilizzavano ancora versioni obsolete e non più supportate di Windows (come Windows XP), lasciandoli esposti

Cyber-In

StuxNet (2010)

Dettagli dell'Attacco

- **Obiettivo Specifico:** Stuxnet non era un malware generico. Era programmato per cercare e colpire specifici sistemi di controllo industriale (SCADA) e Controllori a Logica Programmabile (PLC) della Siemens, utilizzati per automatizzare i processi industriali, in particolare l e centrifughe per l'arricchimento dell'uranio.

- **Modalità di Diffusione:** Per superare l'"air gap" (l'isolamento fisico) della struttura, il worm si diffondeva principalmente tramite chiavette USB in fette econdivisioni di stampanti di rete.

- **Sfruttamento di Vulnerabilità:** Stuxnet era eccezionalmente avanzato, sfruttando ben quattro vulnerabilità "zero day"day"(difetti del software precedentemente sconosciuti) in Windows per infiltrarsi e ottenere il controllo completo dei sistemi senza essere rilevato.

- **Componente Rootkit:** Il worm installava un rootkit per nascondere la sua presenza e le sue attività sia agli operatori umani che ai software antiv ir us, anchegrazie all'uso di certificati digitali rubati che facevano apparire il software come legittimo.

Cyber-In

StuxNet (2010)

La Logica dell'Attacco alle Centrifughe

Una volta infettato un computer Windows,Stuxnet rimaneva dormiente finché non trovava il software Siemens Step 7 che controllava i PLC specifici.

A quel punto:

1.

Monitoraggio e Profilazione: Il worm monitorava la velocità delle centrifughe per circa 13 giorni per assicurarsi di aver raggiunto il bersaglio corretto e comprenderne il normale funzionamento.

2.

Sabotaggio Fisico: Invece di limitarsi a bloccare i sistemi, Stuxnet ne prendeva il controllo e li manometteva fisicamente. Alterava la velocità di rotazione delle centrifughe: le accelerava temporaneamente a 1410 Hz o le rallentava drasticamente a 2 Hz, causando uno stress anomalo e inosservato che portava alla rottura delle apparecchiature nel tempo.

3.

Mascheramento: Contemporaneamente, il worm inviava dati falsi ai sistemi di monitoraggio e agli operatori, facendo credere che tutto funzionaSse normalmente, rendendo il sabotaggio estremamente difficile da individuare.

Conseguenze Si stima che l'attacco abbia danneggiato o distrutto circa 1.000 delle 9.000 centrifughe iraniane a Natanz , ritardando temporaneamente il programma nucleareiraniano. La sua scoperta accidentale nel 2010 ha rivelato al mondo l'esistenza di un nuovo tipo di guerra cibernetica in gra do di causare danni fisici reali alle infrastrutture critiche.

Cyber-In

Colonial Pipeline (2021)

L'attacco alla Colonial Pipeline nel maggio 2021 è stato un attacco ransomware perpetrato dal gruppo DarkSide che ha interrotto le operazioni della pipeline di carburante, causando interruzioni della fornitura nel sud est degli Stati Uniti. Per contenere l'attacco, l'azienda ha spento l'intera pipeline e,nonostante il pagamento di un riscatto di $4,4 milioni (in 75 bitcoin), ha avuto difficoltà a ripristinare i sistemi, anche perché lo strumento fornito da DarkSide era inefficiente.

Cyber-In

IT protegge i dati

OT protegge le vite

La differenza fondamentale: nei sistemi IT, la priorità è confidenzialità e integrità dei dati. Nei sistemi OT, la priorità assoluta è la sicurezza fisica, la continuità operativa e la protezione delle persone.

Il Purdue Model: Architettura di Riferimento

Il **Purdue Enterprise Reference Architecture (PERA)** struttura i sistemi industriali in livelli gerarchici per migliorare sicurezza e gestione dei rischi attraverso la segmentazione delle reti.

Livello 0 -Processo Fisico

Macchinari, valvole, pompe e attrezzature di produzione

Livello 1 -Campo

Sensori, attuatori e dispositivi di misura in tempo reale

Livello 2 -Controllo

PLC, DCS e sistemi di controllo di processo distribuito

Livello 3 -Supervisione

SCADA, MES e sistemi di gestione operativa

Livello 4 -IT Aziendale

Server, database, email e infrastruttura informatica

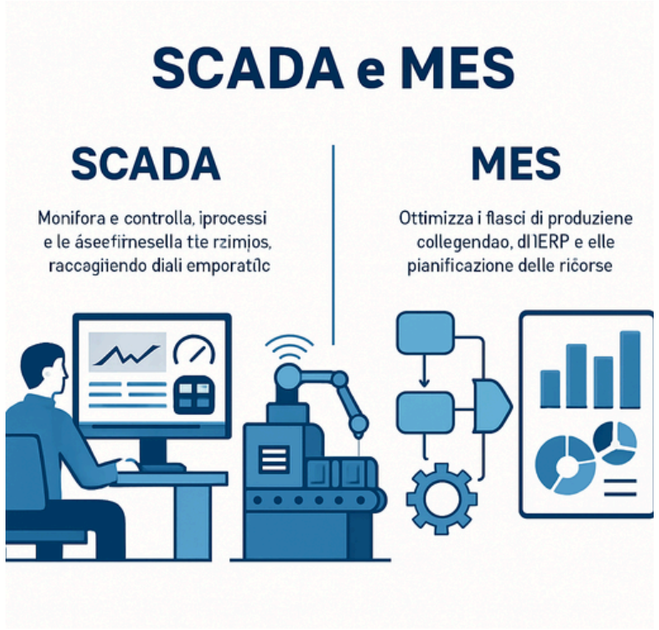
Livello 5 -Gestione

ERP, CRM e sistemi di pianificazione aziendale

SCADA e MES

SCADA e MES sono sistemi di gestione e controllo per la produzione industriale, ma con ruoli distinti:

SCADA (Supervisory Control and Data Acquisition) monitora e controlla i processi e le macchine a livello di campo, raccogliendo dati in tempo reale
MES (Manufacturing Execution System) è un software che gestisce e ottimizza l'intero processo produttivo, collegando i dati SCADA con i sistemi di gestione aziendale come l'ERP.



SCADA

- **Funzione principale:** Monitorare e controllare i processi industriali, le macchine e gli impianti direttamente sul campo.

- **Focus:** Funzionamento dei macchinari, sicurezza operativa e acquisizione dei dati di processo (es. pressione, temperatura,velocità).

- **Livello:** Si colloca a un livello più basso nella piramide produttiva, comunicando direttamente con i PLC (Programmable Logic Controller) e i sensori.

- **Utilizzo dei dati:** Fornisce al MES dati in tempo reale sullo stato delle attrezzature e sui parametri di processo.

MES

- **Funzione principale**: Gestire e controllare in modo olistico l'intero processo produttivo, dalla materia prima al prodotto finito.
- **Focus**: Efficienza, qualità, tracciabilità, gestione delle risorse e ottimizzazione del flusso di lavoro.
- **Livello**: Si inserisce nella parte alta della piramide produttiva, fungendo da ponte tra i sistemi di campo (SCADA) e i sistemigestionali aziendali (ERP).
- **Utilizzo dei dati:** Analizza i dati forniti dallo SCADA, trasformandoli in informazioni utili per prendere decisioni strategiche, migliorare l'efficienza e aumentare la soddisfazione del cliente.

Integrazione tra SCADA e MES

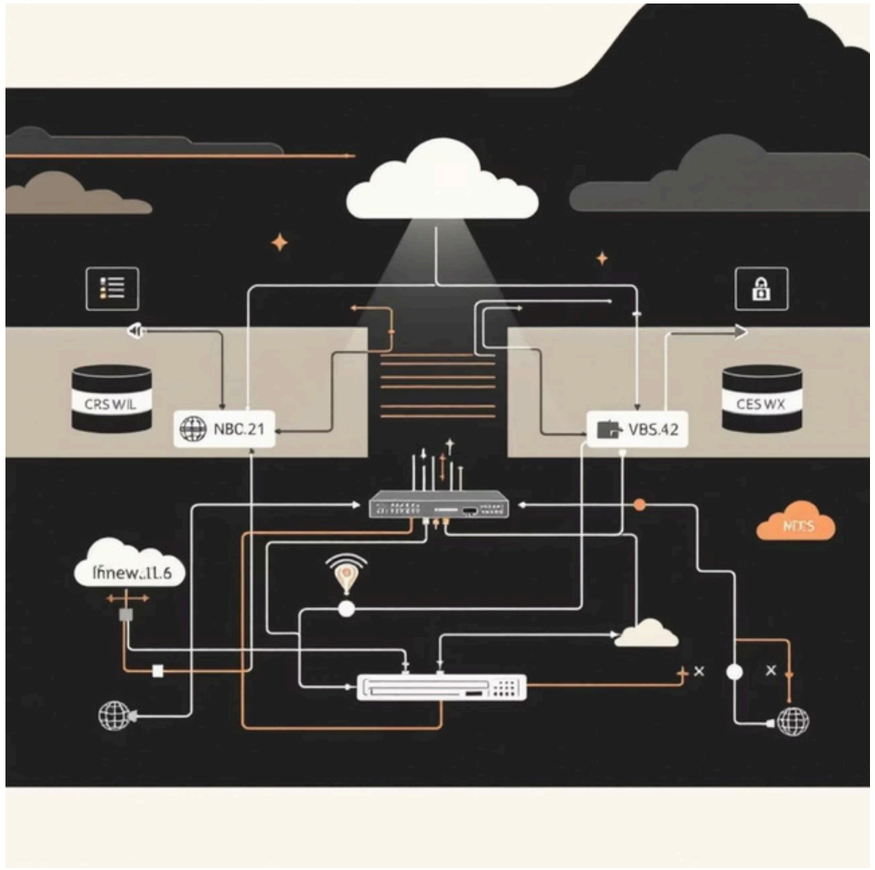
- I due sistemi sono complementari e lavorano insieme in una fabbrica intelligente.
- Lo SCADA raccoglie i dati grezzi direttamente dalle macchine.
- Il MES utilizza questi dati per pianificare, tracciare e gestire l'intero processo produttivo, identificando inefficienze, tempi di fermo macchina e problemi di qualità.
- Insieme, SCADA e MES offrono una visibilità completa e una gestione ottimizzata di tutte le attività produttive.

Segmentazione e Protezione delle Reti

Perché il Purdue Model è Essenziale

La separazione tra livelli riduce drasticamente la superficie d'attacco. Un breach nel livello IT aziendale non dovrebbe compromettere i sistemi OT critici.

- Firewall industriali tra ogni livello
- DMZ (Demilitarized Zone) per isolare traffico IT-OT
- Controlli di accesso basati su ruoli e necessità operative
- Monitoraggio continuo del traffico anomalo



Iniziative Scolastiche per la Cybersecurity

Laboratorio Pratico

Simulazioni di attacchi e difese su reti virtuali, utilizzo di strumenti come Kali Linux e ambienti sandbox per comprendere vulnerabilità e contromisure

Corsi e Workshop

Formazione su riconoscimento phishing, gestione password sicure, privacy online e uso consapevole dei social media per studenti e docenti.

Campagne di Sensibilizzazione

Poster creativi, video educativi e giornate tematiche dedicate alla sicurezza informatica per diffondere cultura digitale responsabile.

Collaborazioni Aziendali

Partnership con aziende locali per incontri tecnici, testimonianze di professionisti e opportunità di stage su tematiche IT/OT security.

Discussione: Sicurezza Digitale a Scuola

Riflettere sui Rischi

Anche le istituzioni scolastiche gestiscono dati sensibili: registri elettronici, informazioni su studenti e famiglie, sistemi amministrativi. Quali vulnerabilità esistono
nelvostro contesto?

Promuovere la Cultura

La sicurezza digitale è responsabilità di tutti. Come possiamo integrare l'educazione alla cybersecurity nei programmi curriculari e nelle attività extrascolastiche?

Progetti Concreti

Quali iniziative potrebbero essere avviate nella vostra scuola? Gare di ethical hacking, certificazioni base in cybersecurity, o club studenteschi dedicati?

Cyber-In

Verso un Futuro Resiliente

> La sicurezza informatica industriale non è solo tecnologia: è una questione **organizzativa, culturale e strategica**. La comprensione delle norme, la conoscenza degli attacchi e l'applicazione di modelli come il Purdue permettono di costruire ambienti più sicuri.

Conoscenza

Formazione continua su minacce emergenti

Prevenzione

Implementazione di controlli e best practice

Resilienza

Capacità di rispondere e recuperare dagli incidenti

Cyber-In

Ricadute sulle classi

Le nozioni coperte in questo breve corso sono destinate a ricadere sugli allievi.

Le tematiche sono sicuramente piu vicine al mondo legato all'automazione industriale.

Per gli altri settori, gli insegnanti estraggono le informazioni che possano risultare utili e interessanti

Co-funded by the European Union

Questionari di valutazione

Quality and helpfulness of the cascade training:

Knowledge and skills evaluation:

Co-funded by
the European Union