Elementi essenziali e gestione della sicurezza informatica (settore energetico)

CSP001

Argomento 2/10: Conoscenze di base e tassonomia della sicurezza informatica nel settore energetico e corpus di conoscenze

PRESENTAZIONE DI: STYLIANOS KARAGIANNIS (PDMFC, PORTOGALLO)

Cyberattacks on Energy

Settore energetico

Il settore energetico come obiettivo primario degli attacchi informatici

- Le interruzioni possono causare caos diffuso, perdite economiche e mettere in pericolo vite umane.
- Infrastrutture critiche: le reti elettriche, le raffinerie di petrolio e gli impianti nucleari sono obiettivi appetibili.
- Motivi economici: i criminali informatici cercano di ottenere guadagni finanziari attraverso ransomware, estorsioni o manipolazioni del mercato.
- Attacchi sponsorizzati dallo Stato: le tensioni geopolitiche possono spingere le nazioni a prendere di mira le infrastrutture energetiche rivali per ottenere un vantaggio strategico.

Cyberattacks on Energy

Perché la sicurezza informatica è fondamentale?

Il settore energetico come obiettivo primario degli attacchi informatici

- Vulnerabilità delle infrastrutture: i sistemi obsoleti, le reti interconnesse e i protocolli legacy sono suscettibili di essere sfruttati.
- Integrità dei dati: la manipolazione dei dati relativi al consumo energetico può compromettere l'equilibrio tra domanda e offerta e causare instabilità economica.
- Interruzione operativa: attacchi malware o denial-of-service possono bloccare la produzione e la distribuzione di energia, causando interruzioni diffuse.
- Rischi ambientali: la manomissione dei sistemi di controllo può portare a disastri ambientali, mettendo in pericolo gli ecosistemi e la salute pubblica.

Cyberattacks on Energy

Crescente complessità nel panorama informatico

Il settore energetico come obiettivo primario degli attacchi informatici

- Gli attacchi alle infrastrutture energetiche possono costituire forme di guerra informatica o terrorismo, rendendo le vulnerabilità energetiche una questione di sicurezza nazionale.
- Le organizzazioni energetiche navigano in un panorama informatico multiforme in un contesto di incertezze geopolitiche.
- Le responsabilità si estendono oltre la sicurezza informatica per includere la decarbonizzazione e la facilitazione della transizione energetica.
- Adattarsi alle complesse connessioni di rete e alle esigenze infrastrutturali in contesti normativi dinamici.

Spina dorsale dell'economia

Il settore energetico come obiettivo primario degli attacchi informatici

- L'energia è indispensabile per settori economici critici:
  - (i) Produzione
  - (ii) Agricoltura
  - (iii) Trasporti
- Le interruzioni nella fornitura di energia possono causare gravi perturbazioni, bloccando la produzione e la logistica.

Case Study: Colonial Pipeline

Caso di studio: attacco informatico alla Colonial Pipeline

Il settore energetico come obiettivo primario degli attacchi informatici

- Nel 2021, Colonial Pipeline, l' più grande degli Stati Uniti operatore di oleodotti
  operatore, è stato colpito da un attacco informatico ransomware.
- La chiusura della Colonial Pipeline ha interrotto la fornitura di carburante a metà della costa orientale, causando un aumento dei prezzi e una carenza di carburante.
- L'incidente alla Colonial Pipeline ha messo in evidenza la vulnerabilità del settore alle minacce informatiche.
- Le vulnerabilità identificate, come le posizioni vacanti nella gestione della sicurezza informatica e le VPN inattive, hanno sottolineato le debolezze sistemiche.

Case Study: Colonial Pipeline

Caso di studio: Allarmi e precauzioni governative

Caso di studio: Colonial Pipeline

- Nell'aprile 2022, il governo degli Stati Uniti ha emesso un avviso per avvertire le aziende energetiche dell'elevato rischio di attacchi informatici.
- Le raccomandazioni includevano:
  - Abilitazione dell'autenticazione a più fattori
  - Modifica regolare delle password di sistemi e dispositivi
- Le aziende energetiche devono dare priorità alle misure di sicurezza informatica per proteggere sia le loro operazioni che i consumatori da potenziali minacce informatiche.
- Misure proattive sono essenziali per mitigare i rischi e garantire la resilienza di fronte all'evoluzione delle minacce informatiche.

Case Study: Colonial Pipeline

Attacchi ransomware

Caso di studio: Colonial Pipeline

Minaccia principale: i criminali informatici utilizzano malware per bloccare l'accesso ai dati di un'organizzazione o minacciano di divulgare informazioni sensibili.

Strategie di mitigazione:

- Sviluppare piani di risposta robusti per la gestione degli incidenti.
- Proteggere i sistemi informatici in modo

proattivo. Caso di studio: Volue Technology

- Il fornitore norvegese di energia verde Volue Technology ha subito interruzioni in 44 paesi a causa di attacchi ransomware.

Cyberattacks

Phishing mobile

Vulnerabilità crescente: il settore energetico registra un aumento del 161% degli attacchi di phishing mirati ai dispositivi mobili.

Rischi: I criminali informatici sfruttano dipendenti i dispositivi mobili che contengono informazioni sensibili.

Risposta: Dipendente formazione sull' identificazione e contrastare tentativi di phishing.

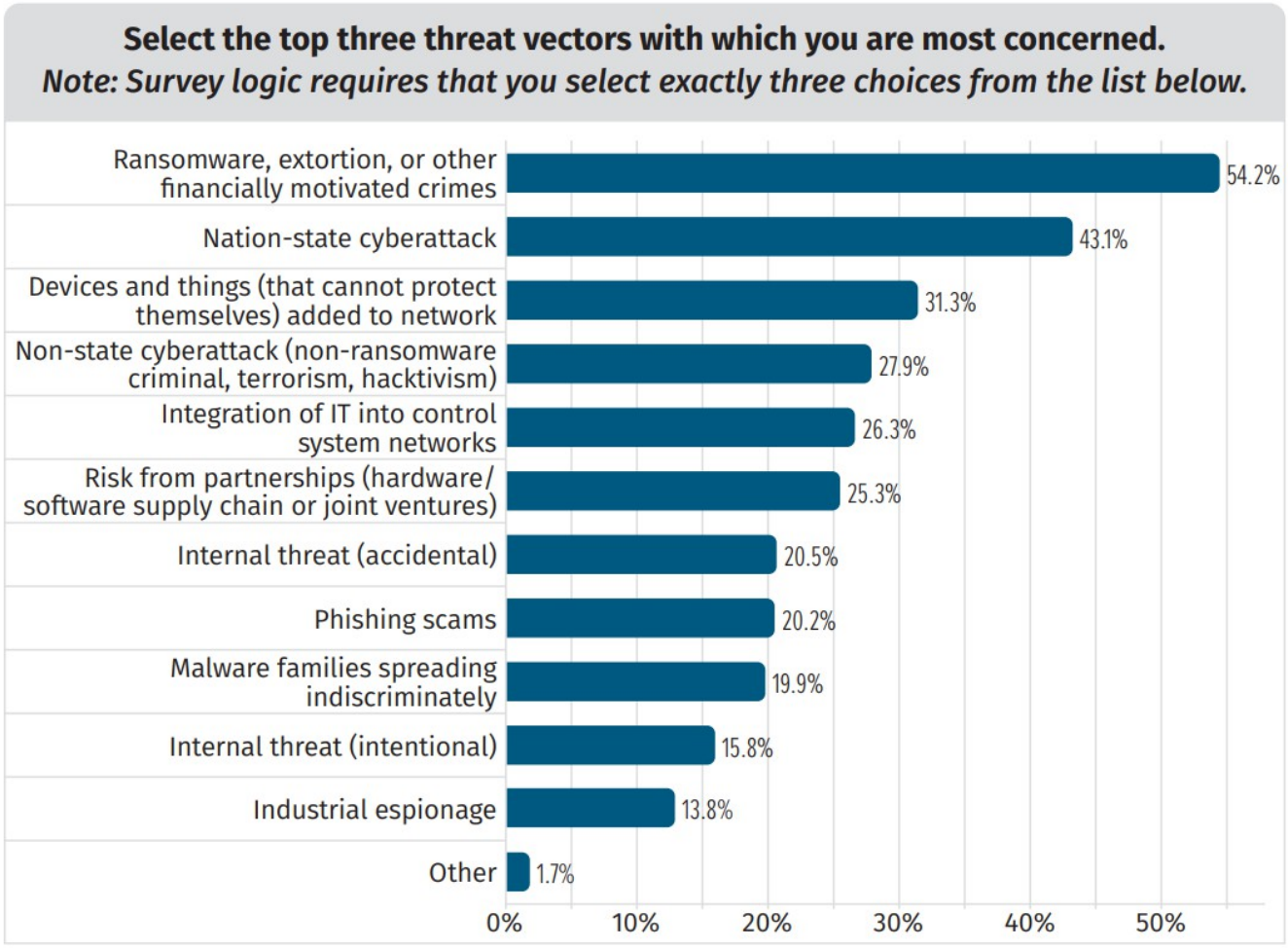
Attacchi alla catena di approvvigionamento

Panoramica delle minacce: i criminali informatici ottengono l'accesso non autorizzato alle reti aziendali attraverso fornitori terzi con protocolli di sicurezza informatica più deboli.

Contromisure: Mandato cybersecurity best practices for third- fornitori di servizi per feste. Assicurarsi che siano in atto piani efficaci di risposta agli incidenti.

Principali vettori di minaccia nel settore energetico

Top Attacks



Bristow, M. (2021). Indagine A sans 2021: Ot/ics cybersecurity. *eng. In*.

Rischio nel tempo

Risk Over Time

Table 3. Threat Actor Risk Over Time

Answer Choices	2021 Rank	2019 Rank	Change
Hackers	1	1	—
Organized crime	2	5	+3 ▲
Current service providers, consultants, contractors	3	3	—
Current employees	4	2	-2 ▼
Activists, activist organizations, hacktivists	5	6	+1 ▲
Unknown (sources were unidentified)	6	7	+1 ▲
Foreign nation-states or state-sponsored parties	7	4	-3 ▼
Domestic intelligence services	8	11	+3 ▲
Former equipment providers	9	12	+3 ▲
Former employees	10	10	—
Current equipment providers	11	8	-3 ▼
Competitors	12	9	-3 ▼
Suppliers or partners	13	13	—
Former service providers, consultants, contractors	14	14	—
Other	15	15	—

Bristow, M. (2021). Indagine A sans 2021: Ot/ics cybersecurity. *eng. In*.

Leading Attacks

Principali vettori di attacco

Osservazione che i principali vettori di attacco, pur non essendo tecnologie di accesso remoto
, sfruttano l'interconnettività come funzione abilitante

- Sfruttamento delle applicazioni rivolte al pubblico: quale livello di connettività o controllo è possibile ottenere dalle applicazioni esposte a Internet e quale architettura è in atto per mitigare i rischi per l'ICS?
- Dispositivi accessibili da Internet: la connettività dei dispositivi bypassa la DMZ?
- Allegati di spear-phishing: un ambiente OT correttamente configurato non dovrebbe avere accesso diretto ai servizi di posta elettronica, eppure il phishing continua a essere un vettore relativamente importante.

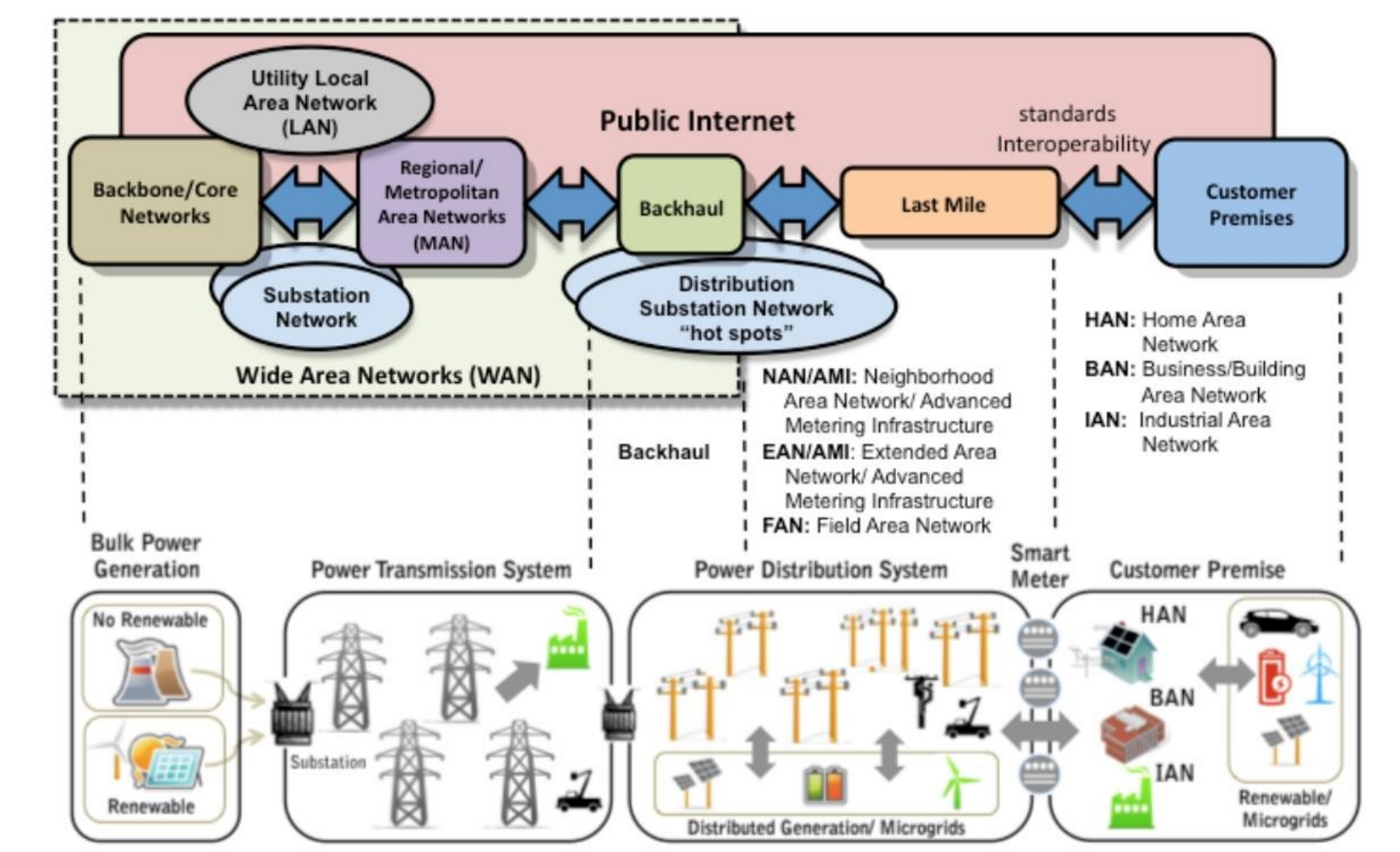
Smart Grids

Reti intelligenti

- Le reti intelligenti integrano le azioni di tutti gli utenti finali connessi. Forniscono comunicazioni bidirezionali tra utenti finali e operatori di rete
- Consumatori (famiglie, imprese) collegati ai DSO tramite contatori intelligenti e rete WAN
- Contatori contatori delimitano DSO infrastruttura infrastruttura e rete locale del cliente
- Aumentare le capacità di automazione e controllo nelle reti di trasmissione e distribuzione
- Tecnologie esistenti (EMS, DMS, SCADA) in fase di aggiornamento per le reti intelligenti

Smart Grids

Reti intelligenti



https://www.enisa.europa.eu/publications/communi
dipendenze-tra-reti-di-comunicazione-nelle-reti-intelligenti

Smart Grids

Reti intelligenti

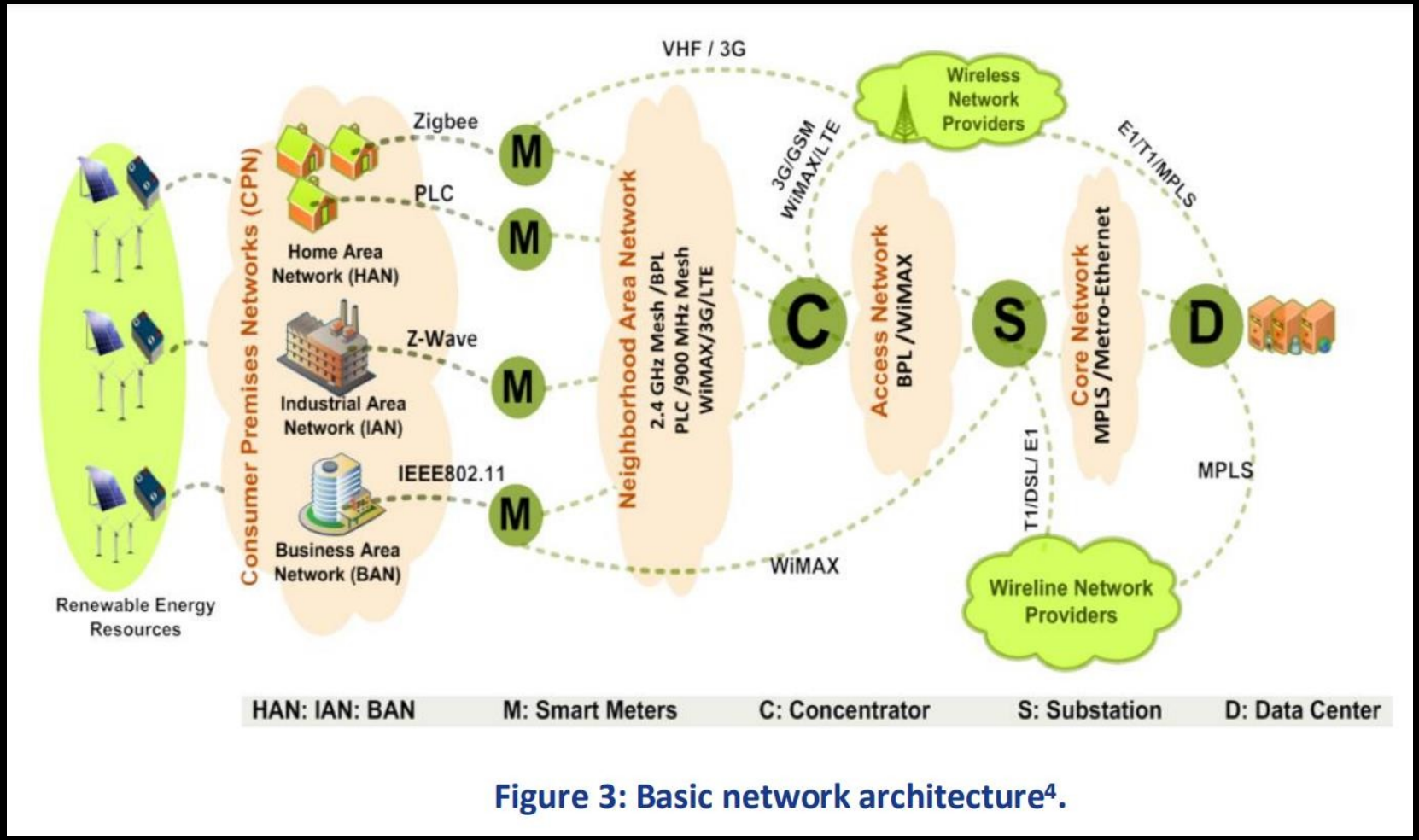


Figure 3: Basic network architecture[4].

https://www.enisa.europa.eu/publications/communi
dipendenze-tra-reti-di-cazione-nelle-reti-intelligenti

e di comunicazione nelle reti intelligenti (Smart Grid)

- Transport Layer Security (TLS): protocollo crittografico per la sicurezza delle comunicazioni di rete, che utilizza la crittografia asimmetrica e la crittografia simmetrica per la protezione dei dati. SSL v3 è un predecessore obsoleto.
- IEC 62351: standard per la sicurezza dei protocolli quali IEC 60870, IETC 61850, IEC 61970 e IEC 61968. Caratteristiche includono TLS ( ) per la crittografia, node authentication (autenticazione del nodo), e autenticazione dei messaggi.
- IEV IEC 61850-90-12: Fornisce linee guida per l'ingegneria WAN, concentrandosi in particolare sulla protezione, il controllo e il monitoraggio tra sottostazioni e centri di controllo.

e di comunicazione nelle reti intelligenti (Smart Grid) dell'

- Internet Protocol Security (IPSec): suite di protocolli per la protezione delle comunicazioni IP con autenticazione e crittografia, che opera sul livello Internet.
- Secure Shell (SSH): protocollo per connessioni remote sicure, che applica la crittografia per la protezione dei dati. Richiede un server SSH operativo sulla macchina remota.
- DNP3 Secure: versione migliorata del protocollo DNP3 con misure di sicurezza aggiuntive come l'autenticazione e la crittografia dei dati, conforme allo standard IEC 62351-5.
- Rete privata virtuale (VPN): rete privata concettuale su reti pubbliche come Internet, che utilizza protocolli di tunneling e crittografia per garantire la sicurezza delle comunicazioni e la riservatezza dei dati.

Sfide nella sicurezza informatica degli impianti eolici

- Gli impianti eolici presentano diversi sistemi di automazione e controllo, che pongono sfide per affrontare i rischi di sicurezza informatica, le misure di mitigazione e le normative a livello settoriale.
- La variabilità nella progettazione degli impianti eolici comprende differenze in termini di dimensioni, capacità di generazione, progettazione della rete, protocolli di comunicazione, strutture dei centri di controllo, pratiche di manutenzione e ubicazioni geografiche.
- L'istituzione di una serie universale di requisiti di sicurezza è ostacolata da queste variazioni, anche se la condivisione di linee guida generali sulla sicurezza rimane fattibile.
- La superficie di attacco si riferisce all'insieme dei sistemi, delle reti o delle risorse informatiche esposti e vulnerabili ad attacchi ostili, che possono causare danni.

Substation Components

Collettore Sottostazione Comunicazioni

- Centro di controllo della trasmissione dell'energia elettrica: questo componente funge da hub centrale per la gestione e il controllo della trasmissione di energia elettrica all'interno della rete elettrica regionale. Supervisiona il funzionamento delle sottostazioni, monitora le prestazioni della rete e coordina la distribuzione dell'energia elettrica attraverso la rete.
- Centro di controllo operativo degli impianti eolici: questo centro di controllo è responsabile della supervisione e della gestione delle operazioni dell'impianto eolico. Monitora le prestazioni delle turbine eoliche, controlla la produzione di energia e garantisce l'efficienza e la sicurezza ottimali delle operazioni dell'impianto eolico.
- Server di previsione: questo server utilizza dati meteorologici e algoritmi predittivi per prevedere le condizioni del vento future. Aiuta a ottimizzare la produzione di energia fornendo informazioni dettagliate sui modelli di vento previsti, consentendo una migliore pianificazione e programmazione della produzione di energia eolica.

Substation Components

Collettore Sottostazione

- Rete di sottostazioni: questa rete collega varie sottostazioni all'interno dell'infrastruttura dell'impianto eolico. Facilita la trasmissione e la distribuzione di energia elettrica tra i diversi componenti dell'impianto eolico e la rete elettrica più ampia.
- Impianto eolico - Rete locale: questa rete comprende l'infrastruttura di comunicazione interna dell'impianto eolico. Collega vari componenti quali turbine, sistemi di monitoraggio e centri di controllo, facilitando lo scambio di dati e il coordinamento per un funzionamento e una gestione efficienti dell'impianto eolico.

Gruppi di minaccia interna

Proprietario/operatore delle risorse (AOO) o aggregatore: responsabile delle operazioni amministrative e della manutenzione, potenziale esposizione involontaria di informazioni critiche.

Produttore di apparecchiature originali (OEM): progetta e implementa apparecchiature per la produzione di energia, vulnerabile ad attacchi mirati e compromissioni della catena di approvvigionamento.

Utility: destinatario dell'energia generata, con potenziali minacce indirette in caso di compromissione.

Manutentori e tecnici: essenziali per la manutenzione ordinaria, privi di standard di sicurezza coerenti.

Integratori/installatori: hanno accesso privilegiato ai sistemi degli impianti eolici, obiettivi primari di compromissione.

Servizi di assistenza di terze parti e e raccoglitori di dati : Integral per aggregazione , soluzioni software, che richiedono un'attenta verifica.

External Threat Groups

Gruppi di minaccia esterni

Proprietari terrieri: possono danneggiare inavvertitamente i beni durante le attività di routine.

Gruppi di attivisti: motivati da preoccupazioni ambientali, rappresentano un rischio di attacchi fisici o proteste.

Elementi criminali informatici e fisici: prendono di mira gli impianti eolici per guadagni finanziari o intenti malevoli, sempre più spesso attraverso attacchi ransomware.

Attori statali: svolgono attività di spionaggio e ricognizione, rappresentando una minaccia significativa per le infrastrutture eoliche e gli interessi di sicurezza nazionale.

External Threat Groups

Potenziali vettori di attacco

Panoramica dei vettori di attacco: mezzi con cui gli avversari ottengono l'accesso iniziale alle reti o ai sistemi.

Classificati in tre gruppi:

- Accesso fisico ravvicinato
- Remoto, mezzi abilitati dal cyber
- Attacchi misti ciber-fisici

Tipi di vettori di attacco: accesso fisico alle turbine eoliche o alle sottostazioni di raccolta. Accesso informatico tramite connessioni remote. Attacchi mirati a risorse informatiche transitorie, ad esempio le attrezzature di manutenzione dei tecnici sul campo.

Industroyer in Ucraina

Caso d'uso: Industroyer in Ucraina 2016

Dicembre 2016: attacco informatico dell'operatore di trasmissione ucraino Ukrenergo a una singola sottostazione di trasmissione vicino a Kiev.

Il malware modulare ha indicato il potenziale per un attacco più ampio e attacco sincronizzato.

Industroyer: framework malware modulare che consente l'interazione diretta con le apparecchiature ICS tramite protocolli industriali.

Industroyer2: una versione rivista nell'aprile 2022 ha preso di mira un fornitore di energia ucraino, limitandosi allo standard IEC 60870-5-104.

Industroyer2: Configurabile con wiper ha utilizzato per distruggere dati e prove dopo l'esecuzione.

Industroyer in Ucraina

1. Accesso iniziale: gli aggressori hanno ottenuto l'accesso alla rete della sottostazione di trasmissione ucraina, probabilmente tramite credenziali rubate o vulnerabilità nel perimetro della rete.
2. Distribuzione del malware: è stato distribuito Industroyer, un framework malware modulare, che ha consentito l'interazione diretta con le apparecchiature ICS tramite protocolli industriali (IEC 60870-5-101, IEC 60870-5-104, IEC 61850 e OPC).
3. Enumerazione e ricognizione: i moduli malware hanno enumerato l'ambiente della sottostazione per identificare gli obiettivi e valutare le vulnerabilità del sistema.
4. Manipolazione del controllo: gli aggressori hanno manipolato il controllo dei processi fisici all'interno dell'ambiente industriale, modificando i valori di setpoint o i parametri, come l'apertura degli interruttori della sottostazione.

Industroyer in Ukraine

Industroyer in Ucraina

5. Denial of Service (DoS): un modulo DoS ha reso inutilizzabile una serie specifica di relè Siemens Siprotec, interrompendo il normale funzionamento dei dispositivi.
6. Perdita di sicurezza: il malware ha compromesso la funzionalità del relè di protezione, causando un evento di perdita di sicurezza all'interno della sottostazione.
7. Furto di informazioni operative: gli aggressori hanno compromesso l'archivio dati, rubando informazioni operative critiche sull'ambiente della sottostazione.

Freeman, S. G., Kress-Weitenhagen, M. A., Gentle, J. P., Culler, M. J., Egan, M. M. e Stolworthy, R. V. (2024). *Superficie di attacco delle tecnologie eoliche negli Stati Uniti* (n. INL/RPT-24-76133-Rev000). Idaho National Laboratory (INL), Idaho Falls, ID (Stati Uniti).

Lessons Learned

Lezioni apprese: Industroyer in Ucraina

Vulnerabilità dei protocolli: gli avversari hanno sfruttato le vulnerabilità dei protocolli industriali ampiamente utilizzati, sottolineando l'importanza di proteggere i protocolli di comunicazione e monitorare i comportamenti anomali.

Adattabilità del malware modulare: la natura modulare di Industroyer ha consentito agli avversari di adattare il malware a vari obiettivi, sottolineando la necessità di meccanismi di difesa flessibili e adattivi.

Rilevamento precoce e risposta: il rilevamento tempestivo di attività anomale e una risposta rapida sono fondamentali per mitigare l'impatto degli attacchi informatici sulle infrastrutture critiche.

Monitoraggio e controllo degli accessi potenziati: l'implementazione di meccanismi potenziati di monitoraggio e controllo degli accessi può aiutare a identificare e prevenire accessi non autorizzati a sistemi e dati critici.

Collaborazione intersettoriale: la collaborazione tra i settori e la condivisione delle informazioni sulle minacce possono migliorare la resilienza contro le minacce informatiche, in particolare quelle che prendono di mira le infrastrutture critiche.

Formazione CSP CSP001: Presentazione di S. Karagiannis, PDMFC, Portogallo

Challenges

Sfide di sicurezza informatica nel settore energetico

Requisiti in tempo reale: alcuni sistemi energetici richiedono una risposta rapida, limitando l'implementazione di misure di sicurezza standard a causa di problemi di latenza.

Effetti a cascata: le reti elettriche e i gasdotti interconnessi possono causare interruzioni di corrente o carenze di approvvigionamento su vasta scala a livello transfrontaliero.

Sistemi legacy e nuove tecnologie: l'integrazione delle infrastrutture legacy con le moderne tecnologie di automazione e controllo, come i dispositivi IoT, comporta rischi per la sicurezza informatica.

Governance ed ecosistema

1. Esiste un elenco aggiornato dei sistemi IT e OT più critici e quali sono le minacce informatiche rilevanti che potrebbero influenzarli?
2. Abbiamo un programma globale di gestione dei rischi informatici (noto anche come sistema di gestione della sicurezza delle informazioni) che copre sia i sistemi IT che quelli OT?
3. Abbiamo una buona comprensione del nostro ecosistema complessivo, delle nostre dipendenze da altre organizzazioni all'interno e all'esterno del settore, dei nostri fornitori e venditori?

Protezione

1. Abbiamo un programma di gestione delle vulnerabilità che garantisce che tutti i sistemi IT e OT siano tempestivamente aggiornati e patchati? In che modo questo programma copre i nostri sistemi legacy?
2. Abbiamo una protezione in atto per l'accesso remoto ai sistemi IT e OT, come l'autenticazione a due fattori, in particolare per gli account privilegiati (amministratore)?
3. Abbiamo una segmentazione nella rete dell'organizzazione e implementiamo i principi dell'architettura di rete zero-trust?
4. Il nostro personale è consapevole delle minacce di phishing e di altre forme di attacchi informatici? Esiste un programma di formazione e sensibilizzazione del personale sulla sicurezza informatica?

Difesa

1. Abbiamo ruoli e punti di contatto chiari per la risposta agli incidenti, sia per gli incidenti IT che OT?
2. Disponiamo di piani e procedure aggiornati per la risposta agli incidenti? Li abbiamo testati di recente?

Resilienza

1. Disponiamo di procedure di backup e ripristino adeguate?
2. Abbiamo abbiamoaggiornati aggiornate business ee piani di emergenza aggiornati? Li abbiamo testati di recente?
3. Abbiamo procedure di gestione delle crisi, sappiamo chi contattare in caso di attacchi o incidenti?

ENISA - PREPARARSI AGLI ATTACCHI INFORMATICI NEL SETTORE ENERGETICO

Grazie

Relatore: Stylianos Karagiannis (PDMFC, Portogallo)

Si prega di inviare tutte le domande a:
stylianos.karagiannis@pdmfc.com