Valutazione e gestione del rischio di sicurezza informatica per il settore energetico

CSP003_S_E

PRESENTAZIONE DA PARTE DI:

- **ARTSIOM YAUTSIUKHIN**
  CNR, ITALIA
- **CRISTINA ALCARAZ**
  UNIVERSITÀ DI MALAGA, SPAGNA
- **JAVIER LOPEZ**
  UNIVERSITÀ DI MALAGA, SPAGNA

Riconoscimento

- *Co-finanziato dall'Unione Europea. I punti di vista e le opinioni espresse sono tuttavia esclusivamente quelli dell'autore o degli autori e non riflettono necessariamente quelli dell'Unione Europea o di HADEA. Né l'Unione Europea né l'autorità che ha concesso il finanziamento possono essere ritenute responsabili.*
- *Accordo di progetto n. 101083594*

Schema

Argomento 1 - Minacce e vulnerabilità per il settore energetico

Argomento 2 - Processi e metodologie di valutazione e gestione del rischio per il settore energetico

Conclusioni

Riferimenti e fonti

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Argomento 1: Minacce e vulnerabilità per il settore energetico

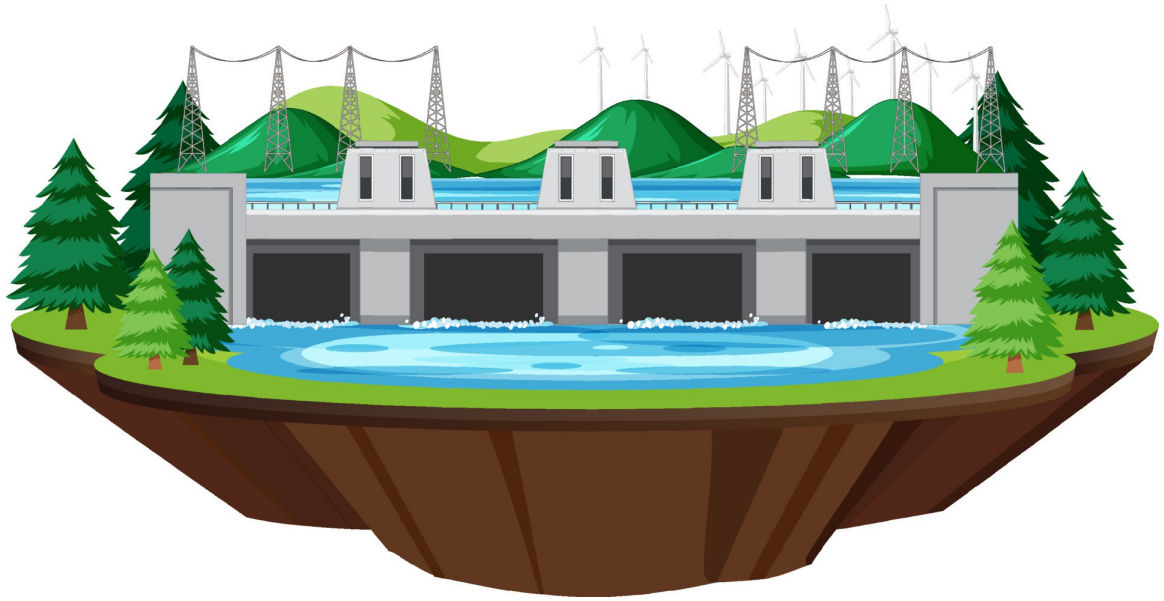
Panoramica

- Una piccola panoramica del settore energetico e delle sue componenti principali
- Panoramica delle vulnerabilità e delle minacce

CSP003_S_E: Cristina Alcaraz e Javier Lopez (UMA), Artsiom Yautsiukhin (CNR)

Sistemi di alimentazione e fasi operative tradizionali

- I sistemi di energia elettrica seguono normalmente procedure sistematiche, in cui un insieme di apparecchiature e dispositivi operativi sono destinati a (1) produrre, (2) trasmettere e (3) distribuire energia agli utenti finali.



Fonte della figura: Vecteezy
URL: vecteezy.com/it-it/arte-vettoriale/44966530-impianti-idroelettrici-isolati-generano-elettricità

CSP003_S_E: Cristina Alcaraz e Javier Lopez (UMA), Artsiom Yautsiukhin (CNR)

Sistemi di alimentazione e fasi operative tradizionali

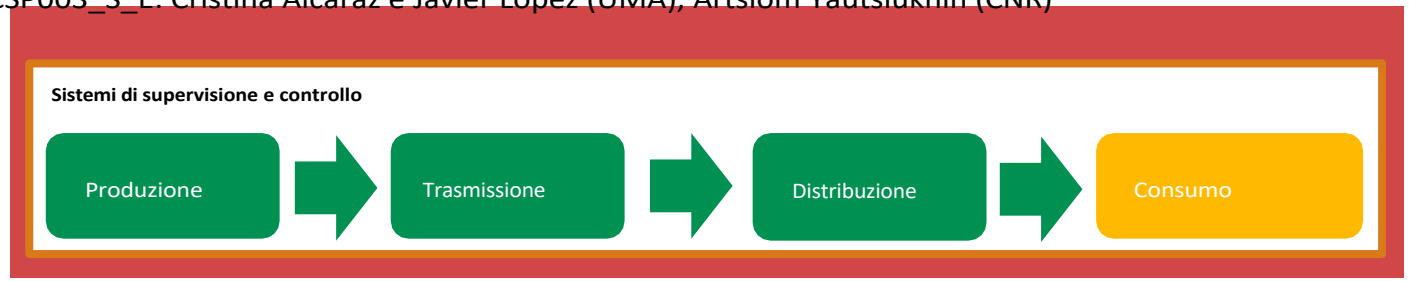
- Le fasi di produzione e distribuzione dell'energia sono le seguenti:
  - **La produzione di energia** comporta l'incorporazione di meccanismi e componenti in grado di generare grandi quantità di energia con la possibilità di immagazzinarla o distribuirla attraverso i tralicci.
  - La **trasmissione di energia** mira a trasportare grandi quantità di elettricità con carichi elevati su lunghe distanze (tramite tralicci), con il supporto di sistemi di accumulo e di generazione nelle sottostazioni.
  - **La distribuzione di energia** consiste nel trasportare l'elettricità ad un'intensità accettabile per il consumo finale, probabilmente con supporto di sistemi di accumulo e generazione in sottostazioni vicine agli utenti finali.

Principali sistemi, componenti e soggetti interessati

- Oltre ai tipici generatori e alle torri ad alta tensione, all'interno di queste tre fasi di produzione e distribuzione dell'energia, emergono anche una serie di Tecnologie Operative (OT), quali:
  - **Dispositivi di campo** come sensori e attuatori
  - **Controllori** come le unità terminali remote (RTU)
  - **Interfacce uomo-macchina** (HMI)
  - **Server SCADA (Supervisory Control And Data Acquisition)** per la supervisione e il controllo delle sottostazioni di controllo.
- Questi OT contribuiscono a fornire un monitoraggio costante degli stati e dei processi operativi delle sottostazioni remote e delle loro risorse critiche, che sono essenziali per la generazione, la trasformazione e la distribuzione di energia.
  - Questo è importante per garantire il corretto funzionamento dell'infrastruttura sottostante e la fornitura di risorse essenziali per il benessere.

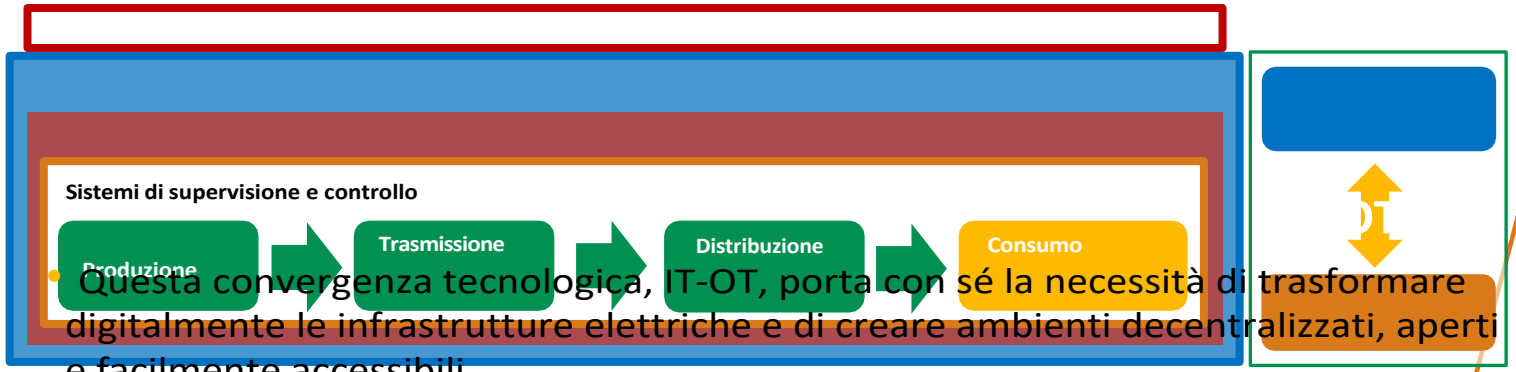
Fasi dell'operazione e soggetti interessati

- Per una produzione e distribuzione coordinata dell'energia, una serie di soggetti interessati fa parte dell'intero processo, come ad esempio:
  - **Operatori di rete/sistema** responsabili della generazione, trasmissione e distribuzione dell'energia, noti anche come Operatori del sistema di trasmissione (TSO) e Operatori del sistema di distribuzione (DSO).
  - **Fornitori o provider** per agevolare l'accesso all'energia
  - **Sistemi di supervisione e controllo**
  - **Le autorità o i regolatori** stabiliscono le regole di funzionamento
  - **Utenti finali** come consumatori o prosumer
  - **Organizzazioni o associazioni** che sostengono l'uso e l'accesso all'energia



Fasi dell'operazione e soggetti interessati

- Per generare, distribuire e controllare in modo efficiente l'energia in base alla domanda effettiva, è necessario creare ambienti iperconnessi basati **sulle nuove tecnologie dell'informazione** (IT) **e sui sistemi di comunicazione.**

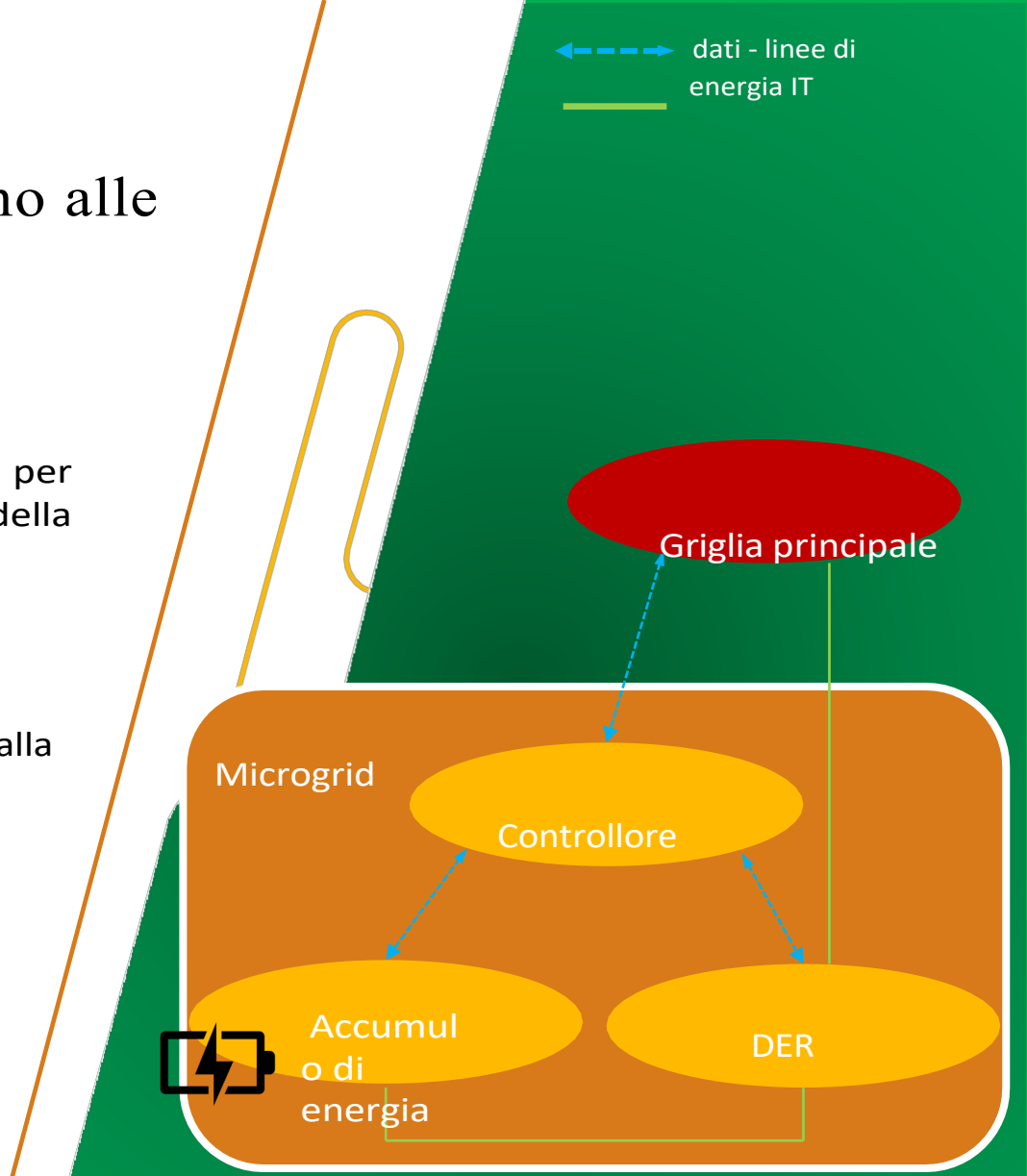


- Questa convergenza tecnologica, IT-OT, porta con sé la necessità di trasformare digitalmente le infrastrutture elettriche e di creare ambienti decentralizzati, aperti e facilmente accessibili.

per il controllo

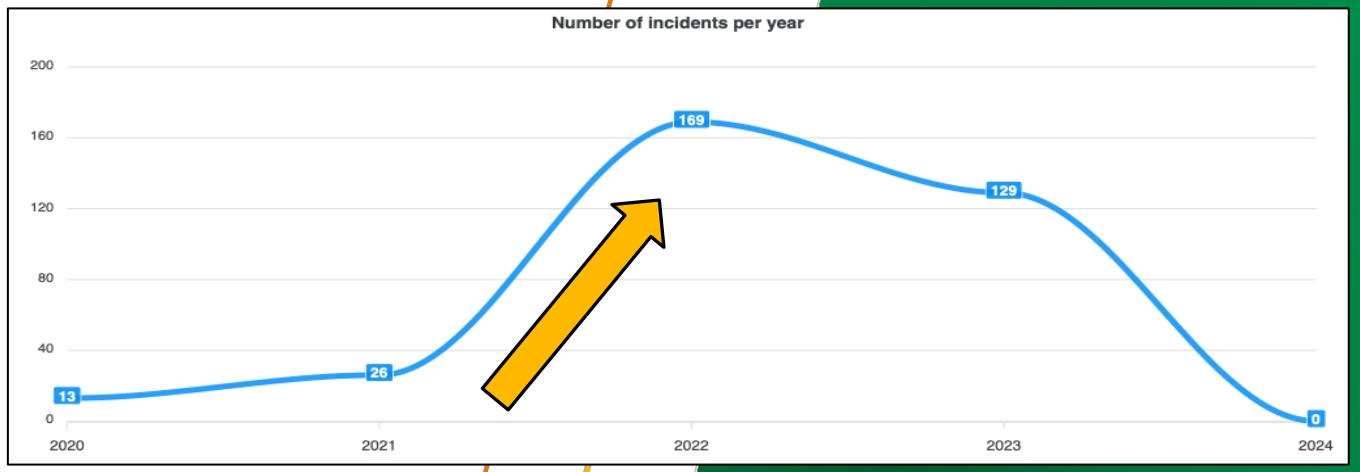
Le fasi di funzionamento più intelligenti portano alle Smart Grids

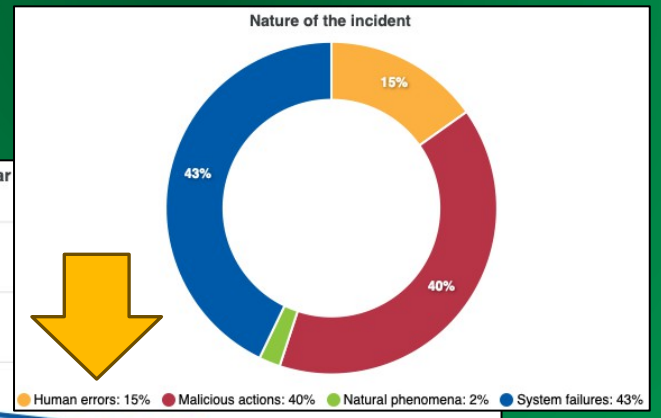
- Di conseguenza, nasce il concetto di **Smart Grid**,
  - in cui i diversi soggetti interessati devono cooperare tra loro per gestire dinamicamente, senza sprechi, l'energia sulla base della domanda effettiva
- Questo concetto può essere a sua volta ridotto nella realizzazione di "**Microgrids**".
  - composto da infrastrutture elettriche modulari digitalizzate collegate alla rete principale, e
  - in grado di gestire risorse energetiche distribuite (DER) composte da fonti di energia quali
    - sistemi rinnovabili e di stoccaggio, batterie di veicoli elettrici, stazioni di ricarica, ecc.
- Questo modo di isolare le operazioni attraverso le isole energetiche fornisce anche **sicurezza e resilienza** contro blackout, malfunzionamenti o attacchi informatici.

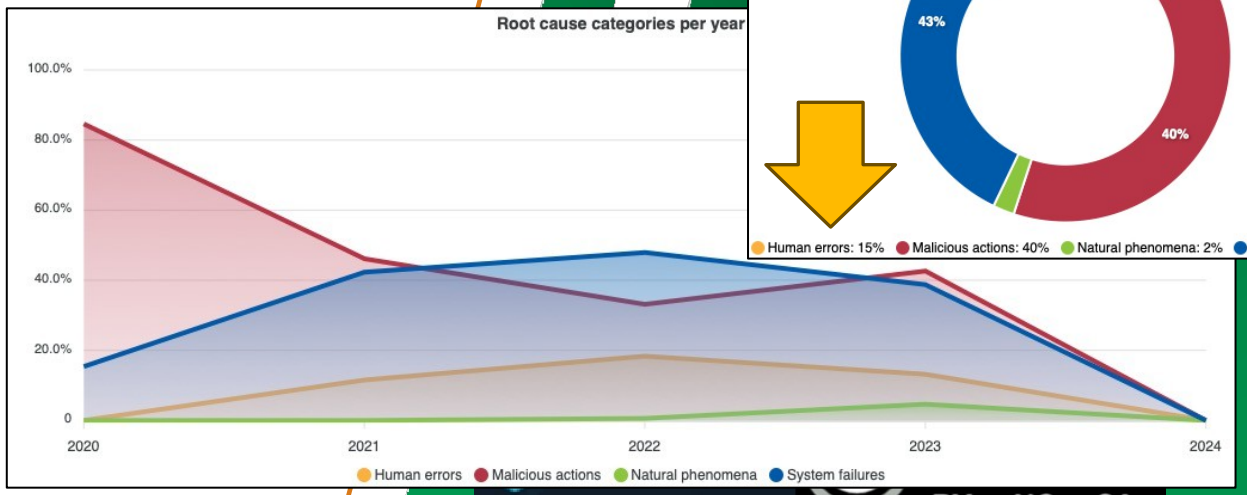


Rischi per la sicurezza nel settore energetico

- Purtroppo il settore è nel mirino degli aggressori, conoscono le conseguenze di un'interruzione di corrente causata da:
  - **Una minaccia deliberata**, come un denial of service, la modifica di valori critici o un attacco di phishing
  - **Una minaccia non intenzionale**, come una catastrofe fenomenale o un errore umano.
- Secondo l'Agenzia dell'Unione Europea per la Cybersecurity (ENISA), attraverso il suo strumento CIRAS,
  - il numero di incidenti informatici nel settore dell'energia è in aumento, anche per quanto riguarda gli errori umani







Fonte: ENISA, CIRAS, 2024

URL: https://ciras.enisa.europa.eu

CSP003_S_E: Cristina Alcaraz e Javier Lopez (UMA), Artsiom Yautsiukhin (CNR)

Vulnerabilità della sicurezza nel settore energetico

- In realtà, parte di questi rischi per la sicurezza sono dovuti anche a **guasti del sistema**, solitamente causati da errori hardware o software che possono essere facilmente sfruttati.
  - Tra le vulnerabilità, le più interessanti per gli aggressori sono quelle basate sulle vulnerabilità ZERO-DAYS
  - Queste vulnerabilità fanno parte degli obiettivi principali delle Advanced Persistent Threats (APT).
- Tutte le vulnerabilità sono segnalate pubblicamente e accessibili da repository quali:
  - MITRE CVE: https://cve.mitre.org
  - NIST NVD: https://nvd.nist.gov
- Come si può vedere nella figura, queste CVE non devono necessariamente essere basate su componenti software.
  - Possono essere collegati agli OT, come i protocolli industriali.

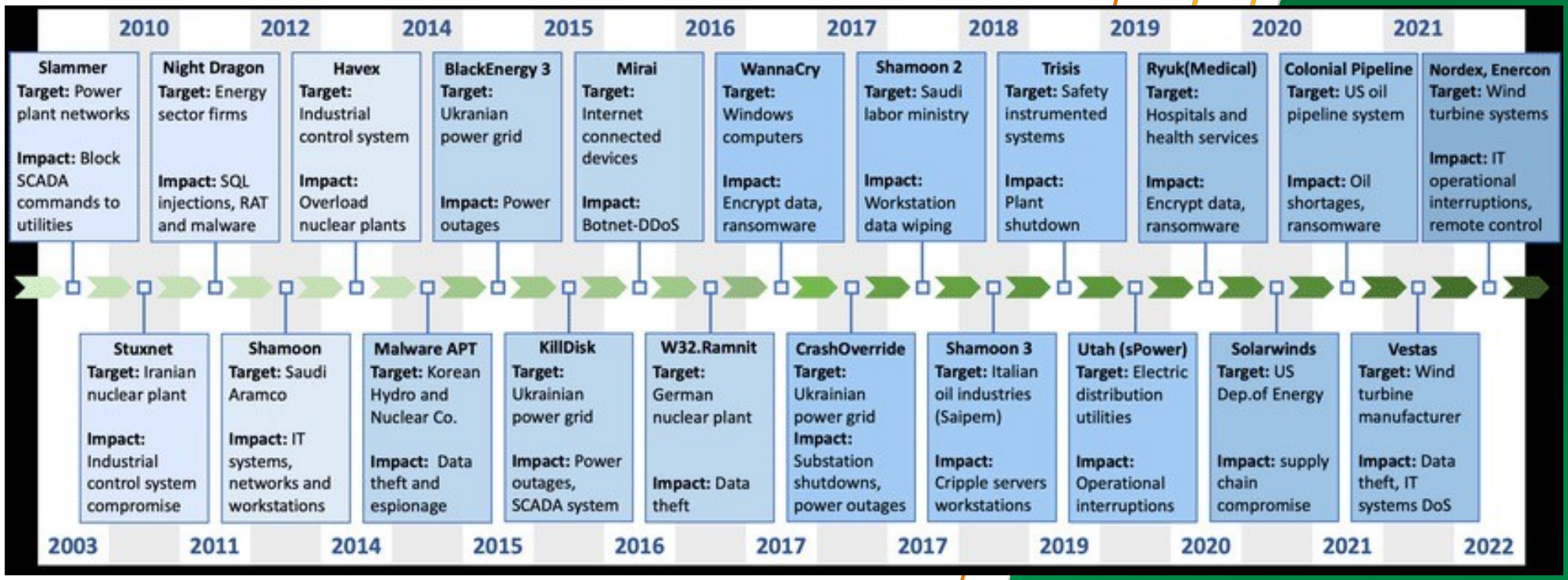
Fonte: MITRE, MITRE CVE, 2024
URL: https://cve.mitre.org
Fonte della figura: MITRE, MITRE CVE, 2024
URL: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=modbus

URL: https://nvd.nist.gov

CSP003_S_E: Cristina Alcaraz and Javier Lopez (UMA), Artsiom Yautsiukhin (CNR)

I rischi per la sicurezza si moltiplicano in questi sistemi

- Inoltre, negli ultimi anni sono emerse molteplici minacce, il cui obiettivo è quello di causare il maggior numero di danni possibile.



Fonte: Zografopoulos, Ioannis, Nikos D. Hatziargyriou e Charalambos Konstantinou. "Prospettive di cybersicurezza delle risorse energetiche distribuite: Vulnerabilità, attacchi, impatti e mitigazioni". *IECESEPSTyRsAteImNIsNJGouMrnaOI* (D2U02L3E) NAME: MODELLO DI PRESENTAZIONE CREATO DA PR

CSP003_S_E: Cristina Alcaraz e Javier Lopez (UMA), Artsiom Yautsiukhin (CNR)

Argomento 2:Rischio Valutazione e Processi e metodologie di gestione per il settore energetico

Panoramica

- Definizioni e processo di valutazione del rischio
- Analisi del rischio
- Strumenti per la valutazione del rischio
- Trattamento del rischio

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Come misurare la sicurezza informatica?

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Come misurare la sicurezza informatica?

Obiettivo:

- ❑ Prendete una decisione razionale per migliorare la vostra sicurezza informatica.

Problemi

- ❑ La decisione deve essere presa per l'**intero** sistema di sicurezza informatica;
- ❑ La decisione deve essere presa dai **dirigenti**, non dai tecnici;
- ❑ Le soluzioni di sicurezza (opzioni) sono **costose** e il budget per la sicurezza informatica è **limitato**;
- ❑ Come prendere una decisione **razionale**? Quali misure/metriche utilizzare?
- ❑ La sicurezza informatica è molto **eterogenea** (comprende la gestione, le politiche, le soluzioni tecniche, diverse piccole opzioni per le soluzioni tecniche, gli aspetti fisici e sociali, ecc.)
- ❑ Anche sistemi IT simili **sono diversi**
- ❑ Il contesto della sicurezza informatica **sta cambiando**

La sicurezza informatica non è solo un problema tecnico!

CYBERSECURITY VENTURES ABOUT RESEARCH LISTS VIDEOS EVENTS JOI

Last year, Cybersecurity Ventures predicted that cybercrime will cost the world $6 trillion annually by 2021, up from $3 trillion in 2015. This represents the greatest transfer of economic wealth in history, risks the incentives for innovation and investment, and will be more profitable than the global trade of all major illegal drugs combined.

Gartner Forecasts Worldwide Information Security Spending to Exceed $124 Billion in 2019

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Valutazione del rischio

La valutazione del rischio in breve:

- ❑ Ponderare le proprie capacità ed esigenze identificando le proprie
  - ❑ attività principali
  - ❑ minacce potenziali
  - ❑ Controlli di sicurezza installati e potenziali
- ❑ Analizzare lo stato attuale e i possibili miglioramenti
  - ❑ Siete soddisfatti dei rischi attuali?
  - ❑ Cosa si può fare per migliorare il proprio livello di rischio.

Pro:

- ❑ Risponde alle vostre esigenze
- ❑ Ottimizza le decisioni
- ❑ Facile da capire e da usare per i manager
- ❑ Supporta la giustificazione delle decisioni prese

Contro:

- ❑ Richiede buone conoscenze (e dati) sulla sicurezza informatica e sulla gestione del rischio.

NOME DEL MODULO DI FORMAZIONE CSP: MODELLO DI PRESENTAZIONE CREATO DA PR

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Gestione del rischio, valutazione e gestione della sicurezza

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Che cos'è il rischio?

Il rischio è la **possibilità** di subire un danno o una **perdita**

[NIST SP800-30]

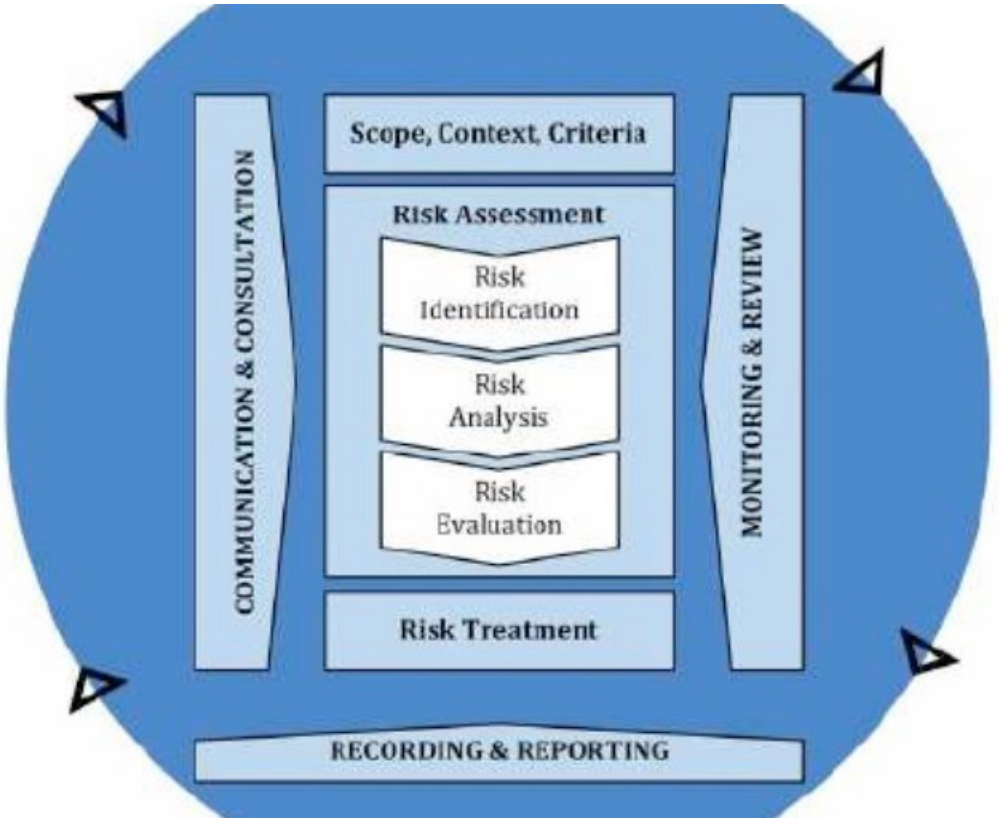
- **Minaccia** - causa del rischio
- **Vulnerabilità** - flusso o debolezza esistente
- **Impatto** - possibile perdita

- **Asset** - qualcosa di valore
- **Incidente** - minaccia che si verifica

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Gestione del rischio

Gestione del rischio - attività coordinate per dirigere e controllare un'organizzazione in al rischio [ISO 31000].



CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Valutazione del rischio

Identificazione del rischio

Minacce, vulnerabilità/controlli, Attività

Analisi del rischio

Esposizione alle minacce

Probabilità di successo

Impatto

Valutazione del rischio

Calcolare il rischio Dare priorità al rischio Valutare il rischio

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Trattamento del rischio

La valutazione del rischio stima il **livello attuale** dei rischi

- Dove ?

Il trattamento del rischio aiuta a pianificare le fasi per **affrontare** i rischi eccessivi.

- Che cosa ?

L'implementazione di maggiori o migliori controlli è solo un modo (riduzione del rischio) per trattare i rischi!

- Trattamento del rischio≠ più controlli
- Trattamento del rischio ⊃ più controlli

I problemi identificati possono (e devono) essere risolti a livello di rischio, con altri strumenti (tra cui l'evitamento del rischio, il trasferimento del rischio e l'accettazione del rischio).

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Gestione della sicurezza informatica

In genere, la gestione della sicurezza si concentra maggiormente

- sugli aspetti tecnici
- sulla riduzione della probabilità che si verifichi una minaccia
- sull'aumento sicurezza.

Non tiene (esplicitamente) del possibile impatto.

Gestione della sicurezza È governata da decisioni di gestione del rischio

La differenza con la gestione del rischio informatico è sfumata e, in pratica, non è cruciale.

- Senza entrare molto nei dettagli, è possibile affermare che
  - gestione della sicurezza= gestione del rischio

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Standard di gestione del rischio/sicurezza

Gestione del rischio informatico

- ISO 31000 - Gestione del rischio - Linee guida
- **ISO 27001 - Sistemi di gestione della sicurezza delle informazioni - Requisiti**
- NIST 800-37 - Quadro di gestione del rischio per i sistemi e le organizzazioni informatiche

Valutazione del rischio informatico

- ISO 27005 - Valutazione del rischio per la sicurezza delle informazioni
- NIST 800-30 - Guida per la conduzione di valutazioni del rischio
- Altre metodologie di gestione del rischio:
  - CIS RAM, OCTAVE, Magerit, Mehari, Microsoft, ecc.

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Elenchi di controllo di sicurezza/linee guida

Elenchi e linee guida dei controlli di sicurezza generali:

- ISO 27002 - Codice di prassi per i controlli di sicurezza delle informazioni
- NIST 800-53 - Controlli di sicurezza e privacy
- Controlli CIS

Linee guida sulla sicurezza informatica per l'energia:

- NISTIR 7628 (rete intelligente)
- IEC 62351 (protocolli)

Linee guida per la sicurezza informatica delle infrastrutture critiche:

- NIST CSF
- NIS /NIS2
- IEC 62443
- NERC CIP
- NIST SP 800-82 Rev. 3

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Valutazione del rischio informatico

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Valutazione del rischio informatico per i sistemi energetici

La valutazione del rischio è uno strumento universale per la gestione di qualsiasi tipo di rischio.

Che cos'è allora la valutazione del rischio **informatico** per i **sistemi energetici**?

- ❑ Si tratta dell'applicazione del processo generico di valutazione del rischio al dominio cibernetico, tenendo conto delle peculiarità del dominio energetico.
  - ❑ Come definire l'**ambito** del sistema di sicurezza?
  - ❑ Quali sono gli **asset** informatici tipici dei sistemi energetici?
  - ❑ Quali sono le minacce informatiche tipiche dei sistemi energetici?
  - ❑ Quali sono i **controlli** di sicurezza informatica per i sistemi energetici?
  - ❑ Come stimare **l'impatto**?
  - ❑ Come stimare **le probabilità e l'esposizione**?

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Processo tipico di valutazione del rischio

Definizione del contesto

Identificazione del rischio

- Attività
- Minacce
- Controlli

Stima/analisi del rischio

- Impatto
- Esposizione
- Probabilità

Valutazione del rischio

- Calcolo del rischio
- Priorità del rischio
- Valutazione del rischio

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Definizione del contesto

Definizione del contesto. Contesto

È necessario comprendere l'ambiente in cui opera il sistema informatico e quanto esso influisca sulla valutazione del rischio.

In particolare, occorre tenere dei seguenti punti:

- Obiettivi, strategie e politiche aziendali delle organizzazioni
- Processo aziendale, funzione e struttura
- Requisiti legali, normativi e contrattuali
- Approccio complessivo dell'organizzazione alla gestione del rischio
- Posizione geografica
- Aspettative delle parti interessate
- Posizione e ambiente socio-culturale

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Definizione del contesto. Ambito e confini

Ambito di applicazione

- garantisce che tutti gli **asset** di sicurezza rilevanti siano presi in considerazione durante la valutazione del rischio.

Confini

- aiuta a concentrarsi sulle **minacce** che potrebbero penetrare attraverso i confini.

Nel contesto informatico, è importante prestare particolare attenzione all'ambito e ai confini a causa della natura distribuita dei sistemi IT:

- Il servizio cloud rientra o meno nei vostri confini?
- Gli asset sui dispositivi collegati dall'esterno della rete devono nell'ambito della valutazione?
- Le risorse presenti sui dispositivi mobili collegati alla rete devono rientrare nell'ambito di applicazione?
- Vengono considerati tutti i dispositivi/sensori/attuatori IoT?

Definizione del contesto. Criteri

Criteri di **valutazione del rischio**

- Questi sono i criteri di valutazione dei rischi per la sicurezza informatica, che comprendono:
  - Importanza strategica dei processi aziendali esistenti
  - Sensibilità degli asset informatici
  - Obblighi legali, normativi e contrattuali
  - Come la riservatezza, l'integrità e la disponibilità delle risorse informatiche influiscono sui processi aziendali.
  - Aspettative degli stakeholder e valore della fiducia e della reputazione.

Criteri di **impatto**

- Questi sono i criteri per valutare un'eventuale perdita:
  - Violazioni (perdita di riservatezza, integrità, disponibilità)
  - Operazioni interrotte
  - Scadenze non rispettate
  - Perdita finanziaria (compresa la perdita di opportunità commerciali)
  - Perdita di reputazione
  - Incapacità di soddisfare i requisiti legali, normativi e contrattuali

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Definizione del contesto. Criteri

Criteri di **accettazione del rischio**

- Questi criteri definiscono quali livelli di rischio sono accettati
- Potrebbe avere diversi livelli
- Potrebbe essere diverso a seconda dei rischi
- Potrebbe dipendere dal profitto atteso

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Identificazione del rischio

Identificazione del rischio. Attività informatiche

Peculiarità nell'identificazione degli asset informatici

- Gli asset informatici potrebbero essere difficili da assegnare a un oggetto fisico (ad esempio, i dati del cliente sono archiviati su un server), perché sono facili da copiare, modificare e scambiare (ad esempio, comunicati via Intranet/Internet, elaborati su un desktop; backup su un NAS o su un cloud, ecc.)
- Le risorse informatiche sono difficili da monitorare. Possono essere copiati in un altro asset informatico. Potrebbero essere elaborati e trasformati in un altro asset (ad esempio, analisi o log).
- Non è banale identificare ed elencare tutte le risorse informatiche. Spesso il valore degli asset informatici viene troppo sminuito (ad esempio, le informazioni di identificazione personale, come la posizione o l'e-mail).
- Alcuni asset informatici sono molto importanti, ma non comportano una perdita immediata o definitiva. Esempio: le credenziali.

- Esistono modi non standard (talvolta innovativi) con cui gli aggressori possono abusare delle vostre risorse o utilizzarle per attaccare altri. Ad esempio, il cryptojacking, le botnet o gli attacchi alla catena di approvvigionamento.
- Le attività potrebbero dipendere l'una dall'altra (ad esempio, la falsificazione dei dati di monitoraggio può portare a un processo aziendale).

Identificazione del rischio. Attività informatiche

Logico

- Processi aziendali
- Informazioni
  - informazioni personali identificabili,
  - informazioni sanitarie personali,
  - informazioni finanziarie
  - Il know-how
  - Informazioni strategiche aziendali
  - Informazioni rilevanti per l'azienda
  - Credenziali
  - Codice sorgente

- Contenitori
  - Banche dati
  - File
  - Applicazioni
  - Comunicazione
  - E-mail
  - Ambiente di sviluppo
  - Servizio web/ sito web

Fisico

- Server
- Rete
- Personale
- IoT, dispositivo mobile
- Desktop
- Supporti (CD, NAS, ecc.)
- Nuvola
- Carta

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Cyber Assets per il settore energetico

Dati personali/finanziari/fatturazione

- Può essere cancellato/crittografato (ad esempio, Ransomware) [Disponibilità].
- Rubato [Riservatezza]

Attacco al gasdotto Colonial

Processo di consegna/generazione/distribuzione dell'energia:

- Monitoraggio/Dati personali [Integrità/Disponibilità]
  - Cancellati/criptati (ad esempio, Ransomware)
  - Modificato (Iniezione di dati falsi)
    - Dati trasmessi (problemi di comunicazione)
    - Accesso fisico ai sensori e alla rete IT
- Applicazioni (ad esempio, applicazione di controllo) [Integrità/Disponibilità].
  - Email (Phishing)
  - Ambiente di sviluppo/distribuzione del software (ad esempio, aggiornamenti porte, ure posteriori)

May 2021
Ransomware attack on French producer of renewable energy
Albioma - Paris, France

05 May 2021
Ransomware at Norwegian energy technology provider
Volue ASA is headquartered in Norway and was very open about the cyber attack.

27 November 2021
Ransomware at energy provider in Australia
CS Energy - Brisbane, Queensland, Australia

Hacker, attacco a Eni dopo il Gse. Massima allerta dell'intelligence

February 2022
Cyberattack on a power company in Italy
Gruppo Dolomiti energia - Rovereto, Trentino, Italy

Il 2015
Blackout in Ucraina

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Identificazione del rischio. Le minacce

Le minacce informatiche sono, in gran parte, intenzionali. Ciò significa che combattiamo contro altri esseri umani:

- Adattabile
- Inventivo
- Collaborare
- Pianificazione
- Paziente
- Potrebbe essere persistente

Le minacce informatiche sono eterogenee e dinamiche

- Appaiono nuove minacce
- Le minacce esistenti si evolvono
- Ricompaiono vecchie minacce.

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Identificazione del rischio. Le minacce

Gli attacchi informatici spesso richiedono diversi passaggi per ottenere il risultato.

- Un utente apre un'e-mail fraudolenta con un virus in allegato.
- Un virus viene eseguito sul dispositivo della vittima. Viene installata una backdoor
- Un aggressore ottiene l'accesso al sistema ed esegue un exploit per ottenere un accesso di livello superiore.
- E...
  - Rubare i dati?
  - Implementare un bot? Un cryptojacker?
  - Ottenere l'accesso a un server?
  - Piazzare un ransomware?

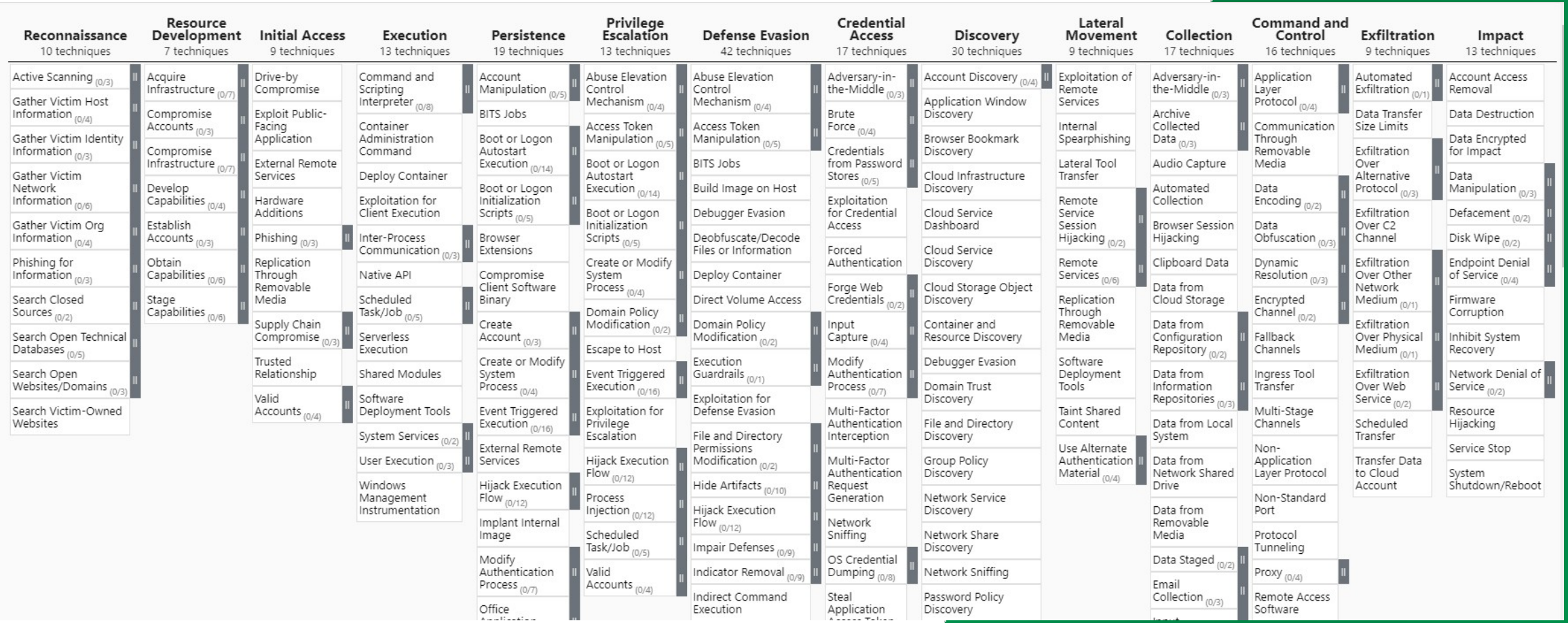
Vengono utilizzate diverse vulnerabilità Si

verificano diverse minacce

L'esito finale (impatto) è incerto

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Matrice MITTRE ATT&CK



Reconnaissance 10 techniques	Resource Development 7 techniques	Initial Access 9 techniques	Execution 13 techniques	Persistence 19 techniques	Privilege Escalation 13 techniques	Defense Evasion 42 techniques	Credential Access 17 techniques	Discovery 30 techniques	Lateral Movement 9 techniques	Collection 17 techniques	Command and Control 16 techniques	Exfiltration 9 techniques	Impact 13 techniques
Active Scanning (0/3)	Acquire Infrastructure (0/7)	Drive-by Compromise	Command and Scripting Interpreter (0/8)	Account Manipulation (0/5)	Abuse Elevation Control Mechanism (0/4)	Abuse Elevation Control Mechanism (0/4)	Adversary-in-the-Middle (0/3)	Account Discovery (0/4)	Exploitation of Remote Services	Adversary-in-the-Middle (0/3)	Application Layer Protocol (0/4)	Automated Exfiltration (0/1)	Account Access Removal
Gather Victim Host Information (0/4)	Compromise Accounts (0/3)	Exploit Public-Facing Application	Container Administration Command	BITS Jobs	Access Token Manipulation (0/5)	Access Token Manipulation (0/5)	Brute Force (0/4)	Application Window Discovery	Internal Spearphishing	Archive Collected Data (0/3)	Communication Through Removable Media	Data Transfer Size Limits	Data Destruction
Gather Victim Identity Information (0/3)	Compromise Infrastructure (0/7)	External Remote Services	Deploy Container	Boot or Logon Autostart Execution (0/14)	Boot or Logon Autostart Execution (0/14)	BITS Jobs	Credentials from Password Stores (0/5)	Browser Bookmark Discovery	Lateral Tool Transfer	Audio Capture	Data Encoding (0/2)	Exfiltration Over Alternative Protocol (0/3)	Data Encrypted for Impact
Gather Victim Network Information (0/6)	Develop Capabilities (0/4)	Hardware Additions	Exploitation for Client Execution	Boot or Logon Initialization Scripts (0/5)	Boot or Logon Initialization Scripts (0/5)	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking (0/2)	Automated Collection	Data Obfuscation (0/3)	Exfiltration Over C2 Channel	Data Manipulation (0/3)
Gather Victim Org Information (0/4)	Establish Accounts (0/3)	Phishing (0/3)	Inter-Process Communication (0/3)	Browser Extensions	Create or Modify System Process (0/4)	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services (0/6)	Browser Session Hijacking	Dynamic Resolution (0/3)	Exfiltration Over Other Network Medium (0/1)	Defacement (0/2)
Phishing for Information (0/3)	Obtain Capabilities (0/6)	Replication Through Removable Media	Native API	Compromise Client Software Binary	Domain Policy Modification (0/2)	Deobfuscate/Decode Files or Information	Forge Web Credentials (0/2)	Cloud Service Discovery	Replication Through Removable Media	Clipboard Data	Encrypted Channel (0/2)	Exfiltration Over Physical Medium (0/1)	Disk Wipe (0/2)
Search Closed Sources (0/2)	Stage Capabilities (0/6)	Supply Chain Compromise (0/3)	Scheduled Task/Job (0/5)	Create Account (0/3)	Escape to Host	Deploy Container	Input Capture (0/4)	Cloud Storage Object Discovery	Software Deployment Tools	Data from Cloud Storage	Fallback Channels	Exfiltration Over Web Service (0/2)	Endpoint Denial of Service (0/4)
Search Open Technical Databases (0/5)		Trusted Relationship	Serverless Execution	Create or Modify System Process (0/4)	Event Triggered Execution (0/16)	Direct Volume Access	Modify Authentication Process (0/7)	Container and Resource Discovery	Taint Shared Content	Data from Configuration Repository (0/2)	Ingress Tool Transfer	Scheduled Transfer	Firmware Corruption
Search Open Websites/Domains (0/3)		Valid Accounts (0/4)	Shared Modules	Event Triggered Execution (0/16)	Exploitation for Privilege Escalation	Domain Policy Modification (0/2)	Multi-Factor Authentication Interception	Debugger Evasion	Use Alternate Authentication Material (0/4)	Data from Information Repositories (0/3)	Multi-Stage Channels	Transfer Data to Cloud Account	Inhibit System Recovery
Search Victim-Owned Websites			Software Deployment Tools	External Remote Services	Hijack Execution Flow (0/12)	Execution Guardrails (0/1)	Multi-Factor Authentication Request Generation	Domain Trust Discovery		Data from Local System	Non-Application Layer Protocol		Network Denial of Service (0/2)
			System Services (0/2)	Hijack Execution Flow (0/12)	Process Injection (0/12)	Exploitation for Defense Evasion	Network Sniffing	File and Directory Discovery		Data from Network Shared Drive	Non-Standard Port		Resource Hijacking
			User Execution (0/3)	Implant Internal Image	Scheduled Task/Job (0/5)	File and Directory Permissions Modification (0/2)	OS Credential Dumping (0/8)	Group Policy Discovery		Data from Removable Media	Protocol Tunneling		Service Stop
			Windows Management Instrumentation	Modify Authentication Process (0/7)	Valid Accounts (0/4)	Hide Artifacts (0/10)	Steal Application Access Token	Network Service Discovery		Data Staged (0/2)	Proxy (0/4)		System Shutdown/Reboot
				Office		Hijack Execution Flow (0/12)		Network Share Discovery		Email Collection (0/3)	Remote Access Software		
						Impair Defenses (0/9)		Network Sniffing					
						Indicator Removal (0/9)		Password Policy Discovery					
						Indirect Command Execution							

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Identificazione del rischio. Scenari

Una possibile soluzione: definire degli scenari.

Uno scenario è un modo specifico per attaccare un sistema e ottenere un determinato risultato. Aiuta a fare chiarezza:

- Chi è l'attaccante
- Quali vulnerabilità vengono sfruttate
- Qual è l'impatto previsto.

In questo caso è possibile capire

- Quali controlli possono prevenirlo
- Quali sono gli asset interessati e in che modo.

Ma

- Esiste una quantità (quasi) infinita di scenari
- Non ci sono (quasi) statistiche disponibili per gli scenari
  - La maggior parte dei dati statistici disponibili si concentra sulle minacce.

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Identificazione del rischio. Attaccanti

Attaccante esterno

- Criminale informatico
- Terrorismo informatico
- Vandalo
- Sponsorizzato dalla nazione
- Virus/worm
- Hacktivista
- Spia industriale

Attaccante interno

- Abusivo
- Hacker

Cliente

malintenzionato

Attaccante fisico

Partner Utente

negligente Guasti

Ambiente

- Locale (inquinamento, riscaldamento, ecc.)
- Globale (terremoto, alluvione, ecc.)

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Minacce informatiche tipiche

Virus, worm e ransomware

I virus e i **worm** sono programmi dannosi che possono modificare il funzionamento e il comportamento del computer. I virus e i worm hanno meccanismi di propagazione indipendenti.

- Virus. Un utente deve consentire l'esecuzione di un virus. Ad esempio,
  - Aprire un allegato di posta elettronica dannoso
  - Consentire l'installazione di un programma infetto
  - Scaricare ed eseguire un file infetto
- Il worm si propaga autonomamente sfruttando le vulnerabilità dei servizi di rete.

Il ransomware è un malware che cripta i dati del computer compromesso, rendendo inutilizzabili i file e il sistema. Di solito, in seguito, viene richiesto un riscatto all'utente.

- Distribuito in diversi modi, tra cui virus e worm, ma può anche essere impiantato da un aggressore che dispone di sufficienti diritti di accesso al computer.

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Attacchi basati sul Web, attacchi alle applicazioni Web

Attacchi alle applicazioni Web - un'ampia serie di attacchi che mirano a sfruttare le vulnerabilità dell'interfaccia grafica e delle API del servizio (ad esempio, attacchi di SQL injection, Cross- Site scripting XSS). Mira a compromettere le applicazioni Web.

Attacco basato sul Web - un'ampia serie di attacchi durante i quali gli aggressori sfruttano le vulnerabilità della codifica per ottenere l'accesso a un server o a un computer. Mira a compromettere un sistema connesso a Internet.

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Attacco di comunicazione D(Dos)

(D) La minaccia **DoS** -Denial of Service mira a bombardare il servizio selezionato con un numero enorme di richieste che rendono il servizio non disponibile per gli utenti legittimi.

- Il Denial of Service (distribuito) utilizza una moltitudine di fonti (bot) che inviano richieste al servizio.

Attacco alla comunicazione - questa minaccia mira a intercettare o manomettere la comunicazione tra le vittime. L'attaccante può trovare un modo per decifrare la comunicazione (con crittografia assente o debole) o sfruttare le vulnerabilità dei protocolli non sicuri.

- Attacchi Man in the middle - un attaccante interrompe la comunicazione tra due vittime e costringe il traffico a passare attraverso di lui, con la possibilità di leggere o modificare la comunicazione.

Attacchi di social engineering Attacchi fisici

Ingegneria sociale - è un insieme di minacce che mirano a manipolare, influenzare e ingannare una vittima per indurla ad agire in un determinato modo (ad esempio, concedere l'accesso a un sistema informatico, condividere informazioni o credenziali segrete).

- **Phishing** - una tipica minaccia di ingegneria sociale che comunica con un utente tramite e-mail, messenger o altri mezzi di comunicazione.
- Gli attacchi di ingegneria sociale richiedono la presenza fisica
  - *Navigazione a spalla*: sbirciare la digitazione della password
  - *Immersione nei cassonetti*: cercate le password nella spazzatura
  - *USB drop* - lasciare che una chiavetta USB infetta venga prelevata e utilizzata da un dipendente.

Attacchi fisici: danni intenzionali all'hardware causati da aggressori (interni o esterni).

Manomissione - modifica fisica di un hardware per alterarne la funzionalità o ottenere l'accesso alla rete.

Insider

Abuser - un dipendente utilizza i propri diritti di accesso per compromettere il sistema. In genere, copia i dati al di fuori dei locali dell'azienda.

Insider attacker - un attaccante che beneficia dell'accesso iniziale al sistema ma che mira ad aumentare i propri privilegi attraverso la compromissione del sistema.

Ex dipendente - un ex dipendente che utilizza le proprie conoscenze sul sistema, le credenziali ancora valide e/o la backdoor precedentemente installata per .

Problema del partner client dannoso

Attaccante **malintenzionato**: un cliente che utilizza i servizi acquistati per sferrare un attacco all'utente o ai suoi clienti.

Cliente **illegale**: un cliente che utilizza il vostro servizio per scopi illegali (ad esempio, invio di spam, hosting di contenuti illegali, fornitura di servizi dannosi, ecc.)

Partner - un partner che attacca il sistema, utilizzando i suoi privilegi nel sistema.

Un **partner** potrebbe essere **compromesso**. L'hacker potrebbe voler attaccare il vostro partner per utilizzarlo come punto di appoggio per attaccare voi - attacco alla catena di approvvigionamento.

Negligenza dei dipendenti

Perdita o **furto di hardware** - una minaccia legata alla perdita fisica di un hardware. In genere, questa minaccia comporta la potenziale perdita di informazioni sensibili contenute in un dispositivo mobile (ad esempio, un computer portatile o un cellulare).

Danno fisico accidentale - un'azione accidentale di un dipendente che causa un danno fisico all'hardware. Ad esempio, il caffè versato su un computer portatile.

Errore logico accidentale - un errore accidentale o un'azione benevola che porta alla compromissione del sistema. Un errore tipico è la condivisione di dati sensibili (ad esempio, concedendo l'accesso a dati sensibili al pubblico o condividendo informazioni senza sapere che sono private).

Minacce tipiche del settore energetico

Ransomware

Iniezione di dati falsi

- segnalazione di dati errati/modificati

Violazione dei dati

Phishing e altre tecniche di dirottamento dell'account

- Accesso a sistemi/applicazioni IT (ad esempio, SCADA)
- Accesso ai dati

Malware

Stuxnet

May 2021
Ransomware attack on French producer of renewable energy
Albioma - Paris, France

27 November 2021
Ransomware at energy provider in Australia
CS Energy - Brisbane, Queensland, Australia

05 May 2021
Ransomware at Norwegian energy technology provider
Volue ASA is headquartered in Norway and was very open about the cyber attack.

Il 2015 Blackout in Ucraina

Hacker, attacco a Eni dopo il Gse. Massima allerta dell'intelligence

Attacco al gasdotto Colonial

March 15, 2022
Cyberattack on an energy provider in Spain
Iberdrola / I-DE Redes Eléctricas Inteligentes - Bilbao, Spain
This resulted in a breach of 1.3 million customer records.

April 25, 2022
1.1 million emails of a Russian service provider for the energy industry leaked
АЛЕТ (ALET) - Moscow, Russia

Il 2015 Blackout in Ucraina

March 2022
Hacker attacks on the power grid in the north of India
Ladakh, India
Affected are systems in the Ladakh region in the north of India.

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Minacce energetiche per AIC

Minaccia	Dati			Processo		
	Disponibile.	Integrità	Conf.	Disponibile.	Integrità	Conf.
Virus, worm, Ransomw.						
Attacchi basati sul web						
Applicazione web att.						
Comunicazione att.						
(D)Dos						
Ingegneria sociale (phishing)						
Attacco fisico						
Manomissione						

Minacce energetiche per AIC

Minaccia	Dati			Processo		
	Disponibile.	Integrità	Conf.	Disponibile.	Integrità	Conf.
Abusivo						
Insider/ Ex dipendente						
Cliente dannoso						
Cliente illegale						
Partner						
Perdita o furto						
Danno accidentale						
Errore accidentale (glitch)						

Vulnerabilità e controlli di sicurezza

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Vulnerabilità e controlli di sicurezza

Semplificazione dell'identificazione delle vulnerabilità:

- Mancanza di controlli di sicurezza= una vulnerabilità

incluso →

← impedisce

Bug specifico

Tecnico di basso livello
Difficile da ragionare

Tipo di bug

Generico di alto livello
Ragionamento più semplice

Controllo di sicurezza

"Facile" da identificare Generico
Elencati negli standard (ISO 27002, CSF, CIS)

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Controlli di sicurezza. ISO 27002

ISO (CIS)

Politiche organizzative

Gestione delle risorse

Conformità Rapporti con

i fornitori

Protezione fisica e ambientale Risorse umane

Controllo degli accessi Crittografia

Sicurezza delle comunicazioni

Sicurezza delle operazioni,

Acquisizione, sviluppo e manutenzione del sistema

Gestione degli incidenti Continuità

aziendale

Controlli di sicurezza. CSF NIST

NIST CSF

Identificare

- Gestione delle risorse, organizzazione, politiche, rapporti con i fornitori, conformità

Proteggere

- Protezione fisica e ambientale, risorse umane, controllo degli accessi, sicurezza delle operazioni, crittografia, sicurezza delle comunicazioni, acquisizione, sviluppo e manutenzione dei sistemi.

Rilevare

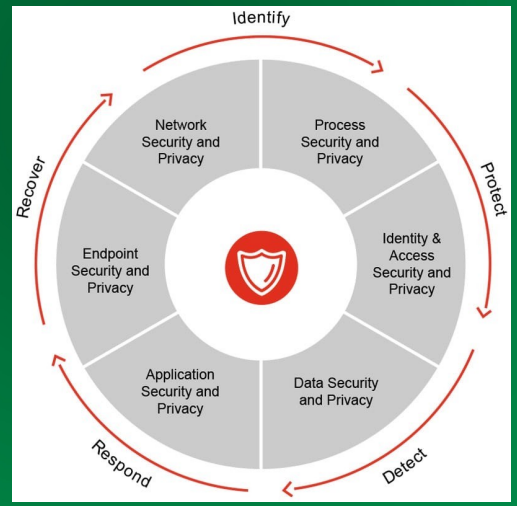
- Protezione del sistema

Rispondere

- Gestione degli incidenti
- Continuità aziendale

Recupero

- Gestione degli incidenti



CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Politiche

Una serie di politiche per la sicurezza informatica dovrebbe essere:

- Definito
- Approvato (dalla direzione)
- Pubblicato
- Comunicate ai dipendenti e alle parti esterne
- Revisione periodica

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Organizzazione

Definire i ruoli e le responsabilità Stabilire i

contatti con le autorità

Definire le politiche per l'uso dei dispositivi mobili e del telelavoro.

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Risorse umane

Eseguire lo screening dei candidati

Definire i termini e le condizioni contrattuali relativi alla sicurezza informatica.

Fare in modo che la direzione si assicuri che le politiche di sicurezza vengano seguite.

Educare e formare i dipendenti

Stabilire un processo disciplinare

Assicurarsi che la procedura di risoluzione del contratto includa le azioni di sicurezza richieste.

Gestione delle attività

Creare, mantenere e aggiornare l'inventario dei beni Definire il proprietario dei beni

Classificare le attività

Gestire i supporti rimovibili Smaltimento sicuro dei supporti Transizione sicura dei supporti fisici

Controllo degli accessi

Definire le politiche per il controllo degli accessi (in particolare, l'accesso alla rete IT).

Definire come registrare e de-registrare un utente

Definire le modalità di concessione o revoca dell'accesso formale

Gestione speciale dei diritti di accesso privilegiato

Specificare un processo di gestione formale per la gestione delle informazioni di autenticazione segrete e assicurarsi che gli utenti lo seguano.

Definire regole formali per la rimozione o la modifica dei diritti di accesso.

Assicurarsi che l'accesso sia concesso in base alle politiche di controllo degli accessi.

Stabilire procedure di accesso sicure e sistemi di gestione delle password.

Limitare l'accesso al codice sorgente.

Crittografia

Definire le politiche per l'utilizzo dei controlli crittografici

Definire le politiche per la gestione delle chiavi

- Come si usa
- Come proteggere
- Durata delle chiavi crittografiche

Protezione fisica e ambientale

Stabilire e proteggere il perimetro fisico Stabilire i controlli

fisici

- Uffici e altre strutture sicure

Stabilire le procedure per lavorare in aree sicure

Definire e implementare le procedure per la consegna e il carico

Implementare protezioni contro disastri naturali, attacchi dolosi e incidenti.

Proteggere e mantenere le apparecchiature, le utenze, i cavi, ecc.

Definire e seguire le procedure per lo smaltimento e la rimozione delle apparecchiature.

Definire politiche chiare per le scrivanie e gli schermi

Sicurezza delle operazioni

Definire le procedure e le responsabilità operative Implementare la protezione dalle minacce informatiche

Implementare procedure di back-up

Implementare procedure di registrazione e monitoraggio

Procedure definite per l'installazione di un software

Implementare procedure di gestione delle vulnerabilità

Pianificare attività di audit

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Sicurezza delle comunicazioni

Definire le procedure di gestione per il controllo della rete

Implementare e mantenere i meccanismi di sicurezza della rete (ad esempio, firewall, IDS/IPS, ecc.).

Segregare le reti (se necessario).

Definire come e quali informazioni possono essere trasferite

Definire le regole per la messaggistica elettronica

Definire i requisiti per gli accordi di riservatezza e di non divulgazione per lo scambio di informazioni.

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Acquisizione e sviluppo del sistema

Definire e implementare i requisiti di sicurezza per i nuovi sistemi informativi (in particolare, il modo in cui le applicazioni scambiano informazioni nelle reti pubbliche).

Definire regole per uno sviluppo sicuro

Definire e implementare il controllo sulle modifiche ai sistemi

Utilizzare principi di ingegneria di sistema sicuri

Ambiente di sviluppo sicuro Definire regole per lo

sviluppo in outsourcing

Utilizzare test di sicurezza e di accettazione del sistema

Rapporti con i fornitori

Definire le politiche di sicurezza per i fornitori

Garantire che i requisiti di sicurezza siano negoziati, concordati e rispettati dal fornitore.

Esaminare e monitorare il rispetto dei requisiti di sicurezza da parte del fornitore.

Gestione degli incidenti di sicurezza delle informazioni

Definire le responsabilità e le procedure per la risposta alle incidenze e garantirne l'esecuzione.

Stabilire procedure di segnalazione di eventi e punti deboli Garantire l'analisi e

la valutazione degli eventi di sicurezza.

Garantire l'esecuzione delle procedure per la risposta agli incidenti

Analizzare gli eventi verificatisi e applicare azioni per ridurre rischi simili in futuro.

Memorizzare le informazioni sugli verificatisi.

Continuità aziendale

Definire i requisiti, pianificare, implementare e rivedere le procedure di continuità operativa.

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Conformità

Identificare le legislazioni e gli accordi contrattuali da rispettare.

Identificare i diritti di proprietà intellettuale e proteggerli

Proteggere i dati di terzi in conformità con la legge (ad esempio, GDPR).

Seguire le normative sui controlli crittografici

Audit

Organizzare una revisione indipendente del vostro sistema di sicurezza informatica Garantire la conformità alle politiche o agli standard di sicurezza

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Strumenti e metodi

Ricerca desktop

Analisi dei documenti aziendali

- Strategia aziendale, strategia aziendale, diagrammi di flusso, assegnazione di ruoli,...
- Inventario dei beni
- Analisi dei log, analisi degli eventi passati, report (compresi quelli audit)...
- Rapporti di scansione delle vulnerabilità (Nessus, OpenVas)

Fonti esterne

- Analisi statistica (ENISA, IBM/Ponemon, Verizon, Accenture, NetDilligence, McAffee, Semantec, Deloitte, PwC, etc.)
- Centri di condivisione delle informazioni (ad esempio, CERT ISAC), rapporti, bollettini.

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Parlare con le persone

- Interviste - colloqui individuali con i principali stakeholder sullo stato attuale della pratica (responsabili della sicurezza, risorse umane, proprietari di risorse, ecc.)
- Workshop - discussione di gruppo con le persone coinvolte nella valutazione del rischio

Metodo Delphi - un metodo di previsione sistematico e interattivo che si basa sulla presa in considerazione dell'opinione di diversi esperti.

  - Gli esperti rispondono a un questionario (fornendo spiegazioni)
  - Le risposte sono riportate in forma anonima ad altri (con spiegazioni)
  - Gli esperti rispondono nuovamente al questionario (correggendo le loro risposte)
  - Fermarsi a un criterio predefinito (ad esempio, un numero fisso di round) e utilizzare il punteggio medio o la medina.

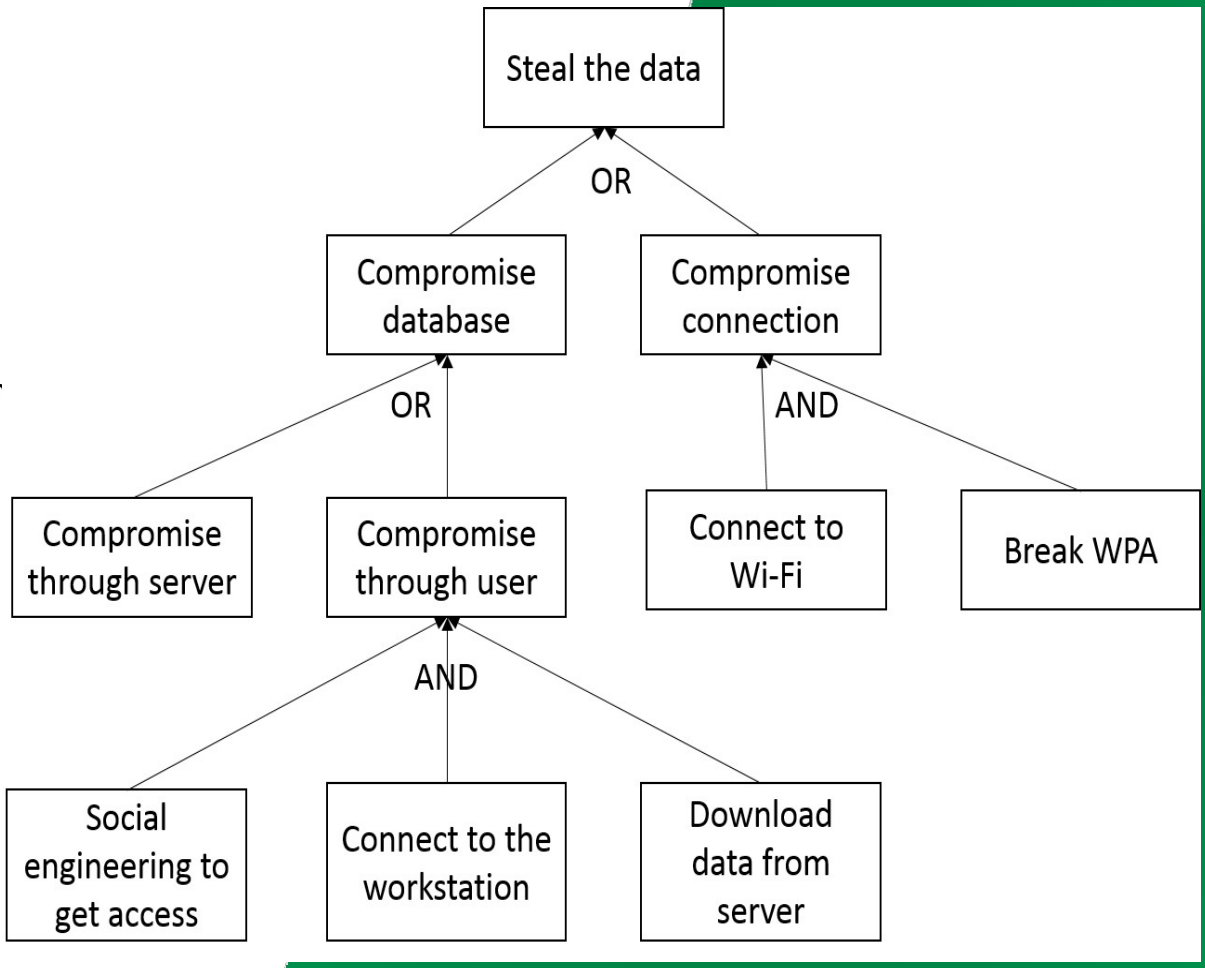
Albero d'attacco

L'albero degli attacchi è una tecnica utile per analizzare in modo strutturato e dettagliato una minaccia.

Iniziare con una possibile conseguenza indesiderata (nodo ir alto).

Scomporre il problema utilizzando gli operatori AND e OR in passi più dettagliati.

Ripetere l'operazione fino a raggiungere il livello di dettaglio desiderato.

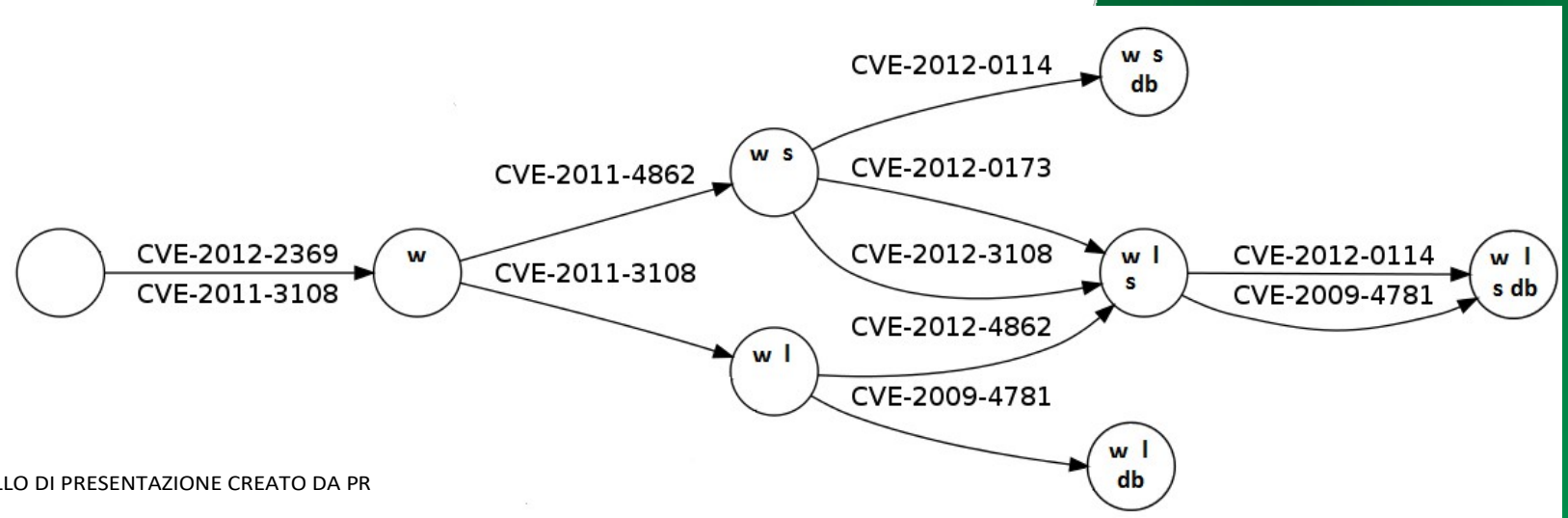


CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Grafico dell'attacco

Il grafo degli attacchi è una tecnica che mira a rappresentare tutti i percorsi (una sequenza di vulnerabilità esistenti da sfruttare) attraverso un sistema che un attaccante può seguire per raggiungere il suo obiettivo finale.

Dopo la scansione delle vulnerabilità, lo strumento di costruzione del grafico degli attacchi le collega in un grafico basato sulle condizioni pre e post per ogni vulnerabilità rilevata.



CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Analisi e valutazione del rischio

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Analisi del rischio quantitativa o qualitativa

Quantitativo

- Opera con un **significato** (reale) valori!
- Vengono definite le operazioni sui valori.
- Fornire risultati monetari (adatti a ulteriori analisi e riutilizzi)
- Difficile da usare

Perdita - misurata in euro [dollari, tugrik, ecc.]

Probabilità - valore reale positivo

Qualitativo

- Facile da lavorare
- Ampiamente utilizzato
- Ha bisogno della definizione di valore
- Necessita della definizione di operazioni

Perdita - {molto bassa, bassa, media, alta, molto alta}

Probabilità - {molto bassa, bassa, media, alta, molto alta}

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Analisi del rischio. Impatto

Una risorsa compromessa causa un impatto.

- L'impatto è stimato come perdita attesa da un singolo evento di minaccia.

Tenere in :

- Interruzione delle attività commerciali
- Perdita diretta
- Violazione di una normativa
- Violazione di un contratto
- Perdita di reputazione
- Perdita del cliente
- Costo della notifica
- Impatto sul personale/utente
- Indagine/recupero della perdita
- Perdita del vantaggio competitivo

Non dimenticate la dipendenza dalle risorse!

Analisi del rischio. Impatto

Dal punto di vista della sicurezza, è importante valutare le perdite dovute all'impatto su uno specifico aspetto della sicurezza:

- Riservatezza
- Integrità
- Disponibilità

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Analisi del rischio. Probabilità

Probabilità= Esposizione× Probabilità[Successo]

- Fonti di minaccia e contesto dell'organizzazione
- Controlli e vulnerabilità
- Competenze e statistiche

L'esposizione è per lo più esterna

- Influenzato dalle tendenze globali e dalla tipologia della vostra organizzazione

La probabilità è per lo più interna

- Interessati dalla vostra protezione

Stima del rischio. Calcolo

Formula generale:

- Rischio= Probabilità× Impatto

Minacce multiple (t) e risorse (a):

- Per attività: $Risk^{a}_{CIA} = \sum_{\forall t} Likelihood^{t} \times Impact^{a}_{CIA}$
- Per minaccia: $Risk^{t}_{CIA} = \sum_{\forall a} Likelihood^{t} \times Impact^{a}_{CIA}$

Stima del rischio. Calcolo del rischio. Qualitativo

	Cappuccio Likeli	**Molto basso**	**basso**	**medio**	**alto**	**Molto alto**
Impatto	**Molto basso**	0	1	2	3	4
	Basso	1	2	3	4	5
	Medium	2	3	4	5	6
	Alto	3	4	5	6	7
	Molto alto	4	5	6	7	8

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Privilegiare il rischio

Definire le priorità dei rischi in base ai criteri di valutazione.

Minacce	Impatto	Probabilità	Il rischio	Classifica
Minaccia A	Molto basso	Molto basso	0	5
Minaccia B	Molto alto	Medio	6	1
Minaccia C	Basso	Basso	2	4
Minaccia D	Molto basso	Alto	4	2
Minaccia E	Medio	Basso	3	3
Minaccia F	Alto	Basso	4	2

Esempio semplice

Consideriamo un sistema (SCADA) che gestisce il processo di trasmissione dell'energia.

In questo scenario, una grande quantità di punti di trasmissione riceve l'energia dalle linee elettriche, la elabora e la dirige ulteriormente. Tutti questi punti raccolgono varie informazioni.

I dati raccolti vengono poi comunicati al centro di gestione, dove vengono utilizzati per valutare lo stato del sistema di trasmissione dell'energia, reindirizzare l'energia in base alle esigenze, evitare situazioni pericolose (ad esempio, la trasmissione di troppa energia attraverso una specifica linea elettrica). Alcuni di questi dati vengono memorizzati nel database per un'analisi basata sullo storico.

Il segnale di controllo viene inviato al punto di trasmissione di potenza, dove gli attuatori regolano il funzionamento del punto.

Gli operatori interagiscono con il centro di gestione solo attraverso la GUI in locale.

Ambito di valutazione del rischio: il centro di gestione + tutti i punti di trasmissione Soglia di accettazione del

rischio: 3

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

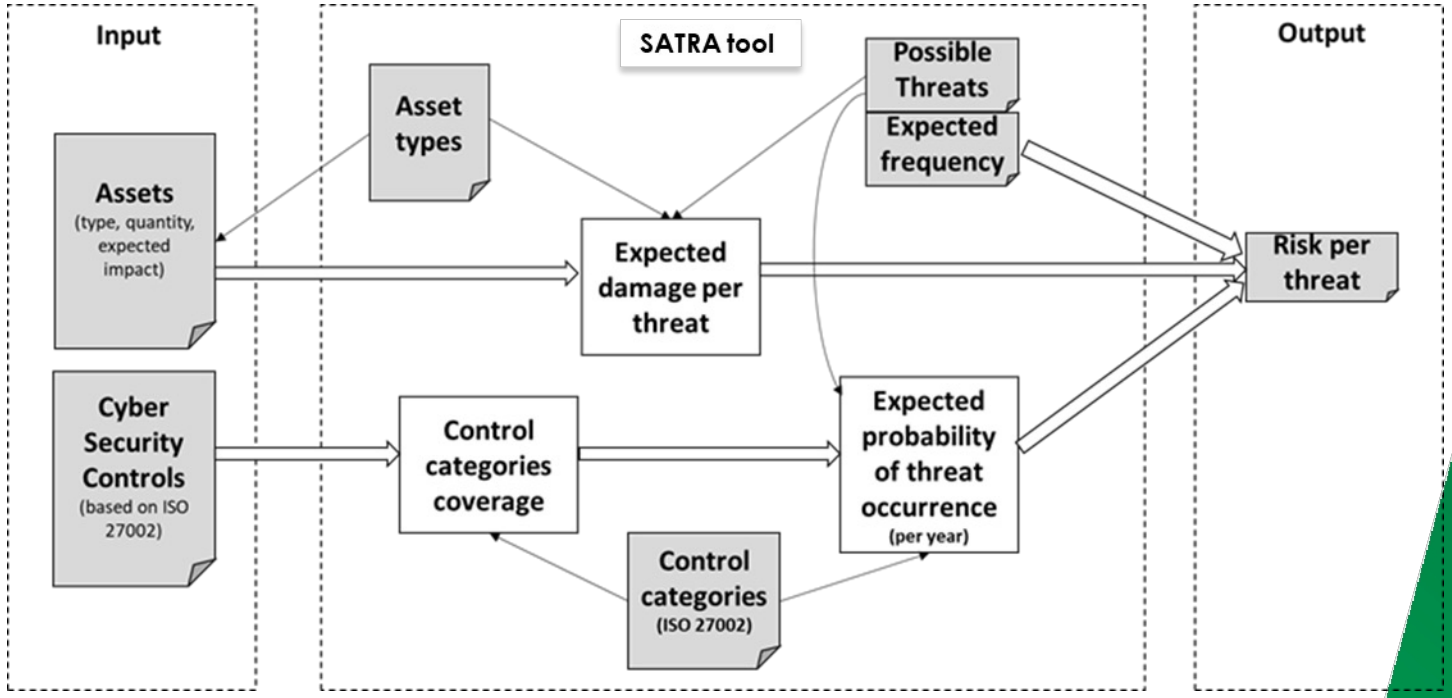
Esempio semplice. Analisi del rischio

	Valore
Descrizione della minaccia	Problema di comunicazione: Man-In-The-Middle. Un aggressore si avvicina fisicamente all'area dei punti di reindirizzamento dell'energia e inizia a inviare dati di monitoraggio falsi alla stazione centrale (bloccando i messaggi autentici), costringendola a indirizzare una quantità eccessiva di energia in questa parte della rete elettrica e a danneggiare le apparecchiature.
Attaccante	Vandalo / Sponsorizzato dalla nazione / Terrorista informatico
Vulnerabilità	Protezione crittografica assente o scarsa dei canali di comunicazione
Livello di probabilità	**medio**
Attività interessate	Dati di controllo - bloccati / modificati durante la trasmissione Processo di controllo - funzionamento errato a causa di dati falsificati Processo di trasmissione di potenza - efficienza impattata o prevenzione della trasmissione di potenza in caso di danni alle apparecchiature
Livello di impatto	**medio**
Il rischio	4
Rischio accettato?	No
Controlli suggeriti	Comunicare i dati solo in forma criptata. Utilizzare protocolli sicuri che prevedano meccanismi di autenticazione dei mittenti e dei destinatari dei dati. Implementare meccanismi di salvaguardia che impediscano la distribuzione di energia potenzialmente pericolosa.

SATRA

SATRA - Strumento di autovalutazione per l'analisi del rischio

L'obiettivo principale è quello di offrire un metodo semplice e veloce per l'autovalutazione del rischio informatico e la pianificazione della mitigazione.



SATRA. Sicurezza Controlli

Questionnaire

Please, answer all questions selecting the most suitable answer from the lists of available answers. Then press Submit.

Page 1/14. Information security policies

Management Direction For Information Security

Are policies for information security defined?
- ○ No
- ◉ Yes

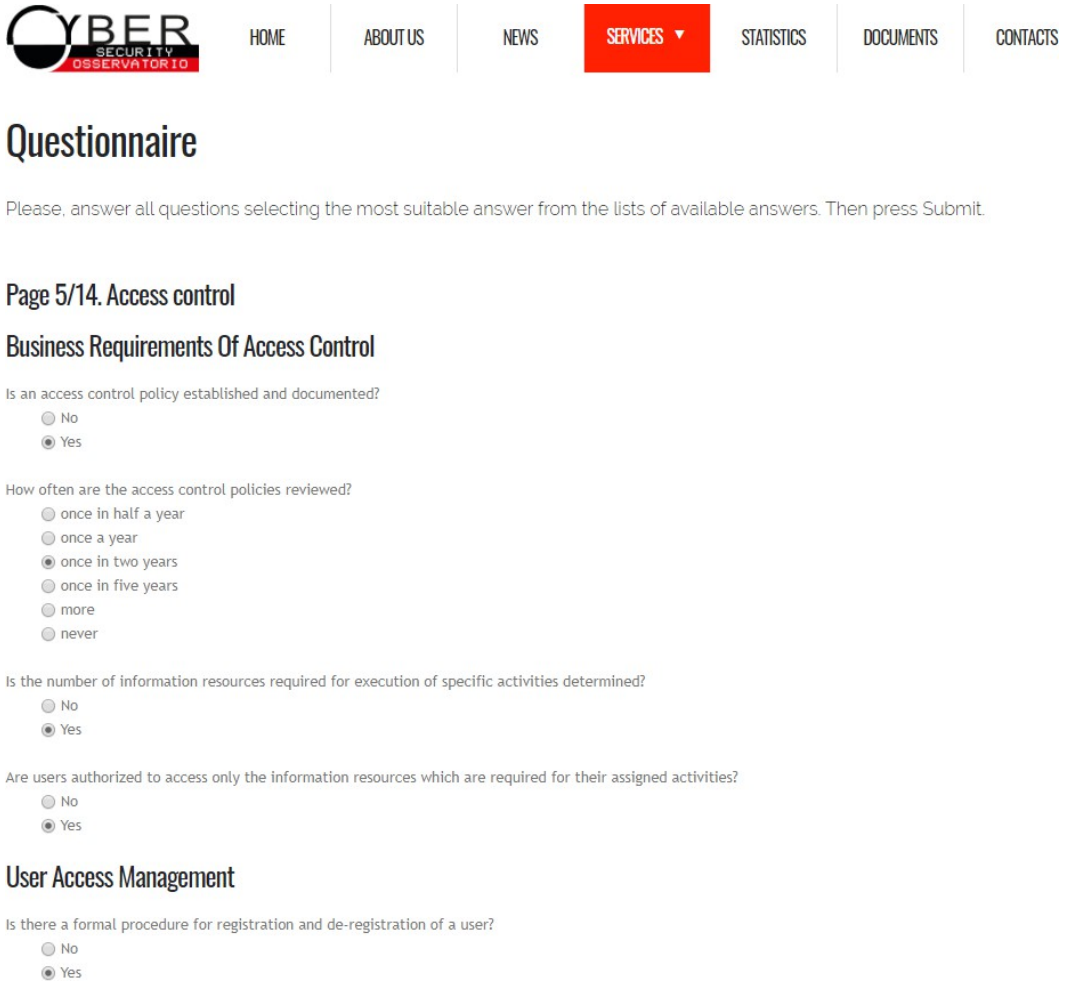
Are policies for information security approved by management?
- ○ No
- ◉ Yes

Are policies for information security published and available for the relevant parties?
- ○ No
- ◉ Yes

Are all employees obliged to study the policies and commit to fulfilling them (e.g., sign an official commitment paper)?
- ○ none
- ○ IT security Staff
- ◉ IT staff
- ○ IT users
- ○ all employees

Are all external parties obliged to study the policies and commit to fulfilling them (e.g., sign an official commitment paper)?
- ○ No
- ◉ Yes

SATRA. Sicurezza Controlli



SATRA. Attività

Asset Identification

ID	Asset	Asset Type	Number of Units	Confidentiality Damage (€)	Integrity Damage (€)	Availability Damage (€)
A1	VMWare	Critical Applications	1	0.0	10000.0	5000.0
A2	Management configuration	Technical documentation	1	500.0	50.0	50.0
A3	Private data of employees	Private records	20	100.0	10.0	20.0
A4	Router Cisco ASR 9k	Auxiliary equipment	1	1000.0	500.0	2000.0
A5	Financial documents	Private records	1	1000.0	500.0	200.0
A6	Contracts	Private records	100	40.0	10.0	10.0
A7	VM OSs	Critical Applications	75	0.0	200.0	200.0
A8	firmware firewall	Private records	1	1000.0	2000.0	3000.0
A9	Services	Web Applications	75	0.0	1000.0	2000.0
A10	Logs DB	Audit/logs	1	1000.0	500.0	200.0
A11	Firmware routers and switches	Auxiliary equipment	6	0.0	500.0	2000.0
A12	Firewall cisco ASA	Private records	1	1000.0	2000.0	3000.0
A13	Service configuration info	Technical documentation	75	200.0	50.0	50.0
A14	Operational data	Private records	20	10.0	40.0	10.0

CREATE ROW DELETE ROW SUBMIT

SATRA. I risultati

Overall Risk

104055.34€

GO TO MITIGATIONS PAGE

Threat title	Risk
web application attacks	25549.72
malware	6643.02
Environmental damage	1191.74
Phishing	4601.79
Physical damage	520.04
System glitch	635.2
Onsite penetration/tempering	4721.53
Communication break	6650.44
Malicious client	5039.01
(D)Dos	8161.62
Employee Negligence	7781.87
Insider Threat	2425.3
System inappropriateness	2050.59
Social engineering attacks	5161.09
Mechanical failure	1702.56
Hardware theft	2120.93
Third Party Problems	6101.59
web based attacks	1672.02
Spam/Infected email	4213.03
ransomware	7112.17

SATRA

Breve demo

Trattamento del rischio informatico

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Trattamento del rischio

Evitare i rischi

- non svolgere attività rischiose

Attenuazione (riduzione) del rischio

- Prevenire/ridurre l'insorgere di minacce o perdite

Trasferimento del rischio

- Assicurazione

Accettazione del rischio (ritenzione/tolleranza)

- Beh... ok.

Trattamento del rischio. Riduzione

Il rischio può essere ridotto in 3 modi:

- Ridurre l'esposizione alle minacce
  - Molto difficile!
  - Non irritare le persone.

- Ridurre la probabilità di minaccia
  - Protezione da malware, protezione della rete, crittografia, gestione degli incidenti

- Ridurre l'impatto delle minacce
  - Piano di continuità aziendale, Back-up, Gestione degli incidenti

Trattamento del rischio. Costo-beneficio Analisi

Analisi costi-benefici

- $Benefit = Risk_{before} - Risk_{after} - Cost$

Rendimento dell'investimento (in titoli)

- $RO\ (S)I = \frac{Risk\ \ before\text{-}Risk_{after}}{Cost}$
- Per l'approccio greedy

Scelte multiple? Possibile soluzione: soluzione di un problema simile a quello dei sacchi a pelo:

- Selezionare un insieme di possibili controlli per
  1. Ridurre al minimo il rischio
  2. Mantenere i costi entro il budget

Trattamento del rischio. Analisi del trade-off. Semi-quantitativo

		Tradeoff Attributes				
		Ease of Maintenance	Purchase Cost	Vulnerability	Productivity Impact	Tradeoff Ranking
Security Technology	Rank	w = .10	w = .25	w = .35	w = .30	$\Sigma w_i v_i(x_i)$
	Vulnerability Assessment Scanner	25	25	40	0	.20
	Secure Email	40	35	20	0	.24
	Smart Card	25	15	30	60	.34
	E-Signature	10	25	10	40	.22

S. Butler "Metodo di valutazione degli attributi di sicurezza: un approccio costi-benefici". Conferenza internazionale sull'ingegneria del software, 2002

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Trattamento del rischio. Evitare il rischio

Cercare di ridurre il

rischio Cercare di

trasferirlo

Se il rischio è ancora troppo alto per ...

Chiudere l'attività che ha portato a questo rischio.

Ad esempio,

- non utilizzare un sistema cloud (ad esempio, se non si hanno le competenze per configurarlo correttamente) oppure
- non affidare la codifica a sviluppatori sconosciuti

Trattamento del rischio. Trasferimento del rischio

Trasferire l'attività ad un altro ente (responsabile della gestione del rischio).

- Sicurezza gestita
- Nuvola
- Esternalizzare lo sviluppo

Ma è difficile trasferire la responsabilità

Assicurazione

- Acquistate un'assicurazione per coprire i rischi che non potete accettare.

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Trattamento del rischio. Accettazione del rischio

Opzione predefinita, ma è necessario essere consapevoli di questa decisione.

Guidati dai criteri di accettazione

Possiamo essere coperti dall'autoassicurazione

Se non si può accettare il rischio - ripianificare il piano di trattamento del rischio

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Gestione del rischio. Altre attività

Comunicazione e consultazione

- Comunicare con le parti interessate
- Consultare esperti esterni

Monitoraggio e revisione

- Monitoraggio dei valori definiti
- Rivedere regolarmente i risultati della valutazione del rischio (o quando vengono rilevati errori gravi).

Registrazione e reporting

- Registrare i risultati per un uso futuro
- Riportare i risultati della valutazione del rischio

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Conclusioni

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Conclusione

- La valutazione dei rischi è una pratica importante per la sicurezza di un sistema informatico.
- La valutazione del rischio richiede:
  - Buona pianificazione
  - Tempo
  - Sforzo
  - Buona conoscenza del sistema informatico
  - Ottima conoscenza della sicurezza informatica
  - Esperienza nella gestione del rischio
- Esistono altri modi per trattare i rischi
  - Non solo riduzione del rischio

Riferimenti e fonti

CSP003_S_E: Artsiom Yautsiukhin (CNR), Cristina Alcaraz (UMA)

Riferimenti e fonti

1. Alcune cifre sono state attribuite da Vecteezy, URL: https://www.vecteezy.com/ - grazie!
2. DeepL Traduttore per la correzione di bozze.
   URL: https://www.deepl.com/translator
3. ENISA, CIRAS, 2024
   URL: https://ciras.enisa.europa.eu
4. MITRA, MITRA CVE, 2024
   URL: https://cve.mitre.org
5. Fonte della figura: MITRE, MITRE CVE, 2024
   URL: https://cve.mitre.org/cgi-bin/cvekey.cgi?keyword=modbus
6. Fonte: NIST, NVD, 2024
   URL: https://nvd.nist.gov
7. Zografopoulos, Ioannis, Nikos D. Hatziargyriou e Charalambos Konstantinou. "Prospettive di cybersicurezza delle risorse energetiche distribuite: Vulnerabilità, attacchi, impatti e mitigazioni", IEEE Systems Journal (2023).

Connettersi con CyberSecPro: come registrarsi e altre informazioni pratiche

1. Sito web: www.cybersecpro-project.eu
2. X (Twitter): https://twitter.com/CyberSecPro_eu
3. LinkedIn: https://www.linkedin.com/company/cybersecpro-euproject/

Grazie

Se avete domande, non esitate a contattarci:

- Artsiom Yautsiukhin
  artsiom.yautsiukhin@iit.cnr.it
- Cristina Alcaraz
  alcaraz@uma.es
- Javier Lopez
  javierlopez@uma.es