UNIVERSITAT POLITÈCNICA DE VALÈNCIA

Ciberconciencia Situacional

2024/2025

Francesco Lorenzoni
PCA25403GU

Trabajo 4

Defending a Smart Grid from a Cyber Attack

Contents

Chapter 1

Tarea 4

Tarea a realizar

Visualiza el siguiente vídeo: youtube.com/watch?v=8edHD2o0pao

Contesta a las siguientes preguntas:

- ◇ Explica las medidas que propone el video para securizar un sistema de Smart Grid
- ◇ Sugiere alguna medida adicional no recogida en el vídeo

1.1 Introducción

La *"low voltage smart grid"* es un soft target que es de importancia crítica para el suministro de *Energía Sostenible* y las *DSO's Billing Operations* ("Operador del Sistema de Distribución").

Ejemplos de tales operaciones incluyen la gestión de recursos energéticos distribuidos (DERs), recarga de vehículos eléctricos (EV), y sistemas de gestión energética del hogar (HEMS).

1.2 Medidas para Asegurar una Smart Grid

El vídeo sugiere seis pasos clave que deben tomar todas las partes involucradas en el suministro para ser robustas frente a ciberataques:

1. "**Regulatory compliance** and **protection** should be considered the *minimum*, not the *desired* level of security"
   Esto ayuda a pensar como un cibercriminal y anticipar sus acciones.
2. "Don't trust **optionality** in security
   Los cibercriminales buscan medidas de seguridad *opcionales* para explotar. Si una medida de seguridad es opcional, es probable que sea ignorada por algunas partes, lo que puede conducir a vulnerabilidades, potencialmente permitiendo a los criminales infiltrarse y desactivar incluso las medidas de seguridad obligatorias.
3. "Don't assume your security is **unique** and that this protects you"
   Los cibercriminales siempre tienen varias herramientas a su disposición, y no dudarán en usarlas. Incluso si piensas que tus medidas de seguridad son únicas, aún pueden ser evadidas por un atacante determinado.
   Los DSO deberían realizar **Pruebas de Penetración** (PT) regularmente para evaluar la eficacia de sus medidas de seguridad, preferiblemente por probadores con experiencia en redes inteligentes de baja tensión.[1]
4. "*Invest* in **threat detection and response**"
   Esto permitiría al equipo de seguridad centrarse en los ataques organizados, como ataques de Ransom o de Denial of Service (DoS), que son más propensos a tener éxito y causar daños significativos.
   Además, una detección robusta es síntoma de *"saber lo que pasa"*, es decir, *Ciberconciencia Situacional*, que es un elemento clave de cualquier estrategia de seguridad.
5. "Provide an effective **deterrent**"
   Explotar las capacidades de detección y respuesta para disuadir a los cibercriminales y construir un conjunto de evidencias contra ellos.
   Esto se puede lograr implementando medidas como **Honeypots** y **Honeynets**, que están diseñadas para atraer

[1] low voltage smart grids

y atrapar a los cibercriminales, permitiendo a los equipos de seguridad recopilar información sobre sus tácticas y técnicas.

6. "**Integrate** your low voltage smart grid with your **corporate security**"
   Esto permitiría al equipo de seguridad tener una visión holística de la postura de seguridad de la organización, facilitando la identificación de ataques multipunto y la coordinación de la respuesta a los mismos.

En última instancia, el vídeo nos recuerda que todos somos víctimas potenciales de ciberataques, sin importar lo débiles o fuertes que sean nuestras medidas de seguridad.
Al fin y al cabo, el punto clave es tener personas, organizaciones y tecnologías en tu organización que puedan pensar como un cibercriminal.

1.3 Medidas Adicionales

Además de las medidas propuestas en el vídeo, existen otras estrategias complementarias que podrían fortalecer significativamente la seguridad de una Smart Grid:

1. **Implementación de blockchain**: Esta tecnología puede proporcionar una capa adicional de seguridad para la autenticación de transacciones energéticas y la protección de datos de medición, creando un registro inmutable de todas las operaciones.
   Esto es un poco más difícil de exploitar por un atacante, y podría ayudar a garantizar la integridad de los datos al menos para algunas operaciones, contrarrestando el riesgo de manipulación de datos..

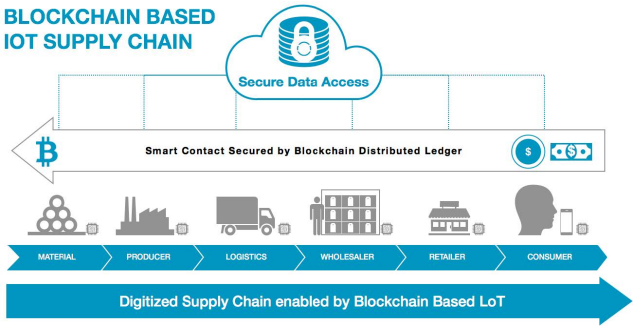

Figure 1.1: Ejemplo de blockchain tracked supply chain

2. **Segmentación de red avanzada**: Dividir la red en zonas aisladas para contener posibles brechas de seguridad, limitando el movimiento lateral de los atacantes mediante técnicas de microsegmentación.
   Se supone que esto está sobreentendido en el vídeo, pero aun así es importante mencionarlo.

3. **Simulación del estado esperado de la red**: Simular el estado esperado de la red para detectar desviaciones que puedan indicar un ataque en curso. Esto puede incluir la monitorización de patrones de tráfico y el uso de inteligencia artificial para identificar anomalías.
   Algo similar a lo que se hace para sistemas idraulicos con `epanetCPA`, pero aplicado a la red eléctrica.
   Esto se puede juntar a medidas de analisis de riesgo dinámico, que permiten actualizar continuamente la evaluación de riesgos basándose en datos en tiempo real sobre amenazas, vulnerabilidades y cambios en la infraestructura.

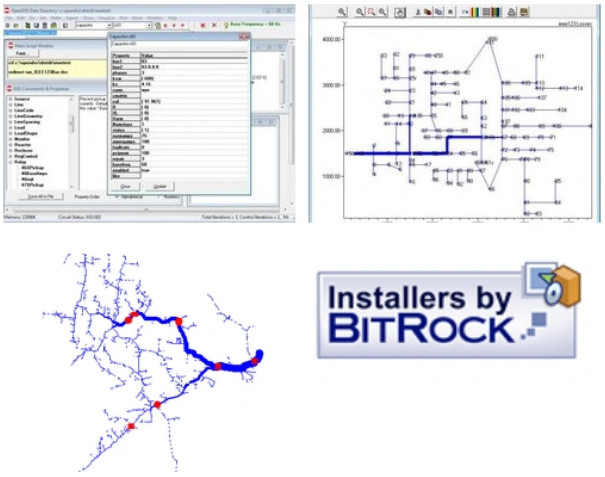

Figure 1.2: OpenDSS, un simulador de sistemas eléctricos de distribución.

4. **Asegurar autenticación y autorización robustas para activos críticos**: Implementar autenticación multifactor (MFA) y controles de acceso basados en roles para garantizar que solo los usuarios autorizados puedan acceder a sistemas críticos.

5. **Modelado de Attack Graphs específicos para Smart Grids**: Desarrollar representaciones gráficas que muestren cómo los atacantes podrían explotar vulnerabilidades interconectadas en sistemas SCADA, medidores inteligentes y redes de comunicación, facilitando la identificación de puntos críticos de fallo.

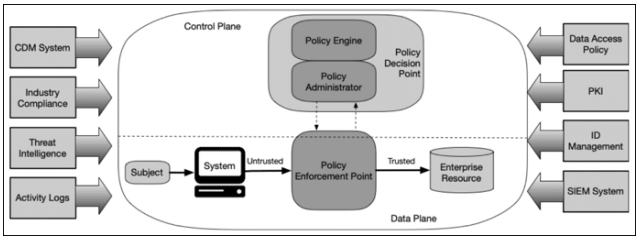

Figure 1.3: Ejemplo de Zero Trust Architecture (ZTA), un paradigma de seguridad que asume que las amenazas pueden estar tanto dentro como fuera de la red, y por lo tanto requiere autenticación y autorización estrictas para cada acceso a recursos.

6. **Actualizaciones de firmware automatizadas y seguras**: Desarrollar mecanismos de actualización automática con verificación criptográfica para mantener todos los dispositivos de la red actualizados contra vulnerabilidades conocidas, incluyendo sistemas de rollback en caso de fallos.
   Esto suele ser especialmente complicado en dispositivos IoT y Legacy, pero es crucial para mantener la seguridad a largo plazo.
7. **UEBA** (*User and Entity Behavior Analytics*) para Smart Grids: Implementar sistemas que establezcan líneas base de comportamiento normal para detectar anomalías que podrían indicar compromisos de seguridad, especialmente en dispositivos IoT y sistemas SCADA.
   Dado que las redes inteligentes tienen probablemente un conjunto estándar de operaciones, ésta podría ser una buena forma de detectar anomalías en el sistema y, por tanto, posibles ataques.
8. **Planificación de continuidad de negocio específica para ciberataques**: Desarrollar planes específicos de recuperación ante desastres cibernéticos que incluyan procedimientos de operación manual temporal y criterios claros para la reconexión de sistemas tras un ataque.

9. **Aislamiento físico de sistemas críticos**: Mantener sistemas de control críticos en redes físicamente separadas (*air-gapped*) cuando sea posible, especialmente para operaciones de protección y control de emergencia.

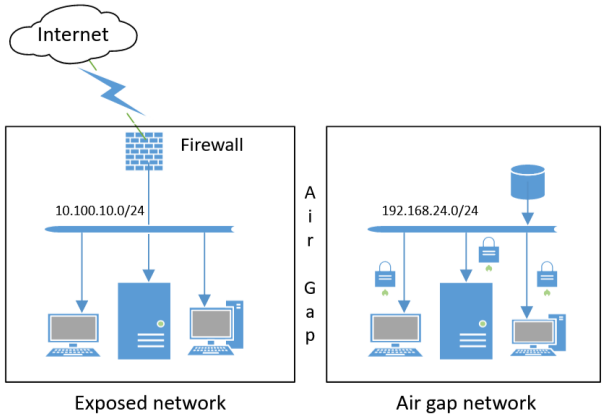

Figure 1.4: Air Gapped network topology example.

10. **Implementación de un Common Operational Picture (COP) para Smart Grids**: Establecer una vista única y compartida de la situación operativa que integre datos de la red eléctrica, sistemas de control y sensores de seguridad, permitiendo que todos los operadores tengan la misma conciencia situacional en tiempo real.
    Esto se relaciona con la integración de la red inteligente con la seguridad corporativa mencionada en el vídeo, pero se centra más en la creación de una imagen operativa común que facilite la toma de decisiones informadas y coordinadas.

Estas medidas adicionales, junto con las mencionadas en el vídeo, conformarían una estrategia de defensa en profundidad más robusta, aumentando significativamente la resiliencia de la Smart Grid frente a ciberataques cada vez más sofisticados.