Metodologías de la Investigación

Sistemas de seguridad empresarial

Tema de Investigación: "Vulnerabilidades y Mitigación de Riesgos en los Sistemas de Seguridad Empresarial: Un Estudio de Caso del Ataque de Ransomware en PAMI"

ÁREA DE INTERÉS: Tecnología y Ciberseguridad

Motivaciones/Razones:

Este tema de investigación me interesa debido a la creciente importancia de la ciberseguridad en el entorno empresarial actual. Los ataques de Ransomware, como el que afectó a PAMI, representan una amenaza seria para la seguridad de la información y la continuidad de las operaciones empresariales. A través de esta investigación, deseo comprender mejor las vulnerabilidades subyacentes en los sistemas de seguridad empresarial y explorar formas efectivas de mitigar los riesgos asociados con estos ataques.

Factibilidad/Dudas:

A FAVOR: Tengo acceso a una amplia gama de recursos en línea y literatura académica que abordan temas de ciberseguridad y ataques de Ransomware. Además, el estudio de caso de PAMI proporciona un ejemplo concreto para analizar las vulnerabilidades y las medidas de mitigación.

DUDAS/DIFICULTADES: Puede ser un desafío acceder a información específica sobre los detalles técnicos del ataque de Ransomware en PAMI debido a la naturaleza sensible del incidente. Además, podría ser difícil evaluar completamente las medidas de mitigación implementadas por PAMI sin acceso directo a su infraestructura de seguridad.

Fuentes de interés:

Mi interés en el tema de la ciberseguridad ha sido alimentado por diversas fuentes que han influido en mi ruta de aprendizaje. Algunas de estas influencias incluyen:

- Experiencias personales: Mi interés en el tema de la ciberseguridad se ha forjado a lo largo del tiempo, pero adquirió mayor relevancia cuando experimenté en carne propia la vulnerabilidad digital. El año pasado, mi cuenta de Twitter e Instagram fue hackeada, lo cual me llevó a tomar medidas más rigurosas para asegurar mi presencia en línea. Este evento personal subrayó la necesidad apremiante de comprender y abordar las amenazas cibernéticas, impulsándome a investigar y aprender en profundidad sobre la ciberseguridad.
- Formación personal: Mi formación se centra en los fundamentos de Linux y redes, y estoy en medio de un curso de preparación para la certificación en ciberseguridad (eJPT). Esta certificación abarcará conceptos profundos de redes, habilidades manuales de seguridad en aplicaciones web, el uso de Metasploit para ataques simples y análisis de protocolos

en capturas de tráfico. Además, aprenderé técnicas de recopilación de información y entenderé el proceso de pruebas de penetración. Este proceso de formación está fortaleciendo mi comprensión de la ciberseguridad y me está preparando para enfrentar los desafíos del entorno digital actual. Estoy entusiasmado por aplicar estos conocimientos y contribuir al campo de la ciberseguridad en el futuro.

Producir Conocimiento:

Ítems de interés que me gustaría explorar para producir conocimientos:

1. ¿Cómo han evolucionado los grupos de Ransomware, como Rhysida, desde su aparición reciente y cómo se están adaptando para atacar a entidades públicas y organizaciones de diferentes países y sectores, como se evidencia en el ataque al PAMI?
2. En base a los métodos de propagación del Ransomware y el reciente ataque al PAMI, ¿cómo podrían las organizaciones mejorar sus estrategias de educación y capacitación para sus empleados, con el objetivo de prevenir y detectar con éxito intentos de phishing y otros vectores de ataque similares?
3. ¿Cuál es el impacto real y potencial de un ataque Ransomware en una organización, como se observa en el caso del PAMI, en términos de la pérdida de datos, la interrupción de servicios esenciales y la exposición de información confidencial? ¿Qué medidas concretas pueden implementarse para mitigar estos riesgos y responder de manera efectiva a tales incidentes de seguridad cibernética?

Estas preguntas exploran diferentes aspectos del ataque Ransomware al PAMI y brindan la oportunidad de profundizar en la comprensión de las amenazas cibernéticas y las estrategias de defensa.