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

Trabajo Práctico N° 3

Antecedentes: Estado de la cuestión

Consignas:

1) En Google académico buscar 10 artículos, capítulo de libro, libro, manual, etc. referidos a mi tema objeto de investigación
2) Selecciona tres referidos al tema objeto de mi investigación.
3) Elaborar un escrito de una carilla destacando como ha sido abordado por otros investigadores, que aspectos han sido desarrollados y que otros no. En relación a ello Elaborar mi propia fundamentación respecto a la innovación/desarrollo que quiero hacer.

Los tres artículos abordados presentan aspectos importantes de la ciberseguridad desde diferentes perspectivas. A continuación, presentaré una síntesis de cómo han sido abordados por otros investigadores y los aspectos que han sido desarrollados en relación con cada artículo.

Artículo 1: "Ransomware y Seguridad Informática"

Este artículo se enfoca en el Ransomware y su impacto en la seguridad informática. Los aspectos destacados y desarrollados por otros investigadores incluyen:

- Definición del Ransomware y sus modalidades de ataque.
- Implicaciones legales y técnicas de los ataques de Ransomware.
- Estrategias de prevención y respuesta a los ataques.

Aspectos adicionales que podrían ser abordados, como:

- Un enfoque más detallado en técnicas específicas utilizadas por los ciberdelincuentes.
- Estadísticas actualizadas sobre la prevalencia y la evolución del Ransomware.
- Desarrollo de soluciones técnicas avanzadas para la detección y prevención.

Artículo 2: "Formación y Concienciación en Ciberseguridad"

Este artículo resalta la importancia de capacitar al personal no técnico en ciberseguridad. Aspectos destacados y desarrollados por otros investigadores incluyen:

- La necesidad de concienciación en ciberseguridad en todos los niveles de la organización.
- La identificación de errores humanos como una amenaza importante.
- La propuesta de modelos de competencias como enfoque.

Sin embargo, aún hay oportunidades para innovar:

- Desarrollo de métodos de formación más efectivos y personalizados.
- Investigación sobre la eficacia a largo plazo de la concienciación en ciberseguridad.
- Evaluación de la adaptabilidad de los modelos de competencias en diferentes contextos organizativos.

Artículo 3: "Modelo de Auditoría de Ciberseguridad (CSAM)"

Este artículo propone un modelo de auditoría de ciberseguridad integral. Aspectos destacados y desarrollados por otros investigadores incluyen:

- La importancia de la gestión de riesgos en ciberseguridad.
- La aplicación del modelo en diferentes contextos organizativos.
- Resultados que respaldan la efectividad del CSAM.

Para avanzar en esta área, podría considerar:

- Desarrollar herramientas o software específicos para implementar y automatizar el CSAM.
- Investigar cómo el CSAM podría aplicarse a nivel nacional y en diferentes industrias.
- Explorar métricas de ciberseguridad más avanzadas para evaluar la madurez cibernética.

Innovación Propia:

Dado el panorama actual de amenazas cibernéticas en constante evolución, podría considerar enfocarme en el desarrollo de sistemas de detección y respuesta temprana de Ransomware que utilicen técnicas avanzadas de inteligencia artificial y aprendizaje automático. Esto podría incluir la detección de comportamientos anómalos en tiempo real y la identificación de patrones de Ransomware antes de que causen un daño significativo.

Además, podría investigar la creación de un marco de gestión de incidentes de Ransomware que permita una respuesta coordinada y eficiente ante un ataque, incluyendo la comunicación con las autoridades pertinentes y la preservación de evidencia digital para futuras investigaciones.

En resumen, esta innovación podría centrarse en el desarrollo de soluciones técnicas avanzadas y enfoques más efectivos para prevenir, detectar y responder a ataques de Ransomware, teniendo en cuenta la dinámica cambiante de las amenazas cibernéticas y la necesidad de una respuesta rápida y coordinada.

Bibliografía:

Ransomware: seguridad, investigación y tareas forenses

Auditorías en ciberseguridad: un modelo de aplicación general para empresas y naciones

Formación y concienciación en ciberseguridad basada en competencias: una revisión sistemática de literatura