Capítulo extraído del libro "**Análisis funcional de sistemas y tecnologías de la información**" de Aníbal Mario Mazza Fraquelli (2025) **ISBN 978-987-26981-3-3**.

Virus y Malware: Amenazas Digitales en los Sistemas de Información

Presentación del tema

Los virus, troyanos, gusanos, spyware y otras formas de malware constituyen categorías de software malicioso diseñadas para infiltrarse, dañar, alterar o explotar sistemas de información sin el consentimiento del usuario. En el contexto de las Tecnologías de la Información (IT), el malware (Malicious Software) representa una de las principales amenazas para la continuidad operativa, la integridad de los datos y la seguridad organizacional.

El malware puede afectar hardware, software, redes, bases de datos y dispositivos móviles, impactando directamente en la infraestructura tecnológica que sostiene los procesos organizacionales. Para los estudiantes de la Licenciatura en Administración, comprender la naturaleza, el funcionamiento y el impacto del malware implica reconocer que los riesgos digitales no son exclusivamente técnicos, sino estratégicos: una infección masiva puede paralizar operaciones, comprometer datos sensibles, generar sanciones regulatorias y afectar la reputación corporativa.

Clasificación del malware

Virus informáticos. Un virus se inserta en archivos o aplicaciones legítimas y se activa cuando estos se ejecutan. Requiere intervención humana para propagarse. Puede alterar o destruir datos. Un empleado que descarga un archivo infectado puede comprometer la integridad de documentos financieros.

Gusanos (Worms). Se replican automáticamente y se propagan a través de redes sin necesidad de interacción humana. Su autopropagación genera saturación de redes y puede paralizar comunicaciones internas. El gusano WannaCry es un ejemplo que cifró sistemas en miles de organizaciones simultáneamente.

Troyanos (Trojans). Se presentan como software legítimo pero ejecutan acciones maliciosas ocultas en segundo plano. Pueden instalar puertas traseras (backdoors), robar credenciales o permitir el control remoto del sistema comprometido.

Ransomware. Cifra los datos del sistema y exige un rescate para restaurar el acceso. Es una de las amenazas de mayor impacto organizacional actual. Su variante moderna combina el cifrado con la exfiltración de datos para ejercer doble extorsión.

Spyware. Recopila información del usuario sin su consentimiento: hábitos de navegación, credenciales, datos bancarios o información estratégica. Puede operar de manera imperceptible durante períodos prolongados.

Adware. Muestra publicidad no deseada y puede servir como puerta de entrada para otros tipos de malware.

Rootkits. Ocultan su presencia en el sistema modificando el sistema operativo. Son especialmente difíciles de detectar y eliminar, y pueden proporcionar acceso persistente a un atacante.

Keyloggers. Registran las pulsaciones del teclado, capturando contraseñas, datos bancarios y comunicaciones confidenciales.

Vectores de infección y controles

Los principales vectores de infección incluyen el correo electrónico (adjuntos maliciosos, phishing), la descarga de software no autorizado, dispositivos USB, sitios web comprometidos y vulnerabilidades no parcheadas.

Los controles preventivos más relevantes son la actualización periódica de parches de seguridad, el uso de soluciones antimalware con actualización continua, la segmentación de red para limitar la propagación, la restricción de dispositivos USB y software no autorizado, la capacitación en reconocimiento de phishing y la implementación de listas blancas de aplicaciones (application whitelisting). Los controles correctivos incluyen el DRP, los backups actualizados y los procedimientos de respuesta a incidentes.

Impacto en la organización y análisis bajo el modelo CIA

El malware ataca los tres pilares del modelo CIA: compromete la confidencialidad al exfiltrar datos, la integridad al alterar registros y la disponibilidad al cifrar o destruir sistemas. Desde la administración, su impacto se mide en pérdida de ingresos durante la interrupción, costos de recuperación y respuesta, posibles multas regulatorias y daño reputacional con clientes y socios.

Conceptos clave

- Malware como categoría general de software diseñado con fines maliciosos.
- Seis tipos principales: virus, gusanos, troyanos, ransomware, spyware y rootkits.
- Vectores de infección: correo, USB, descarga, vulnerabilidades no parcheadas.
- Impacto en los tres pilares del modelo CIA.
- Controles preventivos: parches, antimalware, segmentación y capacitación.

Preguntas de repaso del tema

1. ¿Cuál es la diferencia entre un virus y un gusano?
2. ¿Por qué el ransomware es especialmente disruptivo para las organizaciones?
3. ¿Qué es un troyano y por qué es difícil de detectar?
4. ¿Cómo opera un keylogger y qué información compromete?
5. ¿Cómo impacta el malware en los tres pilares del modelo CIA?
6. ¿Qué vectores de infección son más frecuentes en entornos organizacionales?
7. ¿Por qué la actualización de parches es el control preventivo más importante?
8. ¿Qué es el application whitelisting y cómo reduce el riesgo?

9. ¿Cómo puede la segmentación de red limitar la propagación de un gusano?
10. ¿Por qué una respuesta rápida a incidentes de malware reduce el impacto financiero?