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**.

Las Acciones de los Virus y el Malware

Presentación del tema

Los ataques y acciones maliciosas ejecutadas por virus y otros tipos de malware constituyen una de las amenazas más persistentes y disruptivas en el ámbito de los Sistemas de Información (SI). Estas acciones no se limitan a la mera infección técnica de dispositivos, sino que pueden comprometer procesos críticos, alterar información estratégica, interrumpir operaciones y generar pérdidas económicas significativas.

Las acciones maliciosas se analizan en función de su impacto sobre los tres pilares del modelo CIA. Los virus y programas maliciosos pueden producir interrupción de servicios, intercepción de información, espionaje digital, modificación de datos y destrucción de información. Desde la perspectiva administrativa y de gestión de TI, comprender estas acciones no es solo un ejercicio técnico, sino un requisito estratégico para diseñar políticas de prevención, evaluar riesgos y proteger la continuidad del negocio.

Interrupción de servicios

La interrupción consiste en la imposibilidad temporal o permanente de acceder a sistemas, datos o servicios. Puede producirse mediante ransomware, gusanos que saturan la red, virus que bloquean sistemas operativos o ataques de denegación de servicio (DoS). La interrupción afecta directamente la disponibilidad (Availability) del modelo CIA.

Una empresa de comercio electrónico que sufre un ataque de ransomware durante una campaña de ventas experimenta pérdidas financieras inmediatas y deterioro reputacional. Desde la administración, la interrupción implica costos operativos, pérdida de ingresos e incumplimientos contractuales. La existencia de un DRP reduce el impacto y acelera la recuperación.

Intercepción de información

La intercepción implica acceso no autorizado a información en tránsito o almacenada. Sus modalidades incluyen los keyloggers (registro de pulsaciones del teclado), el malware de sniffing de red y los troyanos con puertas traseras (backdoors). La intercepción afecta la confidencialidad (Confidentiality). Un spyware que captura credenciales financieras puede permitir transferencias fraudulentas. La intercepción suele pasar desapercibida durante períodos prolongados, lo que amplifica su peligrosidad.

Espionaje digital

El espionaje digital es una forma sofisticada de intercepción orientada a obtener información estratégica. Las amenazas persistentes avanzadas (APT, Advanced Persistent Threat) son ataques prolongados y silenciosos diseñados para extraer información sensible como secretos comerciales, planes estratégicos o información de investigación y desarrollo. Desde la perspectiva organizacional, el espionaje afecta directamente la ventaja competitiva y puede pasar inadvertido durante meses.

Modificación de datos

La modificación implica alterar información sin autorización. Sus formas más comunes incluyen cambios en registros contables, manipulación de bases de datos y alteración de configuraciones críticas. La modificación afecta la integridad (Integrity). Un virus que altera valores financieros en un ERP puede generar reportes incorrectos, llevando a decisiones estratégicas erróneas basadas en información falsa. Los ataques sutiles de modificación gradual pueden ser más dañinos que la destrucción inmediata, precisamente porque generan confianza en datos que están corrompidos.

Destrucción de datos

La destrucción implica la eliminación permanente o irreversible de información mediante virus destructivos, borrado masivo de archivos o sobrescritura de datos. Sus consecuencias incluyen pérdida de historial financiero, incumplimiento regulatorio y

daño reputacional. La estrategia de backup 3-2-1 es la principal medida preventiva: tres copias, en dos medios diferentes, con una fuera del sitio principal.

Ataques combinados y propagación interna

En la práctica, las acciones maliciosas suelen combinar múltiples efectos. Un ransomware moderno puede interrumpir servicios, interceptar información, amenazar con su publicación (doble extorsión) y destruir archivos si no se paga rescate. El impacto se multiplica exponencialmente. Una vez dentro del sistema, el malware puede desplazarse lateralmente: la ausencia de segmentación de red amplifica el daño, mientras que el modelo Zero Trust limita la propagación al exigir verificación continua en cada recurso.

Evaluación del riesgo y controles

Las acciones maliciosas se evalúan bajo la ecuación Riesgo = Amenaza × Vulnerabilidad × Impacto. Reducir vulnerabilidades mediante actualización de parches, autenticación multifactor (MFA) y segmentación de red disminuye la probabilidad de éxito del ataque. La capacitación en reconocimiento de phishing reduce las vulnerabilidades humanas que frecuentemente son el punto de entrada inicial. El monitoreo mediante SIEM permite detectar señales tempranas antes de que el impacto sea total.

Conceptos clave

- Seis tipos de acciones maliciosas: interrupción, intercepción, espionaje, modificación, destrucción y combinadas.
- Cada acción impacta en uno o más pilares del modelo CIA.
- La modificación gradual puede ser más dañina que la destrucción visible.
- La propagación lateral amplifica el daño ante ausencia de segmentación.
- Evaluación mediante la ecuación de riesgo para priorizar controles.

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**.

Preguntas de repaso del tema

1. ¿Cómo se relacionan las acciones maliciosas con el modelo CIA?
2. ¿Cuál es la diferencia entre intercepción y espionaje digital?
3. ¿Por qué la modificación de datos puede ser más peligrosa que su destrucción inmediata?
4. ¿Cómo contribuye la segmentación de red a limitar la propagación del malware?
5. ¿Por qué la gestión de riesgos es esencial frente a ataques maliciosos?
6. ¿Qué es un APT y por qué es especialmente difícil de detectar?
7. ¿Por qué la interrupción de servicios tiene consecuencias contractuales para la organización?
8. ¿Cómo puede una organización reducir el impacto de un ataque destructivo?
9. ¿Qué relación existe entre ataques combinados y el modelo de doble extorsión del ransomware?
10. ¿Por qué los controles de capacitación son esenciales frente a las acciones maliciosas?