UNIVERSIDAD AUTÓNOMA DE CHIAPAS.

FACULTAD DE CONTADURÍA Y ADMINISTRACIÓN, CAMPUS I.

LICENCIATURA EN INGENIERÍA EN DESARROLLO Y TECNOLOGÍAS DE SOFTWARE.

SÉPTIMO SEMESTRE, GRUPO: “M”

MATERIA: RESPUESTA A INCIDENTES DE SEGURIDAD.

DOCENTE: MTRO. OBETH REGALADO MORENO.

ALUMNO:

- A210367-Amores Hernandéz Carlos Daniel
- A210016-Coronel Chambé Cristóbal de Jesús
- A210731-Carrasco Zavala Carlos Emmanuel
- A210395-Cruz Leon Jesús Adrian

“ENSAYO E INFOGRAFIA SOBRE TRIADA CIA”

FECHA DE ENTREGA: 4 DE FEBRERO DE 2025.

Impacto del Malware y Virus Informáticos en la Confidencialidad, Integridad y Disponibilidad

Los virus informáticos y el malware representan una amenaza significativa para la seguridad de los sistemas informáticos y pueden comprometer los principios fundamentales de la seguridad de la información: confidencialidad, integridad y disponibilidad (CIA). A continuación, se analiza cómo estas amenazas afectan cada uno de estos aspectos en un entorno empresarial.

Confidencialidad: El malware puede comprometer la privacidad de los datos al permitir el acceso no autorizado a información sensible. Algunos tipos de malware, como los troyanos y spyware, están diseñados para recopilar credenciales, datos financieros o información personal de los usuarios sin su consentimiento. En un entorno empresarial, esto puede traducirse en el robo de información confidencial, como datos de clientes, estrategias comerciales o documentos internos. La filtración de esta información podría derivar en pérdidas económicas, daños a la reputación de la empresa y posibles sanciones legales por incumplimiento de normativas de protección de datos.

Integridad: Los virus informáticos pueden alterar o corromper datos críticos, afectando la confiabilidad de los sistemas. Algunos tipos de malware, como los ransomware o los gusanos informáticos, pueden modificar, cifrar o borrar archivos esenciales para la operación de la empresa. Esto no solo pone en riesgo la validez de la información almacenada, sino que también puede generar confusión en la toma de decisiones basada en datos incorrectos o alterados. La pérdida de integridad en bases de datos empresariales podría traducirse en errores contables,

problemas de cumplimiento regulatorio y afectación a la calidad del servicio ofrecido a los clientes.

Disponibilidad: La propagación de malware en una red corporativa puede ralentizar los sistemas, causar caídas en la infraestructura y bloquear el acceso a información crítica. Un virus informático que infecte servidores clave podría dejar inoperativas aplicaciones esenciales para la organización, impidiendo a los empleados realizar sus tareas. En casos extremos, el ransomware puede bloquear el acceso a los datos y exigir un rescate para su recuperación, generando pérdidas económicas y afectando la continuidad del negocio. La indisponibilidad de los sistemas puede impactar la productividad, generar pérdida de confianza por parte de clientes y proveedores, y causar graves interrupciones operativas.

Acciones Recomendadas: Para mitigar los efectos del malware y proteger los principios de seguridad de la información, es fundamental aplicar estrategias de prevención y recuperación:

1. Medidas de Prevención:
    - Implementación de soluciones antivirus y antimalware actualizadas.
    - Educación y concienciación de los empleados sobre buenas prácticas de seguridad, como no abrir archivos adjuntos de remitentes desconocidos.
    - Uso de firewalls y sistemas de detección de intrusos (IDS/IPS) para monitorear y bloquear amenazas.
    - Aplicación de parches y actualizaciones de seguridad en software y sistemas operativos.
2. Estrategias de Contención y Eliminación:
    - Aislamiento inmediato de dispositivos infectados para evitar la propagación del malware.

- Uso de herramientas de eliminación de malware especializadas para limpiar los sistemas comprometidos.
- Restauración de archivos desde copias de seguridad recientes y seguras.

3. Planes de Recuperación:
    - Implementación de un plan de recuperación ante incidentes que contemple procedimientos para la restauración de sistemas y datos.
    - Realización de copias de seguridad periódicas y almacenaje en ubicaciones seguras y fuera de línea.
    - Evaluación de los sistemas después de la eliminación del malware para garantizar la ausencia de vulnerabilidades residuales.

MALWARE Y VIRUS INFORMATICOS EN LA CONFIDENCIALIDAD, INTEGRIDAD Y DISPONIBILIDAD

¿Que es el malware?

Un software malicioso que afecta la seguridad de los sistemas informáticos, comprometiendo la Confidencialidad, Integridad y Disponibilidad (CID) de la información.

CONFIDENCIALIDAD: RIESGO PARA LA PRIVACIDAD

- Robo de credenciales y datos sensibles.
- Filtración de información confidencial.
- Uso de spyware y keyloggers para monitorear actividad.

◆ Solución: Uso de antivirus, autenticación multifactor y monitoreo de accesos.

INTEGRIDAD: ALTERACION DE DATOS

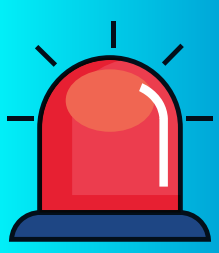
- Corrupción de archivos y bases de datos.
- Manipulación de información financiera o administrativa.
- Ataques de ransomware que cifran datos.

◆ Solución: Copias de seguridad regulares, control de versiones y detección de intrusos.

DISPONIBILIDAD: INTERRUPCION DEL SISTEMA

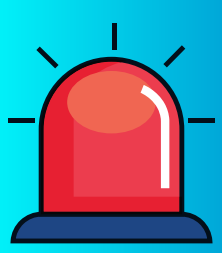
- Ralentización o bloqueo de equipos.
- Pérdida de acceso a datos y servicios.
- Saturación de redes por malware propagado.

◆ Solución: Firewalls, segmentación de red y mantenimiento preventivo.



ESTRATEGIAS DE PROTECCION Y MITIGACION

- **Capacitación:** Concienciación sobre ciberseguridad.
- **Software de Seguridad:** Uso de antivirus y firewalls.
- **Actualizaciones Frecuentes:** Parches y correcciones de vulnerabilidades.
- **Copias de Seguridad:** Respaldo en la nube o almacenamiento externo.
- **Monitoreo y Respuesta Rápida:** Implementación de sistemas de detección de amenazas.



RECUPERACION DE SISTEMAS INFECTADOS

- Aislar dispositivos afectados.
- Usar herramientas de eliminación de malware.
- Restaurar información desde copias de seguridad.
- Reforzar las políticas de seguridad para prevenir futuros ataques.

CONCLUSION

En la actualidad, el malware sigue siendo una de las amenazas más significativas para la seguridad informática, afectando la confidencialidad, integridad y disponibilidad de los sistemas. La implementación de estrategias preventivas y de mitigación es esencial para reducir los riesgos asociados a estos ataques. La educación de los usuarios, el uso de herramientas de seguridad avanzadas y una respuesta eficaz ante incidentes son clave para garantizar la protección de la información y la continuidad de las operaciones en un entorno digital cada vez más expuesto a ciberamenazas.