MINISTERIO DE CIENCIA, INNOVACIÓN, TECNOLOGÍA Y TELECOMUNICACIONES

GOBIERNO DE COSTA RICA

GUÍA DE ACCIÓN ANTE INCIDENTES DE RANSOMWARE

PROCESO DE GESTIÓN DE INCIDENTES

Octubre - 2023

TABLA DE CONTENIDO

Ransomware

El ransomware es un malware que emplea el cifrado para retener la información de una víctima a cambio de un rescate. Los datos críticos de un usuario u organización se cifran para que no puedan ser accesibles, luego se exige un rescate para proporcionar acceso a los mismos. El ransomware a menudo está diseñado para propagarse a través de una red y una base de datos de destino y servidores de archivos, y, por lo tanto, puede paralizar rápidamente a toda una organización. Es una amenaza creciente, que genera miles de millones de dólares en pagos a los ciberdelincuentes e inflige daños y gastos significativos para empresas y organizaciones gubernamentales.

Preparación

La preparación es un componente fundamental para la construcción, capacidades efectivas de respuesta a incidentes. Esta sección proporciona una descripción general de los procesos implementados para ayudar a mitigar el riesgo de ransomware y las funciones y responsabilidades de las partes interesadas clave.

Se recomienda que las secciones descritas en esta fase sean personalizadas para adaptarse a la institución.

- ✓ **Funciones y responsabilidades**

Defina claramente las partes interesadas clave, proporciona funciones y responsabilidades actualizadas y describa las necesidades
acciones si se detecta un ataque de ransomware.

- ✓ **Capacitación en concientización sobre seguridad.**

Implementar la capacitación en seguridad requerida en toda la empresa para comunicar los peligros de las amenazas maliciosas y orientación para identificar actividades sospechosas con medidas para proteger. Educar a los usuarios sobre cómo informar actividad cuestionable a los equipos de seguridad.

- ✓ **Copias de seguridad y recuperación de datos**

Se debe realizar una copia de seguridad de todos los datos y metadatos importantes periódicamente en una bóveda que sea inmutable, con espacios de aire y enjaulados. Se recomiendan simulacros parciales para asegurarse de que los datos sean válidos y recuperables.

- ✓ **Configuración de herramientas de seguridad**

Procure instalar firewall de red y de aplicaciones -WAF, sistema Endpoint Detection Response EDR, para obtener visibilidad en la red.

Asegúrese de que existan programas, políticas y procedimientos para administrar terminales y dispositivos móviles para que los dispositivos sean más resistentes al ransomware y otras infecciones de malware. Ejemplos: endurecer requisitos, instalar soluciones antivirus y antimalware, actualizar sistemas operativos y aplicaciones, etc.

Invierta en soluciones basadas en XDR como Microsoft Defender para Endpoint para proteger sus dispositivos.

- ✓ **Protección de red**

Garantizar que se implementen programas, políticas y procedimientos para monitorear y asegurar la entrada y salida.
apunta a la red: firewalls, uso de acceso con privilegios mínimos, aplicación de autenticación sólida, métodos como la autenticación multifactor (MFA), soluciones antispam para correo electrónico, etc. Invierta en un software basado en SIEM como Microsoft Sentinel para acceder a funciones avanzadas de información valiosa con análisis de comportamiento integrados para adelantarse a los atacantes.

- ✓ **Uso de VPN**

La configuración de una VPN establece un túnel cifrado de comunicación entre el equipo que sale a internet e Internet, estableciendo una conexión segura, garantizando protección frente a amenazas externas.

✓ **Desactivación de unidades externas**

Desactive las opciones Autorun y Autoplay en las unidades externas (CD, USB, etc.), de igual forma minimice el uso de conexión de dispositivos externos por parte de los colabores en los computadores de la organización.

✓ **Configuración de correo corporativo con filtros antispam**

El filtro antispam mantiene la bandeja de entrada libre de spam y phishing, se puede realizar a correos comerciales.

✓ **Plan de auditoría de logs del sistema**

Implemente plan de auditoría de logs permanente, de las actividades de gestión del Directorio Activo, como cambios de contraseñas, eliminación de usuario, creación y/o modificación de cuentas de usuario, etc.

✓ **Programación de pruebas de vulnerabilidad**

Las pruebas de vulnerabilidades aplicadas regularmente permiten revisar y estimar las debilidades de seguridad en la infraestructura de un sistema de información.

✓ **Limitar el uso de escritorio remoto (RDP)**

Los actores de amenazas generalmente acceden una red a través de servicios remotos desprotegidos.

✓ **Políticas de seguridad**

Las políticas de seguridad deben mantenerse actualizadas y aplicarse para todas las identidades, usuarios y cuentas que tienen acceso a los activos y recursos de la empresa.

✓ **Plan de continuidad**

El desarrollo de un plan de continuidad, para definir las aplicaciones de misión crítica que deben ser respaldadas en sitio alterno para la recuperación y restablecimiento de las operaciones según el tiempo tolerable necesario para que los sistemas críticos vuelvan a estar operativos (RTO) y la cantidad máxima aceptable de pérdida de datos entre la última copia de seguridad y la fecha en que ocurre del incidente (RPO).

✓ **Principio del mínimo privilegio – *Zero Trust***

Administre y supervise las cuentas de usuario y el acceso aplicando el principio de mínimos privilegios.

✓ **Deshabilitar macros**

Asegúrese de deshabilitar las macros como predeterminadas, para reducir el riesgo que el ransomware se propague a través de los archivos adjuntos de Microsoft Office.

1. Fase de Identificación

Reconocer un incidente a tiempo puede reducir significativamente los daños potenciales. En la fase de identificación y detección se ha de clasificar el incidente para determinar que es un ransomware, su origen, la criticidad de los sistemas afectados. La identificación de un incidente puede ser activa, estamos observando un incidente en directo, o pasivo, estamos observando ciertos comportamientos anómalos. En cualquier caso, identificar los activos afectados es crucial para contener el problema.

Durante la fase de identificación **es fundamental la comunicación** del equipo con las personas involucradas, debiendo **recopilar y documentar la mayor cantidad de información posible**, para así determinar con mayor eficacia los activos involucrados en el incidente.

Manténgase informado sobre los vectores de ataque más comunes utilizados en ataques de ransomware. Elaborar estrategias y documentar los planes de detección y respuesta de seguridad, pueden diferir según el método de ataque. Además, cree un flujo de proceso para mostrar el proceso de un extremo a otro de incidentes detectados, notificados, clasificados y resueltos.

Métodos de ataque comunes según NIST:

- ✓ Archivos adjuntos de correo electrónico y enlaces maliciosos incrustados.
- ✓ Vulnerabilidades del navegador web.
- ✓ Programas infectados incluidos con malware.
- ✓ Dispositivos USB portátiles.

Los equipos de respuesta a incidentes deben implementar métodos consistentes de evaluación y priorizar eventos de ransomware para determinar las escaladas

requeridas. Crear un incidente matriz de impacto para determinar la escalada requerida.

2. Fase de Contención

Si no es posible ninguna acción de mitigación inicial:

- ✓ Tome una imagen forense del sistema y una captura de memoria de una muestra de dispositivos afectados (por ejemplo, estaciones de trabajo, servidores, servidores virtuales y servidores en la nube). Recopile cualquier registro relevante, así como muestras de cualquier binario de malware "precursor" y observables asociados o indicadores de compromiso (por ejemplo, direcciones IP sospechosas de comando y control, entradas de registro sospechosas u otros archivos relevantes detectados).

- ✓ Conserve la evidencia que es de naturaleza altamente volátil, o limitada en retención, para evitar la pérdida o la manipulación (por ejemplo, memoria del sistema, registros de seguridad de Windows, datos en búferes de registro de firewall).

- ✓ Consulte en la comunidad de ciberseguridad incluso si las acciones de mitigación son posibles, con respecto a los posibles descifradores disponibles, ya que los investigadores de seguridad pueden haber descubierto fallas de cifrado para algunas variantes de ransomware y liberado descifrado u otros tipos de herramientas.

Para continuar con los pasos para contener y mitigar el incidente:

- ✓ Oriéntese bajo una guía confiable (por ejemplo, publicada por fuentes como el gobierno de EE. UU., MS-ISAC o un proveedor de seguridad acreditado) para la variante de ransomware en particular y siga los pasos recomendados

adicionales para identificar y contener los sistemas o redes que se confirma que están afectados.

- ✓ Deshabilitar la ejecución de binarios de ransomware conocidos; Esto minimizará el daño y el impacto en sus sistemas. Elimine otros archivos y valores del Registro asociados conocidos.

- ✓ Identifique los sistemas y las cuentas involucradas en la violación inicial. Esto puede incluir cuentas de correo electrónico.

- ✓ En función de los detalles de incumplimiento o compromiso determinados anteriormente, contener sistemas asociados que puedan usarse para un acceso no autorizado adicional o continuo. Las infracciones a menudo implican la exfiltración masiva de credenciales. Proteger las redes y otras fuentes de información del acceso continuo no autorizado basado en credenciales puede incluir:

- ✓ Deshabilite las redes privadas virtuales (VPN), los servidores de acceso remoto, los recursos de inicio de sesión único y los activos basados en la nube u otros activos públicos.

- ✓ Si una estación de trabajo infectada cifra los datos del lado del servidor, siga los pasos de identificación rápida del cifrado de datos del lado del servidor.

- ✓ Revise las listas Administración de equipos > sesiones y Abrir archivos en los servidores asociados para determinar el usuario o el sistema que accede a esos archivos.

- ✓ Revise las propiedades de archivo de archivos cifrados o notas de rescate para identificar usuarios específicos que pueden estar asociados con la propiedad del archivo.

- ✓ Revise el registro de eventos TerminalServices-RemoteConnectionManager para comprobar si las conexiones de red RDP se han realizado correctamente.

- ✓ Revise el registro de seguridad de Windows, los registros de eventos SMB y los registros relacionados que pueden identificar eventos significativos de autenticación o acceso.

- ✓ Ejecute software de captura de paquetes, como Wireshark, en el servidor afectado con un filtro para identificar las direcciones IP involucradas en la escritura activa o el cambio de nombre de los archivos (por ejemplo, smb2.filename contiene cryptxxx).

- ✓ Realizar análisis extensos para identificar mecanismos de persistencia de afuera hacia adentro y de adentro hacia afuera.
- ✓ La persistencia de afuera hacia adentro puede incluir acceso autenticado a sistemas externos a través de cuentas no autorizadas, puertas traseras en sistemas perimetrales, explotación de vulnerabilidades externas, etc.

- ✓ La persistencia de adentro hacia afuera puede incluir implantes de malware en la red interna o una variedad de modificaciones de estilo de vida fuera de la tierra (por ejemplo, uso de herramientas comerciales de prueba de penetración como Cobalt Strike; uso de la suite PsTools, incluido PsExec, para instalar y controlar malware de forma remota y recopilar información sobre sistemas Windows o realizar administración remota de ellos; uso de scripts de PowerShell).

3. Fase de Mitigación

Actividades encaminadas a erradicar y limpiar o desinfectar las computadoras afectadas. Implementar medidas para evitar la reinfección.
Eliminar determinados componentes, tales como malware, cuentas comprometidas, identificar y mitigar todas las vulnerabilidades que fueron explotadas. Este proceso de erradicación del evento en la red, mediante herramientas tecnológicas o manualmente dependiendo del impacto y complejidad de la situación.
Es fundamental erradicar la **causa raíz** que provocó la brecha de seguridad para que a futuro no vuelva ser explotada. Hasta que esta fase esté completa en su totalidad no se puede volver los sistemas a su normalidad por el riesgo que representa.

4. Fase de Recuperación

- ✓ Vuelva a conectar los sistemas y restaure los datos de copias de seguridad cifradas sin conexión en función de una priorización de los servicios críticos.

- ✓ Tenga cuidado de no volver a infectar los sistemas limpios durante la recuperación. Por ejemplo, si se ha creado una nueva red de área local virtual (VLAN) con fines de recuperación, asegúrese de que solo se agreguen sistemas limpios.

- ✓ Documente las lecciones aprendidas del incidente y las actividades de respuesta asociadas para informar las actualizaciones y refinar las políticas,

planes y procedimientos de la organización y guiar los ejercicios futuros de los mismos.

- ✓ Considere compartir las lecciones aprendidas y los indicadores relevantes de compromiso con las demás instituciones para beneficiar a otros dentro de la comunidad y Ecosistema Digital Costarricense.

5. Fase Post- Incidente

- ✓ Reunión informativa: Analiza lo que salió bien, los desafíos enfrentados y mejoras potenciales.
- ✓ Documentación: Mantenga un informe detallado del incidente, incluidos los cronogramas, sistemas afectados, acciones de respuesta y hallazgos para referencia futura.
- ✓ Actualización del plan: según lo aprendido, actualice el plan de respuesta a incidentes, protocolos y herramientas.

6. Lecciones aprendidas

Identificar los procesos de mejora para documentar los acontecimientos sucedidos, así como las soluciones. Esto es un informe de cierre que contendrá las mejoras en los procesos de forma detallada.
Cierre del incidente:

- Un sumario del incidente.
- Estado actual del incidente.
- Acciones tomadas como solución ante el incidente.
- Evaluación de impacto del incidente.
- Partes involucradas en su resolución.
- Mejoras en los controles (habilitar o ajustar controles).
- Observaciones y comentarios de todas las partes involucradas.

7. Diagrama de flujo