Actividad: Documenta un evento en un diario de gestión de incidentes

Resumen de la actividad

En esta actividad, tendrás la oportunidad de revisar los detalles de un incidente de seguridad y documentarlo utilizando tu diario de gestión de incidentes.

Escenario

Revisa el siguiente escenario. Luego, completa las instrucciones paso a paso.
Una pequeña clínica de atención médica especializada en servicios de atención primaria en los Estados Unidos experimentó un incidente de seguridad un martes por la mañana, alrededor de las 9:00 a.m. Varios empleados reportaron la imposibilidad de utilizar sus computadoras para acceder a archivos como historiales médicos. Las operaciones comerciales se interrumpieron porque los empleados no podían acceder a los archivos y programas necesarios para realizar su trabajo.
Además, los empleados informaron la aparición de una nota de rescate en sus computadoras. Este mensaje decía que todos los archivos de la empresa habían sido cifrados por un grupo organizado de hackers poco éticos, conocidos por dirigir sus ataques a organizaciones en los sectores de salud y transporte. A cambio de restablecer el acceso a los archivos cifrados, la nota de rescate exigía una gran suma de dinero por la clave de descifrado.

Los atacantes lograron acceder a la red de la empresa mediante el uso de correos electrónicos de phishing dirigidos a varios empleados de la compañía. Estos correos contenían un archivo adjunto malicioso que instala malware en la computadora del empleado una vez descargado. Una vez que los atacantes obtuvieron acceso, desplegaron su ransomware, el cual cifró archivos críticos. La empresa se vio incapacitada para acceder a los datos críticos de pacientes, lo que causó interrupciones importantes en sus operaciones comerciales. La clínica tuvo que apagar sus sistemas informáticos y ponerse en contacto con varias organizaciones para reportar el incidente y recibir asistencia técnica.

Diario de Gestión de Incidentes - Entrada de Incidente

Fecha: [23/10/2024]

Número de entrada: 001

Descripción de la entrada:
Una pequeña clínica de atención médica en Estados Unidos sufrió un ataque de ransomware que interrumpió sus operaciones al cifrar los archivos de los pacientes y otros documentos importantes.

Herramientas utilizadas:

- Ninguna herramienta específica utilizada en el momento de este registro.

Las 5 W del incidente:

1. ¿Quién causó el incidente?
   Un grupo organizado de hackers conocido por atacar los sectores de salud y transporte.
2. ¿Qué sucedió?
   Se desplegó un ransomware que cifró los archivos de la clínica tras un ataque de phishing dirigido a varios empleados. Los atacantes exigieron un rescate por la clave de descifrado.
3. ¿Cuándo ocurrió el incidente?
   El incidente ocurrió un martes por la mañana, alrededor de las 9:00 a.m.
4. ¿Dónde ocurrió el incidente?
   Ocurrió en la red informática de una clínica de atención médica en los Estados Unidos.
5. ¿Por qué ocurrió el incidente?
   El ataque ocurrió porque varios empleados cayeron en un ataque de phishing al descargar un archivo adjunto malicioso que ejecutó el ransomware en el sistema.

Notas adicionales:

- La clínica tuvo que apagar todos los sistemas y contactar a organizaciones de soporte técnico y autoridades.
- La importancia de concientizar a los empleados sobre los riesgos del phishing es crucial para evitar futuros incidentes.
- Sería útil implementar un sistema de respaldo de archivos para evitar la dependencia de los atacantes en situaciones similares.