25 DE ABRIL DE 2024

ANÁLISIS DE CASOS DE CIBERDELITOS

NORMATIVA DE CIBERSEGURIDAD

ERIC SERRANO MARÍN
I.E.S MARTINEZ MONTAÑES
CETI

Contenido

Fuentes utilizadas: 2

1. Identificar el ciberdelito o ciberdelitos que se cometieron. 2

2. Identificar en qué artículo del Código Penal aparece y que pena conlleva el ciberdelito cometido según el Código Penal. 2

3. Identificar las vulnerabilidades en el sistema de seguridad. Aportar la información que aparece en la noticia y dar vuestra opinión sobre que podría haber sucedido. 3

4. Identificar como se ha resuelto el problema (en caso de que se especifique) y dar ideas de como se podría haber prevenido el ciberdelito. 4

Fuentes utilizadas:

- Diario Sevilla
- VivaSevilla
- Eldiario.es

Un ciberataque pone en jaque los servidores corporativos internos de Ayesa.

La compañía sevillana Ayesa, proveedor global de servicios de tecnología e ingeniería, ha sufrido un ciberataque que le obligó este miércoles a activar su protocolo de actuación de ciberseguridad con el que logró bloquear un ataque dirigido a sus equipos internos, según informa la empresa a preguntas de este periódico.

1. **Identificar el ciberdelito o ciberdelitos que se cometieron.**

El delito cometido es un caso de ransomware, un tipo de ataque en el que los ciberdelincuentes cifran los archivos de la víctima y exigen un rescate a cambio de proporcionar la clave para descifrarlos. En este caso, el grupo de ciberdelincuentes conocido como "Black Basta" es el presunto responsable del ataque. Este grupo se especializa en la táctica de la "doble extorsión", donde no solo cifran los archivos de la víctima, sino que también amenazan con filtrar datos confidenciales sustraídos si no se paga el rescate.

2. **Identificar en qué artículo del Código Penal aparece y que pena conlleva el ciberdelito cometido según el Código Penal.**

Según la información disponible hasta el momento, el reciente ciberataque perpetrado contra la multinacional andaluza Ayesa involucra la comisión de tres tipos de delitos informáticos, de acuerdo con el Código Penal español.

Artículo	Contenido	Pena
Artículo 197 bis	El que, por cualquier medio o procedimiento, vulnerando las medidas de seguridad establecidas para impedirlo, y sin estar debidamente autorizado, acceda o facilite a otro el acceso al conjunto o una parte de un sistema de información o se mantenga en él en contra de la voluntad de quien tenga el legítimo derecho a excluirlo.	6 meses a 2 años.
Artículo 264	El que, por cualquier medio, sin autorización y de manera grave borrase, dañase, deteriorase, alterase, suprimiese o hiciese inaccesibles datos informáticos, programas informáticos o documentos electrónicos ajenos, cuando el resultado producido fuera grave.	6 meses a 3 años
Artículo 264 bis	El que, sin estar autorizado y de manera grave, obstaculizara o interrumpiera el funcionamiento de un sistema informático ajeno.	6 meses a 3 años

3. **Identificar las vulnerabilidades en el sistema de seguridad. Aportar la información que aparece en la noticia y dar vuestra opinión sobre que podría haber sucedido.**

Las noticias todavía no detallan específicamente sobre la vulnerabilidad que se ha explotado en este caso, sin embargo, las noticias mencionan que el ataque fue llevado a cabo por el grupo de ciberdelincuentes conocido como “Black Basta”, que emplean tácticas de phishing para infiltrarse en los sistemas de sus objetivos.

La vulnerabilidad podría haber sido la falta de medidas efectivas para prevenir ataques de phishing, aunque esto también podría incluir una falta de capacitación adecuada para los empleados en la detección de correos electrónicos de phishing, así como la ausencia de filtros de correo electrónico y sistemas de autenticación robustos para prevenir la entrega de credenciales a los atacantes.

Además, el hecho de que el ataque haya resultado en una doble extorsión sugiere que los datos confidenciales de la empresa también podrían haber sido vulnerables a la explotación. Esto podría indicar deficiencias en las medidas de seguridad para proteger y cifrar datos sensibles.

En resumen, aunque las noticias que tenemos actualmente no proporcionan detalles específicos, lo más probable es que las deficiencias en la prevención de ataques de phishing y la protección de datos confidenciales podrían haber contribuido al éxito de los atacantes.

4. **Identificar como se ha resuelto el problema (en caso de que se especifique) y dar ideas de como se podría haber prevenido el ciberdelito.**

Ayesa ha informado que, aunque se han implementado medidas para contener y mitigar el impacto del incidente, la restauración total de sus sistemas y la recuperación de la normalidad al 100% aún está pendiente.

Las medidas que se han tomado son las siguientes:

- Aislamiento de los sistemas afectados.
- Corte de las comunicaciones para prevenir la propagación.
- Activación de un protocolo de plan de continuidad del negocio para la restauración de sistemas y aseguramiento de redes.
- Se ha colaborado con las autoridades pertinentes y se han activado equipos forenses para realizar análisis y obtener indicadores de compromiso.

En cuanto a como se podría haber prevenido el ciberdelito:

- **Mayor concienciación y capacitación**: Proporcionar formación continua a los empleados sobre la detección y prevención de ataques de phishing y otras tácticas de ingeniería social.
- **Implementación de medidas de seguridad avanzadas**: Utilizar soluciones de seguridad avanzadas, como sistemas de detección de intrusiones y análisis de comportamiento de usuarios, para detectar y mitigar amenazas de manera proactiva.

- **Actualizaciones y parches de seguridad**: Mantener actualizados los sistemas y aplicaciones con los últimos parches de seguridad para corregir vulnerabilidades conocidas.
- **Evaluación de proveedores de servicios**: Realizar una evaluación de riesgos de seguridad cibernética de los proveedores de servicios para garantizar que cumplan con los estándares de seguridad necesarios.