1.a.01 - ¿Estás preparado para ser atacado?

Grupo 4

Álvaro Pérez Rey
Daniel Sánchez Gómez
Ignacio Aragón Polo
Jesús Sayago Mey
Maria Dolores Galán Tajero

09/10/2022

0. Análisis Previo. **2**
0.1. ¿ Qué ha podido pasar y donde ?. 2
0.2. ¿ Quién ha facilitado o iniciado el incidente ?. 2
0.3. ¿ Qué error hemos cometido ?. 2
0.4. ¿ Qué tenemos que hacer para evitarlo ? 3

1. ¿ Qué ha pasado ? **4**
1.1. ¿ Quién ha sido ?. 4
1.2. ¿ Qué afecta ?. 4
1.3. Servicios y sistemas afectados. 4
1.4. Repercusiones legales. 4

2. ¿ Qué ha fallado ? **4**
2.1. ¿ Qué mecanismo o protocolo han fallado ?. 4
2.2. ¿ Cuándo fue el último mantenimiento ?. 5
3.3. ¿ Los trabajadores están concienciados sobre los ciberataques ?. 5

3. ¿Cómo salimos de esta? **5**
3.1. ¿ Qué hay que hacer ?. 5
3.2. ¿ Qué no hay que hacer ?. 5

4. ¿ Qué se ha aprendido ? **6**
4.1. ¿ Qué tendríamos que hacer para evitar esto en el futuro ?. 6

0. Análisis Previo.

0.1. ¿ Qué ha podido pasar y donde ?.

Incidente / Activo	Robo o pérdida	Avería	Infección por malware	Infección con extorsión	Botnet	Denegación de servicio
Puesto de trabajo	✓		✓	✓		
Dispositivos móviles						
Sistemas de almacenamiento externo						
Servidores y redes						
Página web, servidores externalizados o en cloud						

0.2. ¿ Quién ha facilitado o iniciado el incidente ?.

Desde dentro de la empresa: Por despiste o ingenuidad del trabajador, sin mala intención pero descuidado.

Desde fuera de la empresa: Un ciberdelincuente que quiere dañar a la empresa e introducir malware.

0.3. ¿ Qué error hemos cometido ?.

Incidente / Errores	Robo o pérdida	Avería	Infección por malware	Infección con extorsión	Botnet	Denegación de servicio
Uso de equipos o servicios no autorizados						
Contraseña poco segura, por defecto o a la vista						
Dejar los dispositivos desatendidos o sin bloquear						
Acceso desde redes no seguras						
Ser víctima de engaños de ingeniería social	✓		✓	✓		
Mala configuración de los equipos / dispositivos						
Gestión de proveedores sin acuerdos de seguridad y confidencialidad						
Equipos con software no actualizado						
Acceso desde redes wifi públicas a recursos de la empresa						
Dispositivos con información confidencial no cifrada	✓		✓	✓		
Routers o redes con contraseña por defecto o comunicaciones con cifrado débil						
Mala gestión de usuarios (permisos excesivos, cuentas sin uso,...)						
Control de accesos físicos insuficiente						
Equipos viejos y sin mantenimiento						

0.4. ¿ Qué tenemos que hacer para evitarlo ?

Activos/medidas	Puesto de trabajo	Dispositivos móviles	Sistemas de almacenamiento	Servidores y redes	Pág. Web externalizada, o servicios en cloud	Varios activos
Actualizaciones software						
Antimalware	✓	✓		✓	✓	
Cortafuegos	✓	✓		✓	✓	
Sistema de control de accesos físicos						
Sistema de control de accesos lógico	✓	✓	✓	✓	✓	
Gestión de proveedores	✓	✓				✓
Protocolo uso puesto de trabajo	✓	✓				
Protocolo uso móviles y portátiles	✓	✓				
Protocolo uso dispositivos almacenamiento						
Aplicaciones y servicios permitidos						
Procedimiento gestión usuarios						
Procedimiento clasificación y cifrado de información	✓	✓	✓			
Procedimiento copias de seguridad	✓	✓	✓			
Seguros externos						
Procedimiento configuración segura equipos	✓	✓				✓
Formación acceso desde redes externas						
Formación ingeniería social	✓	✓				✓
Formación uso cuentas y contraseñas	✓	✓				✓

1. ¿ Qué ha pasado ?

1.1. ¿ Quién ha sido ?.

En este caso hay diferentes culpables, en concreto tres. El ciberdelincuente por infectar los equipos con un malware, el trabajador que por desconocimiento introdujo el ransomware en el sistema y el equipo de ciberseguridad por no tener diseñado e implementado un sistema de seguridad adecuado para estos casos.

1.2. ¿ Qué afecta ?.

En primer lugar, afecta a la empresa, también a los trabajadores e indirectamente a los clientes, porque la empresa deberá parar o disminuir su actividad hasta solucionar el problema.

1.3. Servicios y sistemas afectados.

Afecta a todos los equipos que haya podido infectar el malware y encriptando los discos duros de los trabajadores.

1.4. Repercusiones legales.

El ciberdelincuente tendría que responder tanto por vía penal como civil por la suplantación de un cliente, la intrusión y vulneración del sistema informático, por la encriptación de los datos de los discos duros de los equipos y por la extorsión. La empresa podría llegar a tener implicaciones legales de acuerdo con la ley orgánica de protección de datos, si se hubieran filtrado los datos de los trabajadores y de los clientes de la empresa (Leak).

2. ¿ Qué ha fallado ?

2.1. ¿ Qué mecanismo o protocolo han fallado ?.

Ha fallado el filtrado de spam del correo y el escaneo del correo entrante y saliente para detectar archivos ejecutables o comprimidos.

2.2. ¿ Cuándo fue el último mantenimiento ?.

La semana pasada, posiblemente el fin de semana o el viernes.

3.3. ¿ Los trabajadores están concienciados sobre los ciberataques ?.

No, si la empresa tuviera un plan interno de concienciación y formación en ciberseguridad para sus trabajadores se habría minimizado la incidencia.

3. ¿Cómo salimos de esta?

3.1. ¿ Qué hay que hacer ?.

- Contactar con el Centro de Respuesta a Incidentes CERTSI de INCIBE para que nos guíe o ayude en el proceso.
- Clonar discos afectados para usarlos como evidencia si denunciamos.
- Cambiar todas las contraseñas de red y cuentas online y volverlas a cambiar cuando el malware haya sido eliminado.
- Pasar un antimalware a los equipos infectados.
- Denunciar el incidente a las autoridades. PN o GC.
- Aislar los equipos infectados.
- Comprobar la última copia de seguridad y restaurarla.

3.2. ¿ Qué no hay que hacer ?.

- Pagar, porque no garantiza que te devuelvan el acceso a los datos, que vuelvan a atacarte, que soliciten una cantidad mayor una vez has pagado y además fomenta el negocio de los ciberdelincuentes.
- Dejar a los ordenadores infectados conectados a la red y seguir abriendo correos de personas desconocidas.

4. ¿ Qué se ha aprendido ?

4.1. ¿ Qué tendríamos que hacer para evitar esto en el futuro ?.

- Tener un plan de actuación, respuesta y prevención ante incidentes.
- Formación y concienciación a todos los miembros de la empresa.
- Actualizar frecuentemente todos los dispositivos y el software para evitar vulnerabilidades.

Enlace al documento de Google

IS-1.a.01-Grupo4