Marsh

5 tipos de ataques cibernéticos

Casos, consecuencias y soluciones

#SoyCiberseguro

Ransomware

Contexto

Un ciberataque de ransomware al principal operador de oleoductos de Estados Unidos, fuente de casi la mitad del suministro de combustible de la Costa Este de ese país, provocó el cierre de toda su red, generando interrupción en sus operaciones. Esto incluyó la afectación del traslado diario de más de 450 millones de litros de gasolina y otros combustibles.

De acuerdo a investigadores que publicaron acerca del caso, el ataque fue producto de malas prácticas de ciberseguridad. Al parecer, el ataque estaba dirigido a la red de TI de la empresa y no a los sistemas de control del oleoducto. Sin embargo, el temor a un daño mayor obligó a la empresa a cerrar el sistema, una medida que hizo evidente las vulnerabilidades en la red del oleoducto.

2

Ransomware

Consecuencias

Los atacantes copiaron 100 GB de datos en dos horas el día anterior al lanzamiento del ataque de ransomware. Los atacantes amenazaron divulgar los datos, a menos que la empresa pagara un rescate por las claves para descifrar los datos.

La compañía decidió cerrar el oleoducto como medida de precaución debido a la preocupación de que los criminales pudieran haber obtenido información que les permitiera llevar a cabo más ataques en partes vulnerables del oleoducto, deteniendo las operaciones por tres días. Debido a la escasez de combustible, varios aeropuertos se vieron afectados, incluso teniendo que cambiar de proveedor.

El FBI confirmó que el grupo responsable de este ciberataque es conocido como DarkSide, una banda criminal con sede en Europa del Este. Las demandas de rescate de DarkSide pueden oscilar normalmente entre US$500,000 y más de US$5 millones.

Recomendaciones para prevenir este tipo de ataques con efectos en el entorno industrial

- Restringir las conexiones externas (p.e. Internet), y aislar los segmentos de red en entornos IT y OT bajo un esquema de zero-trust.
- Restringir los accesos remotos, y en el caso de los entornos OT, habilitar explícitamente cada vez que un usuario externo necesite acceder de manera autorizada y siempre bajo el monitoreo de la organización.
- Habilitar mecanismos de doble factor de autenticación.
- Habilitar mecanismos de doble factor de autenticación.
- Validar y reforzar las capacidades de protección ante malware.
- Monitorear los eventos de seguridad a nivel perimetral e interno de las redes IT y OT.
- Definir un esquema de copias de seguridad offline acorde a los requerimientos de la organización y realizar pruebas de restauración.
- Desarrollar un plan de respuesta ante ciberincidentes y los planes operativos para los principales escenarios de ciberataques. Probar periódicamente las capacidades de detección y respuesta ante ciberincidentes, así como las capacidades para gestionar una crisis por medio de simulacros de cibercrisis.
- Definir y probar periódicamente un Plan de Continuidad del Negocio y un Plan de Recuperación ante Desastres.
- Concientizar y entrenar en ciberseguridad a empleados y terceros con acceso a los sistemas de la organización.
- Tenga presente que un ciberataque es inminente, por lo cual, es importante evaluar el nivel de exposición de la organización ante un ciberataque y conocer el nivel de motivación que pueden tener los atacantes para vulnerar la compañía.

Robo de datos

Contexto

El 17 de agosto de 2021, uno de los operadores inalámbricos más importantes de los Estados Unidos se enteró de que un cibercriminal accedió a sus redes y adquirió datos personales de sus clientes.

Lo anterior ocurrió mediante el aprovechamiento de conocimiento de sistemas técnicos, junto con herramientas y capacidades especializadas, para obtener acceso a sus entornos de prueba, y luego utilizó ataques de fuerza bruta y otros métodos para abrirse camino en otros servidores que incluían datos de clientes.

Este criminal obtuvo acceso por primera vez a los sistemas del operador al menos desde el 19 de julio de 2021.

4

Robo de datos

Consecuencias

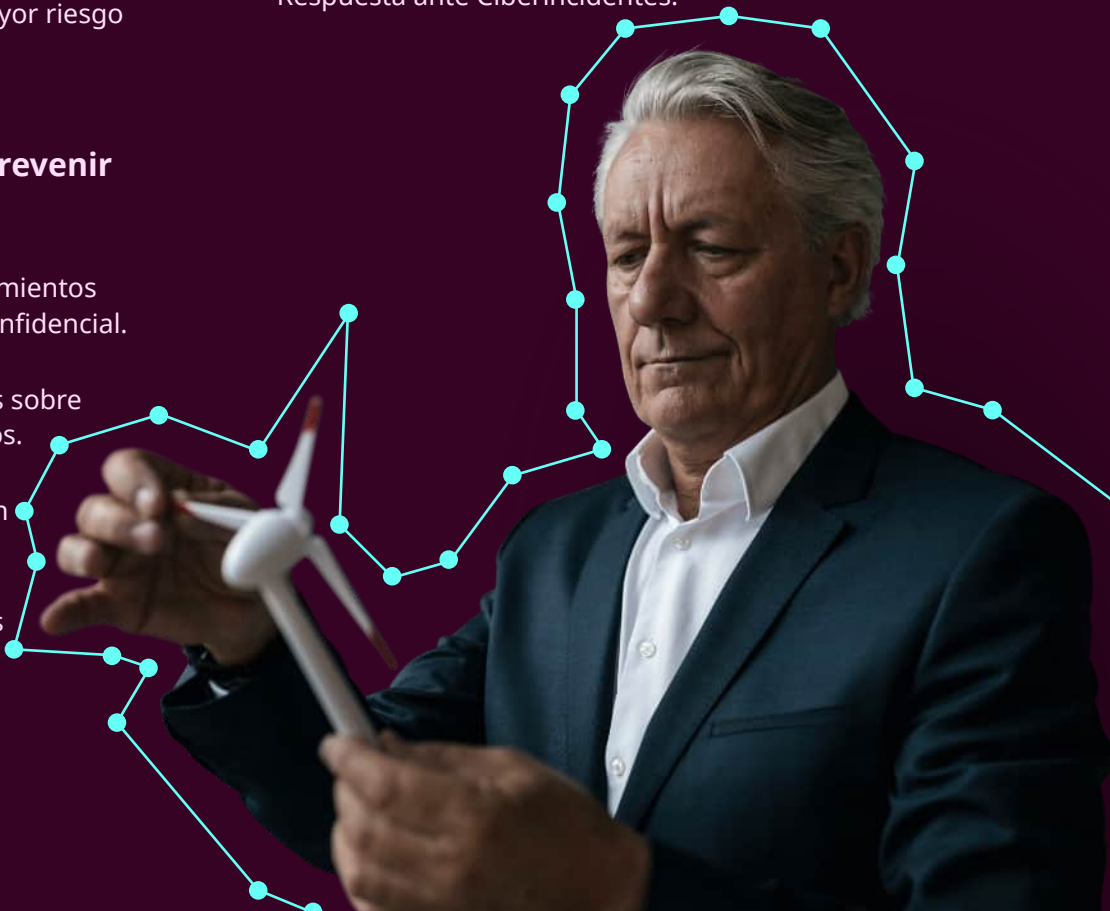
Entre los datos robados se encontraban nombres, licencias de conducir, números de identificación del gobierno, números de seguro social, fechas de nacimiento, PIN prepagos del operador, direcciones y números de teléfono.

Sin embargo, no se tenían indicios de que los datos accedidos incluyeran información financiera como tarjetas de crédito. Con corte al 20 de agosto de 2021, se calculaba que los hackers habían robado información personal de más de 53 millones de clientes (tanto clientes actuales como clientes anteriores y clientes potenciales del operador).

Algunos clientes demandaron a la compañía por daños, indicando en una demanda colectiva que el ciberataque violó su privacidad y los expuso a un mayor riesgo de fraude y robo de identidad.

Recomendaciones para prevenir este tipo de ataques

- Definir e implementar procedimientos para el manejo información confidencial.
- Definir e implementar políticas sobre privacidad y seguridad de datos.
- Asegurar el cifrado de datos en tránsito y en reposo.
- Definir e implementar políticas de configuración de seguridad (hardening) para dispositivos de monitoreo periódicos.
- Implementar una adecuada gestión de vulnerabilidades para los sistemas de la organización.
- Realizar pruebas periódicas de seguridad, para evaluar las capacidades de detección y respuesta ante ciberincidentes.
- Concientizar y entrenar en ciberseguridad a empleados y terceros con acceso a los sistemas de la organización.
- Monitorear los eventos de seguridad a nivel perimetral e interno de las redes IT. Priorizar los activos de información críticos para la organización.
- Definir y probar periódicamente un Plan de Respuesta ante Ciberincidentes.



Ataque a terceros

Contexto

Una firma líder de banca de inversión informó en abril de 2021 sobre una filtración de datos después de que atacantes robaran información personal perteneciente a sus clientes al hackear el servidor Accellion FTA de un proveedor externo. Los clientes de la empresa multinacional incluyen corporaciones, gobiernos, instituciones e individuos en más de 41 países.

El proveedor externo que brinda servicios de mantenimiento de cuentas notificó a la compañía en mayo de 2021 que los atacantes hackearon su servidor Accellion FTA para robar información perteneciente a los participantes del plan de acciones de la firma. El servidor fue atacado al explotar una vulnerabilidad de Accellion FTA en enero, antes de que el proveedor aplicara las actualizaciones de seguridad dentro de los cinco días posteriores al lanzamiento de la solución.

En marzo pasado, el proveedor descubrió la violación de seguridad y el impacto para los clientes de la firma cuando notificó en mayo a la compañía del incidente. No se encontró evidencia de que los datos robados fueran difundidos en línea por los cibercriminales. Aunque los archivos robados se almacenaban de forma cifrada en el servidor comprometido, los atacantes también obtuvieron la clave de descifrado durante el ataque.

6

Ataque a terceros

Consecuencias

Los documentos robados contenían nombres de los participantes del plan de acciones, direcciones, fechas de nacimiento, números de seguridad social y nombres de empresas.

Una declaración conjunta publicada por Accellion y Mandiant en febrero, arrojó más información sobre el ataque, vinculándolos directamente con el grupo cibercriminal FIN11.

Recomendaciones para prevenir este tipo de ataques

- Implementar una adecuada gestión de seguridad con terceros.
- Implementar una adecuada gestión de vulnerabilidades para los sistemas de la organización.
- Realizar pruebas periódicas de seguridad para evaluar las capacidades de detección y respuesta ante ciberincidentes.
- Concientizar y entrenar en ciberseguridad a empleados y terceros con acceso a los sistemas de la organización.
- Monitorear los eventos de seguridad a nivel perimetral e interno de las redes IT. Priorizar los activos de información críticos para la organización.
- Definir y probar periódicamente un Plan de Respuesta ante Ciberincidentes.

Exposición de información por vulnerabilidades en el software

Contexto

Un error en el sitio web de una compañía mundial de automóviles permitió acceder de manera no autorizada a sistemas de la compañía y obtener datos sensibles, como bases de datos de clientes, registros de empleados, tickets internos, etc. La exposición de datos se debió a una instancia mal configurada de Pega Infinity, CRM de la compañía, que se ejecuta en los servidores de la empresa.

El problema fue causado por una vulnerabilidad de exposición de la información en instancias de Pega Infinity configuradas incorrectamente. Para aprovechar esta vulnerabilidad, un atacante primero tenía que haber accedido al panel web de backend de una instancia del portal de Pega Chat Access Group mal configurada. Luego, diferentes parámetros podían permitir a los atacantes ejecutar consultas, recuperar tablas de bases de datos, tokens de acceso, y tomar provecho de privilegios administrativos y de este modo ejecutar consultas.

Exposición de información por vulnerabilidades en el software

Consecuencias

La información expuesta debido a esta vulnerabilidad incluía datos personales como registros de clientes y empleados, números de cuenta, nombres y tablas de bases de datos, tokens de acceso, tickets de soporte interno, perfiles de usuario dentro de la organización, acciones de pulso, interfaces internas e historial de la barra de búsqueda.

Recomendaciones para prevenir este tipo de ataques

- Asegurar el cifrado de datos en tránsito y en reposo.
- Definir e implementar políticas de configuración de seguridad (hardening) para dispositivos y sistemas, además de procedimientos de monitoreo periódicos.
- Implementar una adecuada gestión de vulnerabilidades para los sistemas de la organización.
- Realizar pruebas periódicas de seguridad, para evaluar las capacidades de detección y respuesta ante ciberincidentes.
- Monitorear los eventos de seguridad a nivel perimetral e interno de las redes IT. Priorizar los activos de información críticos para la organización.
- Definir y probar periódicamente un Plan de Respuesta ante Ciberincidentes.

Filtración de datos por un ex-empleado

Contexto

Un exempleado del Hospital Radboudumc en Países Bajos colocó en GitHub, una plataforma en línea donde los desarrolladores de software comparten conocimientos entre sí, archivos como scripts y códigos que permiten la automatización de procesos del hospital, pero también información confidencial como datos personales. Debido a la filtración, los datos de un número desconocido de empleados fueron expuestos.

Filtración de datos por un ex-empleado

Consecuencias

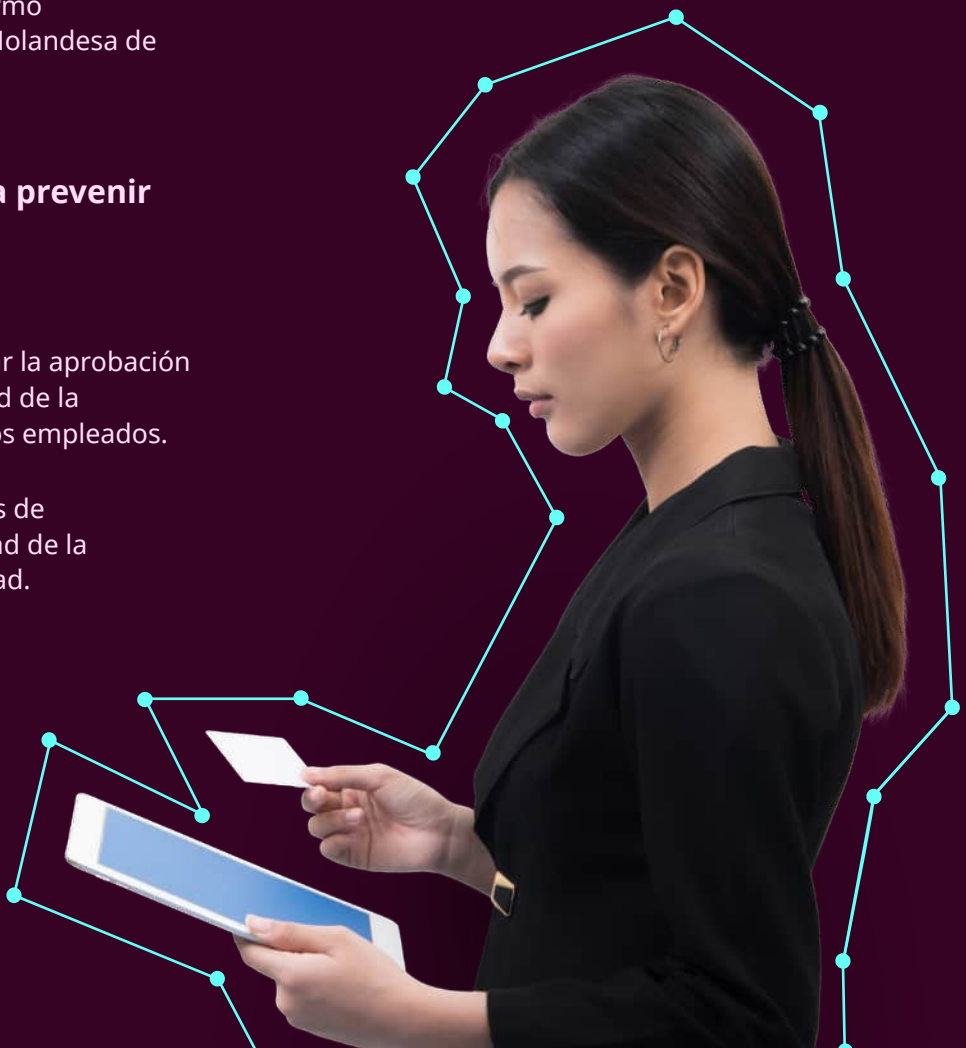
Debido a la información dejada por el ex-empleado en la plataforma, un atacante accedió a los servidores del hospital mediante la información publicada en línea para generar criptomonedas.

Dentro de la información que se filtró se encontraban datos de empleados del hospital como nombres de usuario, correos electrónicos y números telefónicos, así como del personal de organizaciones con las que el hospital trabaja. Sin embargo, hasta agosto de 2021 no se había hecho público ningún dato de pacientes.

El hospital presentó una denuncia contra ambas personas; sin embargo, al día de hoy se desconoce el numero exacto de registros fugados. La filtración se informó previamente a la Autoridad Holandesa de Protección de Datos.

Recomendaciones para prevenir este tipo de ataques

- Definir, comunicar y solicitar la aprobación de las Políticas de Seguridad de la Información por parte de los empleados.
- Realizar sesiones periódicas de concientización en seguridad de la información y ciberseguridad.
- Definir un programa de entrenamiento especializado en personas con roles clave en la organización (p.e. personal de seguridad de la información, equipos de desarrollo de software, propietarios de información, etc.).
- Implementar una Metodología de Desarrollo Seguro.
- Restringir el acceso al código fuente de las aplicaciones.
- Implementar capacidades de ciberinteligencia para identificar información de la organización fugada en Internet o potenciales amenazas.



Edson Villar
Líder Regional de Consultoría en Riesgo Cibernético, Marsh LAC
Edson.Villar@marsh.com

Paulina Vélez
Líder Regional de Seguros de Riesgo Cibernético, Marsh LAC
Paulina.Velez@marsh.com

Marsh