

Análisis de

riesgos.

Cliente: Europe Avellaneda S.A

Comentado [U1]: altera esta
plantilla a tu conveniencia.
Considérala tan solo una guía.
Rellena los campos del
formulario o desprotege el
documento para cambiarlo más a
fondo

Activos implicados en el caso:	2
Descripción del ataque motivo del análisis	3
Amenazas.....	3
Objetivos.....	4
Medidas de seguridad existentes	4
Propuestas	4
Recomendación.....	5

Tema : Análisis de riesgos a la empresa Europe Avellaneda S.A por ataque a la misma
Autor : Ismael Macareno Chouikh Fecha : 06/10/2024
Revisores : -
<p>Resumen :</p> <p>Filtrado de datos de un evento importante de un cliente de la empresa Europe Avellaneda S.A y debido a esto la empresa pierde el evento aparte de dederar un posible ataque.</p> <p>Por lo visto un trabajador vivió unos sucesos extraños con su equipo de trabajo, declara que se le encendió la webcam y apareció una aplicación la cuál no conocía.</p> <p>El cliente de la empresa cancela el evento por completo debido a que un representante de otra empresa le ofreció un precio económicamente más bajo para organizar el evento y los datos de este evento solo deberían conocerlos la empresa Europe Avellaneda S.A por lo que el cliente de la empresa decide cancelar por completo el evento, por falta de confianza.</p>

Activos implicados en el caso :

- Datos :
Datos de cliente y evento del mismo cliente
- Hardware

Portátil

● Software

Aplicación web llamada TESTOR

Descripción del ataque motivo del análisis

Trabajador de la empresa Europe Avellaneda S.A conectado a la red privada de la empresa declara que mientras trabajaba en su portátil conectado a la aplicación web de la empresa TESTOR la cual contiene datos de clientes, proveedores y eventos vio como se le encendió la webcam de su portátil y seguidamente aparecía en la parte baja de su pantalla una aplicación que él no conocía.

Amenazas

Casos:

- Amenaza 1, ransomware: Al haber accedido a la red privada de la empresa tengo el miedo de que el atacante haya podido tener la oportunidad de acceder a la base de datos de la empresa y haberla secuestrado

Activos vulnerables:

- Base de datos de la empresa Europe Avellaneda S.A

Impacto:

- Sobre todo económico debido a que seguramente el atacante hubiese pedido una cantidad elevada para desencriptar la base de datos

- Amenaza 2, Secuestro de aplicación web: Al poder haber accedido a la aplicación web de la empresa esto significa que sin mucho esfuerzo el atacante podría haber sido capaz de suplantar o conseguir las credenciales del administrador y así cambiar las contraseñas de acceso a la aplicación web de la empresa.

Activos vulnerables:

- Aplicación web TESTOR

Impacto:

Análisis de riesgos de Europe Avellaneda S.A

- Posibles demandas de parte de los clientes a la empresa por filtración de datos privados
- Amenaza 3, Gusano: por lo visto el ataque dio acceso al atacante a acceder a la red debido a que para acceder a la aplicación web de la empresa TESTOR hay que estar en la red privada de la empresa porque esta aplicación web no es accesible desde internet. Esto podría haber sido muy grave ya que al tener acceso a la red se podría haber injectado y propagado un gusano en la red y contagiar a todos los componentes Activos vulnerables:
 - Credenciales de trabajadores
 - Equipos, servidores, bases de datos, etc.

Impacto:

- Impacto fatal por exponer datos privados de empresas amparados por la LGPD
- Se pierde disponibilidad para seguir trabajando

O b j e t i v o s

Lograr descubrir el agujero de seguridad por el cuál se han filtrado datos y dar recomendaciones de seguridad para así mejorar la misma.

M e d i d a s d e s e g u r i d a d e x i s t e n t e s

No se indican

P r o p u e s t a s

- Aumentar seguridad del usuario: esto sería implantando un buen antivirus como por ejemplo Kaspersky, limitando conexiones de USB y redes no seguras a los portátiles, impedir que los usuarios puedan instalar aplicaciones etc.
 - Ventajas: así podremos impedir que se ejecuten programas que no deseamos, que el usuario no se encuentre un UBS y lo inserte en un equipo de la empresa, etc
 - Inconvenientes: ninguno
- Costes:
 - De implantación: pago por un buen antivirus que cuente con una buena base de datos
 - De mantenimiento: el pago del antivirus
- Doble factor de autenticación para TESTOR: modificar el método de acceso a TESTOR añadiendo un segundo factor de autenticación usando SMS al número de empresa del trabajador, un TOTP, etc
 - Ventajas: aumenta la seguridad de acceso a la aplicación web de la empresa que contiene datos sensibles
 - Inconvenientes: necesidad de integrar un método confiable de doble autenticación
- Costes:
 - De implantación: pago por una buena solución de doble autenticación, jumpcloud cuenta con una muy buena por un precio bastante asequible
 - De mantenimiento: ninguno
- Segmentación de la red: crear un segmento de red en la red privada de la empresa solamente para TESTOR con su respectiva seguridad, firewall, etc. Pedir login cada vez que se quiera conectar a la red de TESTOR, usar un single sign-on, etc.
 - Ventajas: Previene el acceso desde fuera y pone más capas para dar problemas a los atacantes
 - Inconvenientes: Bastante pocos, sencillamente tendremos que hacer un segmento de red.
- Costes:
 - De implantación: como mucho el precio de un cortafuegos en caso de que no dispongan del mismo.
 - De mantenimiento: se ocupa el departamento de IT.

R e c o m e n d a c i ó n

Análisis de riesgos de Europe Avellaneda S.A

Mi recomendación sería empezar una campaña de concienciación de los empleados para intentar evitar que vuelva a suceder esto en un futuro, esto se podría hacer mediante simulaciones de ataques al usuario, cursos de formación para los que piquen en las simulaciones y para los que no, etc.