**Portada:**

Buenas tardes, somos Álvaro y Adrián y en esta exposición se simula la presentación de una amenaza a la junta directiva de una empresa. La amenaza que vamos a presentar es Caballo de Troya.

El **contexto** empresarial que nos imaginamos en que tendría sentido realizar esta presentación es el de cualquier empresa informática o cualquier empresa que haga uso de sistemas de información y tenga un departamento de TI dedicado a gestionar la informática de la empresa.

**Diap 2:**

Un Caballo de troya es un tipo de malware que se instala en el sistema de la víctima escondiendo su verdadero contenido para engañar al usuario y que piense que es un archivo inofensivo. Según el tipo, su **finalidad** puede variar desde bloquear, modificar o eliminar datos hasta recopilar información y enviarla a terceros.

El nombre de este malware se basa en el **mítico** Caballo de Troya que hacía uso del engaño para pasar desapercibido. En el mundo de la computación, el Caballo de Troya se **disfraza** como un programa o software legítimo, y se instala sin el conocimiento del usuario, creando una puerta trasera en el sistema de la víctima que permite a los atacantes acceder a la información almacenada en él.

**Diap 4:**

Aunque hay muchos tipos de troyanos, nosotros vamos a presentar los más populares e importantes:

* El primero de ellos es el Rootkit, están diseñados para **ocultar** ciertos objetos o actividades del sistema afectado. Normalmente, el propósito principal es prevenir que el usuario se dé cuenta de la existencia de programas maliciosos en el sistema, de esta manera se logra que estos programas permanezcan en el sistema el mayor tiempo posible.
* El Spyware se basa en **observar** la actividad realizada por el usuario, recolectando así información sensible como por ejemplo credenciales de cuentas o datos bancarios, que son entonces enviados al atacante.
* El tercer tipo de caballo de troya a destacar es el Backdoor. Aunque es uno de los más simples, también es uno de los más peligrosos. Esto es porque es capaz de abrir **un túnel de comunicación** secreto entre el malware desplegado y el atacante, y de esta manera el malware recibe las órdenes del atacante. Por lo tanto, puede permitir que el atacante controle el dispositivo infectado y monitorice el sistema, robe datos, o incluso instale software por su cuenta.

**Diap 6:**

En esta diapositiva se hace un análisis de los criterios de seguridad afectados por los tipos de Caballo de Troya presentados. Se han clasificado solo con relación al criterio que afectan principalmente, pero realmente algunos de ellos afectan a 2 o incluso a los 3 criterios.

* El troyano DDoS afecta principalmente a la Disponibilidad, ya que su propósito es interrumpir el correcto funcionamiento de los sistemas atacados o incluso dejarlos completamente inservibles hasta que el problema sea solucionado.
* El Rootkit afecta principalmente a la Integridad, ya que su propósito es ocultar la existencia de programas maliciosos en el sistema afectado y extender al máximo el tiempo que permanecen en el sistema.
* El Troyano downloader, al igual que el rootkit, afecta principalmente a la Integridad, ya que su propósito es que después de ser instalado por el atacante, el propio Caballo de Troya se encargue de descargar más malware de la red.
* Por último, en la tabla de Confidencialidad tenemos el Spyware y el Backdoor. El Spyware está aquí porque su propósito es espiar la actividad del usuario afectado.
* Y por otra parte el Backdoor está aquí porque una vez instalado permite que el atacante tenga acceso a la información del sistema sin que el usuario se dé cuenta. El Backdoor, también afectaría bastante a la integridad, e incluso puede afectar considerablemente a la disponibilidad, dependiendo del uso que el atacante le dé.

**Diap 8:**

Un troyano dedicado al keylogging es un troyano que tiene la capacidad de registrar las teclas que el usuario presiona. Esta información se **almacena en un fichero** que después es enviado al atacante. Este fichero, cuando el atacante lo consulte, contendrá mucha información irrelevante para él, pero si tiene paciencia, puede **filtrar** la información para encontrar información sensible que el usuario haya escrito, como por ejemplo contraseñas o números de tarjeta.

Hoy en día dentro del conjunto de troyanos dedicados a este concepto, hay algunos **más avanzados** que otros, y se diferencian de los otros en que tienen la capacidad de distinguir la **actividad específica** del usuario como por ejemplo el acceso al navegador apuntando a una web o tipo de web específico, como puede ser una web bancaria.

------------

Otro de los riesgos importantes que suponen los Caballos de Troya es la obtención por parte del atacante de información sensible almacenada en los sistemas. Este es un riesgo que afecta principalmente a las **compañías industriales**, que suelen ser el objetivo más apuntado por los atacantes, ya que la información que puedan encontrar en los sistemas de estas compañías les resulta mucho más interesante que la que pudieran encontrar en un ordenador de escritorio del usuario medio.

**Diap 11:**

En cuanto a la contratación de servicios para prevenir esta amenaza, o como mínimo evitar que tenga un impacto serio si ocurre, lo primero que recomendamos es la contratación de **un data center de respaldo**, que debe estar situado en un **área geográfica** alejada del CPD principal para mitigar los problemas causados por catástrofes naturales y sería gestionado por una **empresa externa**.

Este data center permitiría la **recuperación de archivos** que han sido dañados por malware en los sistemas del data center principal. Si lo gestionamos de la manera adecuada, conseguiremos que el hecho de que un atacante consiga acceso a los sistemas principales **no implique** que tenga también acceso garantizado a los sistemas del data center de respaldo, que formarán parte de una red completamente distinta.

El envío de datos entre los dos data centers se realizará con **copias diferenciales,** ya que ofrecen un tiempode **restauración menor**. Pero, si se dispara el **precio de almacenamiento** recomendaríamos el cambio a copias incrementales, ya que requieren menos almacenamiento, aunque habría que tener en cuenta que provocan que el tiempo de **restauración sea mayor**.

**Diap 13:**

Para acabar con la ejecución de cambios internos que se deberían realizar a raíz de esta amenaza, se sugieren los siguientes:

* Por una parte, se debería definir un **apartado específico** para esta amenaza dentro de la política de seguridad de la empresa para tenerla bien documentada y poder realizar una **respuesta ágil** en lugar de improvisar en el momento.
* Por otra parte, se debería **formalizar el proceso** de gestión de riesgos llevando a cabo una serie de **actividades** que incluyen el análisis, estimación, evaluación, aceptación y tratamiento del riesgo.