UNIVERSIDAD AUTONOMA DE NUEVO LEON
FACULTAD DE INGENIERIA MECANICA Y ELECTRICA

Multitarea: Redes y seguridad: sistemas distribuidas.

Nombre: Christopher Angel Santiago Torres

Matricula: 2077856 Carrera: IAS

Profesor: Norma Edith Marin Martinez

SEGURIDAD

La seguridad informática comprende software (bases de datos, metadatos, archivos), hardware y todo lo que la organización valore (activo) y signifique un riesgo si esta información confidencial llega a manos de otras personas, convirtiéndose, por ejemplo, en información privilegiada.

SEGURIDAD DE REDES

Un sistema distribuido se define como una colección de computadoras separadas físicamente y conectadas entre sí por una red de comunicaciones; cada máquina posee sus componentes de hardware y software que el programador percibe como un solo sistema (no necesita saber qué cosas están en qué máquinas). El programador accede a los componentes de software (objetos) remotos, de la misma manera en que accedería a componentes locales, en un grupo de computadoras que usan un middleware entre los que destacan (RPC) y SOAP para conseguir un objetivo.

La seguridad informática es el área de la informática que se enfoca en la protección de la infraestructura computacional y todo lo relacionado con esta y, especialmente, la información contenida o circulante.

Características:

- Para cada uno de los usuarios debe ser similar al trabajo en el Sistema Centralizado.
- Seguridad interna en el sistema distribuido.
- Se ejecuta en múltiples computadoras.
- Tiene varias copias del mismo sistema operativo o de diferentes sistemas operativos que proveen los mismos servicios.

VARIEDAD DE AMENAZAS

Son muchos los tipos de amenazas que hay presentes en la red hoy en día. Hablamos de virus, malware muy variados, páginas fraudulentas... Pero también podemos ser atacados a través de dispositivos físicos como memorias USB, por ejemplo.

Los piratas informáticos pueden tener objetivos muy diversos. Podrían querer robar nuestras credenciales y contraseñas, provocar un mal funcionamiento de nuestros sistemas o simplemente robar datos personales de la víctima para poder enviar publicidad orientada.

PRINCIPALES AMENAZAS DE SEGURIDAD

Memorias USB

Si empezamos por un tipo de amenaza física muy común son las **memorias USB**. Aquí hay que distinguir entre un pendrive que ha sido creado para atacar directamente de otro que ha podido ser infectado al haber estado conectado a un equipo con malware.

Pongamos como ejemplo que nos han dejado un **pendrive** para guardar información. La persona que nos lo ha dejado ha conectado previamente esa memoria en su sistema y posiblemente en otros equipos.

Cables fraudulentos

Un caso parecido también de amenaza física son los **cables fraudulentos**. Es una realidad que hoy en día podemos infectarnos al conectar nuestro móvil a un cable modificado de forma maliciosa y que puede ser una amenaza.

Extensiones de navegador maliciosas

Si comenzamos con aspectos de software, algunas de las amenazas más comunes llegan a través del **navegador**. Aquí hay que prestar mucha atención a las extensiones. Son herramientas muy útiles que nos ayudan en nuestro día a día pero también pueden representar un problema para nuestra seguridad.

Actualizaciones falsas

Las **actualizaciones falsas** se han convertido últimamente en un verdadero problema. Están presentes cuando navegamos por Internet y pueden aparecer en forma de mensaje de alerta diciendo que nuestro navegador tiene que actualizarse o haciendo mención a otra aplicación.

Programas descargados de Internet

Por supuesto los **programas y archivos descargados** de Internet son una fuente de amenaza muy importante. Estamos hablando especialmente de programas pirateados, que normalmente están presentes en páginas de terceros. Esto puede representar una amenaza importante para la seguridad de nuestros sistemas.

TIPOS DE VIRUS

Los virus, técnicamente conocidos como malware, son códigos informáticos creados para infectar nuestros equipos, provocar problemas en el funcionamiento de los mismos o robar información. Aunque se encuentran en constante evolución y cada cierto tiempo aparecen nuevos tipos, vamos a analizar los principales virus y la mejor forma de protegernos frente a ellos.

Adware

Es aquel software que ofrece publicidad no deseada o engañosa. Estos anuncios pueden aparecer en el navegador con pop-ups o ventanas con gran contenido visual, e incluso audios.

Se reproducen de manera automática con el fin de generar ganancias económicas a los creadores. En ocasiones este software provoca que el buscador predilecto del usuario sea cambiado por otro, generando errores en las búsquedas deseadas y entorpeciendo la experiencia de navegación del usuario.

¿Cómo nos protegemos? Evitemos abrir enlaces de descarga de páginas poco fiables y, cuando instalemos software, debemos revisar los pasos para que no se nos instale ningún buscador, programa o complemento sin que nos demos cuenta.

Spyware

Este tipo de virus se encarga de recopilar de manera fraudulenta la información sobre la navegación del usuario, además de datos personales y bancarios. Un ejemplo de este tipo de virus son los *Keyloggers*, los cuales monitorizan toda nuestra actividad con el teclado (teclas que se pulsan), para luego enviarla al ciberdelincuente.

¿Cómo nos protegemos? El primer paso y más importante será la instalación y actualización de un buen sistema antivirus. Otra forma de protegernos es evitar conectar dispositivos desconocidos, como USB o discos duros externos.

Gusanos

Este virus está creado con la capacidad de replicarse entre ordenadores. A menudo causa errores en la red, como consecuencia de un consumo anormal del ancho de banda ocasionado por este *malware*.
Los ciberdelincuentes suelen usar nombres llamativos en los enlaces para que este virus sea descargado como, por ejemplo, las palabras: sexo, apuestas, regalo o premio.

¿Cómo nos protegemos? Al igual que para los gusanos y resto de virus detallados, es importante tener actualizado nuestro sistema y sus defensas para estar protegidos y evitar se infectados, así como desactivar la función de “autoejecutar” los discos externos (memorias USB o discos duros). Si el antivirus está actualizado, también identificará y eliminará este tipo de amenazas que intenten colarse en nuestros dispositivos.

Troyano

Este tipo de virus se presenta como un software legítimo, pero que, al ejecutarlo, le permite al atacante tomar el control del dispositivo infectado. Como consecuencia, nuestra información personal se encontraría en permanente riesgo, a merced del atacante para robar todo lo que quisiera de nuestros equipos infectados.

¿Cómo nos protegemos? Además de todas las medidas anteriores, como tener actualizado el sistema operativo y el antivirus, y analizar los dispositivos USB que se vayan a conectar a nuestro equipo, debemos tener mucho cuidado cuando navegamos por Internet, ya que pueden acabar instalándose algún archivo infectado o al acceder a páginas web fraudulentas.

Ransomware

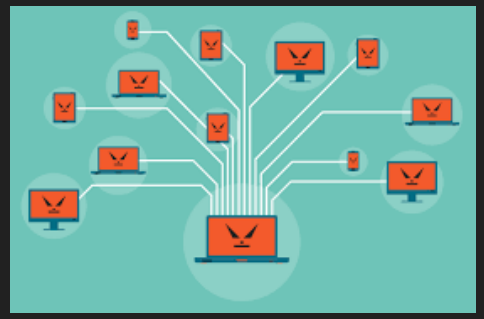
Malware que toma por completo el control del dispositivo bloqueando o cifrando la información del usuario para, a continuación, pedir dinero a cambio de liberar o descifrar los ficheros del dispositivo. Este software malicioso se trasmite en el dispositivo, tal y como lo hace un gusano o un troyano. Pueden llegar camuflados en adjuntos de correos electrónicos o en páginas web poco fiables que nos inviten a descargar algún archivo bajo una inofensiva apariencia. También se aprovechan frecuentemente de fallos de seguridad del sistema operativo o incluso de aplicaciones.

¿Cómo nos protegemos? Mucho cuidado con los correos electrónicos maliciosos con algún adjunto. La mayoría de los ataques por *ransomware* se producen cuando el usuario ejecuta un archivo infectado. También es recomendable realizar copias de seguridad para que, en caso de infección, dispongamos de una copia de nuestros datos en otro lugar de almacenamiento.

Botnets

Son redes de dispositivos infectados que los ciberdelincuentes utilizan para lanzar ataques, como el envío masivo de correos spam, ataques de denegación de servicio o DDoS, robos de credenciales, etc. Una vez que un dispositivo está infectado, entrará a formar parte de la red de *botnets* cuyo objetivo es seguir expandiéndose.

¿Cómo nos protegemos? Lo principal es hacer un buen uso de los dispositivos cuando nos conectamos a la red, teniendo un sistema actualizado con programas antivirus instalados, utilizando credenciales robustas y cambiando las contraseñas regularmente y no entrando en páginas web que puedan ser poco fiables. Otra fuente de infección son los correos maliciosos.



ANALISIS DE PROBLEMAS Y PREVENCION DE DESASTRES

La sociedad actual vive en un camino constante hacia la digitalización, con el uso masivo de los smartphones, la comunicación diaria a través de internet, el uso de la inteligencia artificial, el Big Data, e incluso el IoT, donde los electrodomésticos también se vuelven inteligentes y se conectan a la red.

Todas las **ventajas que aporta esta transformación digital** vienen acompañadas de una serie de amenazas que ponen en riesgo la seguridad de los sistemas y comprometen la privacidad de la información.

En este **entorno digital las empresas deben analizar los riesgos informáticos** y tomar medidas para evitar que se produzcan o para mitigar sus efectos negativos.

Cuando se habla de ciberseguridad, el **análisis de riesgos informáticos** es la **evaluación de los** distintos peligros que afectan a nivel informático y que pueden producir situaciones de amenaza al negocio, como robos o intrusiones que comprometan los datos o ataques externos que impidan el funcionamiento de los sistemas propiciando periodos de inactividad empresarial.

El **análisis y gestión de los riesgo s**previene a las empresas de este tipo de situaciones negativas para su actividad y recoge una serie de factores fundamentales para su consecución.

Identificación de activos

Para realizar un análisis de riesgos efectivo, el primer paso es identificar todos los activos de la empresa. Estos activos incluyen todos los**recursos relacionados con la gestión e intercambio de información de la empresa**, como software, hardware, vías de comunicación, documentación digital y manual e incluso de recursos humanos.

Riesgos y amenazas

Una vez se identifiquen todos los **activos de información que componen la empresa**, deben definirse las amenazas a las que pueden estar expuestos. Estas amenazas pueden ser de diferente índole, como ataques externos, desastres naturales o errores humanos.

- **Ataques externos**. Los ciberdelincuentes siempre tienen en su punto de mira a las empresas y sus sistemas, con el objetivo de robar información (bancaria o de otra índole comercial o personal), tirar sus sistemas o utilizar sus recursos. Dos de las mayores **amenazas que reciben las empresas** hoy en día son ataques de denegación de servicio **DDoS** (inutilizan los sistemas informáticos de la empresa) o **ataques con malware de tipo ransomware** (encriptan los datos de la empresa, solicitando un rescate económico en criptomonedas para liberarlos).
- **Errores humanos.** La intervención humana en los procesos informáticos siempre está expuesta a que se cometan errores (intencionados o no intencionados). Por ejemplo, un empleado sin los conocimientos suficientes, o con privilegios superiores a los de su función, puede realizar acciones que comprometan los datos o produzcan un **malfuncionamiento en los sistemas.**
- **Desastres naturales**. Es posible que se den situaciones que pongan en peligro los activos informáticos de la empresa como inundaciones o sobrecargas en la red eléctrica.

- **Situaciones extraordinarias, como la pandemia del COVID-19.** Las crisis a menudo reducen los niveles de alerta y protección y llevan a los ciberdelincuentes a aprovecharse de esta situación operando bajo esquemas maliciosos. Por ejemplo, las **campañas de phishing**relacionadas con el COVID-19, en las que los cibercriminales se hacen pasar, por ejemplo, por organizaciones de salud acreditadas están en aumento. Por esta razón es importante que las empresas estén atentas a mensajes fraudulentos relacionados con esta pandemia y se recomienda aumentar la conciencia ante el surgimiento de nuevas amenazas.

En esta fase del **análisis de riesgos** hay que **priorizar cada uno de estos riesgos**, siendo preciso consultar datos estadísticos sobre incidentes pasados en materia de seguridad.

- **Detectar vulnerabilidades**

Las **vulnerabilidades** se presentan en activos informáticos y presentan un **riesgo para la información**. Dos ejemplos de vulnerabilidades que suelen encontrarse en el **análisis de riesgos informáticos** son la falta de actualización de los sistemas operativos (por lo tanto, no incluyen los últimos parches en materia de seguridad) y el uso de contraseñas de acceso débiles (contraseñas cortas que no utilizan combinaciones de letras, números, símbolos y mayúsculas/minúsculas, y que son fácilmente descifrables con procesos automáticos).

- **Medidas de prevención y control**

Una vez se tengan identificadas las **amenazas y vulnerabilidades de los sistemas** y se tengan definidos todos los riesgos y sus consecuencias, deben establecerse una serie de medidas y tratamientos de riesgo con dos objetivos claros: **evitar** que se produzca el riesgo o **minimizar su impacto** en caso de que llegue a producirse.

Dentro de este tipo de medidas podemos destacar:

- **Instalación de software de seguridad y cortafuegos** (por software o hardware).
- Implementación de **sistemas de seguridad en la nube** automatizados y planes de Disaster Recovery.
- Añadir **protocolos de seguridad** para reforzar la seguridad de las contraseñas.
- **Revisión de los roles y privilegios de los usuarios** (con especial cuidado en la asignación de los roles con mayores privilegios, como los administradores).

LINEA DEL TIEMPO

- https://www.canva.com/design/DAFPapMu6w0/iTMs7xBsy08n9QfcAsx5Qg/view?utm_content=DAFPapMu6w0&utm_campaign=designshare&utm_medium=link&utm_source=publishsharelink

CONCLUSIÓN

En esta actividad estuvimos conociendo acerca de las redes y seguridad, hablamos acerca de un pequeño contexto de que es la seguridad y que es la seguridad de redes, comentamos acerca de las amenazas que existen, los tipos de virus por mencionar algunos: malware, troyano, gusanos entre muchos mas también mencionamos como podríamos protegernos de estos para luego continuar con los niveles de seguridad que se implementan, y ya por ultimo estuvimos analizando los problemas y la prevención de desastres de información y algunas posibles soluciones, esta actividad fue de mucho aprendizaje ya que pudimos profundizar mas acerca de los temas de la seguridad y conociendo mas sobre las amenazas que existen y como podemos combatir esto o al menos evitarlo.