ACTIVIDAD FUNDAMENTAL 4

REDES Y SEGURIDAD: SISTEMAS DISTRIBUIDAS.

Nombre	Matricula	Carrera
Jonathan Francisco Galvan Villanueva	1959360	ITS
José Amhed Vela Canales	1950074	IAS
Marco Antonio Arreola de Leon	2109542	ITS
Emmanuel Sanchez Aranda	1953575	ITS
Ángel David Gómez González	1961463	ITS
Jorge Alberto Morales Reyes	1895340	ITS

¿QUÉ ES LA SEGURIDAD INFORMÁTICA?

La seguridad informática o ciberseguridad, es la protección de la información con el objetivo de evitar la manipulación de datos y procesos por personas no autorizadas. Su principal objetivo es que, tanto personas como equipos tecnológicos y datos, estén protegidos contra daños y amenazas hechas por terceros.

La seguridad informática es el conjunto de prácticas, estrategias, métodos, herramientas y procedimientos cuyo objetivo final es garantizar la integridad de los equipos informáticos y de la información que contienen.

AMENAZAS CIBERNÉTICAS

Las **amenazas cibernéticas** son aquellos intentos maliciosos que tienen como propósito acceder a información sensible de una empresa, como datos personales de los empleados, de sus clientes o de temas relacionados al funcionamiento de la organización.

VIRUS

Son una clase de malware, es decir, un programa perjudicial que infecta un dispositivo de diversas formas sin que el usuario sea consciente de ello en muchas ocasiones. Al igual que los virus de la vida real, pueden **replicarse y propagarse entre sistemas.**

- ***Adware***. También conocido como software de publicidad, muestra anuncios basados en visitas o búsquedas. Además, reduce la capacidad de cómputo del equipo.
- ***Spybot***. El tipo de virus informático spyware recopila información de un dispositivo para transmitirlo a una entidad externa sin el consentimiento del usuario, posiblemente para extorsionarlo.
- ***Malware.*** Altera el funcionamiento normal del equipo al destruir o corromper el sistema operativo o programas. Puede propagarse mediante códigos por correo electrónico.

•***Ransomware.*** Secuestra la información del equipo mediante cifrado para que el usuario no pueda acceder a ella y, de este modo, solicitarle un rescate económico. De lo contrario, la información podría destruirse o publicarse en internet.

•***Virus informático o gusano.*** Se caracteriza por multiplicarse mediante el envío masivo de copias de sí mismo por correo electrónico u otras vías de contacto. Suele infectar los equipos que se conectan a redes públicas.

•***Troyano.*** Bajo la apariencia de un programa, un documento o un juego legítimo, entra en el sistema porque el usuario lo instala. Al ejecutarlo, accede a toda la información del equipo.

GUSANOS MALWARE

Un gusano informático es un tipo engañoso de malware, diseñado para propagarse a través de varios dispositivos mientras permanece activo en todos ellos.

La diferencia fundamental entre un gusano y un virus es la forma en la que aquel propaga copias de sí mismo a máquinas no infectadas. Si desea una definición de gusano informático, piense en los gusanos como malware autosuficiente capaz de ejecutarse y proliferar sin la interacción del usuario. Ni siquiera tiene que estar usando su equipo para que el gusano se active, se replique y se propague. **Una vez que el gusano ha llegado a su equipo, puede comenzar a propagarse inmediatamente.**

TROYANO

Un caballo de Troya o troyano es un tipo de malware que a menudo se disfraza de software legítimo. Los cibercriminales y hackers pueden utilizar troyanos para tratar de acceder a los sistemas de los usuarios. Generalmente, los usuarios son engañados por alguna forma de ingeniería social para que carguen y ejecuten troyanos en sus sistemas. Una vez activados, los troyanos permiten a los cibercriminales espiarte, robar tu información confidencial y obtener acceso de puerta trasera a tu sistema.

SPYWARE

El spyware es un tipo de malware que intenta mantenerse oculto mientras registra información en secreto y sigue sus actividades en línea, tanto en equipos como en dispositivos móviles. Puede supervisar y copiar todo lo que escribe, carga, descarga y almacena. **Algunas cepas de spyware también son capaces de activar cámaras y micrófonos para verlo y escucharlo sin que usted se dé cuenta.**

Por definición, el spyware está diseñado para ser invisible, lo que puede ser uno de sus atributos más dañinos: cuanto más tiempo pasa desapercibido, más estragos puede provocar. Es como un acosador virtual que lo sigue a través de su uso del dispositivo, recabando al mismo tiempo sus datos personales.

ADWARE

El adware, también conocido como software publicitario, genera ingresos para sus desarrolladores mostrando anuncios en tu pantalla de forma automática, en general, dentro de un navegador web. El adware suele crearse para computadoras, pero también puede encontrarse en dispositivos móviles.

RANSOMWARE

El ransomware es un tipo de malware que bloquea el acceso a archivos y sistemas informáticos para luego pedir el pago de un rescate a cambio de devolver el acceso. El ransomware recurre al cifrado para bloquear el acceso a los archivos infectados, lo que hace que las víctimas no los puedan abrir ni usar. Los ataques que se hacen con este malware tienen como objetivo toda clase de archivos, desde documentos personales hasta aquellos que resultan esenciales para la marcha de una empresa.

INTRUSOS INFORMÁTICOS

Se puede resumir en pocas palabras como una persona que intenta acceder a un sistema informático sin autorización.

Hay 4 tipos de intrusos informáticos:

- **Hacker**

Destaca por su excelencia en programación y electrónica, un conocimiento avanzado en ordenadores y redes informáticas. Su objetivo principal es comprender los sistemas y el funcionamiento de ellos. Buscan y descubren las debilidades de una computadora o red informática.
En seguridad informática se diferencian tres tipos. Sombreros negros o Black Hats, sombreros blancos y White Hats y sombreros grises o Grey Hats.

- **White Hats**

A los sombreros blancos también se les llama hackers éticos. Estos expertos en informática utilizan sus conocimientos para buscar vulnerabilidades y hacer tests de penetración, para estudiar y corregir fallos de seguridad y mejorar los sistemas en materia de seguridad. Alertan de un fallo en algún programa comercial, comunicándoselo al fabricante. Pueden formar parte de un equipo de seguridad empresarial o gubernamental. Se pueden dedicar a detectar y localizar a sombreros negros.

Grey Hats
Como su color indica, tienen una ética ambigua. Suelen utilizar las mismas técnicas que los sombreros negros para encontrar vulnerabilidades y luego venderlas a quién este dispuesto a pagar por ellas. Su clientela abarca gobiernos, servicios militares y otros hackers. Además, se pueden presentar como expertos en seguridad para resolver los fallos encontrados. Su enfoque suele estar en el lucro más que en perjudicar a las empresas de manera directa.

Black Hats
Utilizan sus conocimientos para realizar actividades ilegales, normalmente con animo de lucro y para aumentar su reputación. Suelen ser creadores de tipo de malware.

Crackers
Ser un Crack es ser muy bueno en algo. Ser un cracker es saber romper algo, en este caso sistemas y software. Tienen un conocimiento profundo de programación y electrónica.
Nos pueden sonar de los cracks que permiten utilizar un software sin haber pagado por la licencia. Dicho en otras palabras, la edición desautorizada de software de propiedad. La fascinación de un cracker por romper sistemas y software suele ser motivado por una multitud de razones, desde el lucro, pasando por actos de protesta hasta el simple desafío. Siempre encuentran el modo de romper una protección y estas roturas se suelen filtrar o difundir en la red para el conocimiento de los demás.

TIPOS DE AUTENTIFICACIONES

Los métodos de autenticación son uno o varios **procedimientos informáticos** que permiten **confirmar que un usuario de un sitio o servicio es quien dice ser**.

Proporciona un **control de acceso a los sistemas**, comprobando si las credenciales de un sujeto se ajustan a aquellas registradas en una base de datos de usuarios autorizados o en un servidor de autenticación de datos. Así, se garantiza la **seguridad de los sistemas, los procesos y la información de la empresa.**

Tipos

- **Autenticación QR**

Este modelo utiliza la **cámara** del dispositivo para escanear el código y tener acceso a la información o a la plataforma. Este factor garantiza que solo los usuarios seleccionados puedan acceder a su información.

- **Doble Factor de autenticación**

La **autenticación de dos factores (2FA)** es un sistema de seguridad que requiere **dos medios de identificación diferentes para acceder a algo**. Se utiliza para **reforzar la seguridad de una cuenta, de un dispositivo o de una plataforma** como Facebook.

La autenticación de dos factores suele exigir dos tipos de información del usuario: una **contraseña**, un **número de identificación personal (PIN)**, un **código enviado al smartphone** del usuario o bien una **huella dactilar**.

OTP SMS

El **código de un solo uso (OTP)** es un factor de autenticación para realizar transacciones confidenciales.
Es un método de autorización seguro en el que **se envía por SMS un código numérico o alfanumérico en tiempo real al móvil del usuario para validar una operación.**

Biometría

La autenticación que utiliza **seguridad biométrica** se basa en las **características biológicas únicas de un individuo**. El **reconocimiento facial, lectores de huellas, biometría de voz o el reconocimiento de iris** son algunos ejemplos.

Certificado digital

El certificado digital emitido por una **Autoridad de Certificación** acreditada es una alternativa de gran utilidad para **demostrar la identidad de un usuario**.
La comodidad de poder usarlos desde casa o cualquier otro lugar, a lo que le añadimos su seguridad, hace que sean muy atractivos para los ciudadanos.

NIVELES SEGURIDAD USUARIO

- **Nivel 1**

El primer cambio simple que debe realizar es cambiar su motor de búsqueda predeterminado. En la configuración de todos sus navegadores web, simplemente cambie Google a **DuckDuckGo** o **Qwant** . Este cambio rápido y simple conduce a enormes ganancias de privacidad.

Como mínimo, debe pasar por la configuración de los servicios que usamos y desactivar todo el seguimiento. Por ejemplo, en iOS, no necesita permitir que todas las aplicaciones accedan a su ubicación, micrófono, cámara y contactos. Apague todo y habilite solo los que sean necesarios.

- **Nivel 2**

Este nivel es solo un poco más de esfuerzo, pero da como resultado una protección significativamente mayor. Esto implica descargar un **administrador de contraseñas** y revisar cuentas antiguas para cambiar las contraseñas o eliminar las cuentas por completo. Los sitios web que filtran datos generalmente no invierten mucho en infraestructura de almacenamiento, por lo que eliminar su cuenta significa que es probable que sus datos también se eliminen por completo.

- **Nivel 3**

Este nivel implica mucho más esfuerzo, pero asegurará que sea esencialmente invisible en línea. Sin embargo, requiere cierto grado de experiencia técnica, ya que tendrá que usar sistemas operativos no convencionales como **Ubuntu** o **Tails** junto con sistemas operativos móviles como **GrapheneOS** .
Este nivel implica la construcción de toda su infraestructura de navegación desde cero y, por lo tanto, no se recomienda a menos que sea necesario.

NIVELES DE SEGURIDAD RED

- **Protección firewall**

Un firewall es un programa de software o un dispositivo de hardware que evita que usuarios no autorizados accedan a su red, impidiendo que ingrese tráfico sospechoso y permitiendo que fluya tráfico legítimo.

- **Detección y prevención de intrusiones**

Los sistemas de detección y prevención de intrusiones (IDPS) se pueden implementar directamente detrás de un firewall para proporcionar una segunda capa de defensa contra actores peligrosos.

Trabajando normalmente en paralelo con su predecesor, el sistema de defensa contra intrusiones más pasivo (IDS), un IDPS se encuentra entre la dirección de origen y su destino, creando una parada adicional para el tráfico antes de que pueda ingresar a una red.

- **Control de acceso a la red (NAC)**

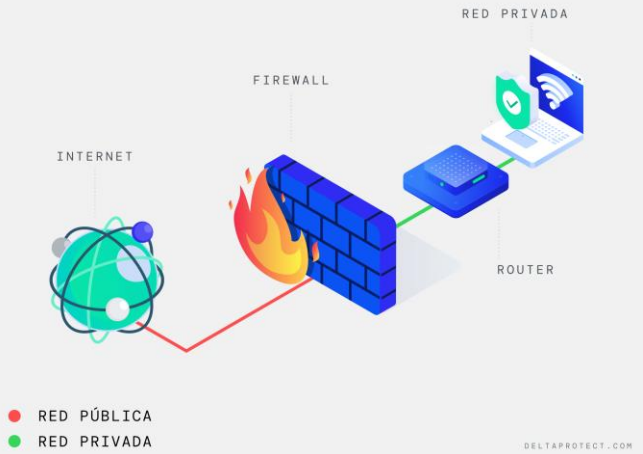
Al estar en la primera línea de defensa, el control de acceso a la red hace exactamente eso: controla el acceso a su red. Usado con mayor frecuencia para "verificaciones de estado de punto final", el NAC puede examinar un dispositivo de punto final, como una computadora portátil o un teléfono inteligente, para asegurarse de que tenga la protección antivirus adecuada, un nivel de actualización del sistema adecuado y la configuración correcta antes de que pueda ingresar.

- **Redes privadas virtuales (VPN)**

Una red privada virtual (VPN) es un software que protege la identidad de un usuario cifrando sus datos y enmascarando su dirección IP y ubicación.

- **Prevención de pérdida de datos (DLP)**

La prevención de pérdida de datos (a veces denominada "prevención de filtración de datos") es un conjunto de estrategias y herramientas implementadas para garantizar que los usuarios de puntos finales no compartan accidental o maliciosamente información confidencial fuera de una red corporativa.



NIVELES DE SEGURIDAD EMPRESAS

Nivel 20
Este nivel se conoce como de seguridad por contraseña. Es decir, los usuarios deben tener una contraseña y un ID de usuario reconocidos por el sistema para poder obtener acceso al sistema. Tanto el ID de usuario como la contraseña inicial los crea el administrador del sistema para los usuarios.

Este nivel de seguridad ofrece a todos los usuarios del sistema autorización total para realizar todo aquello que deseen. Eso significa que pueden acceder a todos los datos, archivos, objetos, etc. del sistema. Esto puede ser adecuado para pequeñas empresas en las que la seguridad interna es de baja prioridad, pero no lo será para

Nivel 30
Este nivel se conoce como de seguridad por recursos. Es decir, los usuarios deben tener un ID de usuario y una contraseña válidos definidos para ellos por el administrador del sistema, y ya no tendrán acceso automático a todos los elementos del sistema. El acceso de los usuarios está limitado por las políticas de seguridad de la empresa.

Nivel 40
Este nivel se conoce como de seguridad de integridad del sistema. Es decir, en este nivel el propio sistema está protegido contra los usuarios. Los programas escritos por usuario no pueden acceder directamente a los bloques de control internos mediante la manipulación del puntero.

El nivel 40 es el nivel de seguridad por omisión de todas las instalaciones nuevas.

Nivel 50
Este nivel se conoce como de seguridad de integridad del sistema ampliado. El nivel 50 es el nivel de seguridad recomendado para la mayoría de las empresas, ya que ofrece el nivel de seguridad más alto actualmente posible. No sólo está el sistema protegido contra programas escritos por usuario, sino que también asegura que los Usuarios únicamente tendrán acceso a datos del sistema, en lugar de a información relativa al propio sistema. Esto ofrece una mayor seguridad contra cualquiera que intente obtener información sobre el sistema.

POSIBLES AMENAZAS

1. El robo de datos de usuarios a empresas plantea un grave peligro porque puede afectar a prácticamente cualquier persona. Los cibercriminales roban y venden esta información personal en el mercado negro, lo que fácilmente puede dar lugar a robos de identidad.
2. Los cibercriminales pueden aprovechar fácilmente las vulnerabilidades del teléfono móvil para obtener datos privados. En algunos casos, estas vulnerabilidades tienen su origen en las aplicaciones que usas o en el propio teléfono. Además, los teléfonos móviles son vulnerables a tipos de malware capaces de registrar pulsaciones de teclas y tomar capturas de pantalla.
3. Cuando los cibercriminales engañan a las personas para que divulguen información confidencial, como contraseñas y números de seguridad social, esta práctica se denomina phishing. Una de las maneras más comunes en que se manifiesta el phishing es cuando una persona recibe un correo electrónico, supuestamente procedente de un banco o un organismo de gobierno, y es dirigida a un sitio que parece legítimo.
4. Uno de los delitos en línea que más ha aumentado es el robo de identidad. Muchos de los temas antes tratados en este artículo pueden derivar en incidentes de robo de identidad, correos electrónicos de phishing y filtraciones de datos.

POSIBLES SOLUCIONES

- VPN SEGURAS PARA PROTEGER LAS COMUNICACIONES
- TELETRABAJO SEGURO: ESCRITORIOS VIRTUALES
- USAR ANTIVIRUS EDR
- PROTECCIÓN AVANZADA DEL CORREO ELECTRÓNICO
- ENCRIPTACIÓN DE DATOS Y DISPOSITIVOS

CONCLUSIONES INDIVIDUALES

- José Amhed Vela Canales : La ciberseguridad es fundamental en el mundo digital actual para proteger la información y los sistemas contra amenazas cibernéticas. Es un desafío constante que requiere una combinación de tecnología avanzada, buenas prácticas de seguridad y conciencia por parte de los usuarios. La colaboración entre empresas, gobiernos y la sociedad en general es clave para abordar los riesgos en evolución y garantizar la integridad y privacidad de los datos en línea.
- Jonathan Francisco Galvan Villanueva: Tanto para empresas, clientes y usuarios la ciberseguridad se ah vuelto parte imprescindible de su trabajo, esto debido a que para trabajar algunas personas hacen uso de computadoras y celulares con sistema operativo que necesita tener desde un antivirus hasta protección en la red para evitar problemas, ciberataques, colapso de dispositivos, y robo de información asi como el sabotaje del trabajo diario
- Jorge Alberto Morales Reyes : Con la mayoría de gente y empresas dependiendo demasiado de computadoras y el internet se vuelva más importante tener equipos seguros, es fácil de ver que la ciberseguridad se vuelva cada vez más crucial. Es importante que vulnerabilidades y fallos que existen dentro del sistema operativo para segur información vital de una impresa o personal.

- Emmanuel Sanchez Aranda : Es fundamental abordar el tema de la seguridad informática en tu vida cotidiana y en las empresas. Estas medidas son cruciales para asegurar que los sistemas de información se mantengan seguros, confidenciales y disponibles. Estos elementos componen un sistema de seguridad de la información que defiende a una organización o usuario contra las amenazas de la red, que van desde desastres naturales hasta ataques cibernéticos. Es necesario que las organizaciones adopten las tecnologías y sigan adaptándose a medida que cambian las amenazas. También, la capacitación de los empleados juegan un papel importante en la preservación de un entorno seguro.
- Marco Antonio Arreola de Leon: Para concluir puedo decir que toda esta información es indispensable para un ingeniero en software ya que le permite detectar amenazas y le permite conocerlas para contrarrestarlas en caso de que se presenten. Me parece fundamental que existan los antivirus hoy en día con todas las amenazas latentes que hay en Internet y aunque no me interesa trabajar en ese ramo no por eso no reconozco que es vital el sector.
- Ángel David Gómez González: Gracias a este trabajo que realizamos pudimos ver y comprender sobre más de la ciberseguridad, ya que esta nos ayuda a poder entender sobre lo que hay detrás de las aplicaciones y las cosas que estas implican, ya que si no tuviesen seguridad dentro de estas, mucha gente que sabe sobre el mundo de la programación podrían robar los datos de las personas para hacer mal y por ende la gente no confiaría en la web, gracias a esto podemos tener "seguridad" dentro de la web para asi poder navegar entre aplicaciones, páginas y demás sitios web, también hay mas maneras de meter seguridad sobre aplicaciones o instrumentos que nosotros utilicemos, se usan las ya conocidas "encriptaciones" que estas nos ayudan a hacer de nuestros archivos y/o documentos mucho mas seguros y así poder mantenerlos más en privado

BIBLIOGRAFÍA

https://latam.kaspersky.com/resource-center/threats/trojans

https://www.avast.com/es-es/c-spyware

https://www.ui1.es/blog-ui1/cuales-son-los-virus-informaticos-mas-conocidos

https://www.conectasoftware.com/magazine/ciberseguridad/hackers-crackers-no-galletas-definiendo-tipos-intrusos/

https://latam.kaspersky.com/resource-center/threats/top-7-cyberthreats

https://es.malwarebytes.com/ransomware/

https://latam.kaspersky.com/resource-center/threats/adware