UNIVERSIDAD CRISTIANA DE HONDURAS

UCRISH

Alumna:

Claudia Eugenia Díaz Merino

Numero de ID:

0501-1989-11162

Cuenta:

1090501315

Catedrática:

Ing. Kati Xiomara Miranda

Asignatura:

Seguridad en Tecnología de Información

Informe:

Seguridad informática

Fecha:

30/05/2021

Introducción

Seguridad informática es el conjunto de normas, procedimientos y herramientas, que tienen como objetivo garantizar la disponibilidad, integridad, confidencialidad y buen uso de la información que reside en un sistema de información.

Cada día más y más personas mal intencionadas intentan tener acceso a los datos de nuestros ordenadores. El acceso no autorizado a una red informática o a los equipos que en ella se encuentran puede ocasionar en la gran mayoría de los casos graves problemas.

Uno de las posibles consecuencias de una intrusión es la pérdida de datos. Es un hecho frecuente y ocasiona muchos trastornos, sobre todo si no estamos al día de las copias de seguridad. Y aunque estemos al día, no siempre es posible recuperar la totalidad de los datos.

Otro de los problemas más dañinos es el robo de información sensible y confidencial. La divulgación de la información que posee una empresa sobre sus clientes puede acarrear demandas millonarias contra esta, o un ejemplo más cercano a usted es el de nuestras contraseñas de las cuentas de correo por las que intercambiamos información con otros.

Seguridad Informática

La seguridad informática, también conocida como ciberseguridad o seguridad de tecnología de la información, es el área relacionada con la informática y la telemática que se enfoca en la protección de la infraestructura computacional y todo lo vinculado con la misma, y especialmente la información contenida en una computadora o circulante a través de las redes de computadoras. Para ello existen una serie de estándares, protocolos, métodos, reglas, herramientas, y leyes concebidas para minimizar los posibles riesgos a la infraestructura y a la propia información.

La ciberseguridad comprende software (bases de datos, metadatos, archivos), hardware, redes de computadoras, y todo lo que la organización entienda y valore como un riesgo si la información confidencial involucrada pudiera llegar a manos de otras personas, por ejemplo, convirtiéndose así en información privilegiada.

La definición de seguridad de la información no debe ser confundida con la de seguridad informática, ya que esta última solamente se encarga de la seguridad en el medio informático, pero, por cierto, la información puede encontrarse en diferentes medios o formas, y no exclusivamente en medios informáticos. La seguridad informática también se refiere a la práctica de defender de ataques maliciosos, a las computadoras y los servidores, a los dispositivos móviles, a los sistemas electrónicos, a las redes y los datos, etc.

En resumen, la seguridad en un ambiente de red es la habilidad de identificar y eliminar vulnerabilidades. Una definición general de seguridad debe también poner atención a la necesidad de salvaguardar la ventaja organizacional, incluyendo información y equipos físicos, tales como los mismos computadores. Nadie a cargo de seguridad debe determinar quién y cuándo puede tomar acciones apropiadas sobre un ítem en específico. Cuando se trata de la seguridad de una compañía, lo que es apropiado varía de organización en organización. Independientemente, cualquier compañía con una red debe tener una política de seguridad que se dirija a la conveniencia y la coordinación.

Tipos de amenazas

1. Amenazas humanas

Un gran número de ataques informáticos son de naturaleza humana que, por mutuos propio, o por error, pueden lograr ocasionar daños severos. Podemos encontrar:

I. Ataques pasivos

Pretenden sustraer la información, pero, sin llegar a modificarla. Pueden ser:

Usuario con conocimientos básicos: Los cuales, ingresan a los dispositivos sin tener una mala intención, utilizando tácticas simples.

Hackers: Son profesionales que emplean sus habilidades informáticas para encontrar defectos y vulnerabilidades. Comúnmente, no son peligrosos, pero mientras menos expuesto estés, mejor.

II. Ataques activos

Manipulan la información para su propio beneficio o para dañar dolosamente. Por ejemplo:

Exempleados: Que aprovechan sus conocimientos del sistema para vulnerar la seguridad.

Crackers: Son profesionales informáticos. Aprovechan sus conocimientos para manipular los sistemas y dañarlos.

2. Amenazas lógicas

Existen dos tipos de software que pueden dañar un sistema informático:

Vulnerabilidades del software: Son posibles errores en el sistema operativo que ponen en riesgo la seguridad del dispositivo si llega a ser encontrado por un atacante.

Software malicioso: Existen programas con objetivos malignos, como, por ejemplo, los virus, gusanos o troyanos.

3. Amenazas físicas

Se originan por 3 causas principales:

Fallo del dispositivo: Ante un agente externo como una caída del sistema eléctrico o por un desperfecto físico del dispositivo.
Accidentes: Que pueden ocurrir por un sinnúmero de razones.
Catástrofes naturales: Como terremotos, tormentas, etcétera.

Otros tipos de amenazas informáticas

La criminalidad cibernética es un problema real, por este motivo, debemos conocer los peligros que acechan la integridad de los datos sensibles para garantizar la estabilidad jurídica operativa de nuestra organización o de nuestro propio dispositivo.

Estos son algunos de los más importantes:

1. Phishing
Se vale de técnicas de la ingeniería social, donde el "phisher" se hace pasar por una persona o empresa de confianza, por lo general por correo electrónico, redes sociales, entre otros, para sustraer información personal y financiera de manera ilegítima.

2. Malware
O, "malicious software", engloba todo programa o código informático cuyo objetivo es causar daño cibernético.

3. Spam
Son mensajes no solicitados, mayormente en términos publicitarios, que son enviados de forma masiva sin autorización ni solicitud alguna para perjudicar de alguna manera al receptor.

4. Spyware o troyano
Es un programa espía un tipo de malware ingresa en un ordenador y recopila información de la computadora, para luego transmitirla a un ente externo sin el consentimiento del usuario.

5. Virus informático

Es un software que su finalidad es alterar el normal funcionamiento de cualquier dispositivo informático sin permiso del usuario.

6. Pharming

Es un tipo de ciberataque que consiste en convencer al usuario en ingresar a un sitio web malicioso redireccionándolo con una URL. Una vez dentro, los cibercriminales buscan que el usuario brinde información privada.

Como proteger la información personal

Teniendo precaución por donde navega: Como primera recomendación y tal vez la más importante, debe ser responsable con los movimientos en Internet. Tener en claro las páginas por las que se navegan, la información que deja en cada una, la razón por la cual se le está solicitando esta información y si va a realizar algún trámite en estas páginas, asegurase de que hacen parte de una entidad reconocida y legalmente establecida.

Tener actualizado el antivirus: El estar atento de las amenazas que puede llegar a recibir su computador o celular es la principal función de su Antivirus, por ello es importante que lo mantenga actualizado con el fin de mantenerse protegido de virus y demás amenazas que pueden llegar a afectar la seguridad de su información.

Desconfía de páginas que generen mucho spam: Si una página le muestra mucha publicidad o genera alguna ventana emergente que no tiene que ver con lo que está realizando dentro de ella, debe desconfiar, así como puede ser solo publicidad, también puede tratarse de algún intento de robo de información o de fraude.

No envíe su información personal por correo electrónico: A su correo electrónico pueden llegar diariamente decenas de emails, desde diversos correos, con asuntos que van desde personales, publicitarios hasta informativos.

Pero siempre es importante en cualquier caso tener presente desde qué dirección de correo se envía, así como tener precaución al momento de responder alguno de estos correos con información personal.

Siempre cierre su sesión: Puede ser su correo electrónico, su Facebook o alguna página de compras; siempre es necesario que cierres su sesión cuando ya no esté utilizando la página web, sin importar si es su computador personal o está en algún otro, ya que tener siempre este detalle en cuenta le ayudará a mantener segura su información personal de un modo mucho más sencillo.

No ingrese por redes de Internet abiertas: Actualmente hay cientos de lugares que ofrecen el servicio de WIFI o Internet gratis, ya sean cafeterías, bibliotecas o incluso en parques; y es al acceder con estas redes que debe tener especial cuidado, ya que, al ser libres, cuentan con bajos niveles de seguridad. Por esto se recomienda evitar realizar transacciones que involucren su información personal o financiera, mientras se encuentra conectado a estas redes.

Realiza transacciones importantes solo desde su computador personal: Para transacciones que requieran información personal muy específica o trámites financieros, siempre es recomendable realizarlo directamente desde su computador personal, al cual no tenga acceso habitualmente ninguna otra persona sin su autorización.

Revise las certificaciones de seguridad: Existen varias certificaciones que garantizan la seguridad de su información en las páginas web donde es depositada.
Dos de las más importantes son:
Certificados de seguridad SSL: La SSL (Secure Sockets Layer) es un sistema de encriptación por el medio del cual la información que es enviada desde el usuario hasta la página web es protegida de cualquier intento de robo por parte de terceros, así como filtrado de la misma. Puedes saber que una página cuenta con este sistema dado que encontrarás las siglas HTTPS antes de la dirección de la página web. Actualmente es un requerimiento obligatorio para cualquier

página que requiera de su información, por ello mismo desconfía de sitios que solicitan su información y que no cuenten con estas siglas.

Protección PCI DSS: Si va a registrar su tarjeta de crédito en alguna página web ya sea para alguna compra o un pago, es importante que tenga presente si la página cuenta con el estándar de protección PCI DSS (Payment Card Industry Data Security Standard), un sistema de cifrado por el cual se da protección a cualquier transacción de pago electrónico.

Conclusión

En esta era de tecnología y de redes informática la ciberseguridad es muy importante ya que sin ella los hacker o todos los programas maliciosos que existen irrumpiera en nuestros en nuestra información personal, aunque allá seguridad siempre habrá quienes cometan malos actos para robar información y que cada vez esta actualizado y con ello conlleva a que la seguridad también este a la vanguardia para cuidar de la información y nosotros como usuarios también debemos mantener siempre nuestras protecciones al máximo como mantener el antivirus actualizado, tener contraseña con alta dificultad para mejor seguridad en todos nuestra información.