CIBERSEGURIDAD Y HACKING

Eric Alejandro Rangel Romero
eric.92.rangel@gmail.com

Erick Gilberto Ramos Rosales
Eramosr1602@alumno.ipn.mx

Dra. Claudia Marina Vicario Solórzano
cvicario@ipn.mx

Instituto Politécnico Nacional
Unidad Profesional Interdisciplinaria de Ingeniería
y Ciencias Sociales y Administrativas

Boletín No. 87
1o. de noviembre de 2021

Resumen

En este artículo se busca exponer la tendencia sobre el auge que tiene la ciberseguridad en el campo de la tecnología, así como su importancia en el campo empresarial, también se busca exponer las ventajas y desventajas de la técnica del hacking, dar a explicar qué es una vulnerabilidad y un exploit, todo esto para finalmente poder explicar por qué la sociedad debería estudiar más acerca de este maravilloso campo de la informática, haciendo notar su auge en el mercado laboral en próximos años.

Palabras Clave: Hacking, vulnerabilidad, exploit.

Abstract

This article seeks to expose the trend on the rise of cybersecurity in the field of technology, as well as its importance in the business field, searching to expose the advantages and disadvantages of the hacking technique too, explain what is a vulnerability and an exploit, all this to finally be able to explain why society should study more about this wonderful field of information technology, noting its boom in the labor market in the coming years.

Keywords: .Hacking, vulnerability, exploit.

Introducción

La ciberseguridad ha tomado gran importancia dentro del desarrollo y la transformación a nivel nacional como a nivel internacional, ya que sin ella los sistemas de transferencias bancarias, como

servidores de almacenamiento de datos en un servidor se vería expuesta cualquier usuario que use una red y que acceda a su sitio, la ciberseguridad debe estar presente en todos los sistemas existentes, por lo que al momento de implementarla generaría confianza y seguridad tanto en la empresa como en los usuarios, por lo que crecería la demanda de un servicio debido a su alta confianza y manejo de la información, si bien es cierto que invertir en mejorar la seguridad de un sistema es tedioso, es bien sabido que al hacer esto la empresa se ahorré mucho dinero en caso del extravío de la información. ”Parece pues cada vez mas claro, que la enseñanza de la ciberseguridad debe ofrecerse en conjunción con la enseñanza de las TIC…”(Nikki Giant 2016 p.10).

1.La ciberseguridad en el área empresarial.

Es bien sabido que el día de hoy las empresas prefieren decantarse por automatizar sus servicios y sistemas para facilitar al cliente la posibilidad de acceder a las bases de datos de dicha empresa como fin para encontrar artículos, servicios o algún otro tipo de cosas que logren llamar su atención desde algún lugar en el que se encuentren pero al hacer esto la empresa se ve forzada a abrir las puertas de su sistema a sus clientes sin tener ni supervisar a cada uno de ellos para verificar que lo que están haciendo entra en un panorama legal para la empresa, entonces podemos decir que a una empresa no le conviene tener muchos empleados para vigilar a tantas personas, de ahí podemos decir que es fundamental para toda empresa que opte por un sistema de información para sus clientes, contar con un sistema basto de seguridad informática para verificar que no existan fraudes ni nada ilícito dentro de la aplicación.

1.1. Riesgos de no saber nada ante las vulnerabilidades de un sistema

Al no conocer un tipo de amenaza cuando esta suceda, la empresa queda totalmente expuesta a perder o a que extraigan información sobre sus estados financieros o sus políticas más sensibles, por lo que antes de querer implementar un sistema de información que bien podría ser una aplicación, una página web o cualquier otro medio en el que los usuarios puedan interactuar con la empresa desde un punto distante, se deben de conocer algunas pautas para evaluar el tipo de amenaza posible que un sistema pueda contraer mediante su implementación y una vez deducido ese estudio la empresa deberá proseguir a la etapa de la implementación de la seguridad en sus servidores.

Implementación y técnicas de hacking más conocidas

Algunas de las técnicas de hacking más conocidas son: Keylogger, denegación de servicio, phishing, virus, troyanos, robo de cookies y escuchas esporádicas que son utilizadas normalmente por personas cuyo fin es alterar, agregar o eliminar información valiosa para una empresa mediante un entorno de trabajo diferente a los habituales como Linux, Windows o macos, mediante Kali Linux para ser más concretos. ”La combinación de dos palabras tan distantes, parece confundir a muchas personas, pues la palabra “ético” siempre nos refiere a algo “bueno”, mientras que “hacking” indica lo contrario.”(Anaid Guevara Soriano, 2012).

1.2. Tipos de Hacking

- WAP Falso:

Crean accesos a internet falsos, los cuales cuando llegan a conectarse le dan acceso a todo tu dispositivo y a robar datos personales, junto con ello archivos.

- Keyloggers:

Este tipo de técnicas últimamente se han vuelto más comunes ya que es más fácil burlar los antivirus así y se encuentran muy apegados a los cores ya que están casi instalados en los sistemas operativos.

Estos se encargan de guardar todo lo que se teclea, por el hecho de que se guarda para después ir depurando la información de cada usuario.

- Ataques DDos:

Este tipo de técnica se encarga de llenar los servidores con bots para hacer imposible el acceso a estas páginas ya sea de uso común o a páginas de ciertas cosas, sin embargo, al realizar este acto el que lo organiza puede tener acceso a la información de la página y a ciertos datos de los usuarios registrados.

- Phishing:

Se encarga directamente de hacer envíos masivos de correos a clientes en general, donde se supone que los usuarios deben de confirmar su dirección o algún dato del usuario, pero es sobre el banco

y al dar click en confirmar te manda a una dirección donde ingresan todos sus datos, y los datos registrados se envían directamente al hacker.

- Robo de Cookies

La mayoría de las páginas web de uso personalizado usan cookies, que son formas de guardar información de manera más rápida y eficaz para evitar estarla pidiendo en cada momento, claramente siempre es recomendable autorizar estas cookies solo en sitios de confianza que cuenten con cosas como el certificado SSL. (Wiki Deep web, 2019)

2.La vulnerabilidad de cualquier usuario.

Si bien los mas vulnerables a un ataque cibernético son las grandes empresas o usuarios que manejan información importante, también debemos tener en cuenta que cualquiera puede ser victima de los ciberdelincuentes que se dedican a robar información confidencial de cualquiera que caiga en sus engaños, esta información puede ir desde cosas como fotos privadas que tengamos en nuestros dispositivos hasta información como cuentas bancarias.

Los usuarios en general toman a broma el caso del robo de información vía internet o digital, pese a que en el periodo de septiembre del 2020 la CONDUSEF (Comisión Nacional para la Protección y Defensa de los Usuarios de Servicios Financieros) registro un aumento del 110 % en casos de robo de identidad cibernética lo cual resulta muy alarmante ya que demuestra la poca atención que ponen los usuarios a su seguridad. (Wiki Deep Web, 2018)

2.1.¿Por que existen tantos casos de violación a la privacidad?

Existen varios factores que provocan el robo de datos y de identidad mientras navegamos en internet, dejando de lado los casos que tienen que ver con cosas como el extravío o robo de nuestro dispositivo móvil, la mayoría de los casos se presentan debido a la falta de información que tenemos sobre los riesgos que existen en internet además que la gente que tiene acceso a esta información la ignora o pasa de ella argumentando que son cosas que no ocurren o no son tan comunes como para darle la debida importancia.

Además de esto, la mayoría de sitios web y aplicaciones no cuentan con las medidas de seguridad necesarias para evitar tanto el robo de información como para evitar que alguien use la información de otro usuario sin su consentimiento. Aplicaciones importantes como las pertenecientes a bancos aun tienen fallos en sus sistemas que dejan vulnerable la información y datos de sus clientes/usuarios. (Redacción/DSC., 2020)

2.2.¿Como podemos detectar sitios fraudulentos?

Actualmente la mayor causa de robo de identidad se presenta debido a los sitios fraudulentos que nos piden información delicada de una u otra forma, siendo las mas comunes aquellas que se hacen pasar por nuestros sitios de confianza y de uso diario, las paginas mas “clonadas” por darles un nombre son las redes sociales y paginas donde realizamos compras como lo son Facebook y Amazon, pero la duda es ¿Cómo podemos darnos cuenta de cuales son estos sitios?

Es muy fácil detectar los sitios fraudulentos en internet, las 3 cosas básicas que debes hacer cuando desconfíes de un sitio web son las siguientes:

A. Revisar el certificado SSL: Muchas veces este consejo se da sin siquiera explicarlo para aquellos que no están relacionados con términos tan técnicos, sin embargo esto no es mas que la verificación que tiene un sitio respecto a que tan seguro es acceder a el. Este certificado siempre se encuentra en la barra de nuestro navegador justo al lado de la liga del sitio en el que estamos, usualmente representado con un candado cerrado cuando es considerado un sitio seguro y por el contrario con un candado abierto cuando se trata de un sitio que puede llegar a ser inseguro.

   Si bien esta forma de identificar un sitio riesgoso es útil cuando se trata de paginas que pertenecen a compañías o marcas importantes sigue sin ser una única señal, ya que sitios independientes pueden no contar con esta verificación aun así se trate de un sitio legitimo.

B. Verificar el enlace: Esto puede sonar de lo mas lógico y común del mundo, sin embargo muchas personas pasan de lado este dato o medida de seguridad que consiste en revisar si el enlace que visitamos realmente es el enlace que deseamos visitar, como ejemplo usaremos Facebook la red social mas popular, al ser un sitio de uso común a nunca nos fijamos en si realmente

estamos accediendo al sitio que deseamos ya que no es lo mismo ingresar a www.facebook.com que ingresar a www.facebook.net si bien a simple vista podemos creer que estamos en el mismo sitio nos encontramos en uno completamente diferente. Pese a que muchas empresas han hecho lo posible por eliminar estas paginas desde comprar todos los dominios que puedan ser utilizados con una mala intención (Como es el caso de www.paypal.com que cuenta con el derecho de la dirección www.paypaal.com) aun sigue existiendo el riesgo de encontrarnos con sitios maliciosos.

C. Medios externos: Si por alguna razón aun no podemos determinar si el sitio web en el que estamos es completamente fiable, aun podemos recurrir a herramientas para conocer opiniones y experiencias de usuarios con determinados sitios web, esto puede ser mediante foros como Reddit o incluso con ayuda de herramientas desarrolladas para este fin como lo es scam analyze la cual se dedica a buscar por ti en la red opiniones de los usuarios respecto al enlace que se le brinde. (Redacción/DSC., 2020)

2.3.¿Qué hacer después de un robo de información?

En el caso de ser un mexicano afectado por la ciberdelincuencia lo primero que debes hacer es guarda la calma y revisar que contraseñas, cuentas o tarjetas fueron robadas y actuar de inmediato sobre estas cuentas, en caso de ser una cuenta debemos cambiar las credenciales de acceso por unas completamente diferentes y revisar si se le dio algún uso indebido a nuestra cuenta como extorsionar contactos o alguna otra actividad que pueda traernos problemas. En el caso de una tarjeta es un tema diferente ya que debemos primero que nada comunicarnos con nuestro banco para que cancele nuestra tarjeta y todos los cargos que se hayan hecho a esta.

El banco te puede dar la opción de solicitar un reembolso de dinero en aquellas compras que no reconozcas desde el día que presentas la queja a 3 meses atrás (Este termino es aplicado dentro de la Republica Mexicana pero puede variar en otros países e incluso en entre los diferentes bancos). (Redacción/DSC., 2020)

3.Señales de que hemos sido hackeados

Existen varias formas de saber o darse cuenta si alguno de nuestros dispositivos móviles está siendo ocupado por algún intruso. (BBC, 2018)

Algunos de esos casos se pueden ver cuando el móvil:

- Funciona mas lento, ya sea en general o en algunas apps.

- Algún sobrecalentamiento, que no sea provocado por los componentes

- La batería se agota antes de lo que ya se tiene como estándar.

- Recibes y envías mensajes desconocidos, ya sea por alguna red social o por SMS.

- Ventanas emergentes, suelen aparecer como virus y puede que alguien este atrás de ese virus tratando de robar todo lo posible.

- Compras y apps sospechosas, que pueden verse mucho después de que lo realicen.

Las cosas que son más comunes son:

- Comportamiento inusual.

- Barra de herramientas adicionales.

- Ventanas de publicidad.

- Los antivirus muestran que están deshabilitados.

- Correos a contactos sobre publicidad.

3.1.Medidas sencillas para evitar hackeos.

Existen bastantes formas de evitar el hackeo de nuestros dispositivos sin embargo algunas de ellas son muy complejas para que un usuario común pueda ejecutarlas, estas son las mejores medidas que cualquier persona puede realizar para mantener su información a salvo. (Redacción Capital, 2018)

- Realizar copias de seguridad.

- Intenta quitar el acceso a internet, y verifica que todo se encuentra en orden.

- Tratar de no instalar apps de fuentes no confiables o de lugares no oficiales.

- Tener contraseñas y claves diferentes en cada usuario que tengas.

- En apps buscar que tengan seguridad de doble factor, y siempre tratar de activarlo.

- Cambiar claves y contraseñas con frecuencias, por lo regular que sea cada 2 semanas o por muy tardado 3 meses.

Conclusiones

Para concluir podemos decir que la ciberseguridad en el campo de la informática está teniendo auge en gran medida debido a que, con el paso del tiempo, la tecnología va evolucionando, pero a la vez también los riesgos que se obtienen al tener un sistema de información van cambiando y mejorándose al mismo ritmo que los avances de la tecnología, por ende, es indispensable que cualquier persona que estudie informática o redes de computo entienda los fundamentos básicos del hacking para evitar cualquier tipo de información corrupta en el sistema, así como también la penetración, explotación o extracción de la información en un sistema de la información.

También se recomienda que antes de descargar o entrar a alguna pagina tener antivirus pero sobre todo checar si la pagina es confiable o no y existen varias paginas que te manifiestan si es seguro el sitio al que estas accediendo, además de revisar los indicios que muestran si una pagina es o no segura para ti como usuario, mismos indicios ya citados y explicados dentro de este articulo.

“Es claro que el comportamiento del malware tradicional y técnicas de hacking han cambiado y están evolucionando, haciéndose cada vez más difíciles de detectar; el camuflaje y la suplantación, más el uso creciente de técnicas de ingeniería social, hacen que los sistemas de detección y control tradicionales sean inefectivos”. Javier Santiago E. y Sánchez Allende J.(2017)

Referencias

1. Guevara Soriano A (**2012**). *Hacking Ético: Mitos y Realidades. Seguridad,*12(1),1-6. https://revista.seguridad.unam.mx/numero-12/hacking- %C3 %A9tico-mitos-y-realidades.

2. Javier Santiago E. y Sánchez Allende J.(**2017**). *Riesgos de la ciberseguridad en las empresas. Tecnologi@ y desarrollo*15(1),1-31. https://revistas.uax.es/index.php/tec_des/article/view/1174/964

3. Raphaël RAULT, Laurent SCHALKWIJK, ACISSI, Marion AGÉ, Nicolas CROCFER, Robert CROCFER, David DUMAS, Franck EBEL, Guillaume FORTUNATO, Jérôme HENNECART y Sébastien LASSON.(**2015**). *Seguridad informática - Hacking Ético: Conocer el ataque para una mejor defensa (3ª edición). Barcelona: Ediciones ENI.* https://books.google.com.mx/books?id=4X32wbgtNfUC&lpg=PA50&ots=PsFQxlBbLp&dq=hacking %20etico&lr

4. Giant,N (**2016**). *Ciberseguridad para la i-generación: Usos y riesgos de las redes sociales y sus aplicaciones. Madrid: Narcea Ediciones.* https://books.google.com.mx/books?id=AX69DAAAQBAJ&lpg=PA11&ots=Hrmp1Aja28&dq=ciberseguridad&lr&

5. Piña Libién, H. (**2019**). *Cibercriminalidad y ciberseguridad en MéxicoIus Comitialis,* 2(4), 47-69. https://iuscomitialis.uaemex.mx/article/view/13203

6. Aldeco Pérez R. ,Aguilar Torres G., Cruz Cortés N. ,Domínguez Perez L. ,Escamilla Ambrosio P. ,Gallegos García G. ,... (**2020**). *Introducción a la Ciberseguridad y sus aplicaciones en México. Mexico:*Gina Gallegos García. http://amexcomp.mx/files/LibroCiber-ISBN-V2.pdf

7. (**2020, October 16**). *Robo de identidad y fraudes, otra pandemia en México.Almomento Noticias, Información Nacional e Internacional.* https://almomento.mx/robo-de-identidad-y-fraudes-otra-pandemia-en-mexico/

8. (**2020**). *7 señales de que tu teléfono móvil fue hackeado (y qué hacer al respecto). (s.f.). BBC News Mundo*Recuperado Noviembre 15, 2020. https://www.bbc.com/mundo/noticias-42722806