LA IMPORTANCIA DE LA CIBERSEGURIDAD (THE IMPORTANCE OF CYBER SECURITY)

La Importancia de la Ciberseguridad (The Importance of Cyber Security)

Muñoz Mederos Jorge
jmunozm1700@alumno.ipn.mx
Alumno de M. en I. SEPI UPIICSA IPN
Dra. Vicario Solórzano Claudia Marina
marina.vicario@gmail.com
IPN-UPIICSA
Dr. Álvarez Cedillo Jesús Antonio
jaalvarez@ipn.mx
IPN-UPIICSA

Resumen

En el día a día nos encontramos expuestos a múltiples situaciones que pueden poner en riesgo no sólo nuestra integridad física sino también nuestra privacidad y datos confidenciales, al navegar en el ciberespacio podemos encontrarnos gran cantidad de información de nuestro interés y a la vez podemos encontrar gran cantidad de malware, entender a qué estamos expuestos, como protegernos y en que nos puede afectar es de lo que trata este trabajo cuya finalidad es entender más sobre ciberseguridad.

Abstract

On a daily basis we are exposed to multiple situations that can put at risk not only our physical integrity but also our privacy and confidential data, when navigating in cyberspace we can find a lot of information of our interest and at the same time we can find a great quantity of malware, understanding what we are exposed to, how to protect ourselves and what can affect us is what this work is about, the purpose of which is to understand more about cybersecurity.

Introducción

La vida ha evolucionado desde el principio, ahora es evidente esta verdad, independientemente de la religión que profesemos. Desde siempre hemos tenido que adaptarnos para poder sobrevivir, estas adaptaciones son inherentes en los seres humanos y me atrevería decir en los seres vivos en general, nos hacen resistentes y hasta inmunes a enfermedades causadas por distintos factores externos como bacterias, virus, parásitos entre otras.

Como resultado esta evolución nos ha hecho seres sumamente inteligentes, nuestra inteligencia nos ha permitido desarrollar distintas destrezas en diversos tópicos que nos han hecho idear "artefactos" tan simples como la rueda y tan complejos como las computadoras que han facilitado nuestras labores diarias y nada nos debe sorprender el hecho de que nuestros "artefactos" también puedan evolucionar, estar inmersos en un ciclo de mejora continua lo cual muchas veces conlleva a la innovación, creando "artefactos" nuevos, más poderosos y más livianos.

Las computadoras poco a poco se han metido en nuestras vidas, primero en los ambientes plenamente científicos donde fueron creadas y preparadas para realizar distintas actividades, posteriormente en nuestros centros de trabajo ayudándonos a realizar nuestras labores diarias, dicha característica las introdujo en nuestros hogares donde continuaron facilitando la labor escolar de nuestras familias, ahora no es sorprendente encontrarlos en el bolsillo de las personas, pero el hecho de que estos "artefactos" hayan evolucionado y se hayan propagado por cada uno de los lugares que habitualmente ocupamos como el trabajo, banco, hogar y con nosotros mismos como compañeros de viaje nos hace vulnerables a cualquier cosa que los afecte, es decir, al mantener información personal en ellos nosotros mismos quedamos expuestos en caso de que exista una intrusión no autorizada en los mismos.

El que estos "artefactos" estén con nosotros en cada aspecto de nuestra vida, controlando las actividades prioritarias como transacciones bancarias, comunicaciones con nuestros familiares y amigos, brindando control de acceso a nuestros lugares de trabajo y hogares los hace un blanco sumamente interesante para todos aquellos que quieran obtener control sobre todo lo que se involucra en cada una de esas actividades.

"La ciberseguridad es un proceso que implica prevención, detección y reacción o respuesta, y debe incluir un elemento de aprendizaje para la mejora continua del proceso en sí" (A. M. Rea-Guaman, I. D. Sánchez-García, T. San Feliu, J. A. Calvo-Manzano, 2017, p1). Ésta será la herramienta de la que se hablará a continuación.

¿Cómo nos interconectamos y a que estamos expuestos?

La vida es maravillosa, nos muestra a cada instante lo grandiosa que es, vivir hoy en día podría parecer más sencillo comparado con lo que en otros siglos ha sido, ya que desde nuestra casa o incluso desde nuestro dispositivo móvil llámese celular, Smartphone, Computadora portátil o tableta electrónica podemos realizar infinidad de operaciones bancarias, comprar y

administrar bitcoins, pagar nuestros servicios, vigilar a nuestros niños que están con la niñera en casa o en el colegio, ver videos online, etc., sin embargo, contrario a lo que todos podrían pensar hoy en día vivir es tan o más peligroso como hace siglos, pues en este preciso momento el enemigo está oculto en un mundo que pocos conocen y aún menos son capaces de ver lo que sucede en él.

La sensación de seguridad en el mundo real está dada por un conjunto de medidas "simples" hasta cierto punto, como lo son colocar el cerrojo en las puertas, decirles a tus hijos que no hablen con extraños, quitar cualquier cosa que pueda obstruir el paso en caso de evacuación, etc. Pero ¿Qué sucede cuando el enemigo del que debes protegerte se encuentra en tu casa, escondido donde no lo puedes localizar fácilmente, junto a las personas que más amas, esperando a ser activado o transmitiendo todo lo que realizas en tu computadora e incluso viendo lo que pasa por tu red?, pues bien, todas esas "amenazas" son tan reales como los asaltantes de la cuadra y tan o más peligrosos que ellos.

Pero ¿Desde cuándo existen estas amenazas?, ¿Cómo entraron en tú casa? Todas esas preguntas y más son las que se intentará responder para brindar una perspectiva más amplia con el fin de crear una conciencia de lo vulnerable que podríamos ser ante estas "ciberamenazas".

Se iniciará hablando de eso que hace posible que desde cualquier lugar seamos capaces de conectarnos a internet y realizar múltiples actividades desde nuestro Smartphone, aquello que usamos pero que no tenemos entendimiento pleno de ello, y eso es el ¿Cómo nos conectamos desde nuestro celular, tableta u otro dispositivo a internet?

La mayoría de las conexiones que realiza nuestra computadora, celular, tablet o dispositivo electrónico por medio de las apps que instalamos para nuestras labores diarias las realiza a través de la arquitectura cliente servidor donde "diversos dispositivos se conectan con un servidor central" (Marco Todescato, Andrea Carron, Ruggero Carli, Gianluigi Pillonetto, Luca Schenato, 2017, p. 284), que ha sido también denominada por los mismos autores como "comunicación de estación uno a base", en ella cada una de las apps que operamos se comunica de manera centralizada a un servidor configurado por quien realizó la aplicación, de este servidor obtiene los datos solicitados necesarios para satisfacer el requerimiento del cliente, estos pueden ser desde el clima en alguna localidad determinada hasta el estado actual o histórico de su cuenta de nómina bancaria, sin embargo existe otra arquitectura de comunicación llamada p2p (*peer to peer*) utilizada para el intercambio de archivos entre usuarios iguales próximos "vecinos", hasta por los ya mundialmente conocidas bitcoins o blockchains, dentro de este tipo de arquitecturas de comunicaciones, quizá la más utilizada para cometer actos denominados ilegales es la última mencionada (p2p) puesto que permite la transmisión "anónima" de contenido legal o ilegal no obstante es un medio denominado "idóneo aunque ineficiente" (Félix Brezo, Yaiza Rubio, 2017, p. 36) para darle soporte a las transacciones realizadas con bitcoins y blockchains.

Una vez presentada la manera de operar de estas arquitecturas básicas de comunicación entre nuestros dispositivos y el mundo exterior falta definir el medio de comunicación es decir la manera en que viajan nuestras peticiones desde nuestro dispositivo hasta el servidor que atenderá nuestro requerimiento, estrictamente hablando sólo existen dos maneras distintas de hacerlo la primera por medio de un medio físico (alámbrica) y la segunda sin necesidad de un medio físico denominado de manera inalámbrica, para la mayoría de las personas la manera más sencilla de conectarnos a la red es por medio inalámbrico sin embargo también es la más riesgosa, se tratará esto en dos partes, primero se describe la comunicación alámbrica: "Es aquella forma de comunicación eléctrica en la que se necesita un soporte físico para la transmisión de la señal electromagnética"(Carvajal P., 2017, p. 71), el medio físico puede ser cable utp, coaxial, fibra óptica o algún otro medio físico de transmisión, es decir, para que un dispositivo envíe la señal al servidor depende de la existencia del medio físico, sin él dicha transmisión no existiría, la configuración de los distintos tipos de cable es diferente, un medio físico puede transportar diversos tipos de datos como son mensajes, datos, voz y video. La velocidad de transmisión de datos es distinta también entre cada medio alámbrico, siendo el más rápido la fibra óptica. Ahora bien, como parte dos se describe la conexión inalámbrica, la comunicación inalámbrica básicamente es aquella realizada a través de un emisor y receptor inalámbrico y que hace el uso del espectro radio eléctrico como medio de transmisión de datos por medio de un proceso conocido como modulación de la onda portadora, todos los datos que se pueden transmitir de manera alámbrica son también posible transmitirlos de manera inalámbrica, sin embargo, la velocidad de transmisión de manera inalámbrica es menor que la de manera alámbrica.

Hasta este punto hemos sido testigos de otra "evolución", en este caso en la manera de cómo se comunican nuestros dispositivos, es decir, en un inicio la única manera de comunicarse era de manera alámbrica, que hasta cierto punto brindaba seguridad efímera ya que solamente las computadoras conectadas al medio físico eran capaces de recibir y transmitir información entre ellas haciendo que cualquier persona que quisiera atacar nuestros equipos debiera estar físicamente presente en el lugar en el que se realizaría el ataque o por lo menos debería tener acceso a un nodo de nuestro hub/switch para las empresas que tenían únicamente intranet como medio de comunicación con las distintas áreas de la misma, aquí es donde llega el siguiente paso "evolutivo" para las empresas, el cual fue la creación y el uso de internet (llamada también red de redes) esta evolución brindaba una nueva gama de posibilidades a las empresas permitiendo acercarse a los clientes para brindar una nueva experiencia en cuanto a la venta de productos y servicios se refiere. Cuando una empresa tiene algún sitio en la red sólo "expone" los servidores que tienen sus aplicaciones ejecutándose, dicha exposición en el inicio de internet carecía de medidas de seguridad adecuadas posibilitando el ataque desde internet hacia la compañía permitiendo que el ataque se realice remotamente, a veces hasta por distintos equipos alrededor del mundo. Con la tecnología inalámbrica, esto empeoro, ya que cualquier equipo de comunicación inalámbrico con la configuración inadecuada y/o por

medio de herramientas sofisticadas capaces de hacerse pasar por algún dispositivo perteneciente a nuestro dominio le permite acceder a algún atacante a nuestros dispositivos sean de nuestra empresa, trabajo u hogar, cabe resaltar que sin importar la manera en que nos comuniquemos, es decir, el medio que usemos la información que enviamos puede ser interceptada y vista por personas no deseadas, para complicarles esta tarea a los atacantes se han establecido diferentes medidas de seguridad, ya que es seguridad en nuestro mundo virtual se le denomina ciberseguridad, en cualquiera de los mecanismos de conexión antes descritos podríamos ser blanco de algún ataque cibernético ya sea al utilizar la arquitectura cliente-servidor, peer-to-peer, utilizando conexión alámbrica o inalámbrica en cualquiera de esas situaciones en nuestra vida cotidiana a veces sin saberlo podríamos ser vulnerables a los siguientes ataques: Virus Informáticos, Ingeniería Social, footprinting, scanning y enumeración, sniffers, etc.

Pero ¿Desde cuándo existen estas amenazas? El primer registro de virus informático que afectó a internet del que se tiene registro ocurrió en 1988, por lo que estas amenazas no son nuevas, y han tenido también como característica la peculiaridad llamada evolución, tal como los "artefactos" que afectan, esto ha hecho que se diversifique el tipo de virus, el tipo de objetivos que atacan y otras características más de su comportamiento.

Ahora bien ¿Por qué somos más vulnerables? La respuesta parece ser simple, anteriormente la mayoría de las familias de clase media en los Estados Unidos de Norteamérica tenía cuando mucho una computadora en casa (1998), computadora que se utilizaba para realizar múltiples actividades diarias, concluir trabajos atrasados de la oficina, realizar tareas escolares, ver videos en la red, etc., pero últimamente el "abaratamiento de la tecnología" ha hecho estos dispositivos de más fácil acceso permitiendo que existan hasta más de dos por familia de clase media sin contar a los smartphones y tabletas, este número se multiplica hasta por tres en las familias pertenecientes a la clase alta.

Pero como ya se comentó, existen dispositivos que viajan con nosotros, mismos a los que les prestamos poca atención y que pueden ser el principal blanco de un ataque ya que la mayoría de ellos o tiene poca seguridad o carece de ella, al igual que pueden tener una puerta de entrada permanentemente abierta y sin protección por medio del bluetooth, se trata de los dispositivos móviles y algunos dirían que hasta los wearables que recopilan información de nosotros en cada momento, tal como ¿Cuánto tiempo dormimos?, ¿Cuantos pasos dimos en el día? ¿Cuántos periodos de inactividad tuvimos en el día?, etc.

Existen diferentes acciones que se han tomado para brindar seguridad en el mundo virtual, esto forma parte de lo que es llamado ciberseguridad, entre las diferentes medidas que se han establecido para salvaguardar las conexiones inalámbricas destacan los cifrados WEP (Wired Equivalent Privacy), WPA(Wi-Fi Protected Access) y WPA2 (Wi-Fi Protected Access 2) y con ellos la IEEE introdujo el estándar 802.11 mismo que se ha modificado y actualizado en muchas ocasiones con la finalidad de hacerlo más seguro, la versión 802.11i es el estándar certificado predilecto al día de hoy, esta versión usa el cifrado AES (Advanced Encryption Standard), cabe resaltar que a pesar de que los primeros dos fueron obsoletos desde hace algunos años y el que parecía más "estable" y/o "robusto" ya ha tenido problemas con algo llamado KRACK Attack (Key Reinstallation Attack) detectado por el investigador Mathy Vanhoef (2017), mismo que dice lo siguiente: "este ataque básicamente le otorga acceso al atacante a ciertos sectores de la comunicación permitiéndole incluso acceder y modificar datos sensibles", entre estos datos se encuentran los números de tarjetas de crédito, cuentas bancarias y otros mecanismos de pago, sin embargo una de las "ventajas" por llamarlo de alguna manera de esta vulnerabilidad es que el atacante debe estar dentro de nuestra red WiFi, es decir, debe estar en las inmediaciones de nuestra zona de alcance, dando pie a que sea detectado y detenido ya que se encuentra cerca del perímetro y no pertenece a la organización cual sea que sufra una ataque por esta vulnerabilidad, como es evidente esta vulnerabilidad no permite ataques desde internet sólo desde nuestra red local, sin embargo, las compañías fabricantes de tarjetas de red inalámbricas, sistemas operativos, modems, routers y otros dispositivos de conexión inalámbrica están trabajando en parches para resolver estos inconvenientes. Al momento de escribir este ensayo únicamente Microsoft había publicado el parche en cuestión por medio de su servicio Windows Update para todos los dispositivos que utilicen ese sistema operativo como parte funcional de ellos.

Lo anteriormente comentado es sólo un ejemplo de ataque cibernético, muy parecido al llamado "Man in the middle" en el que un tercero monitorea toda la actividad que tenemos en la red infectada, de acuerdo con Zhe Chen (2017) en este ataque: "Dos amenazas básicas incluyen la intercepción de datos en el radio de alcance de la interfaz y el acceso ilegítimo a servicios inalámbricos. La intercepción de los datos del usuario puede ocasionar la pérdida de confidencialidad de la información sensible del usuario. El uso ilegítimo del servicio no solo es motivo de preocupación con respecto a la facturación correcta, sino también de preocupación con respecto al enmascaramiento: hacerse pasar por un operador de red o un proveedor de servicios para interceptar los datos del usuario". Con este ataque, alguien obtiene acceso a nuestras publicaciones, fotos compartidas en Facebook/Twitter/Instagram/Tumblr, el acceso a esas cuentas de redes sociales, al igual que a nuestros usuarios y contraseñas de correo electrónico y de cuentas bancarias, es decir cualquier cosa que hayamos realizado en esa red, las redes públicas o gratuitas son las que principalmente están expuestas sin contar a las de los hogares, ahora bien existen artículos científicos donde se ha expuesto la vulnerabilidad en las redes de compañías celulares, el autor Ulrike Meyer (2004) dice que: "un intruso puede

espiar todo el tráfico iniciado por la estación móvil en redes 3G", es decir, se pudo obtener información relevante de los usuarios de esas compañías simplemente analizando el tráfico que existía sobre ellas al momento de atacar la red.

¿Pero cómo estamos en México?, ¿Es una amenaza vigente en nuestro país el KRACK Attack o Man in the middle para la Estrategia Digital Nacional, en específico en cuanto a conectividad se refiere?, No es raro creer que nos encontramos estancados en este punto en especial cuando el Gobierno Federal a través del programa llamado "México Conectado" como parte de la Estrategia Digital Nacional ofrece conexiones gratuitas a internet en ciertos puntos en todo el país, una estrategia funcional pero plenamente peligrosa en especial después de exponer las nuevas vulnerabilidades encontradas y de todos los atacantes que se pueden encontrar alrededor de este punto de acceso gratuito, el portal del programa no ofrece información respecto a actividad alguna para solventar la vulnerabilidad mencionada ni mucho menos información sobre si existe alguna especie de monitoreo en cada punto de acceso, lo cual no sólo es peligroso sino existe, pues de existir cualquier tráfico generado en ella ha sido y será visto por un tercero, por lo que este punto específico dentro de la Estrategia Digital Nacional debería ser revisado y a las personas que usen este servicio del Gobierno Federal se les debiera notificar si es que sus datos están siendo expuestos a escrutinio de un tercero ya sea legalmente o no, violando la privacidad de los usuarios del mismo.

Los ataques de los que anteriormente se ha hablado han causado que los estándares sean cada vez más complejos de implementar en especial si se desea compatibilidad con cifrados anteriores como es el caso de WPA2 que ofrece compatibilidad con cifrado WEP, por medio de cómputo de cifrado intensivo WPA-AES, como es esperado, no todos los productos son compatibles/susceptibles de ser actualizados, los que no lograron ser actualizados en el uso del protocolo WPA2 por práctica de seguridad deberían ser desechados ya que son un riesgo inminente para la seguridad de la compañía u hogar que los posea y utilice como acceso a la red inalámbrica.

Conclusión

Necesitamos más herramientas de software y hardware que nos ayuden a realizar nuestras labores diarias, estas herramientas no sólo deben satisfacer la necesidad por la cual fueron fabricadas sino que también deben ofrecernos algún mecanismo de seguridad para garantizar que solamente el propietario y si acaso el fabricante puedan tener acceso a ellos ya sea para realizar un simple diagnóstico remoto o para extraer el contenido de su tarjeta de memoria, el internet de las cosas (IoT) y su evolución el internet del todo (IoE) son cibertendencias que está por venir y de las cuales ya se escucha bastante, a pesar de lo nuevo de esta última cibertendencia (IoE) terminará utilizando algún medio y arquitectura de comunicación con nosotros mismos por medio de dispositivos de cómputo pero sobre todo con el medio exterior por medio de conexiones con distintos dispositivos, nuestra capacidad tecnológica debe

incrementarse aún más al grado de mantener a raya a todas estas nuevas “puertas” que se abrirán en nuestros hogares ya que de no ser así seremos vulnerables en más de un sentido.

Referencias:

1. A. M. Rea-Guaman ; I. D. Sánchez-García ; T. San Feliu ; J. A. Calvo-Manzano (2017) Maturity models in cybersecurity: A systematic review, IEEE Xplore DOI: 10.23919/CISTI.2017.7975865.

2. Félix Brezo y Yaiza Rubio (2017), Bitcoin: La tecnología Blockchain y su investigación, Barcelona España, Editorial 0xWord, ISBN: 978-84-617-6979-7
3. Francisco Carvajal Palomares, 2017, Manual. Instalación y actualización de sistemas operativos, España, Editorial Transversal, ISBN: 978-84-681-7816-5
4. Izaskun Pellejero, Fernando Andreu, Amaia Lesta (2006), Fundamentos y aplicaciones de seguridad en redes WLAN, Barcelona España, Editorial Marcombo, ISBN 84-267-1405-6
5. Marco Todescato, Andrea Carron, Ruggero Carli, Gianluigi Pillonetto, Luca Schenato (2017), Multi-robots Gaussian estimation and coverage control: From client–server to peer-to-peer architectures, Automatica 80 (284–294)
6. Mathy Vanhoef, 2017, Key Reinstallation Attacks Breaking WPA2 by forcing nonce reuse, Recuperado el 20 de Noviembre de 2017, de https://www.krackattacks.com/
7. Ulrike Meyer, Susanne Wetzel (October 2004), A man-in-the-middle attack on UMTS, 90-97, ISBN:1-58113-925-X
8. Zhe Chen ; Shize Guo ; Kangfeng Zheng ; Yixian Yang (2007), Modeling of Man-in-the-Middle Attack in the Wireless Networks, IEEE Xplore