Revista Científica y Tecnológica UPSE, Vol. III, N. 2, Pág. 113-117 (Jun., 2016)

18

SEGURIDAD INFORMÁTICA O SEGURIDAD PERSONAL, EVOLUCIONANDO CON LA TECNOLOGÍA.

José Ramírez Mejía, Karina Villao Rodríguez, Omar Orrala Palacios, Juan Garcés Vargas.

SEGURIDAD INFORMÁTICA O SEGURIDAD PERSONAL, EVOLUCIONANDO CON LA TECNOLOGÍA

José Ramírez Mejia[1]; Karina Villao Rodriguez[2]; Omar Orrala Palacios[3]; Juan Garcés Vargas[4]
[1]Escuela Superior Politécnica del Litoral
[2, 3, 4] Universidad Estatal Península de Santa Elena
jl.ramirez@outlook.com[1], kvillao@upse.edu.ec[2], omarorrala@upse.edu.ec[3], jgarces@upse.edu.ec[4]

Resumen

El presente artículo tiene como finalidad mostrar como la seguridad personal deja de ser una actividad que requiere solo atenciones físicas, sino que debido a la constante evolución de la tecnología y su proyección al always connected (forever Online) pasa a ser necesario darle nuestra atención en el plano virtual. Y, ¿qué es el plano virtual? El plano virtual hoy en día todos lo conocemos y es el Internet, esta plataforma es donde muchas empresas colocan sus productos o servicios que desde una primera instancia parecen ser inofensivos y brindan mucha facilidad a los usuarios (nosotros) para conseguir la información necesaria de nuestro día a día, pero ¿realmente es así? ¿Cuánto conocemos sobre nuestra exposición en la gran red de redes? ¿Nos encontramos realmente seguros? estas y otras preguntas son las que irás resolviendo en la lectura de este artículo.

Palabras Claves: *seguridad, evolución, tecnología, virtual, Internet, servicios, exposición.*

Abstract

This article shows us how the personal security ceases to be an activity that only requires physical attention. Due to the constant evolution of technology and the concepts always connected (forever Online), we must pay attention to the virtual mode. However, what is the virtual mode? The virtual mode is something we all know about it is Internet, this platform is where many companies place their products or services, at first glance, it seen is to be harmless while it provides facilities to users (ie ourselves) in order to get the necessary information for our everyday life; but is it really so? How much we know about our exposition to the Internet? Are we really safe? These and other questions are the ones you will solve through reading of this article.

Keywords: *security, evolution, technology, virtual, Internet, services, exposure*

1. Introducción

Debido al constante avance tecnológico y a la creciente demanda de productos sobre el Internet, las empresas del mundo brindan una gama amplia de servicios a sus clientes, facilitando de esta manera las actividades que necesiten realizar dentro o fuera de las organizaciones, sin necesidad de asistir de manera personal a las instalaciones de la misma.

Sin embargo, muchas empresas olvidan lo importante y necesario que es contar con seguridad de la información dentro de su infraestructura tecnológica con los suficientes procedimientos que permitan eliminar las grietas de acceso no autorizadas que dan paso a la fuga de información que luego es utilizada con fines maliciosos.

Pero, ¿son las empresas realmente las únicas culpables de brindar información por no tener el cuidado respectivo? No. Nosotros como usuarios tenemos mucha responsabilidad y participación en tener nuestra información publicada y es necesario aplicar recomendaciones de seguridad para mitigar las amenazas a la cual nos encontramos expuestos en el Internet de las cuales se aprovecha el mundo real.

¿Y en donde son esos lugares en los que se encuentra publicada nuestra información? Muchos de esos lugares van a depender de cuan socializados nos encontremos en la actualidad y no nos referimos a visitar a los amigos o atender a los vecinos, sino al hecho del uso de las redes sociales en Internet,que van simplemente desde usar las aplicaciones mayormente difundidas en el mercado como lo son Facebook, twitter, instagram, etc.

Figura 1.1. Redes Sociales interrelacionadas

No obstante, dejar de usar estas aplicaciones u otras parecidas no nos va a garantizar que estaremos realmente seguros y en el anonimato total ante un atacante, y esto es simple, dado a que no existe la seguridad al 100%.

2. Evolución de la tecnología

Regresando un poco en el tiempo, recordaremos que el acceso tecnológico era prácticamente limitado, nuestros padres, abuelos, tíos se comunicaban por medio de cartas, una visita a los familiares, llamadas telefónicas del sistema analógico (convencional), etc. de esta manera es como se mantenía una comunicación a la antigua. Luego, este sistema fue evolucionando, comenzaron aparecer los computadores personales, telefonía celular y hasta el mismo Internet que en sus inicios fue una plataforma única de solo texto.

La tecnología no conforme comenzó a incorporar interfaces gráficas, juegos interactivos, equipos inteligentes, ¿equipos inteligentes? Sí es lo que denominamos smartphones, tablets o todo aquello que contenga un sistema operativo base como es el Android, Apple IOS, Windows, etc. Esto nos cambió la forma de ver al mundo, puesto a que ya no es necesario ir a una biblioteca de manera presencial para saber un poco más de historia, o de correr a un diccionario a descifrar el significado de una palabra.

Para donde apunta todo esto, según las investigaciones de tendencias tecnológicas esto va al punto que todo lo coloquemos como ropa, es decir sea de alguna manera inteligente (wearable) y que de alguna forma nos encontremos conectados al mismo tiempo al Internet.

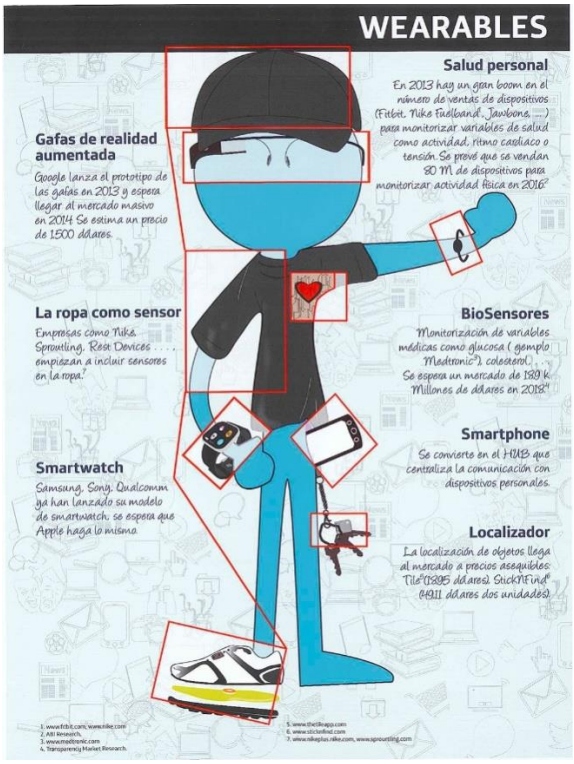

Figura 2.1. Tendencia futurista de la tecnología [0]

Muy bien, entonces si la tendencia es ésta ¿qué ocurre con nosotros? Lo que ocurre es que nos estamos olvidando de progresar en conjunto a la tecnología, no es suficiente con adaptarnos. Cada cambio tecnológico involucra que también nos informemos lo suficiente del pro y contra para sacarle el mejor provecho al producto vigente, con esto minimizamos nuestro riesgo a la exposición conociendo qué tipo de información estamos permitiendo al fabricante leer y publicar en la red de redes.

Y, si no presto atención a esto o no evoluciono con la tecnología ¿qué podría ocurrir? Podríamos decir que en la vida no hay víctimas...solo voluntarios.

En cambio en las organizaciones debido a las exigencias del mercado y para brindar mayor flexibilidad a sus clientes, colocan varios servicios en Internet sin los controles y permisos de acceso necesarios que garanticen la integridad, disponibilidad, confidencialidad y no repudio de sus sistemas. Esto se debe, que aún en la cultura de las empresas se toma muy ligeramente los temas relacionados con la seguridad de la información (especialmente nuestro país), lo que resulta en pensar que es suficiente colocar un único equipo firewall multipropósito que proteja sus redes contra los diferentes ataques de los crackers.

Figura 2.2. Hackers, crackers, personaje desconocidos del Internet

El ejemplo típico es una entidad financiera pyme quién tienen este tipo de solución única que le genera un punto de fallo con poca capacidad de procesamiento de hardware (procesador, memoria y disco) soportando todo el tráfico de entrada y salida de la red, concentrando el esfuerzo de seguridad en un diseño de red perimetral pobre dependiente de un solo dispositivo, constando que los diferentes servicios en línea que tienen las instituciones financieras están expuestos a una gran cantidad de amenazas que afecta el correcto funcionamiento de sus productos en Internet.

3. Seguridad informática o seguridad personal

A lo expuesto, debemos analizar entonces como protegernos desde un punto de vista informático y es allí donde podemos tomar en referencia un libro de la colega en materia de Seguridad de la Información Ing. Karina Astudillo, que nos da una pauta sobre los términos y acciones de hacking que se manejan hoy en día.

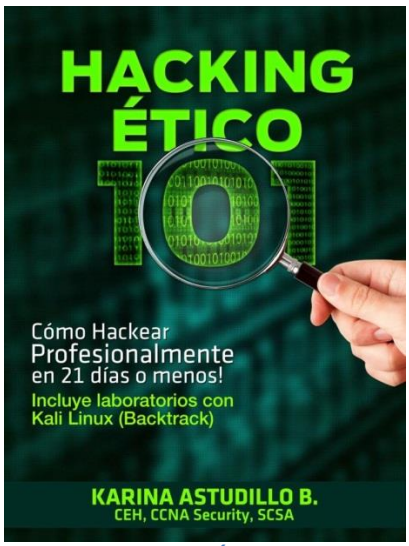

Figura 3.1. Libro de Hacking Ético de nuestro mercado nacional

La finalidad de la lectura del libro señalado no es volvernos unos expertos en la materia, para esto necesitamos años de estudio e investigación pero si vamos hacer referencia al punto denominado "ingeniería social", que refiere a la obtención de la información a través de la manipulación de las personas, es decir que aquí el hacker adquiere datos confidenciales valiéndose del hecho bien conocido de que el eslabón más débil de la cadena de seguridad de la información son las personas.

La ingeniería social normalmente es usada en la fase de levantamiento de información o como le denominan los especialistas en la materia la fase de "Reconocimiento" y como sabemos consiste en obtener información de la víctima que en nuestro caso es la persona. Obtener esta información no es nada complicada, para ello vamos hacer una pequeña lista de los servicios que la ofrecen:

- Redes Sociales (Facebook, Twitter, Instagram, Periscope, Snapchat, Tinder, etc.)
- Universidades (listado de estudiantes aprobados, trabajos publicados, proyectos académicos, etc.)
- Servicios públicos del estado (Consulta de información en línea)

Pero, ¿cómo funciona esto? Sencillo, pensemos como un atacante que tiene una persona objetivo para cualquier fin de beneficio propio, en la actualidad ¿qué podría hacer? Simple:

1. Iniciar una búsqueda con los nombres de la persona en el gran motor del Internet, "Google". Desde algo tan básico como colocar puramente el nombre en la caja de texto del buscador o como usar el Google Dorks que de referencia tenemos el sitio de exploit-db.
2. Comenzar a revisar las redes sociales y comprobar donde se encuentra registrado publicando estados sin restricciones o para todos.
3. Gracias a la búsqueda en Google (Bing, Dogpile, duckduckgo, etc.) podríamos obtener información de la universidad a la que asiste, clásico un listado de haber aprobado una materia, un trabajo o el pre-universitario de la U.
4. Consultar los servicios del estado del país al que perteneces (en nuestro caso Ecuador), lo que nos daría el número de cédula, completar información académica, verificar información del registro civil e incluso confirmar si posee un número convencional de teléfono que nos daría acceso casi de manera indirecta a la

dirección del domicilio, haciendo uso de sitios como consulta de títulos de bachilleres, títulos registrados, registro civil, CNE, SRI, consulta de citaciones CTE, etc.

Con esto un atacante en nuestro país puede formar un perfil casi exacto de la víctima y conocer nuestros movimientos como por ejemplo: Si estamos en casa, salimos de viaje, bienes que poseemos, propiedades, parentescos, lugares que frecuentamos. Dando posibilidades a que seamos voluntarios a un acto no deseado como robo de nuestro domicilio, secuestros exprés, acoso, extorción o sin ser tan extremistas también podemos tener una buena sorpresa como una bella serenata quizás, ¿Por qué no?

Todo esto con el simple hecho de realizar un levantamiento de información de la víctima a través de la ingeniería social, por esto la seguridad informática deja de ser un atributo único de las empresas (indiferente de su tamaño) sino que debe ser considerado como parte de nuestra seguridad personal con el mundo virtual que hoy manejamos.

Entonces, ¿Es posible eliminar toda nuestra información pública? Si y no, si podemos restringir el acceso a la información que ya tenemos en la gran red, y eso lo logramos conociendo y modificando las características de seguridad que trae las aplicaciones que manejamos, un ejemplo de ello sería:

1. Nuestras publicaciones no deben ser abiertas a todo el público.
2. No divulgar nuestras ubicaciones de manera inmediata de donde nos encontramos.
3. No aceptar usuarios o perfiles que desconozcamos.
4. No creer en todo correo que nos llega por que de seguro trae escondido consigo un software o programa malicioso que puede extraernos información de nuestro equipo.
5. Deshabilitar GPS de nuestro dispositivo cuando hacemos transmisiones en línea para no delatar nuestra ubicación, como en el caso de periscope.
6. Usar más de una forma de autenticación, es decir no solamente el famoso usuario y clave, sino también generadores de claves únicas temporales (OTP) que validen como según factor de autenticación, ¿esto existe para los usuarios finales? Sí existe, lo tiene Microsoft, Google hasta el mismo Facebook de manera gratuita.

Sin embargo respecto al no, podemos indicar que no es posible eliminar toda la información pública que ya existe, porque para ello muchas empresas locales deben cambiar su forma de ver la disponibilidad del servicio versus la incorporación de metodologías base de seguridad que imposibilite a cualquier sencillo husmeador obtener acceso a ella.

¿Y las empresas que podemos hacer? Comenzar a trabajar en nuestra cultura organizacional y difundir el nuevo mensaje de seguridad de la información a nuestros usuarios internos, esto involucra al mismo personal de sistemas, quién cree que colocar un único firewall lo soluciona todo apostando que el siguiente modelo de red es más que suficiente para proteger a la organización:

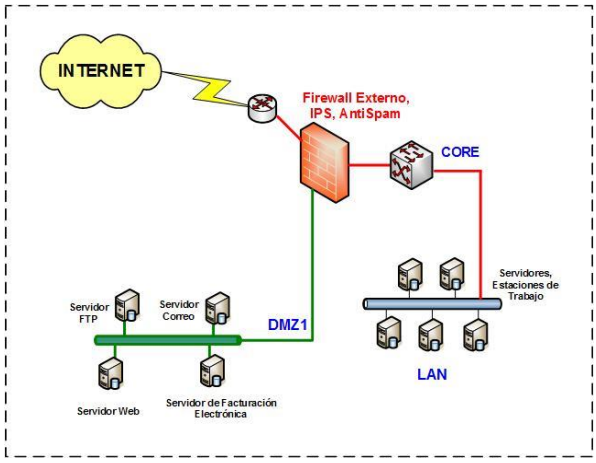

Figura 3.2. Diseño actual de las redes organizacionales despreocupadas

¿Qué podemos hacer si nos encontramos de esta manera? Es tiempo de realizar una propuesta de re-diseño de la red perimetral de la organización incorporando recomendaciones de seguridad tomando como marco referencial las regulaciones y mejores prácticas existentes para las empresas del sector, un ejemplo sería el sector financiero donde las normativas son dictaminadas por la Junta Bancaria y Auditadas en su cumplimiento por la Súper Intendencia de Bancos (SBS) del Ecuador.

Un extracto general de las resoluciones consideradas en la actualidad a nivel perimetral es:

1. Resolución JB-2012-2148, Literal 4.3.8.3 [1]
2. Resolución JB-2012-2148, Literal 4.3.11.5 [1]
3. Resolución JB-2012-2148, Literal 4.3.11.8 [1]
4. Resolución JB-2014-3066, Artículo 22 Literal 22.7 [2]

Aunque las resoluciones son muchas más, las señaladas con su respectivo literal indican que debe incorporarse en la red dispositivos que contribuyan con el control, aseguren la integridad, disponibilidad, confidencialidad de la información de la organización mitigando la posibilidad de captura de los datos por terceros no autorizados. Para cumplir con lo señalado

en los literales mencionados, se considera la inclusión mínima de los siguientes equipos en el nuevo diseño de red perimetral:

1. Mitigador de ataques con módulo IPS
2. Implementación de firewall externo
3. Implementación de firewall interno
4. Firewall de aplicaciones web

Sin olvidarnos de las buenas prácticas donde la primicia es descentralizar la carga de trabajo, incorporamos los siguientes dispositivos para crear diferentes capas de seguridad y acceso hacia nuestra red:

5. Implementación proxy server
6. Sistema anti spam y de cifrado de correo electrónico
7. Balanceador de tráfico

Seccionando el esquema de nuestra red a un nuevo diseño perimetral que tendrá las siguientes zonas establecidas [3]:

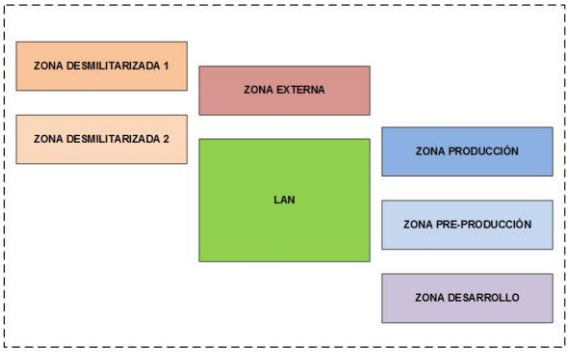

Figura 3.3. Definición de zonas protegidas de la red

El re-diseño de la red ahora incorpora recomendaciones de seguridad locales (vigentes en Ecuador) e internacionales [4] (tomadas de Cisco Systems) para la institución financiera (pyme).

4. Conclusiones

Ya no vivimos en una era sencilla, ahora la tecnología nos acompaña en todo momento recopilando cada vez más información nuestra, exponiéndonos a situaciones no deseadas, por esto ya no podemos tomar a la ligera el mantener siempre nuestra conexión en línea sin incluir las debidas restricciones de acceso a esa información por parte de terceros.

Podemos ver que ahora esto no es solo una actividad de las compañías del mercado, sino que requiere de nuestra colaboración y participación activa obteniendo al máximo los beneficios del uso de la tecnología a nuestro favor sin afectar la privacidad de nuestras vidas.

Las soluciones recomendadas para las organizaciones van a mostrar estabilidad y eficiencia a través de los controles aplicados al tráfico de la red generado por los usuarios internos/externos de la organización, y darán la flexibilidad de personalizar cada política en caso de que sea necesario, pero no olvidemos que sólo estamos fortaleciendo el 20% de nuestra red y que aún necesitamos trabajar sobre el 80% de donde se originan los ataques (que provienen del usuario interno).

Y sí, invertir organizacionalmente en seguridad requiere de un presupuesto bien justificado para que nuestra alta directiva considere necesario apostar por este rubro.

5. Bibliografía

[0] Los wearables ya forman parte de nuestra vida http://www.masquenegocio.com/2014/04/16/los-wearables-ya-forman-parte-de-nuestra-vida/

[1] Junta Bancaria del Ecuador - SBS, ResoluciónJB-2012-2148,http://www.sbs.gob.ec/practg/sbs_index?vp_art_id=760&vp_tip=2, Publicada el 26 de Abril del 2012

[2] Junta Bancaria del Ecuador - SBS, Resolución JB-2014-3066, http://www.sbs.gob.ec/practg/sbs_index?vp_art_id=760&vp_tip=2, Publicada el 2 de Septiembre del 2014

[3] IBM Red Book, Understanding IT Perimeter Security, http://www.redbooks.ibm.com/redpapers/pdfs/redp4397.pdf, Fecha de consulta Enero del 2016

[4] Cisco Systems, Designing Perimeter Security, http://docstore.mik.ua/cisco/pdf/Cisco.Designing.Perimeter.Security.pdf, Fecha de consulta Enero del 2016.