FUTURO DE LA SEGURIDAD EN EL HOGAR

DAVID CAMILO PARRA ARIAS, MANUEL FERNANDO RAMIREZ CHAPARRO

Abstract- Every day technology is becoming more a part of our environment and our daily activities, creating a risk to our sensitive information and becoming a target for attackers. Few people know about the issue of security devices and we could work together to improve this type of problem.

Key words: IT Security, smart electronics, storage devices, vulnerability

Resumen- Las tecnologías forman cada día parte más de nuestro entorno y de nuestras actividades diarias, generando un riesgo de nuestra información sensible y convirtiéndose en un objetivo para los atacantes. Muy pocos conocen sobre el tema de la seguridad y los dispositivos que nos podrían colaborar a mejorar este tipo de problemática.

Palabras clave, seguridad informática, electrodomésticos inteligentes, dispositivos de almacenamiento, vulnerabilidad

I. INTRODUCCIÓN

Hoy en día las personas están acostumbradas a vivir el constante cambio tecnológico que se vive alrededor de nuestras vidas. Cada vez las personas adquieren más cantidad de electrodomésticos los cuales hacen la vida más fácil y ofrecen un valor agregado, los cuales pueden llegar a ser controlados desde internet.

Los medios de almacenamiento de la información han ido en aumento con el avance de la tecnología en el hogar, ya no se utiliza únicamente el computador para almacenar información o navegar en internet, ya que dentro de nuestros electrodomésticos también se puede guardar información debido a que cuentan con unidades de almacenamiento, que en algunos casos son disco duros internos o externos, en estos espacios de almacenamiento podemos almacenar datos sensibles, como por ejemplo nuestras agendas digitales que tiene todos nuestros itinerarios, sitios que visitamos, próximos cumpleaños, datos que un atacante utilizaría para ganar confianza o atacar en un punto específico.

La seguridad informática se ha enfocado en las grandes empresas o en el cuidado de equipos como computadores y desde hace muy poco los celulares que ya cuentan con sistemas operativos robustos, pero aún no se cuenta con la cultura suficiente para identificar qué pasa con nuestros electrodomésticos, como funcionan, entre otras preguntas de esta nueva tecnología que es conocida como electrodomésticos inteligentes, que muy seguramente ya contamos con dicha tecnología en nuestros hogares y estamos desinformados de buenas prácticas para el manejo de los mismos.

De forma paralela en que la tecnología avanza, de igual manera aumenta la forma en la que las personas utilizan la tecnología como un medio para un fin diferente para el cual fue creado inicialmente, como por ejemplo acceder a información de las personas sin autorización previa de los mismos, entre muchas otras.

II. OBJETIVOS

- Identificar vulnerabilidades de electrodomésticos inteligentes
- Realizar una muestra de la población colombiana para identificar la cultura hacía las nuevas tecnologías
- Identificar vulnerabilidades asociadas a las nuevas tecnologías
- Establecer estrategias para disminuir el riesgo asociado a la fuga de información por medio de electrodomésticos en el hogar

III. ESTADO DEL ARTE

El instituto nacional de tecnologías de la comunicación de España INTECO, con la ayuda de Panda Security, describe en un documento llamado, “guía de herramientas de seguridad para hogares”, en donde presentan conceptos como: antivirus, antiespías, cortafuegos, control parental, anti-phishing, y protección web, para iniciar y dar soporte con el tema de la seguridad en el hogar. También, ofrecen una lista de herramientas gratuitas y pagas, de las que los usuarios pueden hacer uso, para brindar seguridad con sus equipos del hogar. Como se puede observar evidencian el uso de herramientas de seguridad tal vez en algún momento solo con fin empresarial.

La información que recolectan nuestros dispositivos electrónicos aumentan día tras día, empezamos a salir del computador con nuestros celulares inteligentes, los que en un comienzo eran simples agendas digitales, ahora tienen sincronizadas más de una cuenta, lo cual genera mucha información en un dispositivo. La mayoría de tablets tienen conexión solo wifi, lo que ocasiona que se utilicen red privadas (Hogar, empresas), ocasionando que cuando no se dispone de las mismas se hace uso de redes públicas, exponiendo nuestra información sensible que en un principio solo se manejaba en el hogar.

Para el futuro la neveras inteligentes, que comprarán por nosotros tendrán acceso a nuestros datos personales, tendrán servicios de pago online, lo cual genera un gran riesgo para nuestra información y un objetivo más para el atacante. Desde los autos podremos realizar todo tipo de compras, utilizar nuestras agendas en cualquier medio digital, ocasionando un riesgo eminente.

IV. INVESTIGACIÓN

Para llevar a cabo esta investigación se requirió hacer uso de blogs, foros, noticias de hackers, debido a que el tema no se ha visto tan explotado, ni expuesto al público a través de los medios, como prensa, televisión, radio etc. pero sin que sean reportados los objetivos del hogar han ido creciendo y no han vulnerado de manera mundial para ser atendido por los medios. Los hogares carecen de poca protección, muchos de los dispositivos no cuentan con un antivirus, un analizador de spyware (agentes espías), así que a continuación se enunciarán los hallazgos encontrados por varios amantes a la investigación de riesgos y vulnerabilidades, recordando que para llegar a descubrir que se logró entrar a un dispositivo se puede realizar procedimientos de informática forense.

Dentro de la investigación encontramos que ninguna empresa ha realizado anuncios de envió de información o análisis de electrodomésticos comprometidos por hackers, redes de robos de información o de las misma empresas productoras de los equipos, pero observamos que si existen consultores que revelan lo contrario. Un analista de tecnología dedicado a la consultoría Jason Huntley, reveló en su blog que una compañía que se dedica a la fabricación y venta de televisores ahora inteligentes, realiza envío de información del usuario con el fin de llevar a cabo un estudio de mercado para enviarle publicidad, pero dentro de las capturas que ejecuto Jason, descubrió que también realizaba envío de la información almacenada en las USB que se conectaban, dentro de muchos países este tipo de eventos no es un delito, pero cada día las legislaciones son más fuertes contra este tipo de actividades, como se ve en Colombia con el manejo de almacenamiento de información Ley 1581.

VICENTE MOTOS en la página HackersPlayers, realiza un análisis de los elementos presentes dentro de un hogar, mostrando la vulnerabilidades encontradas en cada uno de ellos, estos elementos son: Router, Receptor Satelital, Smart Tv, Apple Tv, Teléfono IP, Termostato, Sensores de seguridad física, cámara IP, impresora, etc.,

V. ENCUESTA

Con el fin de saber el estado de la cultura hacia el tema de la Seguridad Informática en los hogares Colombianos se realiza una pequeña encuesta encaminada a una

muestra de 16 personas que cuentan con conocimientos en tecnología y son de diversas edades, para lo cual tenemos los siguientes resultados de las preguntas que se consideraron de mayor importancia dentro de la encuesta.

Con el fin de identificar de forma inicial el conocimiento acerca del tema, los resultados fueron muy optimistas desde el punto de vista que las personas están un poco conscientes que la información alojada en los dispositivos tecnológicos que se encuentran en sus hogares (Ver Figura 1) no está del todo segura y que pueden estar expuestas a alguna amenaza de tipo informático.

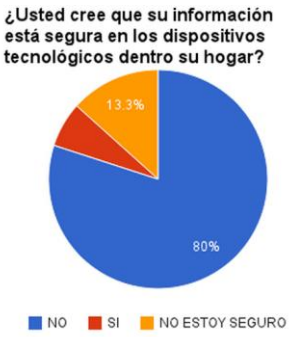

Figura 1. – Resultado de pregunta 1 de la encuesta – Autores: Camilo Parra, Manuel Ramírez

Se evidencia que hay una pequeña población que no están seguros de la respuesta, con lo cual se puede identificar que a pesar de que estas personas tengan conocimientos en áreas tecnológicas, desconocen las amenazas a las cueles pueden llegar a estar expuestas, posterior a la misma, se realiza una pregunta teniendo como base una lista de electrodomésticos que normalmente utilizamos en nuestros hogares, como lo son las neveras, equipos de sonido, lavadora y juegos de consola, para lo cual tenemos:

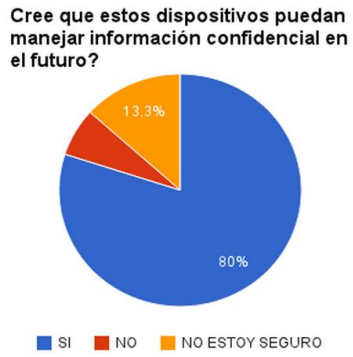

Figura 2. – Resultado de pregunta 2 de la encuesta – Autores: Camilo Parra, Manuel Ramírez

Curiosamente para la presente pregunta se obtienen los mismos porcentajes que la pregunta inmediatamente anterior, los cuales son resultados esperados en consecuencia de que la muestra escogida este respondiendo las preguntas de forma objetiva y con plena sinceridad, en esta pregunta (Ver Figura 2) se buscaba identificar si la muestra escogida cuenta con proyección tecnológica, ya que en ámbitos de tecnología enfocada a la seguridad mientras que aparece un parche de seguridad para corregir una vulnerabilidad, hay “N” amenazas y vulnerabilidades nuevas.

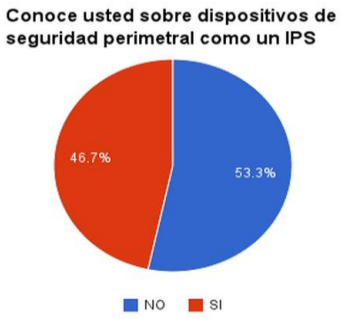

Figura 3. – Resultado de pregunta 3 de la encuesta – Autores: Camilo Parra, Manuel Ramírez

Entrándonos un poco más en los campos de la seguridad informática, se busca identificar si en la muestra existen los conocimientos de seguridad, específicamente de los dispositivos de seguridad perimetral, con los cuales se busca cuidar lo que normalmente tenemos expuesto en internet, para lo cual un poco menos de la mitad (Ver Figura 3) de la población tiene conocimiento de estos dispositivos, es decir que a pesar de que son personas que tienen que ver directamente con temas tecnológicos desconocen los temas de seguridad.

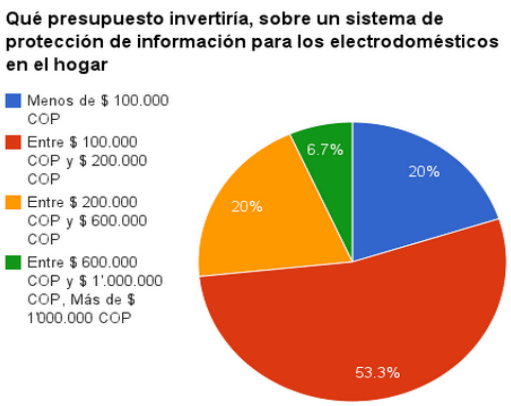

Figura 4. – Resultado de pregunta 4 de la encuesta – Autores: Camilo Parra, Manuel Ramírez

Por último, se busca establecer si las personas estarían dispuestas a invertir en dispositivos de seguridad, y de ser así en los montos que llegaría a invertir para poder salvaguardas la información confidencial de la información, en lo cual se encuentra que más de la mitad de la muestra (Ver Figura 4) no invertiría más de 200 mil pesos, lo cual es un parámetro claro e indispensable para las empresa que buscan diseñar dichos dispositivos y de igual manera puede ser el comienzo de muchas estrategias en las cuales se pueden ver involucrados diferentes entes como el estado con el fin de proteger la información, ya que los mismo pueden llegar a generar bonos o subsidios en buscar de hacer que los dispositivos que sean un poco más costosos sean más exequibles para las personas.

VI. PROTECCIÓN

Uno de los puntos que normalmente buscan las personas con conocimientos en seguridad informática, es llegar a las personas que tienen conocimiento de la infraestructura, o en su defecto que sea un usuario de la misma, ya que como es bien sabido el eslabón más débil de la seguridad son las personas. Por lo mismo uno de los aspectos más importantes para poder prevenir o mitigar los riesgos existentes es realizar sensibilizaciones a las personas que están involucradas en estos procesos, ya que de nada cuesta tener los mejores y más costosos dispositivos de seguridad, con una correcta configuración si las personas involucradas son incrédulas o no tienen conocimiento ante el tema.

Es claro que la proyección de los ataques informáticos no solo van a ser a las grandes organizaciones que cuentan con un robusto sistema de seguridad, ya que de igual manera van a estar encaminados a espacios que pueden llegar a ser más sencillos de explotar o vulnerar y que cuentan de igual manera con

información importante o catalogada como sensible.

Posiblemente un dispositivo que puede llegar a reducir los riesgos asociados es un WAF (*Web Application Firewall*), ya que con este dispositivos no solo vamos a poder abarcar la parte WEB que se ve vulnerada con otros dispositivos de seguridad.

De igual manera en forma de contribución y en búsqueda de brindar un mejor servicio, los ISP deberían otorgar a sus clientes niveles de seguridad robusta para poder bloquear de forma masiva las amenazas que se van identificando de acuerdo a las tendencias globales.

La conexión hacia internet para la mayoría de hogares es basada en el modem entregado por el proveedor de servicios, el cual no tiene mayor protección, por otro lado están los equipos que requieren la conexión a internet, que son: los computadores, los celulares, las tablets, las impresoras, etc.

Antes la protección se basaba en el antivirus de los computadores, el cual es el más promocionado como protección de información. Pero existen muchos más dispositivos y aplicaciones que sirven para garantizar los principios de la seguridad: confidencialidad, integridad y disponibilidad. Algunos de ellos son como por ejemplo un router inalámbrico convencional, no es solo para las comunicaciones, para poder integrar más dispositivos a mi red del hogar, dentro de sus funciones incluye servicios de firewall, de filtrado por MAC, de filtros por servicios, de análisis de tráfico, de protecciones de denegación de servicios, que muy posiblemente son sobre valorados y estos quedan configurados por defecto. Existen aplicaciones de proxy gratuitas de fabricantes reconocidos, que generan reglas con perfiles definidos para control parental o simplemente para evitar consultas a paginas maliciosas. Los antivirus de los dispositivos móviles como celulares, tablets, agendas digitales son descartados por falta de conocimiento sobre las vulnerabilidades y riesgos que poseen elementos electrónicos de uso general y de actividades diarias.

VII. FUTURO

Evaluando en un plano que es optimista, se evidencia un futuro en el cual los electrodomésticos son unos aliados, ya que con su avance tecnológico ayudan a optimizar procesos de las vidas de las personas, las neveras realizaran los pedidos de mercados que hacen falta en nuestros hogares, las aspiradoras se programaran para que automáticamente realicen sus labores y nos envíen un reporte a nuestros correos electrónicos para saber el resultado de la actividad realizada, nuestros televisores no solo se podrán conectar a internet sino que también serán nuestras agendas personales o familiares.

Claramente cuando se habla del futuro en temas tecnológicos, el único limitantes es nuestra imaginación, por lo cual se debe generar fuertes jornadas culturales con el fin de mitigar los riesgos asociados a ver vulnerados los pilares de la información en nuestros hogares.

Cuando la tecnología en el hogar se masifique y cada persona en el mundo tenga al menos un dispositivo conectado a internet, existirán tantos ataques que no será fácil controlarlos, actualmente los ataques en el hogar se ven sobre los computadores lo cuales son los que mayor información manejan, pero en el futuro los televisores podrán realizar compras, manejar información sensible como movimientos de dineros, sitios de interés, sitios por visitar, etc. Las neveras inteligentes tendrán mayor información sensible, debido a que son ellas las que realizaran las compras para no tener que ir al supermercado, su sistema operativo tendrá que procesar números de tarjetas de crédito, información del cliente y más datos sensibles que serán de gran interés para los atacantes.

En los próximos años aparecerán más dispositivos que puedan ser contralados desde internet, para ello es útil diseñar dispositivos como detectores de intrusos con firmas diseñadas específicamente para el hogar y los electrodomésticos que lo componen.

VIII. CONCLUSIONES

La seguridad informática en los hogares Colombianos estará directamente influenciada en los entornos educativos y tecnológicos en donde se destacan las estrategias comerciales para reducir los costos y genera múltiples opciones en el mercado, dentro del cual realizando una proyección prospectiva, el ministerio de las TIC´s en conjunto con los múltiples fabricantes de dispositivos de seguridad y electrodomésticos deberán alinear las estrategias para mitigar las amenazas de intrusiones externas en los hogares colombianos.

Debe ser de carácter obligatorio que las entidades educativas generen sensibilizaciones periódicas en el área de seguridad informática en donde se haga conocer a todo el personal de las mismas la importancia de la seguridad informática y se instruya en los principios rectores, esto con el fin de sensibilizar a la población colombiana y generar cultura en este ámbito para la población colombiana.

Dentro de la investigación se observa que el tema no ha sido investigado en profundidad, lo cual nos generó realizar la investigación prospectiva de los electrodomésticos.

Las encuestas nos demostraron que existen muchas falencias en conocimientos sobre dispositivos de seguridad la información y que a su vez la gente es consciente de su información

Las estrategias del ministerio de las TIC´s deben generar atención a usuarios en todos los barrios, localidades, municipios, veredas y ciudades con el fin de brindar el apoyo pertinente en el área de seguridad informática.

La seguridad informática en los hogares es directamente dependiente del desarrollo educativo, económico y tecnológico de su entorno, por este motivo se debe sensibilizar a todo el personal que adquiere un electrodoméstico inteligente en donde se le haga conocer las ventajas, riesgos y amenazas a las cuales está expuesto si no genera buenos hábitos de utilización de los mismos en el hogar.

IX. BIBLIOGRAFIA

[1] Guía de herramientas de seguridad para hogares, Instituto nacional de tecnologías de la comunicación de España INTECO, con la ayuda de Panda Secutiry, describe en un documento llamado, “”,

[2] Rikke Kuipers, Eeva Starck, Hannu Heikkinen - “Smart TV Hacking: Crash Testing Your Home Entertainment” - Codenomicon

[3] BENZMULLER Ralf, “cada 15 segundos se general un malware”, G data Software

[4] INTERNATIONAL BUSINESS TIMES, “LG Electronics”

[5] Sí, tú casa está llena de dispositivos que pueden ser “hackeados”, Vicente Motos- Pagina Hack Players

http://www.hackplayers.com/2013/08/si-tu-casa-esta-llena-de-dispositivos-hackeables.html

[6] XATAKAHOME, “Así será el hogar del futuro según Microsoft”.

[7] MIERES Jorge, "Buenas prácticas en seguridad informática", Analista de seguridad de ESET, Latinoamérica.