Ciberseguridad y ciberterrorismo

Diego J. Amórtegui T.

Las tecnologías de comunicación, especialmente internet, han abierto un gran universo de posibilidades de acceso a la información, y al mismo tiempo han generado nuevos riesgos que hace unos años no vislumbrábamos. Este es un momento crítico de cambio, hay una gran apertura en las comunicaciones y posibilidades para compartir información en internet, que demanda más seguridad para cada acción que tomemos; es necesario emplear y desarrollar mecanismos de seguridad informática más robustos y amigables, así como generar patrones de conducta que permitan salvaguardar la vida virtual de las personas.

Así mismo, esta gran apertura genera nuevas posibilidades para que los riesgos de la vida real se filtren a la vida virtual de las empresas y las personas. En este caso es el terrorismo y todas las acciones que pueden vincularse a dicha actividad, toda vez que en el caso específico de un ciberataque, las capacidades están disponibles en manos de algunos, como es el caso de las botnets, los cuales pueden ser rentados por unos miles de dólares. Aunado a esto está el anonimato y la posibilidad de estar a miles de kilómetros de distancia para realizar actividades relacionadas al terrorismo.

Universos antagónicos, ciberseguridad y ciberterrorismo

Desde el año 2000 internet era una idea que comenzaba a gestarse en las empresas y hogares colombianos, las velocidades de aquella época eran un logro admirable, en comparación con lo que recibimos actualmente. Hace 10 anos tener una conexión de 256 Kb era un hecho memorable.

A medida que nos hemos ido introduciendo en este mundo virtual de internet, el cual ya tiene permeado hasta los más pequeños rincones de nuestro entendimiento, las formas en las cuales nos comunicamos y exponemos son cada vez más diversas y desconocidas, como por ejemplo twitter, que en 140 caracteres genera un flujo de conversación tan constante que podría rivalizar con cualquier aplicación de chat existente.

De la investigación realizada para identificar las piezas claves de la ciberseguridad encontré que la mayoría de los autores tienen un mismo enfoque, el de la defensa proactiva. En una conferencia de Chema Alonso publicada en *youtube*, de la cual se pueden extractar tips muy valiosos como por ejemplo, la necesidad de contar con los parches del sistema operativo al día, tener un antivirus actualizado, disponer de firewall, passwords robustos, entre otras precauciones. Son elementos esenciales, tips que pueden resultar suficientes para algunos usuarios. En la misma conferencia se advierte sobre el cuidado que se debe tener en los sitios por donde navegamos y la necesidad de disponer de todo el software actualizado, ataques de día 0, hasta pensar en realizar un hardening a nuestro PC. Para algunos esto puede resultar exagerado y para otros sólo sentido común.

Pero, ¿por qué tomar tantas medidas? Manifestar “yo no soy una persona importante”, “a mí que me van a robar si sólo tengo poco dinero en mi cuenta” son comentarios que me hacia una persona con la que hablaba hace poco, y en cierta manera tenía razón, ¿Por qué? Después de analizar sus planteamientos entendí que la respuesta es muy simple: porque hay personas que pueden vivir con un nivel bajo de “ciberseguridad”, porque este es el adecuado para realizar lo que necesitan. Aclaro que, en mi concepto, es bajo el nivel de ciberseguridad de esta persona.

Pero ese antivirus, firewall y la cantidad de “Anti” que nos venden ahora las grandes empresas, ¿van a permitirnos tener un adecuado nivel de seguridad mientras estemos en línea? En mi opinión la respuesta es NO. Para pensar en forma adecuada con relación a la ciberseguridad, debemos imaginar situaciones de riesgo en las cuales podemos vernos en la vida real y simplemente transferir este conocimiento a la actividad virtual, toda vez que hasta hoy, ni McAfee ni Symantec han inventado un guardaespaldas virtual, que pueda mantenernos seguros y vigilados las 24 horas del día. Lo que pueden hacer es sugerirnos qué puede ser potencialmente seguro y qué no. Lo demás queda a voluntad de ese “tic” generado en el dedo índice cuando se observa un link llamativo y hacemos clic.

La ciberseguridad como la conocemos es un tema de muchas entradas y pocas salidas, nuestra vida social en línea poco a poco está sobrepasando la que posiblemente tenemos en la vida real; estamos conectados 24 horas por medio de un blackberry o un Smartphone a internet y a las redes sociales, y como duramente lo aprendí hace poco, *no hay antivirus para facebook*, (me infecté a causa de ese tic que les comenté). Ya instalé un app de bitdefender, el cual estoy seguro podrá ahorrarme unas neuronas para decir no a hacer clic sobre lo que no debo, y éste me solicitó acceso a casi todo mi perfil. En ese momento sentí que entregaba en comodato mi vida virtual, aunque ya puedo orgullosamente decir que soy usuario de un antivirus en la nube.

¿A qué va todo esto? La verdad todos los días es necesario tomar conciencia sobre la información que tenemos y manejamos en la cotidianidad, aunque parezca trivial y sin importancia, para otros es un foco de dinero y en algunos casos poder. El ejemplo de “no tener dinero en la cuenta”, ese dato puede ser útil para los “muleros” aquellas personas que se encargan de conseguir “mulas”, por medio de correos electrónicos, en los cuales les ofrecen una comisión por la recepción de importantes sumas de dinero en sus cuentas personales, haciéndose pasar por compañías extranjeras o nacionales, o también a través de mi cuenta de correo electrónico, que permite a algunos enviar SPAM o en algunos casos, phishing.

¿Qué es ciberseguridad?

Para responder esta pregunta accedí a Internet y coloqué en google, “cybersecurity”. Lo primero que esperé fue encontrar un artículo de Wikipedia que me diera una definición pero, asombrosamente, no lo encontré. Lo más cercano fue una definición de “cybersecurity standards”, con una lista para aplicar, lo que me permitió entender que la

ciberseguridad no es una fórmula mágica. Se trata de “aplicar las medidas necesarias, para garantizar que la identidad virtual de cada persona, pueda ser salvaguardada en las mejores condiciones, además de permitir el acceso adecuado a medios virtuales, ya sean redes sociales, consulta de información de cualquier tipo por cualquier medio de comunicación, usando Internet por medio de dispositivos creados para tal fin”.

Tal vez no es la mejor definición, pero a mi manera de ver es lo más cercano a lo que en mi concepto debe ser la seguridad en ambientes virtuales. De acuerdo con esta definición, creo que no hay un código de mejores prácticas que pueda recomendarnos el mejor camino a seguir, pero si hay algún elemento indicador de que por esa calle virtual roban, pues pueda usar tal consejo para evitar que me pase algo malo. También creo que los señalamientos de Chema son los mejores puntos de partida para identificar nuestra inseguridad virtual, y poder tomar las medidas adecuadas para asegurar en lo posible nuestra vida por tales espacios. Señalo “en lo posible”, porque las actividades ilegales están a la orden del día.

Los malos al acecho

El malware es más silencioso y efectivo, troyanos como Zeus son los ninjas del nuevo milenio, son “callados”, indetectables y pueden acabar con una persona o una empresa en cuestión de segundos. Se acabaron las épocas doradas de los fabricantes de antivirus cuando dominaban el mercado de la seguridad; ahora el malware dicta el paso e impone las tendencias. La seguridad de las compañías ya se ha movido de los antes indispensables firewalls corporativos, a la seguridad del punto final, donde cada vez se ven elementos de software más modernos, con mayores capacidades y completamente integrados con todas las actividades que realizamos, desde el envío de un correo electrónico, hasta el rechazo o aprobación para copiar un archivo sensible en una USB, por medio de un agente de DLP.

También veo cómo mi buzón se llena de correo basura y algunos mensajes legítimos pueden ser clasificados como spam; las técnicas de evasión de firmas son cada vez mejores y, en algunos casos, también son tema de niños. La industria del malware es muy organizada y efectiva, una o unos pocos crean una pieza de software que por ejemplo explota una vulnerabilidad de día 0, otros se encargan de ponerle un propósito, como robarnos todas nuestras claves, accesos, cookies, hacer de la máquina un zombie, hasta patrón de navegación o todas. Y, finalmente, otros se encargan de aprovecharse de nuestro instinto ya casi natural de hacer clic al correo que viene con el virus o dirige a la persona a una página que puede infectar el PC.

El concepto del hacker (usaré este término para hablar de quien busca causar daño o robar información) que muchos tuvimos en la cabeza hace algunos años gracias a Hollywood, ya es tema del pasado; estas personas no son retraídos sociales ni genios y tampoco adictos a los videojuegos, los hackers de ahora son personas con vidas sociales activas, y no son virtuales, trabajan en empresas, estudian en universidades, asisten a fiestas; el hacker de ahora es una persona tan común como cualquiera.

Causar daño ya no la intención, la razón es que ser muy ruidoso no es rentable ni beneficioso. Existen virus que parchan el equipo para evitar que otro pueda tomar control de la máquina; ahora simplemente se envía un troyano a que realice un man in the browser o cualquier otro proceso, para obtener nuestra información y permitirnos el acceso.

En ningún momento digo que el trabajo de hacking esté desvirtuado, de hecho es una práctica que aún se emplea y que cada vez es más prestigiosa, pero al mismo tiempo que ésta se valida en ambientes más y más diversos. Los verdaderos cerebros de las redes de robo de información emplean a estas y otras personas para que hagan uso de su intelecto y puedan sacar provecho de cualquier situación, desarrollando programas, métodos de evasión, mejorando los actuales programas o simplemente haciendo carding cuando la operación lo permita.

La práctica del crimen es cada vez más rentable. Ya se habla de “crime as a service”, en el cual con unos cuantos miles de dólares es posible rentar una botnet con varios niveles de servicio (bronce, plata y oro), además si lo desea puede entregarse al administrador la información deseada; quien renta obtiene acceso a una consola de C&C, donde puede revisar el progreso e información recopilada por este medio.

Describo estas formas de realizar crímenes informáticos, para poner en perspectiva lo fácil que puede ser para un individuo o un grupo de personas realizar ataques de diversos tipos sobre cualquier infraestructura tecnológica, o de comunicaciones. De la misma manera como indagué sobre el significado de ciberseguridad en Google, hice lo mismo con ciberterrorismo, y aunque esta vez sí encontré una definición, no me pareció adecuada. Revisando otros links encontré un muy buen video en youtube sobre ciberterrorismo, vinculado en la página de dragonjar, en este video según Whitfield Diffie (uno de los creadores del algoritmo Diffie-Hellman) el ciberterrorismo es “motivado políticamente, no quisiera llamarlo un crimen motivado con fines económicos, el terrorismo se caracteriza por atacar a una persona inocente y así asustar a alguien más para conseguir que haga algo”.

De acuerdo con el diccionario de la lengua española, el terrorismo es “la sucesión de actos de violencia ejecutados para infundir terror”; por mi experiencia la definición de ciberterrorismo es poder forzar a uno o un grupo de personas a hacer algo, por medio de métodos coercitivos y usando principalmente la internet para lograr sus objetivos, los cuales pueden tener fines políticos, económicos o de cualquier otra índole; en la definición uso el término ***principalmente*** porque el prefijo “ciber” denota un ámbito electrónico, que no necesariamente incluye la internet. Considero también que un ciberataque en un contexto netamente terrorista, es una forma de confirmar el proceso de ciberterrorismo por medio de hechos concretos.

Ahora y según las facilidades actuales, cualquier persona puede ser un ciberterrorista, sólo se necesita el elemento fundamental que es infundir terror entre las personas, ya sea por medio del uso de correos electrónicos, publicaciones en blogs, redes sociales, usando las páginas en internet de los medios de comunicación de un país, el uso de

videos en youtube, tweets, o de la manera en la cual pueda imaginarse. Para ilustrar un poco más esta idea, existen unos muy buenos ejemplos en la página de la escuela asiática de ciber leyes, (en este sitio colocan una definición muy cercana a la que yo planteo como ciberterrorismo). No soy abogado y tampoco quiero enredarme con conceptos y palabras, pero en esta página hay un ejemplo que creo vale la pena resaltar y es el siguiente:

"Un grupo de personas que matan a un hombre de 50 años de edad hospitalizado al darle un medicamento al cual es muy alérgico. Esto es un crimen.
El hombre de 50 años es la cabeza de una comunidad de minorías religiosas y los asaltantes, que pertenecen a otra comunidad religiosa, lo han matado para crear miedo en la mente de la comunidad minoritaria. Aunque esto sigue siendo un delito, también es un acto de terrorismo.
Si los asesinos habían hackeado en la red del hospital y alterado los medicamentos prescritos, entonces sería un acto de ciberterrorismo".

Actos como los del ejemplo son posibles debido a la disponibilidad de comunicaciones a través del mundo, las cuales permiten que un ciberterrorista ubicado en el otro extremo del globo pueda efectuar un ataque contra una organización, el gobierno de otro país o del propio. En el mundo de hoy y como lo mencioné anteriormente, se puede contratar los servicios de una botnet para efectuar el ataque desde múltiples sitios del mundo, disminuyendo la posibilidad de ser encontrado.

Sumado a esto, está la falta de una identidad virtual clara y definida; internet permite que cualquier persona pueda ocultar o cambiar su identidad a gusto, manteniendo en muchas ocasiones un anonimato al momento de efectuar un ataque, siendo los más elementales los cientos de web proxy que se encuentran actualmente en el ciberespacio.

¿Y qué pasa con los hackers?, ahí están, y son una parte fundamental de un proceso de ciberterrorismo, aún no conozco un grupo proclamado como ciberterrorista integrado por hackers, tampoco conozco grupos ciberterroristas.

Los grupos terroristas han empezado a poner más atención al mundo informático y ya tienen capacidades claras de ejecutar acciones contra diversos objetivos. Según un estudio de la universidad de Dartmouth realizado en 2003, unos de los principales grupos de presión a tener en cuenta son los países islámicos, los cuales han trabajado desde hace varios años en mejorar sus capacidades informáticas. Estos grupos no solamente entrenan hackers, también los reclutan, o contratan para efectuar y apoyar los procesos terroristas de estos grupos. Según otro artículo, China también está mejorando sus habilidades técnicas para efectuar este tipo de ataques, pero en mi opinión, esta afirmación no es objetiva, porque la mayoría de los estudios realizados provienen de Estados Unidos.

En el ciberterrorismo, el ciberterrorista no sólo emplea internet como herramienta de coerción, también es usado como medio de propaganda, reclutamiento, entrenamiento,

recaudo de dinero, comunicación, y escogencia de objetivos. No veremos un Google maps con un marcador que diga “bomba aquí”, pero sí es posible usar esta tecnología para planear rutas de acceso y salida de sitios, y con la ayuda de street view, también pueden conocer visualmente el sitio con todas sus características.

También redes sociales como Facebook permiten realizar un perfil a la o las personas que desean convertir en un objetivo; en estas redes sociales es importante tener una buena configuración de qué se publica y cómo, además de tener la certeza de a qué personas permitirles pertenecer a mi círculo social virtual.

Sin dejar a un lado las capacidades técnicas de una persona, es vital recordar que las herramientas más simples pueden ser usadas para planear y en algunos casos ejecutar terrorismo, pero ¿este proceso de uso de tecnologías de internet, trasladado a la vida real, permite definir a un terrorista como un ciberterrorista? Pregunta que en mi concepto es muy difícil de responder, debido al razonamiento sobre el tema que cada persona aplique.

Realizar ataques, generar comunicados entre otros es sólo una parte de las posibilidades que internet le abrió al terrorismo; sólo hay que pensar que las mismas herramientas que protegen la seguridad y confidencialidad de las empresas y personas, así como las que les permiten trabajar en conjunto y a distancia, también son usadas por grupos terroristas en internet, para transmitir mensajes que solamente ellos puedan descifrar.

Dentro de poco me imagino que la lista de los más buscados por el FBI no estará conformada solamente por nombres y fotos, sino también por avatars y nicks; la CIA interceptando e-meetings de webex, células terroristas en second life ubicando objetivos, ciberterroristas usando augmented reality de playstation para planear ataques sin dejar rastros físicos, o reclutamiento y entrenamiento virtual por medio del sistema kinect de la Xbox. De hecho ya hay una ciber carrera armamentista la cual tiene dos frentes, el primero es quién puede tener el troyano más sigiloso y segundo, quién tiene la botnet más grande, y ninguna de estas es liderada por un Estado.

Los gobiernos de algunos países se están armando para protegerse de un ciberataque terrorista, pero aún a muchos (gobiernos y personas) les cuesta quitarse la imagen del fatídico botón rojo con el que podían lanzar un misil y borrar todo al alcance de éste; quizá si pintamos todas las teclas enter del mundo de color rojo, esto pueda generar una conciencia más profunda, porque aún tememos más a una muerte rápida que a una donde nos afecte de a poquitos.

Conclusiones

El momento por el cual estamos viviendo es de cambio y de adaptación, las capacidades que internet brinda en la actualidad son casi ilimitadas, y aún se están descubriendo nuevas posibilidades, tanto para el bien como para el mal. Estar protegido y seguro en la red es una labor de todos los días, y no todos requieren el

mismo nivel de seguridad, el cual puede ser definido de acuerdo con la persona y al nivel de confidencialidad que requiera o desee.

Pero al mismo tiempo que nos adaptamos, el cibercrimen crece y también se adapta a pasos agigantados, generando nuevas preocupaciones que las empresas de seguridad luchan por cubrir, las cuales están disponibles para cualquier persona que desee hacer el mal, incluido los ciberterroristas, quienes están aprovechando en la actualidad estas nuevas posibilidades que ha acarreado la globalización de las comunicaciones, así como los mecanismos de seguridad creados para mantener la seguridad de las personas en el mundo virtual, siempre apoyado con el velo del anonimato que admite internet

Referencias

[1] http://www.youtube.com/watch?v=Y98OyB6bulg
[2] https://www.facebook.com/bitdefender.safego
[3] http://es.wikipedia.org/wiki/Comodato
[4] http://en.wikipedia.org/wiki/Cyber_security_standards
[5] http://blog.fortinet.com/adaptive-crime-services/
[6] http://en.wikipedia.org/wiki/Botnet
[7] http://www.dragonjar.org/ciberterrorismo.xhtml
[8] http://buscon.rae.es/draeI/SrvltConsulta?TIPO_BUS=3&LEMA=terrorismo
[9] http://www.asianlaws.org/
[10] http://www.asianlaws.org/library/cyber-laws/defining_cyber_terrorism.htm
[11] http://www.ists.dartmouth.edu/library/164.pdf

Diego J. Amórtegui T. *Ingeniero de sistemas graduado de la Universidad Católica de Colombia ha realizado estudios en redes de datos y seguridad de la información, con nueve años de experiencia laboral en áreas tecnológicas, especialmente en administración de redes y seguridad de la información. Actualmente, se desempeña como Director de seguridad lógica de una importante entidad financiera y cursa estudios de MBA.*