SEGURIDAD INFORMÁTICA UN LARGO CAMINO

COMPUTER SECURITY A LONG WAY

Ingeniera Pereira Carrero Sandra Ximena
Especialización de Seguridad Informática ESI 19
risacbotella@hotmail.com
Universidad Piloto de Colombia

Resumen—Se realiza un análisis de los requerimientos tecnológicos, de personal capacitado e inversión de recursos para proteger el activo más valioso para una organización que es su información, la de sus clientes y transacciones comerciales y financieras, teniendo en cuenta que hoy en día existe en Colombia legislación para la protección de la información y tipificación de los delitos informáticos en Colombia. Además que existe ya un mercado internacional que nos excluye si no garantizamos la protección de esa información.

Abstract -An analysis of technological requirements, trained and investment of resources to protect the most valuable asset for an organization that is their information, their customers and staff trade and financial transactions carried out, considering that today there in Colombia legislation for the protection of information and classification of computer crimes in Colombia. In addition there is already an international market that excludes us if we do not guarantee the protection of such information.

Indice de Términos **–** legislación colombiana, tipificación de delitos informáticos, ingeniería social, ingeniería social inversa, trashing, ataques de monitorización, ataques de autenticación, Denial of Service.

I. INTRODUCCIÓN

Cada día, la seguridad de la información cobra más fuerza dentro de las empresas, espacios que contemplan los escenarios de protección, entre sus preocupaciones fundamentales. Las crecientes anomalías electrónicas, unas regulaciones vigentes, unas tecnologías de protección cada vez más limitadas y una mayor dependencia de la tecnología en forma de hacer negocios, muestran cómo la necesidad de proteger la información es más relevante.

En esa misma óptica se observan unos ejecutivos de la seguridad más preocupados por utilizar lenguajes cercanos a la organización, para proveer soluciones que armonicen las relaciones de funcionalidad y protección, dentro del marco del negocio.

La realidad supone prácticas concretas que se conviertan en un tema de cultura entre las empresas y los usuarios. Y aunque cabe destacar que existen normas para sectores específicos, como el Financiero, de Defensa, no hay una regla ‘suprema’ para las empresas que manejen información en todas las áreas.

A Colombia aún le falta un largo recorrido para adoptar medidas que vayan más allá de la teoría. A pesar que existen leyes que tienen que ver con la información como: ley 1273 tipificación de los delítos informáticos, ley 1581 tratamiento a los datos personales, ley 527 de comercio electrónico, entre otras, aún no estamos preparados jurídicamente ni técnicamente con herramientas

tecnológicas y lo principal como personal capacitado, experto e idóneo para exigir el cumplimiento interno y externo de ésta legislación, que cada día es importante pero que por desconocimiento obviamos el cumplimiento obligatorio de la misma. Por ejemplo gracias a la Ley 527 de 1999 las empresas y entidades públicas colombianas pueden identificar de manera inequívoca a una persona en medios electrónicos haciendo uso de la certificación de firma digital, así mismo, si hablamos de garantizar la fecha y hora exacta que sucede en una transacción electrónica existe el estampado cronológico o sello de tiempo, y si se trata de contar con un repositorio de evidencia digital que archive y conserve los documentos electrónicos se puede emplear el archivo confiable de mensaje de datos.

II. SEGURIDAD INFORMÁTICA UN LARGO CAMINO

A nivel organizacional apenas se está viendo la importancia de implementación del Sistema de Gestión de Seguridad de la Información, al ver la necesidad de tener y asegurar la información de nuestros clientes, proveedores, archivos y transacciones, se espera que se exija como un requisito indispensable la aplicación de éste sistema como obligatorio cumplimiento para poder establecer roles y responsabilidades de acuerdo a perfil y necesidades.

De aquí la importancia de certificar las organizaciones en la norma ISO 27001 y los encargados de las tecnologías de la información y seguridad informática.

En el último año una de las mayores conmociones que se ha gestado a nivel mundial a causa de las legislaciones se deriva de los acuerdos y la legislación aprobadas que regulan el uso de la información de Internet y endurecen los derechos de autor y la propiedad intelectual, llegando hasta penalizar las violaciones al copyright, tema también que cobra importancia teniendo en cuenta la ley de derechos de autor.

Es una realidad, que con el uso de internet y con el flujo de información que transita en la red, los riesgos de un ataque cibernético son cada vez más altos, por ello se hace necesario contar con una estrategia clara de ciberdefensa y ciberseguridad en un país como Colombia en donde, según las últimas declaraciones del Gobierno, esta es una prioridad nacional.

Hoy en día los problemas de seguridad en el internet no solo se pueden considerar una preocupación empresarial, toda persona que navega por este medio tiene derecho a la privacidad. Las empresas han detectado actividades informáticas delictivas en las que ya han venido trabajando para superar las violaciones más conocidas en contra de la información: el uso de cuentas y tarjetas de crédito, la suplantación de las identidades, y la fuga de información al interior de las organizaciones, son algunos de los problemas más comunes.

Sin embargo, se cree por costumbre que seguridad informática es sinónimo de compras de tecnologías, dejarse influenciar de todo lo que vende el mercado, y se adquieren tecnologías inapropiadas, no funcionales, inseguras, que no satisfacen nuestras necesidades y tampoco nos brindan protección a nuestra plataforma tecnológica.

Quienes se proyectan sus actividades comerciales al extranjero ya ven la necesidad de implementar esos controles para la protección de la información e inclusive certificarse, debido a que países como Estados Unidos, y algunos de la Unión Europea han hecho avances en la reglamentación de la seguridad de los datos, las empresas de esas regiones que desean buscar mercados internacionales tendrán que tener cuidado con las normas de cada Gobierno para entrar a los mercados. Es así que, si Colombia se fortalece en materia de normatividad, podrá ser un

nicho más atractivo para la importación de las compañías internacionales, que verán no solo rentabilidad, sino estabilidad en los negocios que realicen dentro del territorio nacional.

Las empresas de cualquier tamaño deben desarrollar flexibilidad para soportar ataques inesperados y necesitan manejar los riesgos más allá de los que tradicionalmente se tratan, cada día los ataques cibernéticos serán más sofisticados por eso nuestras herramientas tecnológicas deberán avanzar a la par o un paso adelante ante esta situación, acompañado por la actualización de conocimientos del personal especializado. Deben existir una serie de procesos y utilidades determinadas para reducir los posibles peligros al área física de la organización o a la información. La seguridad informática comprende lo lógico (bases de datos, información), hardware (computadores, servidores, impresoras, etc.) y todo lo que la entidad considere de mucha importancia y signifique una alarma en el caso de que la información pase a manos indebidas.

Existen muchos tipos de ataques en contra los recursos humanos, tecnológicos y de la información en una empresa, tales como ingeniería social, ingeniería social inversa, trashing, ataques de monitorización, ataques de autenticación, Denial of Service, ataques de modificación, etc., todos con el fin de atacar algún módulo específico de la organización. Mientras aumentan los avances tecnológicos en materia de nuevos métodos de infiltración, crece la necesidad de las empresas de identificar y retener especialistas expertos que posean habilidades más sofisticadas que las amenazas cibernéticas y que tengan un alto grado de previsión. Sin embargo, la realidad es otra: la demanda de estos expertos en el mercado se mantiene escasa y estable.

Por lo anterior el reto no es solo evitar que los sistemas de información de las compañías sean vulnerados, también es un reto encontrar al personal altamente capacitado para hacerse cargo de esa responsabilidad.

Los gastos de seguridad en las organizaciones colombianas se centran como primera medida, en las evaluaciones de seguridad de las plataformas.

Se deben considerar ambos mundos, pruebas internas y externas como mecanismos válidos de uso común. Situación asociada a las tendencias mundiales sobre gestión de vulnerabilidades y pruebas de intrusión, como mecanismos adecuados para validar los controles de las organizaciones.

La seguridad informática se vuelve parte de nuestro día a día y las empresas están destinando espacios físicos y en las estructuras de su organización, para que equipos de expertos trabajen de forma ininterrumpida en la protección del activo más valioso de las compañías: La información. De hecho, se han conocido casos donde un integrador de noticias que tras un ataque cibernético, estaba siendo extorsionado por los perpetradores del hecho, a cambio de revertir el daño causado, ya debemos ver este tipo de conductas extorsivas y perjudiciales ante la intimidad de las personas y vulnerabilidades de sus derechos, por consiguiente todas éstas conductas son castigadas en Colombia.

Para la industria de seguridad de la información es clave utilizar buenas prácticas encaminadas a la construcción de modelos más adecuados que se amolden a las necesidades de las organizaciones, en los que la personalización es la variable importante para obtener un modelo exitoso.

Hay que tener en cuenta que la seguridad informática es un proceso dinámico, es decir, suele siempre estar encaminado a la actualización permanente de mecanismos, procesos, métodos, técnicas y procedimientos que ayudan a contrarrestar los ataques o amenazas informáticas que cada día aparecen en internet, redes y demás medios en donde puedan realizar sus procedimientos con objetivos determinados.

A nivel mundial vemos cómo los gobiernos se preocupan más por el ciberespacio, al que algunos

denominan la nueva frontera de las guerras venideras. De otro lado, el sector educativo ve con preocupación la seguridad, teniendo en cuenta los repetidos ataques a sus infraestructuras, originados por los débiles diseños que exigen mejorar los esquemas. Por su parte, los sectores financieros se ven enfrentados a cumplir con una serie de controles para cumplir con ese competido negocio, considerando la globalización de las economías y la normatividad nacional e internacional.

De acuerdo con un estudio de la empresa Fortinet, el gobierno colombiano es víctima del 3 % de los ataques cibernéticos en el país.

Colombia está bien posicionada en el mundo en manejo de ciberseguridad, de acuerdo con la clasificación global de la Unión Internacional de Telecomunicaciones (UIT). El informe ubica el país en el quinto lugar en la lista de las Américas, por encima de Chile y México, y ocupa el noveno lugar en la tabla mundial, frente a países como Francia, España, Egipto y Dinamarca.

La UIT publica el Índice Mundial de Ciberseguridad (IMC), que evalúa el grado de desarrollo de la ciberseguridad en cada país y, según la propia organización: "tiene el objetivo fundamental de fomentar la cultura mundial de la ciberseguridad y su integración en el núcleo de las tecnologías de la información y la comunicación".

La empresa de seguridad informática Fortinet realizó un diagnóstico sobre los ataques que reciben los sistemas del gobierno colombiano. Según las cifras que recolectó, la Nación es víctima del 3 % de los ataques, lo que no necesariamente significa que sea víctima de los piratas cibernéticos. Pero es claro que los delincuentes intentan robar datos del Estado mediante ataques.

El año anterior el gobierno Santos había anunciado la creación de la ‘Agencia Nacional de Seguridad Cibernética’, que estaría liderada por el ministerio de Defensa con la colaboración del MinTic, pero el proyecto sigue en estructuración. Mientras tanto, las amenazas que recibe el Gobierno las enfrenta el Centro Cibernético Policial, adscrito a la Policía Nacional.

De acuerdo con el boletín 002 de la entidad, la Policía nacional evitó más de 822 sitios de pornografía infantil en el 2014 y ha realizado más de 422 capturas por delitos informáticos. En cuanto a la seguridad de sitios gubernamentales, se registraron más de 200 denuncias de ataques cibernéticos a sitios con información sensible para los colombianos.

Además del robo de información o amenaza que reciben los entes estatales están el daño en la imagen hacia sus ciudadanos por la negación de los servicios en línea. Esto quedó demostrado en las elecciones del 2014, en donde la Policía detectó varios intentos de ataque a las páginas de las instituciones electorales que no fueron materializados gracias a los complejos sistemas de detección y confección de ataques que desde el 2010 el Gobierno viene implementando para el aseguramiento de los comicios electorales.

De acuerdo con el estudio que realizó Fortinet, los ataques cibernéticos dirigidos a entidades gubernamentales tienen impacto en toda la población ya que pueden inhabilitar servicios como suministro de agua potable, electricidad, cámaras de vigilancia, información personal sobre los ciudadanos, transporte aéreo y terrestre, además de las operaciones del Gobierno.

Más allá de las cifras el Estado colombiano ha reconocido la importancia de proteger sus portales de virus o robos de información. Aún más si se tienen en cuenta antecedentes como la intromisión en el correo electrónico que sufrió Humberto de la Calle, jefe del equipo negociador en La Habana.

En Colombia desde hace algún tiempo las instituciones del Gobierno vienen blindando sus infraestructuras tecnológicas contra amenazas de todo tipo, como una incitativa gubernamental para

proteger la infraestructura crítica y por ende todos aquellos procesos que son vitales para la estabilidad del país.

Dichas medidas de control están enfocadas a prevenir ataques como la denegación de servicio, el código malicioso y otros más elaborados que buscan dañar la reputación de las instituciones del Estado.

En los dos últimos años la demanda ha sido construir centros de datos; inversión en sistemas de virtualización, en almacenamiento y en poner muchos sistemas en la nube. Se trata de una infraestructura que después se va a tener que proteger. Por eso en el 2015 y 2016 el repunte tendrá que ser fuerte.

Es urgente pisar el acelerador en este tema. Una mayor vinculación del sector privado (pero no de esas de 'cumplamos y ya'), y una socialización vigorosa de los roles y divisiones de las políticas de ciberseguridad y ciberdefensa que se han definido desde Gobierno se hacen prioritarias.

El Gobierno Nacional ha estado avanzando en este punto y es de reconocer, por ejemplo, la creación del Grupo de Respuesta a Emergencias Cibernéticas de Colombia (Colcert). Para este tipo de iniciativas es importante el análisis de personal calificado, expertos en el tema de la seguridad cibernética.

De acuerdo con una investigación adelantada por Fortinet, empresa especialista en protección de redes, usuarios y datos, señala que actualmente los directivos de las organizaciones, tanto grandes como medianas, tienen cada vez más presiones por mantener la empresa segura y que esto ha situado al tema de seguridad en una posición primordial y protagónica sobre otras iniciativas de negocio.

La Encuesta Global de Fortinet, que incluyó respuestas de profesionales de TI de países latinoamericanos como Brasil, Colombia y México, reveló que el 63% de los tomadores de decisiones de TI admite el abandono o el retraso de por lo menos una nueva iniciativa de negocio debido a los temores de seguridad cibernética.

Si bien la tecnología abrió un sin número de posibilidades, también ha traído consigo brechas que facilitan riesgos y problemáticas en seguridad de la información. Aunque la mayoría de las vulnerabilidades conocidas en la actualidad son de vieja data, estas se han venido reinventando o haciéndose más específicas a medida que los sistemas de seguridad se han hecho más fuertes, pareciera entonces ser un proceso cíclico en espiral que no tiene fin.

Porque lo peor que nos puede pasar es que, como ha sido característico en la seguridad informática, nos mantengamos a la espera de los golpes de los malos para reaccionar.

CONCLUSIONES

- Las regulaciones nacionales e internacionales son mecanismos que apoyan el fortalecimiento de los sistemas de gestión de seguridad de la información. Hoy en Colombia existen normativas como la regulación en los sectores financieros y la ley de protección de datos personales. Las regulaciones Internacionales inclinan la balanza hacia la seguridad de la información y nos enfrentan a un panorama todavía denso, en materia de ataques informáticos, tecnología y personal especializado.

- La industria en Colombia exige más de dos años de experiencia en seguridad informática, como requisito para optar por una posición en ésta área.

- Aunque el mercado de especialistas en seguridad de la información toma fuerza, la oferta de programas académicos formales es limitada y hace que las organizaciones contraten profesionales con poca experiencia en seguridad, para formarlos localmente.

- La realidad nacional refleja un avance alrededor de la gestión de incidentes; aunque no está bien, se nota el esfuerzo por entender este escenario como parte fundamental del modelo de seguridad de la información en la organización. Así mismo, se han venido fortaleciendo las relaciones con los entes judiciales, acciones emprendidas por los diferentes tipos de industrias, en pro del mejoramiento.

- Los presupuestos son uno de los grandes desafíos de los responsables de seguridad de la información en la actualidad; conseguir estos limitados recursos para diseñar programas encaminados a proteger al negocio, es uno de los retos importantes.

REFERENCIAS

[1] http://www.semana.com/tecnologia/articulo/que-tan-preparado-esta-el-gobierno-contra-ataques-ciberneticos/431602-3

[2] http://www.elheraldo.co/tecnologia/como-va-el-mundo-en-seguridad-informatica-182638

[3] http://www.milenio.com/financial_times/ciberataques-seguridad_informatica-amenazas_tecnologicas_0_438556144.html

[4] http://www.acis.org.co/revistasistemas/index.php/ediciones-revista-sistemas/edicion-131/item/164-tendencias-2014-encuesta-nacional-de-seguridad-inform%C3%A1tica

Autora

Sandra Ximena Pereira Carrero
Ingeniera de Sistemas Corporación Unificada Nacional