Cuaderno Activa
Revista científica de la Facultad de Ingeniería

Factores y causas de la fuga de información sensibles en el sector empresarial.

Factors and Causes of Sensitive Information in the Corporate Sector.

Wilmar Alejandro Cabarique Álzate*
César Augusto Salazar Romaña**
Yeiler Alberto Quintero Barco***

Tipo de artículo: Reflexión.

Recibido: 31 de agosto, 2015
Aceptado: 24 de octubre, 2015

Resumen

En la actualidad se da gran valor a la información y datos sensibles de las compañías, por lo cual la protección y seguridad de los mismos toma gran importancia en las políticas empresariales, que buscan salvaguardar tres propiedades principales: confidencialidad, integridad y disponibilidad. Con el presente artículo se pretende demostrar qué tanto las fallas tecnológicas, como los factores humanos, facilitan el acceso no deseado a información confidencial. Una fuga de información es aquel dato sensible de una empresa que es extraído sin autorización por cualquier individuo, vulnerando los sistemas y dejando en riesgo a la misma organización; para minimizar tales riesgos, se hace necesario implementar algunos mecanismos idóneos para salvaguardar datos personales de usuarios y clientes corporativos, con lo cual se les brindar seguridad y confianza, al mismo tiempo que se cumple la normatividad colombiana que exige a entidades estatales y privadas un tratamiento responsable para dicha información. Además, se entrega una reflexión acerca de las fugas de información en las compañías.

Palabras clave: Información sensibles, fuga de información, políticas de seguridad.

Abstract

At present, companies' information and sensitive data are given great value, so that the protection and security of them becomes very important in business policies which seek to safeguard three main properties: confidentiality, integrity and availability. The purpose of this article is to show that both technological failures and human factors facilitate access to confidential information. A leak of sensitive information is a company's data obtained without authorization from an individual violating the systems and leaving the company at risk. So it is necessary to implement some appropriate mechanisms to safeguard personal data, thus providing customers with security and confidence and complying with Colombian law, which forces state and private entities to provide adequate treatment to data. A reflection on information leakage in companies is provided.

Keywords: Sensitive information, information leakage, security policies.

* Ingeniero de Sistemas. Analista de Seguridad y Cumplimiento. Compañía de Financiamiento Tuya S.A. cabarique@gmail.com.

** Ingeniero de Sistemas. Ingeniero de Soporte. Universidad de Antioquia. cesarsalazar1002@gmail.com.

*** Especialista en Seguridad de la Información. Docente. Fundación Universitaria María Cano. yeilerq@gmail.com.

Introducción

Las compañías son instituciones legalmente autorizadas para realizar operaciones financieras, tecnológicas, educativas, entre otras, lo que hace que su materia prima sea constituida principal y fundamentalmente por la información y datos que suministran sus clientes para el desarrollo de su objeto social, por lo que a nuestro juicio poseen un alto riesgo de ser atacadas con el fin de capturar información confidencial y de esta forma dar un manejo inadecuado a ésta.

La fuga de información es un incidente que permite que una persona ajena a la organización tenga conocimiento de datos que solo deberían conoce el personal corporativo; estos ataques pueden ser externos o internos, intencionales o accidentales. Se demostró que las más significativas fugas de información ocurren en el ámbito interno en las compañías, dado que los empleados conocen las debilidades y vulnerabilidades que tienen los mecanismos de seguridad implementados, adicional a esto, los medios más utilizados para acceder y obtener información reservada son de uso común como UBS y celulares.

Se relacionarán algunos de los casos reales más significativos que han sufrido grandes empresas en los contextos nacional e internacional, y se abordará la legislación colombiana que reguló el tema de protección de datos personales con la finalidad de establecer parámetros que deben seguir las entidades públicas o privadas para ofrecer la seguridad necesaria y evitar de esta forma la fuga de información.

Marco teórico

Datos sensibles.

Se entiende por datos sensibles la información privada de un individuo que no es de público conocimiento, dado que está revestida de carácter de confidencialidad (Universidad Nacional de Colombia, 2012). El presente artículo se centrará en las entidades financieras, toda vez que por el objeto social que desarrollan son las más propensas a ataques que buscan acceder a información de carácter confidencial, circunstancia que en el área de la seguridad de la información se conoce como fuga de información, la cual se presenta cuando se da una salida no controlada de datos a personas no autorizadas, o cuando el responsable de garantizar su seguridad pierde el control de la misma (Pernet, 2011).

Clasificación de la información sensible.

Privada: cumplimiento de normativas, información sobre cuentas bancarias, números de tarjetas de crédito, información de contacto, datos sobre historias clínicas.

Propiedad intelectual: Documentos estratégicos, competencia, código fuente, especificaciones de ingeniería, precios.

Confidencial: Reputación, resultados de la compañía, estrategias, correos internos, conversaciones internas (Dubra, 2010).

Fuga de información sensible.

Se denomina fuga de información al incidente que pone en poder de una persona ajena a la organización, información confidencial que sólo debería estar disponible para integrantes de la misma; este tipo de incidente puede tener un origen interno o externo, y a la vez ser intencional o no. Los principales medios utilizados para facilitar fugas de información son: USB, correo electrónico corporativo, email gratuito por Internet, redes inalámbricas, CD/DVD, impresos.

El 59% de los ex-empleados se llevan consigo, al momento de su salida, datos de la compañía como: Listado de clientes y contactos, datos de empleados actuales, información financiera. El 68% de ellos piensa utilizar los datos robados en su futuro empleo. También se realizó un sondeo entre 300 empresas de 19 países, en el cual se detectó que el 60% de ellas habían tenido problemas por fuga de información (CIO Perú, 2009).

Factores internos y externos por actos intencionales o accidentales de fuga de información sensible.

Compañía: Generalmente, la fuga de información es endilgada a la entidad financiera por falta de políticas de seguridad y/o de divulgación, de auditorías, de dispositivos de seguridad y errónea clasificación de la información sensible.

Empleados: De otro lado, se ha evidenciado responsabilidad en los empleados de la compañía por desconocimiento de las políticas de seguridad o porintenciones inequívocas de dar un uso inadecuado a la información.

Clientes: En algunas ocasiones, los incidentes de fuga de información son atribuibles a los propios clientes por exceso de confianza en el tema de seguridad, falta de interés en la protección de sus datos y desconocimiento de las políticas de seguridad.

Según estudios realizados por la empresa Symantec, el 69% de las compañías encuestadas ha sufrido fuga de datos en el último año, e indican que estas complicaciones podrían ser prevenidas si las entidades monitorearan, mejoraran y optimizaran el funcionamiento de sus sistemas de seguridad (Gallego, 2013).

Señalaron que la seguridad de las compañías se ve vulnerada en mayor medida con la incursión de dispositivos inteligentes (smartphones), habida cuenta que los empleados tienen medios de almacenamiento rápidos, agiles, y que en la mayoría de las oportunidades pasan desapercibidos por los controles establecidos para garantizar un adecuado tratamiento de la información confidencial.

Un ejemplo de lo anterior es el uso de las cámaras de los teléfonos móviles, con las que se puede captar información, sin que exista un mecanismo que permita controlarlas o monitorearlas. Además, nos enfrentamos al desafío del envío de datos a través de correos electrónicos personales, teniendo en cuenta que es una herramienta de uso común y de la cual se tiene acceso desde cualquier dispositivo con conexión a Internet.

Por otro lado, las empresas no tienen la cultura de clasificar adecuadamente su información en las categorías de públicas y privadas o confidenciales, dado que la primera hace referencia a la información que es de libre acceso para cualquier persona; por el contrario, cuando hablamos de datos privados o confidenciales, se habla de información que requiere un tratamiento especial, con acceso limitado de usuarios y medidas de seguridad.

No proteger adecuadamente la información confidencial trae como consecuencia grandes pérdidas económicas cuando los datos se utilizan para efectuar transacciones fraudulentas y se ocasiona un desmedro en el buen nombre de la entidad financiera, pues se ve menoscabada la confianza que los clientes han depositado en la organización, haciendo que éstos busquen esa seguridad en otras entidades financieras que garanticen el respaldo anhelado.

De otro lado, el Gerente de Investigación y Educación ESET Latinoamérica indicó que era posible dividir el problema de la fuga de información en dos ramas: la primera relacionada con la tecnología y la segunda con las personas, obedeciendo esta clasificación a la forma de propagación de la información y el lugar donde se almacena.

En tal virtud se deben implementar mecanismos que garanticen la protección de la información, como el software diseñado para ese fin, que envíe señales de alerta cuando se presenten incidentes y bloquee las acciones que no se encuentran permitidas. Los hallazgos encontrados nos permitirán corregir las falencias con la finalidad de evitar futuras pérdidas de información, sensibilizando a las personas sobre la fuga de información y las consecuencias de la misma.

Casos reales de fuga de información sensible

Entre los casos más significativos y relevantes de fuga de información encontramos los siguientes:

Renault fue víctima del espionaje industrial cuando sus altos directivos vendieron información confidencial sobre su vehículo eléctrico, investigación en la que habían invertido más de 4.000 millones de euros (Pérez, 2011).

81 estaciones de gasolina de Miami y Florida robaron información de las tarjetas de crédito de sus clientes (Diario las Américas, 2015).

La empresa CardSystems (procesador de operaciones de tarjetas de crédito) permitió el robo de información de las 200.000 tarjetas de crédito de usuarios que realizaron compras por Internet y en persona en los Estados Unidos (La Nación, 2005).

Robaron los datos de 77 millones de cuentas de la empresa Sony, entre los que se encontraban información sobre tarjetas de crédito, fecha de vencimiento, nombre de clientes, direcciones, teléfonos, e-mail y demás. (La Vanguardia, 2011).

Bancolombia frustró el robo del siglo gracias a sus medidas de seguridad, cuando un grupo de hackers logró traspasar 160.000 millones de pesos a cuentas Bancolombia. Debido a los controles internos, los delincuentes solamente tuvieron acceso al 4% de lo que pensaban hurtar. (El Espectador, 2014).

Leyes colombianas sobre seguridad informática

Con el transcurrir de los años, la seguridad de la información manejada por empresas públicas y privadas ha cobrado gran importancia en el objeto social que desarrollan, y conforme a lo expuesto en precedencia, se ha demostrado que el robo de dicha información por parte de terceros es una práctica que se hace poco a poco más fácil de realizar, por lo que el legislador se vio en la obligación de regular el tema, incluso, dispuso como causal justa de terminación del contrato laboral que el trabajador revele secretos técnicos o comerciales del empleador (Congreso de la República de Colombia, 1950).

Adicional a esto, en el año 2012 entró a regir la Ley Estatutaria 1581 que regula las disposiciones generales para protección de datos y que tiene por objeto desarrollar el derecho constitucional a la privacidad, consagrado en el artículo 15 de nuestra Constitución Política, y el derecho a la información previsto en el artículo 20.

La normatividad es aplicable a todos los datos personales registrados en cualquier base de datos susceptible de tratamiento por entidades públicas o privadas (Ley 1581 de 2012, art. 2), las que conforme al literal d del artículo 17 de la esta ley estatutaria tienen la obligación de: "Conservar la información bajo las condiciones de seguridad necesarias para impedir su adulteración, pérdida, consulta, uso o acceso no autorizado o fraudulento."

Así mismo, nuestro Código Penal en el numeral 1 del artículo 270 prevé una pena de prisión de 2 a 5 años y multa de 20 a 200 salarios mínimos legales mensuales vigentes para quien "Publique, total o parcialmente, sin autorización previa y expresa del titular del derecho, una obra inédita de carácter literario, artístico, científico, cinematográfico, audiovisual o fonograma, programa de ordenador o soporte lógico."

¿Cómo evitar la fuga de información sensible?

A continuación se brindan algunos consejos a tener en cuenta ante este escenario, de tal modo que sea posible evitar las principales causas de fuga de información, principalmente enfocados al ámbito corporativo:

1. Conocer el valor de la propia información. Realizar un análisis de riesgos y un estudio de valuación de activos para poder determinar un

plan de acción adecuado que permita evitar posibles filtraciones.

2. Concientizar y disuadir. Diseñar una estrategia de concientización sobre la responsabilidad en el manejo de la información y sus posibles consecuencias laborales y legales.

3. Utilizar defensa en profundidad. Considerar la aplicación del modelo de defensa en capas a fin de que las distintas medidas que se toman cubran todos los aspectos del acceso a la información (físico, técnico y administrativo) y así evitar centralizar las soluciones o promover puntos únicos de falla.

4. Incluir herramientas tecnológicas. En ámbitos corporativos, contar de ser posible con una solución técnica de protección, por medio de hardware, software, o combinación de ambos, tanto a nivel de redes como de equipos (servidores y estaciones de trabajo). Además, las soluciones contra el malware son particularmente indispensables.

5. Seguir los estándares. Alinearse con estándares internacionales de gestión de la seguridad permite disminuir el riego de que puedan ocurrir incidentes, así como también de que el negocio se vea afectado por un determinado evento de filtración.

6. Mantener políticas y procedimientos claros. Relacionado con el punto anterior, se debe tener una clara definición y comunicación de las políticas de seguridad y acuerdos de confidencialidad, aceptados y firmados por todos los usuarios. Esto minimiza potenciales fugas de información, al contar con un consentimiento firmado del usuario para no realizar ciertas acciones.

7. Procedimientos seguros de contratación y desvinculación. En estos dos momentos se conecta o desconecta una nueva pieza externa con el motor de la organización, por lo que deben tenerse en cuenta de manera muy particular, controlando especialmente los accesos y registros de los usuarios en sus primeros o últimos momentos de trabajo (Pacheco, 2011).

8. Seguir procesos de eliminación segura de datos. Es fundamental que los datos que se desean eliminar sean efectivamente eliminados, y los medios de almacenamiento adecuadamente tratados antes de ser reutilizados.

9. Conocer a la propia gente. Se recomienda tener presente que en las organizaciones puede haber personas conflictivas o disconformes, que podrían ser foco de cierto tipo de problemas relacionados con la confidencialidad. Si bien puede ser dificultoso detectar estos casos, el hecho de conocer en profundidad al propio personal ayuda a entender la situación general en que se encuentra una empresa y los posibles riesgos.

10. Aceptar y entender la realidad. Es necesario hacer lo posible para comprender que se deben tomar medidas concretas y definir un plan realista. No se pueden controlar absolutamente todas las acciones de todas las personas en todo momento, por lo que siempre habrá un margen de error que quedará abierto, y que deberá intentar reducirse al mínimo a medida que pasa el tiempo. Con esta lista se puede tener una idea general de los puntos más importantes a tener en cuenta a la hora de combatir la fuga de información. Como es de esperarse, muchas medidas aplican también a la solución de los más diversos problemas relacionados con la seguridad, y justamente es por esto que conviene contar con una estrategia global, que incluya todos los aspectos de interés para una organización. (Pacheco, 2011).

Reflexión

En lo referente a la leyes colombianas, se advierte que nuestro ordenamiento jurídico ha regulado lo concerniente a la protección de datos, por lo que

se observa que establecer políticas de seguridad en las compañías no sólo las beneficia para evitar futuras fugas de información que ocasionen pérdidas económicas y afecten su buen nombre, sino que es una obligación legal brindarle a sus clientes la seguridad necesaria para garantizar que sus datos no sean objeto de un uso inadecuado o fraudulento.

Ahora bien, se evidencia conforme a los casos reales presentados anteriormente, que la fuga de información sensible suele presentarse dentro de las compañías, pese a que cuenten con políticas de seguridad y controles contra la misma (DLP – Data lose prevention, Protección contra la fuga de información), por lo que cobra gran importancia concientizar al personal interno de que los datos de los clientes son sensibles, y que su mal manejo no sólo acarrearían consecuencias respecto del contrato de trabajo sino responsabilidad penal.

La Corte Constitucional, en la Sentencia T-987 de 2012, indica que las compañías deben garantizar a sus clientes que la información suministrada será resguardada bajo la seguridad necesaria, y que será utilizada exclusivamente para los fines que autorice el titular de la misma; por lo tanto no podrá ser entregada a terceros sin previa autorización del cliente, ni podrá ser trasladada a otras bases de datos.

Se tiene entonces que la fuga de información sensible es una amenaza constante que sufren todas entidades, bien sean públicas o privadas, que evoluciona conforme se mejoran los mecanismos para salvaguardad su integridad y confidencialidad, por lo que las políticas de seguridad también deben estar en constante desarrollo. El factor humano siempre constituirá el riesgo más alto, dado que en la actualidad el bien más valioso es la información, y si se pone a disposición de personas ajenas a las organizaciones no sólo habrá significativas pérdidas económicas, sino que se afectará irreversiblemente la confianza que los clientes puedan tener sobre los servicios prestados.

Ahora bien, con la expedición de la Ley Estatutaria 1581 de 2012 se reguló en gran medida la protección de datos personales, y la Ley 1266 de 2008 dictó las disposiciones sobre el manejo de la información contenida en bases personales, especialmente de carácter financiero, crediticio, comercial, entre otros. Estas dos normas guían al operador de la información sobre los procedimientos que debe implementar y los protocolos que se deben respetar para cumplir las leyes, por lo que consideramos que implementar las políticas de seguridad es un trabajo progresivo que debe ir de la mano con la legislación colombiana que regula el régimen de protección de datos personales y la tecnología, se trata de un trabajo conjunto para blindar a las compañías de las denominadas fugas de información.

Conclusiones

Las compañías tienen un alto riesgo de sufrir ataques que puedan filtrar información confidencial, no sólo de sus clientes, sino también de sus proyectos más importantes, por lo que es necesario -en primer lugar- clasificar los datos y documentos, establecer quiénes deben garantizar su seguridad e implementar políticas internas para salvaguardar la misma.

Con una correcta clasificación de la información y una herramienta DLP, las compañías pueden detectar con facilidad cualquier fuga de información para adoptar las acciones correspondientes que permitan corregir las falencias presentadas.

Con la entrada en vigencia de la Ley Estatutaria 1581 de 2012, varias organizaciones han implementado controles de seguridad para garantizar el uso adecuado de la información, los cuales integran recursos humanos y tecnológicos.

Muchas compañías mantienen en secreto la pérdida de información para salvaguardar la imagen de la empresa, por lo que se cuentan con pocos casos públicos sobre fuga de información.

Referencias

CIO Perú. (2009). CIO Perú. Recuperado de http://cioperu.pe/articulo/718/el-59-de-los-trabajadores-despedidos-roban-datos/

Congreso de la República de Colombia. (1950). Código Sustantivo del Trabajo. Bogotá: Diario Oficial.

Diario Las Américas. (2015). Detectan dispositivos para robos de tarjetas en gasolineras del estado. Recuperado de http://www.diariolasamericas.com/4842_locales/3067514_detectan-dispositivos-robos-tarjetas-gasolineras-miami-dade.html

Dubra, A. (2010). Fuga de información, Un negocio en crecimiento. Recuperado de http://www.symantec.com/content/es/mx/enterprise/images/vision/slides/Track3-Session4.pdf

El Espectador. (2014). El robo del siglo no alcanzó. Recuperado de http://www.elespectador.com/noticias/judicial/el-robo-del-siglo-no-alcanzo-

Gallego, L. (2013). Metodología para prevenir la fuga de información. Medellín: Universidad Nacional de Colombia.

La Nación. (2005). Mercado negro de tarjetas de crédito en Internet. Recuperado de http://www.lanacion.com.ar/723688-mercado-negro-de-tarjetas-de-credito-en-internet

La Vanguardia. (2011). La Vanguardia. Obtenido de http://www.lavanguardia.com/internet/20110427/54146138829/sony-

Pacheco, F. (2011). Fuga de información: ¿una amenaza pasajera? Buenos Aires: ESET Latinoamérica

Pérez, P. (2011). Renault, víctima del espionaje industrial. Recuperado de http://www.lavanguardia.com/lectores-corresponsales/20110107/54098992912/renault-victima-del-espionaje-industrial.html

Pernet, C. (2011). Fuga de información. Manejo de divulgación intencional de información interna. Societe Generale.

Universidad Nacional de Colombia. (2012). Política de tratamiento de protección de datos personales de los titulares. Bogotá: Universidad Nacional de Colombia.

"La educación no cambia el mundo, cambia a las personas que van a cambiar el mundo".

Paulo Freire.

Passiflora parritae x antioquiensis / Autor: Diego Alonso Rivera Vergara