No.14 / Julio-Agosto 2012 ISSN: 1251478, 1251477

.Seguridad

Cultura de prevención para TI

14

Gestión de Seguridad y Riesgos

Distintos enfoques en la práctica segura

Datos Biométricos | PenTest | Gerencia | Incidentes Seguridad | Riesgo Tecnológico | Voto Electrónico

Contenido

.Seguridad
Cultura de prevención para TI

Editorial

Gestión de seguridad y riesgos: Distintos enfoques en la práctica segura

La guerra épica entre la seguridad y la funcionalidad implica un constante cambio, un ciclo continuo de altas y bajas que busca el equilibrio adecuado. Por un lado tenemos el batallón de la administración y los usuarios finales, quienes buscan practicidad, ahorro y soluciones. Por el otro, están los guerreros de la seguridad, ellos resguardan, protegen y neutralizan.

Ambas partes se necesitan una a la otra. Esta dualidad de seguridad y funcionalidad, este síncope entre armonía y contraste es lo que permite ganar una batalla aún mayor, la lucha contra los ataques a la tecnología.
En tu revista .Seguridad Cultura de prevención para TI queremos ofrecerte una visión integral, con un certero bosquejo de los aspectos gerenciales y operativos de la seguridad, pero al mismo tiempo con valiosas aproximaciones a la cultura de protección de datos, a la importancia de analizar riesgos, de entenderlos y neutralizarlos.

Te invitamos a encontrar en los artículos de esta edición, la bitácora de guerra de la lucha entre la Gestión de seguridad y los riesgos tecnológicos: Distintos enfoques en la práctica segura.

L.C.S Jazmín López Sánchez
Editora
Subdirección de Seguridad de la Información

.Seguridad
Cultura de prevención para TI

.Seguridad, Cultura de prevención TI / Número 14 / Julio-Agosto 2012 / ISSN No. 1251478, 1251477 / Revista Bimestral

Leyes de protección de datos personales en el mundo y la protección de datos biométricos – Parte II

Isai Rojas González, Gabriel Sánchez Pérez, Linda Karina Toscano Medina, María del Carmen Prudente Tíxteco, Gualberto Aguilar Torres

la primera entrega del artículo se describieron conceptos básicos referentes a la protección de datos personales y a la biometría, se hizo una breve introducción a las leyes y acuerdos de protección de datos personales que existen en el mundo y se enumeraron algunos de los casos más relevantes con el objetivo de dar a conocer los antecedentes que existen respecto a cómo son considerados los datos biométricos por las leyes de protección de datos personales de distintos países en el mundo.

En esta segunda parte se describen algunos de los riesgos que están asociados al uso de datos biométricos y que motivan a la búsqueda de medidas de protección, se habla de la forma en que éstos son considerados a nivel internacional, sobre el contexto de las leyes de protección de datos personales y sobre una serie de recomendaciones emitidas por organismos internacionales referentes a cómo deben ser obtenida y procesada esta información.

Riesgos asociados al uso de los datos biométricos

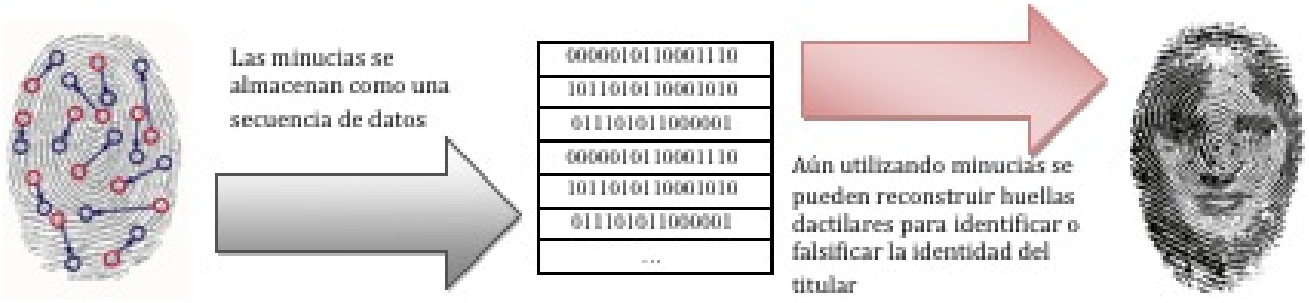
Un sistema biométrico que no es protegido adecuadamente puede facilitar la obtención de información personal sensible. Por ejemplo, si un atacante roba la base de datos de un sistema de reconocimiento facial en el cual se almacenan fotografías, se podría inferir la raza de cada uno de los usuarios, lo que podría ser causa de discriminación u otras acciones.

Algunos datos biométricos pueden ser obtenidos realizando el proceso inverso de captura y almacenamiento, como es el caso de las huellas dactilares. Éstas tienen rasgos únicos conocidos

como minucias, durante el proceso de captura, estos son identificados y codificados para después almacenarlos como una secuencia de datos denominada plantilla de minucias, de tal forma que, en lugar de almacenar una fotografía de la huella dactilar, se almacenan plantillas de minucias. Se dice que una huella dactilar reconstruida a partir de la plantilla de minucias tiene un resultado positivo en más del 90% de los casos, y que este tipo de reconstrucciones son más frecuentes de lo que se podría suponer. Esto indica que pueden identificarse personas o falsificar identidades mediante huellas dactilares que son obtenidas exitosamente, en su forma

La recolección de datos biométricos es otro aspecto de preocupación, así lo señala la Comisión Nacional de Informática y Libertades (Francia) en su informe de actividades del año 2007, que en uno de sus fragmentos dice: …

Algunos datos biométricos presentan la particularidad de poder ser recabados y utilizados sin que el interesado se dé cuenta. Es el caso de las huellas genéticas, ya que todos vamos dejando involuntariamente un rastro de nuestro



[1] Plantilla de minucias: Se denomina al conjunto de características ínfimas de una huella dactilar que se almacenan como un patrón de datos único que hace identificable de manera inequívoca al titular de la huella.
[2] Fingerprint Biometrics: Address Privacy Before Deployment. Publicado por el Comisionado de Información y Privacidad de Ontario en noviembre de 2008.

original, incluso desde una base de datos de plantillas de minucias.

En 2003, el Grupo de Protección de las Personas en lo que Respecta al Tratamiento de Datos Personales, creado en virtud de la Directiva 95/46/CE del Parlamento Europeo y del Consejo, adoptó un documento de trabajo sobre biometría, en la introducción del documento se puede apreciar la siguiente inquietud:

…Una utilización amplia y sin control de la biometría es preocupante desde el punto de vista de la protección de los derechos y libertades fundamentales de las personas. Este tipo de datos es de una naturaleza especial, ya que tienen que ver con las características comportamentales y fisiológicas de una persona y pueden permitir su identificación inequívoca…

cuerpo, aunque sea ínfimo, del cual se puede extraer el código ADN. Lo mismo sucede con las huellas dactilares, de las que también vamos dejando un rastro, más o menos fácil de procesar, en nuestra vida cotidiana .

La Comisión indica que la biometría con rastro requiere de medidas de seguridad especiales para garantizar la protección de las personas afectadas.

Protección jurídica de los datos biométricos

Por su naturaleza, los datos biométricos son datos personales, sin embargo, en muy pocas legislaciones en el mundo se consideran de manera explícita como datos personales y menos aún como datos personales sensibles, lo anterior da origen a diversas controversias.

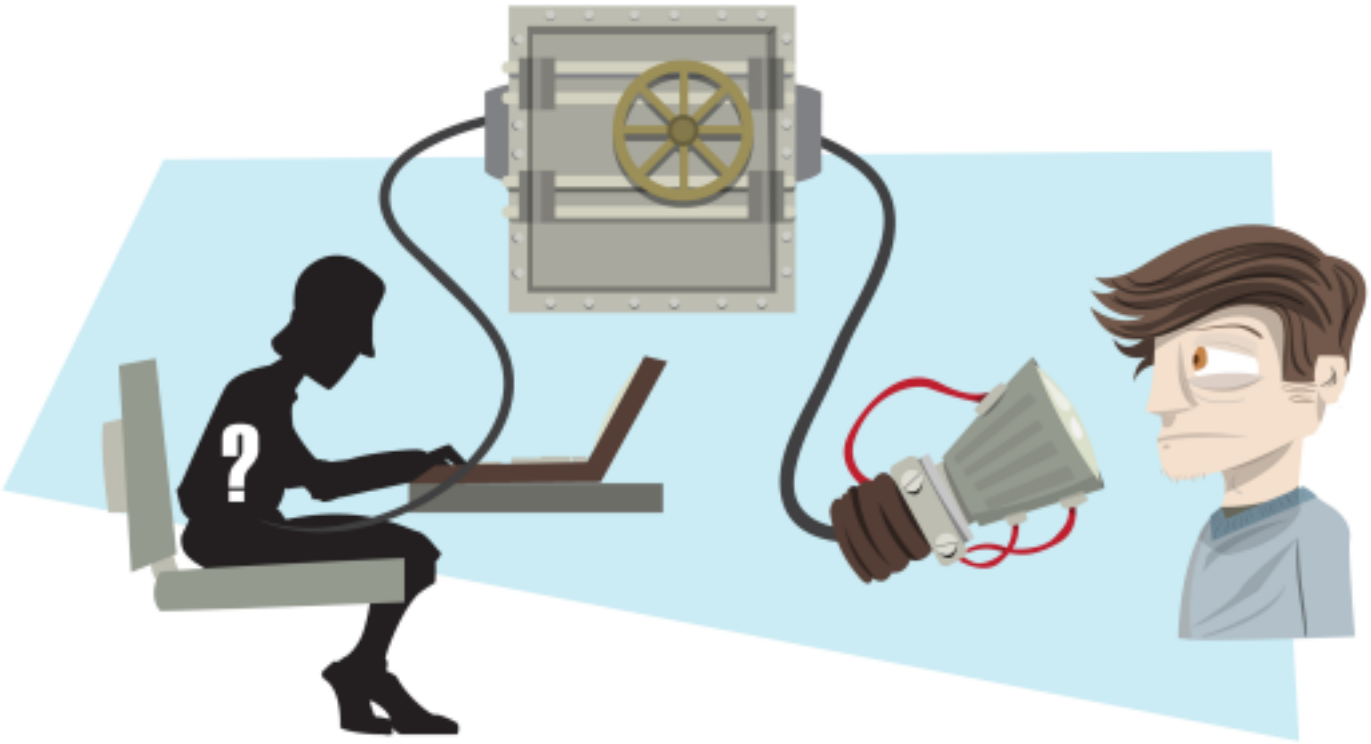
En España y Argentina, las leyes de protección de datos personales, no han tipificado de manera explícita a los datos biométricos, es por ello que organismos regulatorios han sido los encargados

de debatir y emitir resoluciones para cada caso específico de controversia, lo han hecho evaluando las circunstancias particulares de cada situación.

En el año 2006, la Agencia Española de Protección de Datos resuelve que el uso de la huella dactilar como medio para controlar el acceso de alumnos al colegio resulta excesivo y desproporcionado para esa finalidad.

Australia. El comité de reforma de la ley de privacidad, recomendó que se agregaran los datos biométricos a la definición de datos sensibles. El cambio aún no ha sido incluido en la versión actual de la ley con fecha del 4 de julio de 2011.

Rusia. Actualmente, se encuentra en proceso de modificación a su ley federal de protección de datos de 2006, el propósito es mejorar algunos



Por otro lado, en Argentina en el 2009, la Dirección Nacional de Protección de Datos Personales resolvió, respecto a un banco de datos de aficionados al fútbol, que pueden ser tratados los datos biométricos, por ser datos estrictamente de identificación, cuando sean necesarios para la finalidad pretendida (seguridad en estadios de fútbol). La mayoría de las leyes de protección de datos personales en el mundo se encuentran en una situación de ambigüedad en lo que se refiere a los datos biométricos. La legislación en México tiene el mismo inconveniente, la ley en sí no hace mención explícita de los datos biométricos ni de su tratamiento.
Algunos países comienzan a incluir de manera explícita el concepto de datos biométricos y la manera en que estos deben tratarse y protegerse:

aspectos de seguridad. Uno de los cambios indica que el reglamento establecerá los requisitos de seguridad para el procesamiento de datos biométricos.

Perú. Recientemente adoptó la ley número 29.733 que se refiere a la protección de datos personales y señala en su artículo 2º que los datos biométricos son datos personales sensibles.

Futura legislación en Colombia. El documento con el texto conciliado y aprobado del proyecto de ley estatutaria número 184 de 2010 Senado, 046 de 2010 Cámara en Colombia, especifica en su título III, artículo 5º que los datos biométricos son considerados datos personales sensibles.

Convenios internacionales

El Consejo de Europa (Council of Europe) ha publicado un documento llamado: “Informe de situación relativo a la aplicación de los principios de la convención 108 sobre la recogida y al proceso de los datos biométricos”, el informe contiene una serie de pronunciamientos respecto a los datos biométricos y su uso. A continuación, se presenta la idea básica de cada punto:

1) Los datos biométricos deben ser considerados como una categoría específica de datos, ya que estos siguen siendo los mismos en distintos sistemas y son inalterables de por vida.

2) Antes de recurrir a la biometría, se deben evaluar: las finalidades previstas para los datos, las ventajas contra los inconvenientes que afecten la vida privada de la persona involucrada, y se deben tener posibles soluciones alternativas que supongan un menor atentado contra la privacidad.

3) No se debería optar por la biometría únicamente por el hecho de que su uso resulte práctico.

4) Los datos biométricos deben ser utilizados con fines determinados, explícitos y legítimos. No deben ser procesados de manera incompatible con esas finalidades.

5) Los datos deberían ser adecuados, pertinentes y no excesivos en comparación con la finalidad del proceso; si basta con patrones, se debería evitar el almacenamiento de la imagen biométrica.

6) A la hora de elegir la estructura del sistema, se debería proceder teniendo en mente los aspectos de seguridad.

7) La estructura de un sistema biométrico no debería ser desproporcionada respecto a la finalidad del proceso; si basta con la verificación, no se debería desarrollar una solución de identificación.

8) La persona afectada debería ser informada de la finalidad del sistema y de la identidad del responsable del proceso. Además, conocer los datos procesados y las categorías de personas a las que se comunicarán esos datos.

9) La persona afectada tiene derecho de acceso, rectificación, bloqueo y cancelación de sus datos.

10) Se deben prever medidas, técnicas y organizativas, que sean adecuadas para proteger los datos biométricos contra la destrucción y la pérdida accidental, también se deben proteger contra el acceso, modificación o comunicación no autorizada y deben ser resguardados de cualquier otra forma de procesamiento ilícito.

11) Se debería desarrollar un procedimiento de certificación y de control, con el fin de establecer normas de calidad para el software y la formación del personal responsable del registro y la verificación de datos biométricos. Se recomienda una auditoría periódica que pruebe las cualidades técnicas del sistema.

12) Si una persona, registrada en un sistema biométrico, es rechazada, el responsable de proceso debería, a petición de ésta, volver a examinar el caso y si fuese preciso, ofrecerle soluciones de sustitución adecuadas.

Actualmente, hay varios países que cuentan con leyes de protección de datos personales, pero pocos son los que incluyen en sus postulados, de manera explícita, a los datos biométricos y el tratamiento que éstos deben tener, el precedente legal lo establecen países como Rusia, Perú y Colombia.

Es necesario regular al respecto del uso de los datos biométricos en los sistemas de información, son datos muy íntimos que acompañan a su titular de por vida y que no pueden ser cancelados o restablecidos; si a un usuario le roban y falsifican su huella dactilar, esta no podrá ser cancelada, su huella seguirá siendo la misma.
La regulación legal de los datos biométricos ayuda a prevenir ambigüedades que pueden generar controversias y además establece las reglas necesarias para el correcto resguardo de la información sensible de las personas.

Referencias Bibliográficas (Parte 2)

[1] Remolina A. N. (2011). Sistemas de identificación biométrica y protección de datos personales: ni "tecnofobia", ni "tecnofascinación", pero sí "tecnoreflexión". Consultado en: http://www.ambitojuridico.com/BancoConocimiento/N/noti-111116-06_(sistemas_de_identificacion_biometrica_y_proteccion_de_datos_personales)/noti-111116-06_(sistemas_de_identificacion_biometrica_y_proteccion_de_datos_personales).asp

[2] Comité consultivo de la Convención para la protección de las personas respecto al proceso automatizado de los datos de carácter personal (T-PD) (2005). Informe de situación relativo a la aplicación de los principios de la convención 108 a la recogida y al proceso de los datos biométricos

[3] Sitio Web Kimaldi Electrónics. Tratamiento de la huella digital de los trabajadores/as.

[4] Agencia Española de Protección de Datos:
• Proporcionalidad del tratamiento de la huella dactilar de alumnos de un colegio. Informe 368/2006
• Tratamiento de la huella digital de los trabajadores.
• Resolución de archivo de actuaciones. Expediente Nº E/00016/2007

[5] Segalis B. (2011). Russia Amends Federal Data Protection Law; Privacy Enforcement on the Rise. Consultada en: http://www.infolawgroup.com/2011/07/articles/international-2/russia-amends-federal-data-protection-law-privacy-enforcement-on-the-rise/

[6] Kindt E. (2007). Biometric applications and the data protection legislation. Datenschutz und Datensicherheit.

[7] Woo R. B. Challenges posed by biometric technology on data privacy protection and the way forward

[8] Liu Y. (2007). Introduction to biometrics from a legal perspective. University of Oslo.

[8] Liu Y. (2008). Identifying Legal Concerns in the Biometric Context. Journal of International Commercial Law and Technology Vol. 3, Issue 1. University of Oslo.

[9] Iglezakis I. (2010). EU data protection legislation and case-law with regard to biometric applications. Faculty of Law, Aristotle University of Thessaloniki.

[10] El Congreso de Colombia. Texto conciliado y aprobado del proyecto de Ley Estatutaria número 184 de 2010 Senado, 046 de 2010 Cámara. "Por la cual se dictan disposiciones generales para la protección de datos personales".

[11] Cavoukian A. (2008). Fingerprint Biometrics: Address Privacy Before Deployment

[12] Article 29 of Directive 95/46/EC – Data Protection Working Party. Working document on biometrics (2003)

[13] Australia. Privacy Act 1988. Act No. 119 of 1988 as amended. This compilation was prepared on 4 July 2011 taking into account amendments up to Act No. 60 of 2011.

Enlaces Web:
[1]http://cyberlaw.stanford.edu/profile/david-banisar

[2]http://eurlex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:es:HTML

[3]http://www.statewatch.org/news/2004/feb/biometric-wp80_en.pdf

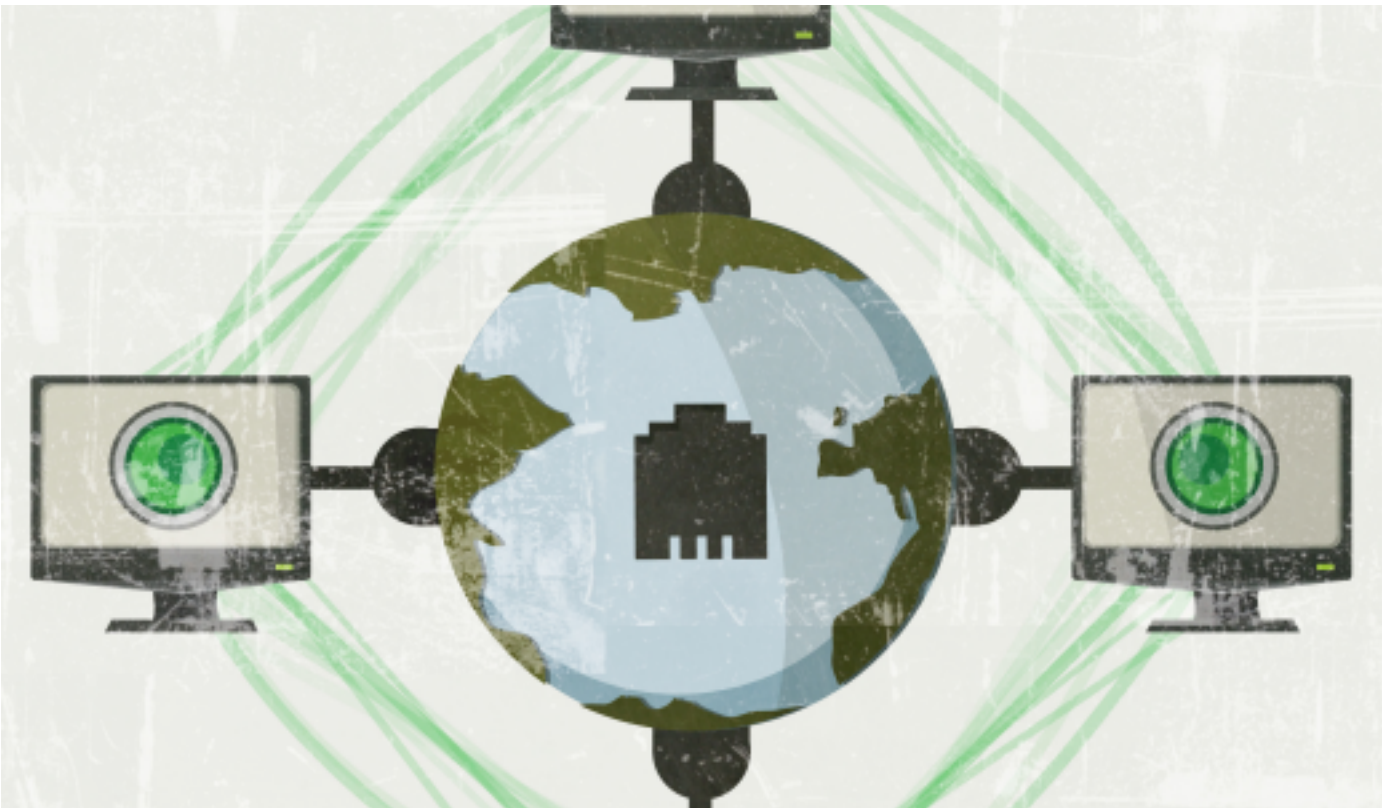
[4]http://www.martinaberastegue.com/seguridad/privacidad/legislacion-internacional-en-materia-de-proteccion-de-datos-y-privacidad.html

[5]http://www.agpd.es/portalwebAGPD/canaldocumentacion/textos_interes/common/pdfs/informe-principios-convencion-108.pdf

Gestión de incidentes de seguridad informática con agentes inteligentes

Msc. Johnny Villalobos Murillo

En este artículo se propone la aplicación de agentes inteligentes como un medio para facilitar la gestión de incidentes de seguridad informática. Los agentes inteligentes propuestos tendrían funciones específicas de búsqueda y selección de incidentes según especificaciones previamente establecidas por la organización. Se toman como base las investigaciones realizadas sobre la aplicación de algoritmos de inteligencia artificial colectiva.



Incidentes de seguridad

Los diferentes ataques que sufren los sistemas conectados a Internet son conocidos como incidentes de seguridad informática. Éstos amenazan el buen funcionamiento de cualquier organización y violan implícita o explícitamente las políticas de seguridad [1]. Al aceptar Internet como medio de interconexión global, gran cantidad de transacciones de negocios se realizan de esta forma, por lo que se requieren mecanismos de respuestas rápidas a incidentes de seguridad para evitar que la organización se exponga a pérdidas irreversibles. Se le denomina un incidente de seguridad informática a cualquier evento que sea considerado una amenaza para la seguridad de un sistema.

Existen diversos tipos de amenazas y seguirán apareciendo cada vez más.

Entre las más conocidas tenemos:

- Instalación de software malicioso
- Acceso sin autorización al sistema o a sus datos
- Interrupciones indeseadas
- Denegación de servicios
- Uso desautorizado de las bases de datos
- Cambio en el hardware, firmware o software del sistema

Es posible clasificar los incidentes de seguridad en dos tipos [2]:

- Incidentes automáticos
- Incidentes manuales

Se denominan incidentes automáticos a los incidentes producidos por programas de cómputo tales como virus, gusanos y troyanos. Los incidentes manuales son aquellos incidentes en los que de manera intencional se ataca un sistema utilizando, por ejemplo, escaneo de vulnerabilidades, inyección SQL o ingeniería social, aunque bajo ciertas circunstancias, también se pueden realizar de forma automática.

Agentes inteligentes como gestores de incidentes de seguridad informática

Podemos definir a un agente inteligente como un programa de cómputo que actúa con autonomía en nombre de una persona o una entidad [3]. La característica de autonomía se le otorga debido a que actúan sin intervención humana o de otros sistemas externos.

Existen muchas clasificaciones de agentes, pueden catalogarse por autonomía (capacidad de actuar solos), reactividad (capacidad de ejecutar acciones en forma inmediata) y proactividad (metas u objetivos específicos a cumplir) entre otros [4].

Suponga un grupo de agentes inteligentes que colaboren con un CERT o Equipo de Respuesta a Incidentes de Seguridad Informática (Computer Emergency Response Team por sus siglas en inglés), ayudando a determinar qué tipo de incidente está ocurriendo en un sistema que esté bajo ataque, con base en los síntomas que éste presenta. Los agentes proporcionarían alertas, soluciones inmediatas y medidas en forma automática para controlar dicho incidente.

El grupo de agentes estaría formado por agentes buscadores de tipo autónomo y seleccionadores del tipo proactivos. Los agentes buscadores trabajan en forma independiente y con recorridos al azar en la red, localizando información sobre incidentes en la red mediante algoritmos de inteligencia artificial, y almacenándolos en una base de datos.

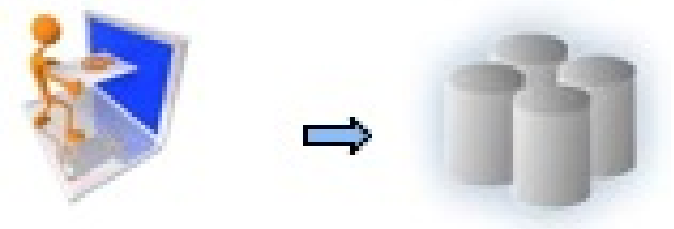
El comportamiento de estos agentes, es similar al de una colonia de hormigas que realizan búsquedas para llevar comida a sus hormigueros. La base de datos sería entonces la bodega de alimentos de los hormigueros, la información almacenada es definida por la organización, pero en forma general deberá registrarse por ejemplo el nombre y tipo de incidente, la fecha en que ocurrió y la plataforma informática o tecnológica en donde se presentó.

Los agentes seleccionadores por su parte, tienen la tarea de escoger aquellos incidentes que se adapten más a los criterios definidos por la organización, e informar mediante alertas la aparición de un incidente de seguridad para que se tomen las medidas respectivas.

La propuesta de utilizar los agentes inteligentes en los CERTS u otras organizaciones, facilitaría la gestión de incidentes de seguridad en tanto sus algoritmos, especificaciones de búsqueda y selección garanticen de forma razonable su eficacia y eficiencia.

La información que es almacenada estaría a disposición de otras organizaciones interesadas, ayudando así en la divulgación de incidentes y protección de información.

Si los incidentes de seguridad se realizan con tecnologías, entonces debemos aplicar tecnologías para su prevención y corrección.



Referencias

[1] ISO27001 Sistema de Gestión de Seguridad de la Información ISO - International Organization for Standardization

[2] NIST 800-61 Computer Security Incident Handling Guide: National Institute of Standards and Tecnology. U.S. Departament of Commerce

[3] Using Intelligent Agents", Lecture Notes in Artificial Intelligence, Springer-Verlag, Vol. 4496, pp. 82-91

[4] Juan L. Dinos-Rojas. Arquitectura de un sistema basado en agentes para la recuperación de metadatos rdf con base en una ontología de documentos.Departamento de Ingeniería Eléctrica y Computadoras, 2004.

Riesgo tecnológico y su impacto para las organizaciones - Parte I

Ing. Alexandra Ramírez Castro

Origen del riesgo tecnológico ¿Cómo nos afecta?

El riesgo tecnológico tiene su origen en el continuo incremento de herramientas y aplicaciones tecnológicas que no cuentan con una gestión adecuada de seguridad. Su incursión en las organizaciones se debe a que la tecnología está siendo fin y medio de ataques debido a vulnerabilidades existentes por medidas de protección inapropiadas y por su constante cambio, factores que hacen cada vez más difícil mantener actualizadas esas medidas de seguridad.

Adicional a los ataques intencionados, se encuentra el uso incorrecto de la tecnología, que en muchas ocasiones es la mayor causa de las vulnerabilidades y los riesgos a los que se exponen las organizaciones.

El riesgo tecnológico puede verse desde tres aspectos, primero a nivel de la infraestructura tecnológica (hardware o nivel físico), en segundo lugar a nivel lógico (riesgos asociados a software, sistemas de información e información) y por último los riesgos derivados del mal uso de los anteriores factores, que corresponde al factor humano como un tercer nivel.

Si se revisan las definiciones de las metas, objetivos, visión o misión de las organizaciones, estás no se fundamentan en términos técnicos o con relación a la tecnología. Sin embargo, al analizar de forma profunda y minuciosa este tipo de planteamientos gerenciales, se encuentra que su aplicación trae como base el desempeño de una infraestructura tecnológica que permita darle consecución a dichas cualidades. Por ello, el cumplimiento correspondiente con la prestación de los servicios y desarrollo de los productos ofrecidos por la empresa, el mantenimiento de la actividad operativa e incluso la continuidad del negocio, dependen del cuidado y conservación que se tenga de la base tecnológica y por supuesto, del personal que la opera.

Medidas de aseguramiento ante el riesgo tecnológico

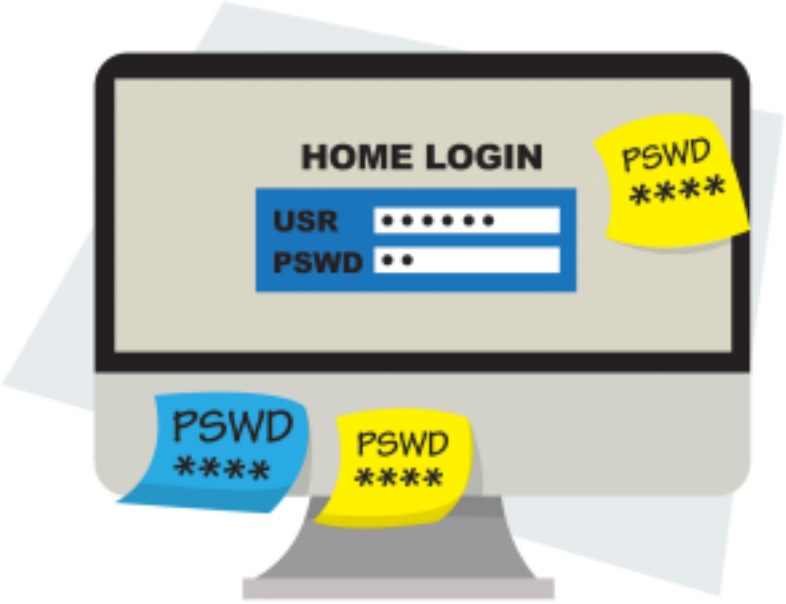
Hablar de controles y medidas que permitan a las organizaciones contrarrestar este tipo de riesgo puede ser complicado, pero es posible tomar acciones que lleven a su mitigación. El aseguramiento puede realizarse desde los tres niveles antes mencionados.

En el nivel físico, las medidas a tomar son de carácter técnico o de seguridad informática, referidas a la aplicación de procedimientos de control y barreras físicas ante amenazas para prevenir daño o acceso no autorizado a recursos e información confidencial que sea guardada en la infraestructura física. Dentro de éstas se encuentran:

- Controles de acceso físico, que pueden incluir el uso de sistemas biométricos y vigilantes para acceso en áreas específicas.
- Manejo de tokens o tarjetas de identificación.
- Controles a nivel de equipos, tales como ubicación y protección, seguridad en cableado o mantenimiento periódico de equipos.
- Servicios básicos (energía, agua y alcantarillado, entre otros) de soporte para continuidad.
- Gestión de medios de almacenamiento removible.
- Controles de vulnerabilidades técnicas, entre otros.

En el nivel lógico, las medidas a tomar se dan con respecto al uso de software y sistemas, enfocadas a proteger los datos y garantizar el acceso autorizado a la información por parte de los usuarios a través de los procedimientos correctos. Como parte de estas medidas se pueden tomar:

- Controles de acceso lógico con la gestión de usuarios, perfiles y privilegios para acceso.
- Controles de acceso a la red interna y segregación en redes y controles para asegurar servicios de la red.
- Controles a nivel de teletrabajo y equipos móviles.
- Soluciones de protección contra malware.
- Respaldos de bases de datos e informació crítica.
- Protocolos para intercambio de información y cifrado de información.
- Monitoreo de los sistemas, sincronización de relojes y protección sobre registros.
- Limitación en tiempos de conexión a aplicativos y cierres de sesión por inactividad.
- Gestión de control de cambios, entre otros.



El tercer nivel y el más crítico dentro de las organizaciones, dada su naturaleza impredecible, es el personal o recurso humano. Las medidas a este nivel deberían ser más procedimentales, ligadas a la regulación y concienciación.Dentro de éstas se pueden incluir:

- Definición de políticas de seguridad que presenten las correspondientes violaciones con el fin de dar cumplimiento.
- Controles relacionados a acuerdos con

terceros, prestación de servicios que se puedan dar con éstos y segregación de funciones.
- Controles a nivel contratación de personal.
- Gestión antes, durante y después de la terminación de los contratos.
- Educación y capacitación continua en aspectos de seguridad.
- Procedimientos e instructivos para manejo de información.
- Políticas de escritorio y pantalla limpia.
- Cumplimiento de legislación aplicable, entre otros.

Riesgo tecnológico como raíz de otros riesgos

El riesgo tecnológico puede ser causa y consecuencia de otro tipo de riesgos, una falla sobre la infraestructura puede implicar riesgos en otros ámbitos, como pérdidas financieras, multas, acciones legales, afectación sobre la imagen de la organización, causar problemas operativos o afectar las estrategias de la organización. Si pensamos en el caso de un empleado descontento que puede representar un riesgo operativo, podría implicar también un riesgo tecnológico por manipulación inapropiada de sistemas e información.

A continuación, se presentan algunos ejemplos que ilustran lo anterior:

- El reciente descubrimiento en mayo de 2012 del malware Flame, el cual tenía como objetivo ataques de ciberespionaje en países de oriente medio. Este ataque representó pérdida de información confidencial y crítica. [1]
- Otro caso de ciberespionaje industrial es el malware encontrado en archivos de AutoCad, cuya finalidad es el robo de información sensible como planos arquitectónicos. [2]
- Un ataque muy nombrado en marzo del año pasado es el relacionado al robo de información realizado a RSA, que implicó riesgos para la banca en línea. [3]
- Por último, el ataque que sufrió Sony en 2011, donde robaron información de cuentas de usuarios. [4]

Todo lo anterior, confirma la posibilidad de daños y perjuicios que puede desencadenar un fallo en la seguridad a nivel tecnológico.

Con estas aproximaciones damos por terminada la primera parte de este artículo, en una próxima entrega hablaremos sobre la importancia de las buenas prácticas y el marco de referencia COBIT en algunas de sus versiones.

Referencias

[1] Meet 'Flame,' The Massive Spy Malware Infiltrating Iranian Computers, Revista Wired, Mayo de 2012. Disponible: http://www.wired.com/threatlevel/2012/05/flame/

[2] Malware en archivos AutoCad podría ser inicio de ciberespionaje industrial, Subdirección de Seguridad de la Información - Información y servicios de seguridad en cómputo.Disponible: http://www.seguridad.unam.mx/noticia/?noti=420

[3] En riesgo más de 40 millones de usuarios de banca electrónica, blog de tecnología ALT1040, Marzo 2011. Disponible en: http://alt1040.com/2011/03/en-riesgo-mas-de-40-millones-de-usuarios-de-banca-electronica

[4] Sony admite un robo adicional de datos que afecta a casi dos centenares de usuarios en España, Diario El mundo España, Mayo 2011. Disponible en: http://www.elmundo.es/elmundo/2011/05/03/navegante/1304383366.html

Sin la gerencia no hay paraiso

Jeffrey Steve Borbón Sanabria

En muchas ocasiones, grandes ideas y proyectos en torno a la seguridad de la información quedan lejos de ser una realidad en las organizaciones debido a que no se involucra a la dirección en estas iniciativas, más allá de solicitudes de recursos económicos u otros requerimientos afines. El presente artículo presenta algunas situaciones reales de cómo NO se debe ofrecer la seguridad de la información a la dirección; y qué buscar en estas áreas administrativas al trabajar dentro de una organización.

En organizaciones donde la razón de ser del negocio no es la tecnología, no se cuenta con normas referentes a la seguridad de la información o simplemente no existe una obligación frente a este importante aspecto, aquellos quienes han tenido la experiencia de ofrecer planes, proyectos o iniciativas sobre seguridad de la información son conscientes de cuán complicado puede ser el vender esta idea a la alta dirección. Vale la pena indicar que a diferencia de lo que ocurre con las áreas de tecnología, en la seguridad de la información no existe formalmente un retorno de inversión, es por ello que es visto por la dirección o aquellas áreas que toman las decisiones de invertir, más como un gasto que como una oportunidad.

Con base en lo anterior, se requiere de experiencia, claridad en las explicaciones y propuestas; e incluso de llegar a contar con aliados estratégicos dentro de las organizaciones, para presentar estas iniciativas a la dirección y contar con su apoyo y compromiso. Aquí realizo una distinción: usualmente encontramos que se habla de apoyo en virtud de soporte, impulso a las ideas e iniciativas. Por otro lado, acuño el término compromiso con base en qué tanto se involucran, aportan y gestionan los recursos e insumos necesarios para la realización de los proyectos planteados. Esto último resulta una tarea compleja, pero no imposible y su consecución puede llegar a ser la causa de éxito del proyecto o iniciativa a desarrollar.

Fallos, fallos y más fallos

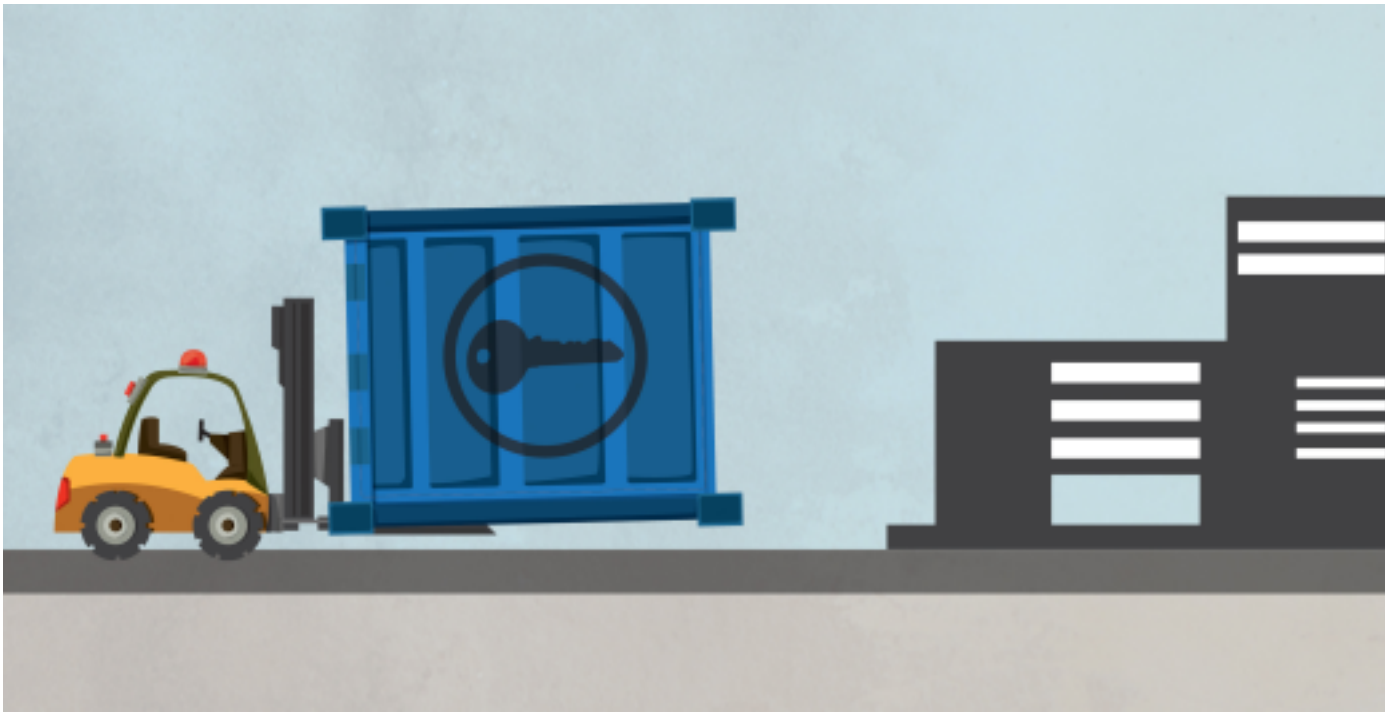
A continuación, se abordan algunos errores que se comenten regularmente al ofrecer los proyectos o iniciativas de seguridad de la información a la dirección:

* Ausencia de claridad en la propuesta:
Si las soluciones, proyectos o ideas a presentar no son concretas o lo suficientemente claras para quienes toman decisiones, difícilmente serán tomados en cuenta. Recurrir a la simplicidad y explicar con ejemplos puede ser una excelente estrategia.

* Lenguaje extremadamente técnico
Uno de los talones de Aquiles de quienes trabajamos con tecnología es explicar temas haciendo uso en exceso de un lenguaje especializado plagado de expresiones complejas o tecnicismos de difícil comprensión para aquellas personas que no se involucran directamente en las tareas. Esto puede significar perder la atención de la audiencia y echar abajo las posibilidades de contar con el interés y respaldo de la dirección.

* No siempre funciona el terrorismo
Partiendo de la premisa de que la seguridad de la información suele ser vista como un gasto más que una inversión, es común acudir a técnicas de sugestión y terror empleando situaciones adversas de otras organizaciones para inspirar miedo y generar una sensación de inseguridad en la audiencia. Es importante comprender que ninguna organización funciona con la misma lógica, por lo que no siempre es posible hablar en términos de pérdidas económicas o multas, también deben abordarse otro tipo de impactos tales como la reputación e imagen, el impacto legal y otros aspectos, todo esto sin llegar a ejemplos extremos o terrorismo.

* Propuestas no alineadas con el negocio
Es común que en una organización surjan ideas que pueden resultar descabelladas, pero que realmente aportan a favor del negocio, esto ocurre porque directa o indirectamente se encuentran enfocadas al logro de objetivos y cumplimiento de la misión. Sin embargo, el mayor fracaso de una idea desde que es concebida, radica en que pueda encontrarse en contravía con lo que desea la organización, ya que no aportará valor y puede generar una inversión innecesaria reduciendo el capital de inversión para otros proyectos.



* Costos de soluciones imposibles
La teoría de gestión de riesgos establece que, en caso de que el mecanismo a través del cual se controla o reduce el impacto de un riesgo cuente con un valor más elevado que el mismo activo, no es viable aplicar dicho control. Lo anterior puede aplicarse para otras situaciones tales como solicitar inversión para tecnologías o

soluciones a nivel de seguridad de la información que son más costosas que la misma infraestructura, o cuya utilidad como control o protección es mínimo con respecto al costo. Es necesario buscar soluciones viables organizacionalmente, económicamente y que aporten al negocio.

* No ofrecer utopías: la seguridad total no existe

Es una realidad que no existe la seguridad total, nada puede llegar a un 100% de seguridad. Ofrecer esta idea o fundamentar una solución o proyecto en esta mentira puede ser negativo para la imagen del área o personal de seguridad, en caso de que acontezca un incidente que evidencie que la protección total no existe. Siempre existirá un riesgo residual, un porcentaje de amenaza con el que la organización debe convivir, no se puede ignorar la presencia del mismo.

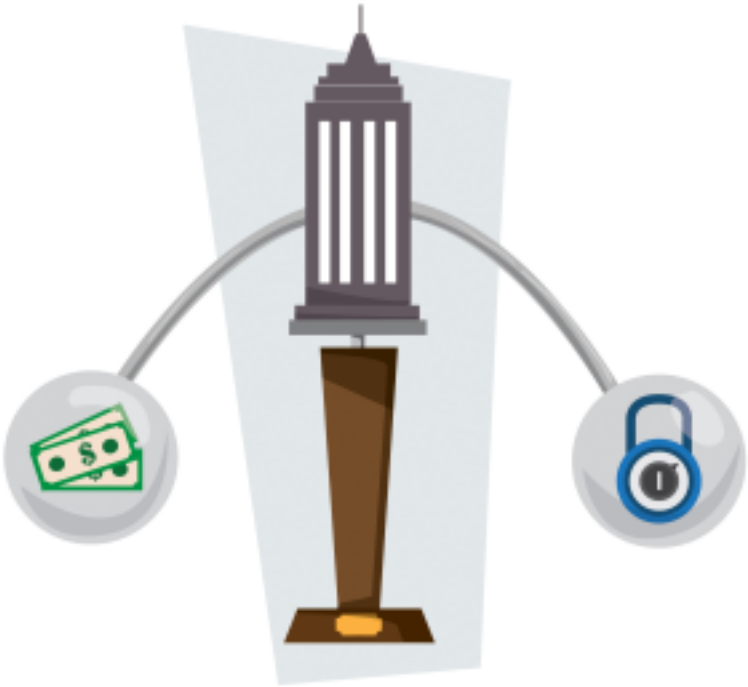
* Presentaciones interminables

La capacidad para presentar una idea en el tiempo adecuado, recurriendo a la síntesis y simplicidad, es una de las mayores cualidades que se deben potenciar al trabajar con temas de seguridad. Es muy probable que no exista tiempo para atender estos temas y cuando lo hay es demasiado corto, así que hay que fortalecer la capacidad de presentar rápidamente los problemas y las soluciones para lograr contar con la atención de aquellos que toman decisiones dentro de la organización. No hay que morir ante el desagradable: “Tiene 5 minutos para su presentación”.

¿Qué buscar en la gerencia?

Una vez analizados los casos que plantean posibles fracasos, es importante recalcar que no es fácil dejar de lado esos fallos que tantas veces han hecho ir en lastre nuestros proyectos. Sin embargo, es necesario e imperativo conseguir el apoyo y compromiso de la dirección durante todos los proyectos y actividades, pues es la dirección la que puede solicitar el cumplimiento de las políticas o la colaboración en los mismos, así como es la que aportará los recursos humanos, económicos, logísticos, entre otros, que se requieren para hacer realidad proyectos de seguridad de la información, y también es quien puede aplicar los correctivos y sanciones cuando la seguridad de la información no es tomada con la debida seriedad en la organización.

Como se puede evidenciar, hay mucho por mejorar y realizar para llegar a ese público tan complicado como lo es la dirección, gerencia, administración o al área equivalente en donde se toman las decisiones en una organización.



Otras recomendaciones

Así como existe el ROI (retorno de inversión) como una medida para identificar la ganancia obtenida en virtud del capital invertido y es una de las maneras de cómo las áreas de tecnología suelen sustentar sus requerimientos y compras, la seguridad de la información cuenta con una métrica similar denominada ROSI (retorno de la inversión en seguridad), con el cual es posible referenciar las pérdidas que podría tener la organización contra los costos de los controles (tecnológicos, de recursos humanos, etc). Al igual que el ROI, el éxito del ROSI radica en justificar y demostrar que la inversión a realizar no es mayor al valor del activo y de la pérdida, ya que no tiene sentido aplicar controles más costosos que el activo a proteger.

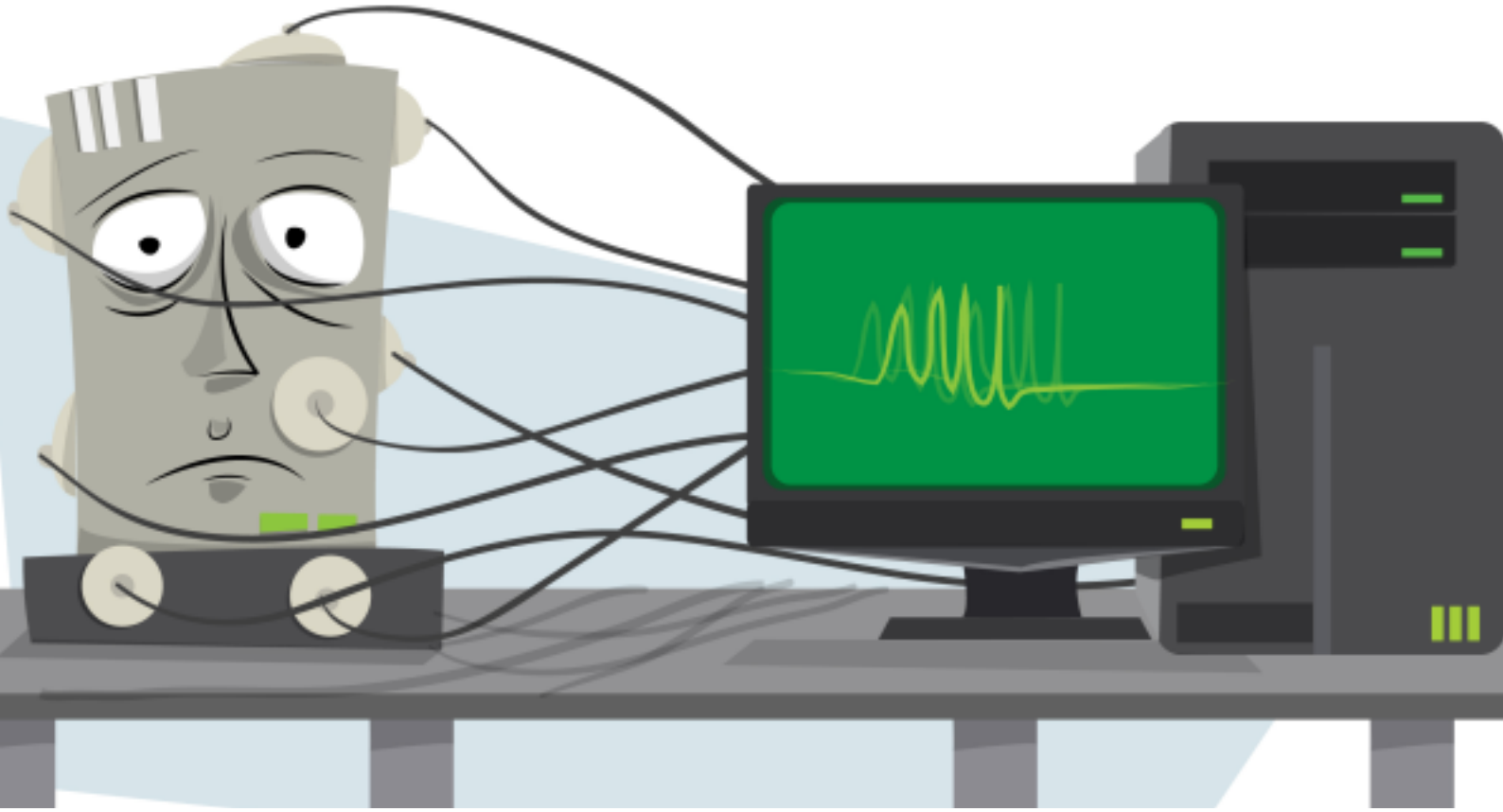
Para más información acerca del ROI, se recomienda leer un artículo realizado por el consultor Dejan Kosutic

Referencias

[1] http://blog.iso27001standard.com/2011/06/13/is-it-possible-to-calculate-the-return-on-security-investment-rosi/

[2] http://www.iso27001standard.com/en/rosi/return-on-security-investment

[3] http://services.nsw.gov.au/sites/default/files/backup_migrate/manual/ROSI%20Calculator%201.2.xls



La importancia de las pruebas de penetración - Parte II

Ing. Erika Gladys De León Guerrero

El presente artículo está constituido por dos partes, la primera ha sido publicada en la edición número12 (http://revista.seguridad.unam.mx/sites/revista.seguridad.unam.mx/files/revistas/pdf/Para%20PDF_12.pdf), el objetivo es brindar al lector un panorama general sobre el concepto y las ventajas de realizar pruebas de penetración, introducirse en cada etapa de realización de auto-evaluaciones y comprender la importancia de la revisión periódica de seguridad.

En esta parte del artículo se analizará el concepto junto con algunas técnicas de escaneo de vulnerabilidades, de explotación y reporte.

Para hablar de las etapas, es necesario tener una concepción clara de lo que son las pruebas de penetración. Son una evaluación de seguridad ejecutada exactamente como lo haría un atacante real, es decir, se descubren vulnerabilidades y se lanzan exploits intentando obtener acceso no autorizado, modificación de paquetes, negación de servicio, etc., llegando hasta el punto más crítico; el objetivo es dar a conocer a la institución o dueño del activo, las consecuencias que podría tener en caso de no contar con las medidas necesarias de seguridad, agregando elementos para la toma de decisiones en la estrategia de seguridad.

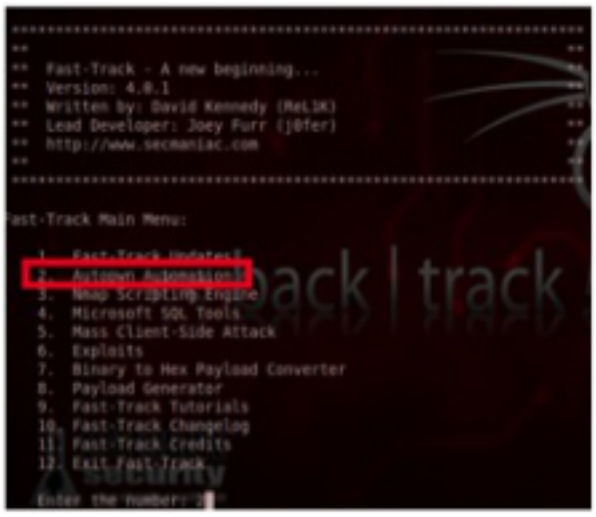


Figura 1. Menú Fast-Track

Figura 2. Opción Autopwn Automation

El escaneo de vulnerabilidades permite identificar debilidades en el sistema evaluado, toma como base los detalles obtenidos durante las fases previas, el objetivo es identificar el método de ataque más efectivo y prever el tipo de información que se obtendrá cuando se explote la vulnerabilidad encontrada. Se debe tomar el mismo enfoque que tomaría un atacante real, ver a la organización como un adversario potencial e intentar causarle el mayor daño posible.

Existen distintos métodos para descubrir vulnerabilidades, así como también existen distintas herramientas automatizadas que pueden ayudar en esta fase. Se mencionan a continuación algunas técnicas que pueden ser utilizadas para descubrir vulnerabilidades:

1. Verificar la versión de software: Es una de las técnicas más comunes, basta con identificar el número de versión y compararlo con las listas de versiones vulnerables públicas gratuitamente en distintos sitios de seguridad. En este punto, se deben verificar también los parches y upgrades aplicados que podrían eliminar la vulnerabilidad. Aquí podrían ser utilizadas las herramientas libres nmap y amap.

2.Verificar la versión del protocolo de comunicación: Probablemente la versión de software no contenga vulnerabilidades, pero podría usar algún protocolo de red con problemas de seguridad.

3. Verificar la configuración: Es necesario analizar los diferentes accesos que se podrían dar, remotos, locales y con distinto tipo de privilegios, no basta solo con analizar si se tiene configuración por default, es necesario revisar si las configuraciones aplicadas por el administrador bastan para evitar problemas de seguridad.

4.Ejecución de exploits: Se pueden ejecutar exploits sin conocer las vulnerabilidades presentes, tomando como base el prestigio del exploit y la información obtenida durante las fases previas. Esta técnica puede ser peligrosa ya que podría causar daños al sistema, incluyendo negación de servicio. Sin embargo, es posible representar una técnica muy cercana a lo que pasaría en caso de ser sometidos a ataques reales. Para la ejecución de esta técnica existen herramientas como fast-track.py con la opción de autopwn Automated, es una herramienta escrita en python que forma parte de Metasploit y permite lanzar automáticamente gran cantidad de exploits con tan solo indicar la dirección IP (ver Figura 1 y 2)

Por otro lado, existen herramientas automáticas

que permiten la identificación de vulnerabilidades, entre las más comunes se pueden mencionar las siguientes:

1.Nessus: es una herramienta con opción comercial y gratuita, tiene como ventajas la creación de distintos perfiles de escaneo (políticas) dependiendo del tipo de evaluación que se requiera y del sitio desde el cual se ejecuten las pruebas. Proporciona un formato gráfico de interacción (ver Figura 3).

Nessus genera reportes categorizando las vulnerabilidades encontradas de acuerdo al impacto y asocia un identificador para cada una de ellas que facilita la búsqueda de información relacionada con la explotación (ver Figura 4).

Se puede obtener una breve descripción de la vulnerabilidad, una posible solución, referencias

Figura 3. Nessus

y una calificación dada por la calculadora CVSS disponible en http://www.patchadvisor.com/PatchAdvisor/CVSSCalculator.aspx,
la cual asigna un valor al impacto tomando en cuenta distintos parámetros
(ver Figura 5).

Plugin ID	Count	Severity	Name
51192	5	Medium	SSL Certificate Cannot Be Trusted
57582	2	Medium	SSL Self-Signed Certificate
57608	1	Medium	SMB Signing Disabled
53491	1	Low	SSL / TLS Renegotiation DoS
14272	32	Info	netstat portscanner (SSH)
22964	19	Info	Service Detection
10736	8	Info	DCE Services Enumeration
10107	7	Info	HTTP Server Type and Version
10863	5	Info	SSL Certificate Information
45410	5	Info	SSL Certificate commonName Mismatch
56984	5	Info	SSL / TLS Versions Supported
20301	2	Info	VMware ESX/GSX Server detection

Figura 4. Reporte

2.OpenVas: Es otra opción de software libre que posee flexibilidad en la aplicación de distintos perfiles de evaluación, es una herramienta cliente-servidor, a pesar de no ser tan “amigable” como Nessus, es una buena opción para verificar las vulnerabilidades arrojadas por otras herramientas (ver figura 6).

Figura 5. Detalles de vulnerabilidad

La variedad de herramientas para detección de vulnerabilidades es muy amplia, algunas con licencia comercial como Core Impact, Saint, Retina o Qualys.

Una vez identificado el método de ataque de mayor viabilidad, es necesario considerar cómo se tendrá acceso al objetivo, es decir, llega la fase

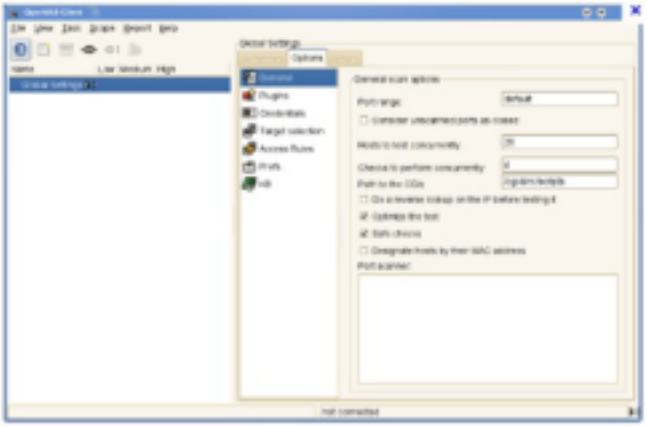


Figura 6. OpenVas

de explotación. Es la parte más interesante de la ejecución de pruebas de penetración y la que lo hace diferente a un escaneo de vulnerabilidades, muchas veces llamado incorrectamente “análisis de vulnerabilidades”, donde solo se llega hasta la etapa anterior, solo se localizan las vulnerabilidades sin comprobar si pueden ser explotadas.

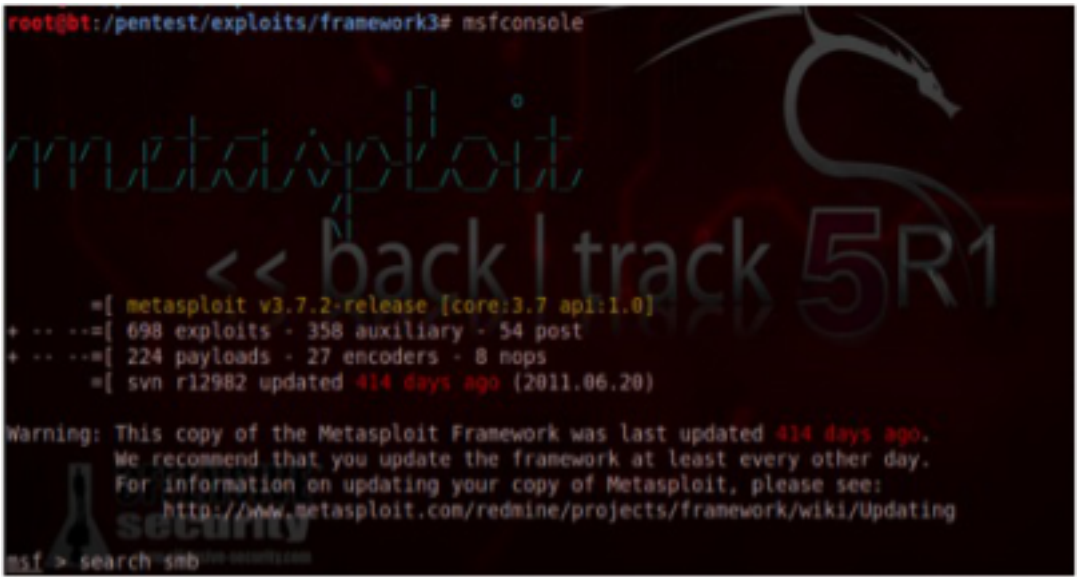


Figura 7. Búsqueda de smb

Esta etapa dependerá totalmente de los resultados obtenidos en las etapas anteriores, por lo que cada prueba será diferente de acuerdo a los servicios existentes y las vulnerabilidades presentes. En esta etapa se pueden realizar distintas acciones como resultado de la explotación, por mencionar algunas:

- Copiar archivos hacia el objetivo
- Copiar archivos desde el objetivo

pueden ser encontrados exploits independientes y existen frameworks completos de ataque, uno de los más útiles e importantes es Metasploit, el cual contiene cientos de exploits aplicables a distintos sistemas operativos, a distintos servicios y a distintas versiones, contiene tres tipos de interfaces que facilitan la ejecución.

Se mostrará un ejemplo de uso de Metasploit como primer punto, es necesario buscar el exploit

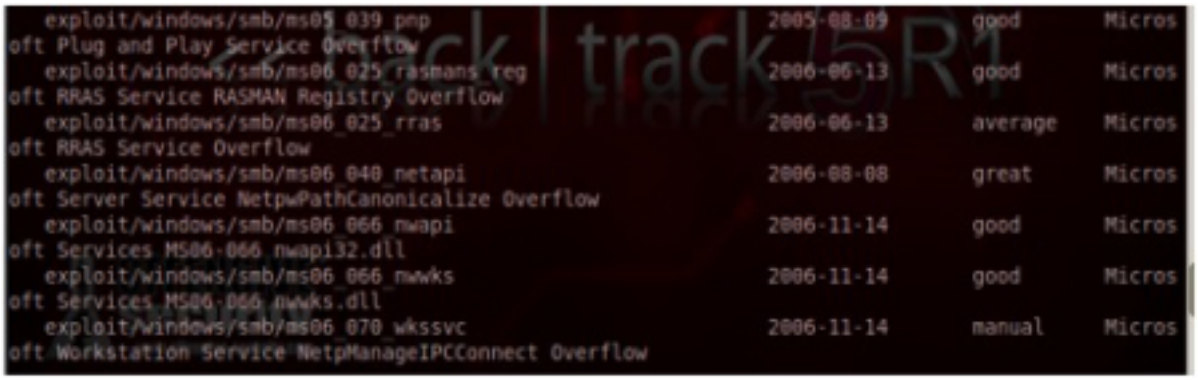


Figura 8. Resultados de búsqueda

- Visualizar tráfico confidencial
- Reconfigurar el objetivo
- Instalar software
- Tomar control total
- Causar negación de servicio
- Usar un objetivo para llegar a otro
- Obtener contraseñas

Existe una vasta cantidad de herramientas para explotar vulnerabilidades, hay sitios donde

que se quiere ejecutar, o bien el servicio que está presente en el sistema, en este caso se realizará la búsqueda de smb (ver Figura 7).

Los resultados arrojan los exploits relacionados con smb (ver figura 8)

Se selecciona el siguiente exploit:
auxiliary/dos/Windows/smb/ms09_050_smb2_negotiate_pidhigh
elcualafectaalossiguientessistemasoperativos:
• Windows Vista
• Windows 7
• Windows Server 2008 R2

Se selecciona el objetivo con la siguiente instrucción:
set RHOST 192.168.1.71

```
msf > use auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh
msf auxiliary(ms09_050_smb2_negotiate_pidhigh) >
```

Se selecciona el objetivo con la siguiente instrucción:
set RHOST 192.168.1.71

```
msf auxiliary(ms09_050_smb2_negotiate_pidhigh) > set RHOST 192.168.1.71
RHOST => 192.168.1.71
msf auxiliary(ms09_050_smb2_negotiate_pidhigh) >
```

Se selecciona el puerto:
set RPORT 445

```
msf auxiliary(ms09_050_smb2_negotiate_pidhigh) > set RPORT 445
RPORT => 445
```

Para comprobar las opciones seleccionadas se ejecuta: show options

```
msf auxiliary(ms09_050_smb2_negotiate_pidhigh) > show options

Module options (auxiliary/dos/windows/smb/ms09_050_smb2_negotiate_pidhigh):

   Name    Current Setting  Required  Description
   ----    ---------------  --------  -----------
   OFFSET  65535            yes       The function table offset to call
   RHOST   192.168.1.71     yes       The target address
   RPORT   445              yes       The target port
```

Y finalmente, se ejecuta:

```
msf auxiliary(ms09_050_smb2_negotiate_pidhigh) > run

[*] Sending request and waiting for a reply...
```

En el otro lado, en el objetivo, se puede observar una falla en el sistema. El ejemplo mostrado anteriormente solo es una pequeña parte de lo que un pentester realiza al comprobar vulnerabilidades, existen otras herramientas para explotación, algunas comerciales y algunas libres, es necesario hacer una combinación entre las distintas herramientas. Por otro lado, en algunos casos no existe el exploit para comprobar determinadas vulnerabilidades, por lo que es necesario generarlo, para lo cual también existen distintas herramientas y frameworks, incluyendo nuevamente Metasploit.

La etapa final y la más importante, es la creación del reporte de hallazgos, ya que es en esta fase donde se comunica qué se hizo, cómo se hizo y cómo la organización puede eliminar las vulnerabilidades detectadas durante el análisis, por lo que es de gran importancia generar reportes con la mayor calidad posible.

El formato de un reporte puede ser muy variable, pero a continuación se muestran algunos puntos que deben ser presentados:

- Tabla de contenido
- Resumen ejecutivo
- Metodología utilizada
- Hallazgos ordenados de acuerdo al impacto
- Evidencia detallada incluyendo screenshots del hallazgo

Es recomendable presentar la evidencia de manera jerárquica, ya que tomando como hecho que todas las vulnerabilidades deben ser eliminadas, existen algunas que pueden representar mayor impacto a la organización, por lo que es prioritaria la solución inmediata.

Es posible creer que el reporte no es importante cuando se realiza un pentest interno, pero es necesario tener una bitácora que almacene el historial del los problemas de seguridad que se han tenido, esto podría ayudar a resolver problemas en el futuro.

Para concluir, es necesario decir que la tarea de un pentester no es fácil, pero es determinante para una buena estrategia de seguridad, por lo que es recomendable realizar evaluaciones internas y periódicamente (1 o 2 veces por año) solicitar servicios profesionales.

Referencias

[1] Mati Aharoni. Et Al. Metasploit. The Penetration tester's Guide. EUA. No starch press. 2011.

[2] SANS. Security 560. Network Penetration Testing and Ethical Hacking. 2009.

[3] Allen Harper. Et Al. Grey Hat Hacking. The Ethical Hacker's Handbook. EUA. Mc. Graw Hill. 2011.

México, el voto electrónico y el 2012

Gunnar Eyal Wolf Iszaevich

Un reclamo muchas veces escuchado es que, dado que es imposible confiar en los individuos, corruptibles por naturaleza, la responsabilidad del escrutinio de los votos debería recaer en un sistema computarizado, siempre limpio, eficiente y honesto. De eso hablaremos a continuación.

¿Qué hace una urna electrónica?

Las urnas electrónicas se han propuesto desde hace mucho tiempo y muchos países (o jurisdicciones menores) las han adoptado.
En el corazón de todas las propuestas de voto electrónico está la urna electrónica. Esta es básicamente una computadora con una interfaz de usuario limitada para solo permitir un conjunto específico de operaciones, construida dentro de una caja o maletín que dificulte el acceso a cualquiera de sus componentes, fuera de aquel expresamente autorizado y encargado de recibir cada uno de los votos, convirtiéndolos en información almacenada electrónicamente. Por medio de un procedimiento previamente diseñado, las autoridades electorales pueden indicarle que deje de recibir votos y que entregue los totales que cada una de las opciones
que capturó.

Las primeras urnas electrónicas que cumplen con esta definición, las llamadas DRE voting machines (Direct-Recording Electronic, máquinas de voto electrónico de grabación directa) fueron puestas en práctica ampliamente hacia 1996. Al día de hoy, votan de esta manera la totalidad del electorado de países tan grandes como la India y Brasil, así como amplios segmentos de otras naciones como los Estados Unidos.

La confianza y los aguafiestas

Si una cosa caracteriza al gremio de los desarrolladores de software es la cantidad de errores (tanto accidentales como inducidos, lo que es mucho más peligroso) que pueden aparecer en

un programa, no lo perdamos de vista. El mero hecho de que exista un área de especialización tan importante como la seguridad informática lo hace patente: La complejidad hasta de los sistemas más sencillos hace imposible asegurar con toda certeza que una computadora haga lo que debe hacer.

Para ilustrar: Son pocas las computadoras en el mundo que no utilizan una solución antivirus en la actualidad. Estos programas se hicieron necesarios dadas las grandes deficiencias de diseño que tuvo el sistema operativo más popular del planeta ante la realidad de estar permanentemente conectados a una red hostil. No importa si nuestro sistema es el más seguro, es necesario estar al tanto de todas las actualizaciones y notas de seguridad si queremos confiar en que nuestra computadora responde únicamente a nuestras órdenes y que lo hace de forma confiable.

Incluso ante el mismo programador, como proféticamente lo demostró en 1984 Ken Thompson al aceptar el premio Turing (reconocido en nuestro campo como el premio Nobel de la Ciencia de la Computación) con el artículo Reflexiones acerca de la confianza en la confianza ; un programador siempre confía ciegamente en un conjunto de programas sobre los cuales construye (compilador, ligador, sistema operativo) y por tanto, un atacante determinado sólo tiene que bajar lo suficiente para plantar un troyano.

Desconfiando del DRE… y de lo demás

Expertos en seguridad informática no tardaron en señalar diversas fallas elementales en el voto DRE; la principal, la confiabilidad. Si los votos únicamente son grabados en la memoria electrónica ¿Cómo puede asegurarse que reflejen fielmente el sentido del voto de cada individuo? O puesto de otro modo, ¿cómo podría asegurarse un recuento de los votos en caso de ser necesario?

La respuesta no se hizo esperar: A cada voto emitido, sería impreso un comprobante o testigo del voto, mismo que serviría para contar los votos manualmente en caso de impugnación. Este

esquema es conocido como VVPAT (Voter-verified paper audit trail, rastro auditable en papel verificado por el votante).

Si bien ha sido aceptado por numerosos sistemas electorales en el mundo, sigue sin ser suficiente. Como sugiere Federico Heinz , hay varios esquemas que podrían reventar una elección con este planteamiento. Por ejemplo, si las personas interesadas en sabotear una urna, tras votar, reclaman ante la mesa de autoridades indicando que la urna registró un voto contrario a lo que se le solicitó, podrían llevar a la anulación de todos los sufragios emitidos por dicha urna, dado que son potencialmente ilegítimos.
Por otro lado, podría presentarse nuevamente el escenario que se dio en la ciudad de Nueva York en 2010 : Al calentarse las urnas electrónicas, se emitían votos aleatorios por error. Se estima que esto pudo haber invalidado hasta el 30% de los votos efectivos de algunas mesas.

La futilidad de los simulacros

Este 2012, el principal proyecto de implementación de voto electrónico en México será en las elecciones locales del estado de Jalisco. Uno de los muchos puntos preocupantes de este ejercicio es que, como pruebas previas a la instalación de más de mil urnas electrónicas en dos distritos electorales y un municipio, las únicas pruebas de confiabilidad disponibles para ser analizadas públicamente son cinco simulacros.

¿Qué puede comprobarse en un simulacro? Que en el mejor de los mundos posibles y sin ninguna intencionalidad maligna, las urnas funcionen como dicen funcionar. En caso de haber algún componente malicioso en las urnas, es del total interés de quien lo haya sembrado que no cause ningún comportamiento inusual (para no perder su agente encubierto sin obtener la ventaja que le llevó a introducirlo). Un simulacro busca demostrar que, bajo condiciones controladas, la elección no colapsa. Lo peor del caso es que en este sentido, 3 de los 4 simulacros que habían ocurrido hasta la fecha en que este documento fue escrito, registraron fallos diversos que hacían (a menos de dos meses del proceso electoral) replantearse si se emplearían o no . En el Distrito Federal, la implementación de urnas electrónicas licitadas a la misma empresa que las provee en Jalisco fue rescindida, en parte, por haberse encontrado 28 fallas .

¿Un simulacro exitoso aseguraría que no habrá fallas el día de la elección? ¡De ninguna manera!

Por restricciones de espacio, en este texto apenas me ha sido posible arañar algunos de los puntos más notorios del voto electrónico y de por qué, comprendiendo puntos básicos de seguridad en cómputo y estando conscientes de la gran importancia que tiene el voto dentro de un sistema democrático representativo, como el que aspiramos tener en nuestro país, resulta imposible confiar en que las urnas electrónicas resuelvan nuestros problemas de confianza, muy por el contrario.

Se ha hablado de emplear al voto electrónico para resolver otros problemas, como el del costo o la agilidad de la transmisión de resultados. Estos puntos pueden desmenuzarse y descartarse con todavía mayor facilidad que el aquí presentado.

Si este breve artículo resultó de su interés, les invito a leer el artículo publicado a fines de 2011, así como el abundante material que al respecto ha generado la Fundación Vía Libre (Argentina), destacando el libro Voto electrónico: los riesgos de una ilusión, publicado en 2009 .

Referencias

1 Reflections on Trusting Trust, Ken Thompson, Communications of the ACM, Vol. 27, No. 8, August 1984, pp. 761-763

2 Urnas electrónicas: con imprimir el voto no alcanza, Federico Heinz, Fundación Vía Libre, septiembre de 2010; http://www.vialibre.org.ar/2010/09/12/urnas-electronicas-con-imprimir-el-voto-no-alcanza/

3 Machine Casts Phantom Votes in the Bronx, Invalidating

Real Ones: Report, The Empire, mayo de 2012; http://www.wnyc.org/blogs/empire/2012/may/09/reports-find-machine-errors-led-uncounted-votes-2010/

4 Pide diputada que IEPC esté listo a llevar a cabo elección tradicional, Zaira Ramírez, El Informador, 8 de mayo de 2012; http://www.informador.com.mx/primera/2012/374801/6/pide-diputada-que-iepc-este-listo-a-llevar-a-cabo-eleccion-tradicional.htm

5 Urnas electrónicas tienen 28 fallas: IEDF, Jonathan Villanueva, El Universal, 13 de abril del 2012; http://www.eluniversal.com.mx/ciudad/111073.html

6 Voto electrónico: ¿Quién tiene realmente la decisión?, Construcción Colaborativa del Conocimiento (IIEc-UNAM), Gunnar Wolf, 2011; http://seminario.edusol.info/seco3/pdf/seco3_apend3.pdf

7 Fundación Vía Libre — Voto electrónico http://www.votoelectronico.org.ar/

8 Voto electrónico: los riesgos de una ilusión, Fundación Via Libre, 2009; http://www.vialibre.org.ar/wp-content/uploads/2009/03/evoto.pdf

UNAM

DGTIC

DIRECCIÓN GENERAL DE CÓMPUTO Y DE
TECNOLOGÍAS DE INFORMACIÓN Y COMUNICACIÓN

UNAM
CERT

Revista .Seguridad Cultura de prevención para TI
No.14 / Julio-Agosto 2012 ISSN: 1251478, 1251477