UNIVERSIDAD DE PALERMO

FACULTAD DE CIENCIA Y TECNOLOGIA

AUDITORIA Y SEGURIDAD EN SISTEMAS

CONTROLES PARA LA AUDITORIA Y LA SEGURIDAD EN EL E-COMMERCE

Alumnos: *Colatruglio, Guillermo*
Fournier, Agustina
Knoblauch, Christian

Profesor: *Ing. Patricio E. Rey*

Indice **Página**

Qué es E-Commerce?

Hay distintas acepciones para este termino, pero en general cuando se habla de e-commerce se hace referencia a las transacciones comerciales en las cuales el pedido efectivo de un producto o servicio se efectúa por medios electrónicos.

Modalidades de E-Commerce

B2B Business to Business	Sitios de transacciones comerciales entre empresas.
B2C Business to Consumer	Sitios de venta al consumidor final.
C2C Consumer to Consumer	Remates y sitios de intercambios de bienes o servicios entre personas.
C2B Consumer to Business	Sitios en los que las personas de agrupan para realizar negocios con las empresas.

Business to Business (B2B)

La modalidad B2B se refiere a las transacciones entre empresas. Muchas de las etapas del comercio entre empresas se simplifican con las posibilidades en Internet, como por ejemplo la toma de pedidos.

Business to Consumer (B2C)

Esta modalidad de e-commerce es sin lugar a dudas la mas promocionada. Apunta, precisamente, a los consumidores finales, y es a través de los medio masivos de comunicación como se llega a ellos.

Consumer to Consumer (C2C)

Son ejemplos de ellos los sitios de remates, en donde la oferta de productos y la compra de los mismos es realizada por personas y no por empresas.

Consumer to Business (C2B)

Los usuarios se ponen de acuerdo para realizar una compra en grupo a una empresa, obteniendo mejores condiciones de compra.

Amenazas al e-commerce

Como todo fenómeno social, el e-commerce no está exento de posibles repercusiones negativas. Una de ellas es que sus beneficios se conviertan en una fuente de marginación social.

El e-commerce tiene el futuro casi asegurado. Una amenaza significativa para su futuro desarrollo viene de la falta de seguridad para las transacciones. Para comerciar en Internet en forma segura deben solucionarse primero algunos problemas, una solución es la encriptación de la información enviada a través de la red utilizando códigos de identificación personalizada.

Por ahora la sustitución del trato personal y directo, característica esencial del comercio tradicional, por uno distante e impersonal, como el que supone el e-commerce, plantea a empresas y consumidores múltiples interrogantes respecto a la seguridad de las formas de pago, la validez de los contratos y las atribuciones de las distintas instancias, nacionales e internacionales, para solucionar posibles disputas mercantiles. También es común la resistencia de los usuarios a proporcionar información personal, como dirección, número telefónico e ingresos,

ante el temor de que un manejo inapropiado de ésta información implique su privacidad.

En gran medida los riesgos y temores asociados con el uso del e-commerce son consecuencia directa del desafío que plantea, para las prácticas y la lógica habituales de empresarios, consumidores y gobiernos, la irrupción de un nuevo modelo de negocios.

No se debe perder de vista que el mundo de lo técnicamente posible es mucho más amplio que el de lo socialmente aceptable.

Ventajas del e-commerce

Las ventajas competitivas del e-commerce sobre el comercio tradicional han generado un gran impacto que ya ha comenzado a sentirse en algunos sectores de la economía:

- ✓ Costos reducidos en comparación con otros medios;
- ✓ Actualización inmediata de la información sobre los productos y servicios de la empresa (promoción, ofertas, etc);
- ✓ Acceso a un mercado de millones de clientes potenciales;
- ✓ Aumento de competitividad;
- ✓ Reducción de costos, como por ejemplo personal de ventas, mailings, teléfono, etc.;
- ✓ Presencia 24 horas al día, 7 días a la semana, 12 meses al año;

- ✓ Obtención de datos de los clientes, lo que permite personalizar la oferta.

Estado actual del comercio electrónico por Internet

Actualmente, muchas de las empresas que venden productos por Internet le comunican al comprador, antes de comenzar a llenar la orden de compra, que el procedimiento que se va a realizar cuenta con un mecanismo de seguridad, que por lo general es de encriptación.

También, desde hace unos meses, las páginas Web de algunas empresas muestran su aval de certificación.

La certificación de los usuarios es un proceso que está menos avanzado, pero seguramente terminará imponiéndose como requisito para efectuar determinadas operaciones en Internet.

La alternativa al uso del número de las tarjetas de crédito en las transacciones comerciales por Internet es el dinero electrónico, pero pasará un tiempo hasta su implementación definitiva y global.

Definición de seguridad

Se define como la protección contra riesgos, o las medidas que se pueden tomar contra el espionaje, el sabotaje, o el delito. En el caso de comercio electrónico, la seguridad es un aspecto muy importante, ya que el consumidor debe sentir

confianza al momento de realizar una transacción electrónica de que sus datos no serán utilizados para otros fines que los que él específicamente dio su consentimiento.

Para lograr dicha confianza en el cliente, son importantes los siguientes aspectos:

- ✓ **Disponibilidad**: es la característica que asegura que los recursos del sistema y la información estarán disponibles a los usuarios autorizados siempre que éstos los necesiten.
- ✓ **Integridad**: Involucra la protección de los datos almacenados o en tránsito contra toda modificación.
- ✓ **Autenticación**: es la capacidad de un individuo o entidad de probar su identidad electrónicamente.
- ✓ **Autorización**: implica el control de acceso a determinada información para usuarios autenticados.
- ✓ **Confidencialidad**: es la característica que asegura que las personas no tienen acceso a los datos a no ser que estén autorizadas para conocerlos.
- ✓ **No repudio del envío del mensaje**: el emisor de un mensaje no puede negar haberlo enviado.

Garantizar la seguridad en el comercio electrónico es un pre-requisito fundamental antes de que cualquier actividad comercial sensible a la información pueda llevarse a cabo. A pesar de que a lo largo de varios años, se ha avanzado bastante, aún quedan muchos desafíos que enfrentar en esta área, y combinado con los negocios

y los requisitos legales para el comercio electrónico, la seguridad sigue siendo un asunto importante dentro de lo que es el e-commerce.

Se puede definir a la seguridad como las medidas tomadas contra sabotajes o espionajes, ataques, delitos, etc. Garantizar la seguridad involucra diferentes métodos y políticas, y en un ambiente comercial, incluye más que la seguridad en las transacciones financieras sino también concierne a la información privada de la corporación la cual debe ser resguardada debidamente.

Potenciales amenazas y ataques a los cuales las son susceptibles actividades comerciales a través de redes:

- ✓ Acceso no autorizado a recursos de red
- ✓ Destrucción de información y de recursos de red
- ✓ Alteración, inserción o modificación de información
- ✓ Conocimiento de información por personas no autorizadas
- ✓ Interrupciones o disrupciones en los servicios de red.
- ✓ Robo de información y/o recursos de red
- ✓ Negación de servicios recibidos y/o de información enviada o recibida
- ✓ Alegación/afirmación de haber enviado o recibido información no suministrada.

FUNCIONES Y REQUERIMIENTOS

Hay varios requerimientos para la creación de un ambiente seguro en e-commerce. Estos son la base de la seguridad en el e-commerce y todos se relacionan entre sí. Ellos se pueden dividir en:

Autenticación

Es la habilidad de un individuo, organización o computadora, de probar su identidad. Las partes involucradas deben saber que están haciendo los negocios con quien ellos creen. Los sistemas de seguridad logran la autenticación verificando información que el usuario provee contra la que el sistema ya conoce del usuario en cuestión. Los métodos de autenticación pueden estar basados en los siguientes factores:

Demostración del conocimiento de algún tipo de información como por ejemplo una password.

Posesión de alguna clase de objeto, como una key o una card.

Demostración de alguna característica biométrica, como las impresiones digitales.

Evidenciar que ya un tercero que es confiable ha validado la identidad.

Estos factores se suelen consideran en combinación. Algunos de los métodos más comunes son, como se dijo antes, las passwords, los números de identificación personal (PINs), firmas digitales y certificados.

Autorización

Implica el control de acceso a una determinada información, una vez que ya se ha validado la identidad del usuario. Se trata de limitar las acciones que puedan tener los diferentes usuarios autenticados, basados en varios niveles de identidad. La autorización abarca mecanismos de control de acceso, que son entidades de red, recursos de red y derechos de acceso.

Los derechos de acceso describen los privilegios o permisos de la entidad y bajo qué condiciones esa entidad puede acceder a un recurso de red, y de qué forma están habilitados a acceder.

Estos privilegios los puede controlar un usuario o administrador empleando una lista de control de accesos (access control list – ACL) en la cual se detallan recurso por recurso, los permisos de cada usuario autenticado.

En el otro extremo, la autorización también se relaciona con las publicaciones y la protección de los derechos intelectuales.

Confidencialidad

La confidencialidad atañe a la reserva o confidencia de los datos o información, y a la protección de accesos no autorizados a dicha información. En E-Commerce, la confidencialidad es de suma importancia para resguardar la información financiera de la compañía, información de desarrollo de productos, estructuras de organización, etc. Una lista de precios, o un informe confidencial puede precisarse

que sea altamente confidencial durante un cierto período de tiempo, y luego de ese tiempo libremente disponible. Para adecuar las distintas necesidades, deben incluirse políticas relativas a la circulación de información, las cuales determinarán, no sólo si un objeto puede o no librarse sino también qué recargos se le darán, etc. Encriptación.

La confidencialidad debe asegurar que la información no puede ser leía, copiada, modificada o divulgada sin la propia autorización y que las comunicaciones a través de redes no serán interceptadas. Para satisfacer estos requisitos se diseñan técnicas de encriptación basadas en criptografía.

Integridad

Abarca la protección de los datos en tránsito o almacenados contra toda modificación (altas, bajas, modificaciones o reordenamientos de los datos). Los sistemas de comercio electrónico deberán tener la capacidad de garantizar que los datos que se transmiten por una red son recibidos en su destino en las mismas condiciones en que fueron enviados.

No repudio del origen

Trata de la protección contra una parte que en una transacción o comunicación luego intenta negar (falsamente) que la transacción ocurrió. Los servicios de no repudio del origen deben poder demostrar a una tercera parte, la prueba del origen, entrega, cesión y transporte de la información en cuestión. La necesidad de este tipo de servicios refleja las imperfecciones de los ambientes de comunicaciones, ya sea por red o no.

AUDITORIA DE LA SEGURIDAD Y CONTROL DEL NEGOCIO

La administración de la seguridad implica el control de la confiabilidad en las transacciones digitales como en la fijación y cumplimiento de normas de seguridad para garantizar que los requisitos de los servicios de seguridad pueden lograr sus objetivos. No se trata de un aspecto adicional al comercio electrónico sino más bien que es uno de los aspectos más fundamentales para su correcto funcionamiento. Los consumidores, entendiblemente, evitan aquellos sitios en los cuales saben o intuyen que la información que provean no será manipulada confidencialmente, así como escaparán de compañías que no adopten medidas de seguridad para proteger su propia base de datos. Para destacar esta necesidad de controles de negocio en sistemas de comercio electrónico seguro, los resultados que mostraron las encuestas realizadas por Ernst & Young LLP, el FBI y el Computer Security Institute (CSI), un 46 por ciento de los sitios corporativos de Internet ya habían quebrado.

Las políticas de seguridad son generalmente un conjunto de reglar que definen el alcance y tipo de medidas de seguridad que se usarán en su estrategia de e-commerce. Por ejemplo, la norma de seguridad puede listar las posibles amenazas de las que deberían protegerse, los recursos de red que deberían protegerse y los métodos y niveles de protección que se pondrían en práctica. Una política de seguridad debería definir los límites de comportamiento aceptable del sistema, determinar las acciones que se deberían llevar a cabo cuando ocurriera algún tipo

de violación a la seguridad, y también, especificar los protocolos y permisos a usarse en ese sistema de seguridad.

El plan de acción de seguridad puede clasificarse según distintos componentes: (1) políticas de responsabilidad, (2) políticas de control de acceso, (3) políticas de confidencialidad y (4) políticas de integridad de los datos. La primera debe determinar dos procedimientos principales, que son, el determinar qué entidades deben autenticar su identidad y establecer un path de procedimiento confiable. Esto conlleva el determinar qué paths de comunicación se deberían usar entre dos entidades autenticadas en el sistema, así como los tipos o acciones permitidas en los mismos. Las políticas de control de acceso deberán decidir qué entidades dentro del sistema deben ser controladas así como los privilegios de las mismas. Las normas de confidencialidad de los datos establecerán los tipos y alcances de los procedimientos de protección de divulgación de la información, así como los mecanismos de encriptación punta a punta que se utilizarán. Finalmente, las reglas de integridad se refieren al tipo y alcance de los mecanismos de protección de los datos contra modificaciones.

Todos estos mecanismos deben ser controlados por medio de auditorías y análisis de riesgos. Una auditoria de seguridad en e-commerce incluye registrar y reportar todos los eventos que ocurran por red que tengan relevancia para la seguridad. Este proceso se lleva a cabo por etapas. La recopilación y organización de información de auditorías, la cual puede estar en varios formatos por haber sido

recogidas de servidores diferentes. Determinar la importancia y uso de los datos; clasificación y filtrado de información. Luego según el caso determinar si se necesitan procedimientos de recuperación por violaciones de la seguridad.

Las auditorias de la seguridad en e-commerce son un componente esencial de los controles del negocio en sí mismo. Un ejemplo conocido: un empleado de banco puede maliciosamente ir deduciendo de las cuentas de los clientes fracciones de centavos, lo cual por ser tan aparentemente insignificante podría pasar desapercibido por los contadores. Los controles de auditoria son métodos muy efectivos para casos como éste.

Dependiendo de la situación y aplicación, los controles pueden ser llevados a través de los campos legales, técnicos, contractuales, etc, conforme a guías bien establecidas, procedimientos, normas, prácticas y estándars.

Aspectos de seguridad

La seguridad en el e-commerce se debe dar en tres aspectos:

- ✓ seguridad del lado del cliente
- ✓ seguridad en los mensajes
- ✓ seguridad en comunicaciones
- ✓ seguridad en los servidores

La seguridad del lado del cliente es un concepto general que es aplicable a cualquier uso de Internet y excede el espectro de el presente trabajo. Para el comercio electrónico nos enfocaremos en las transacciones y el servidor.

Seguridad en los mensajes

Internet es, en su forma más rudimentaria, una infraestructura de comunicación entre computadoras. La seguridad en la Red de Redes es algo difícil de implementar a bajo nivel, ya que el tránsito de la información a través de distintas redes hace imposible asegurar un camino confiable e inviolable por parte de terceros para la comunicación entre dos equipos. Por ello, dicha comunicación debe ser protegida en otros niveles, procurando compensar la inseguridad del canal de transmisión con seguridad en el mensaje mismo transmitido.

Las maneras de proveer al mensaje transmitido con la confiabilidad, integridad y autenticación necesarias son varias:

encriptación de mensajes

firma digital y certificados digitales

Encriptación de mensajes. La encriptación de mensajes se refiere a la codificación o firma digital de un mensaje mediante el uso de una clave. Mediante la encriptación se cumple el requisito de confidencialidad de la información.

Existen dos formas de encriptación:

codificación del mensaje: ocurre cuando se toma un mensaje, se le aplica una fórmula matemática basándose en una clave y se transmite el mensaje codificado resultante.

firma del mensaje: por ello se refiere a la generación de un número por medio de una fórmula matemática utilizando una clave, utilizando el contenido del mensaje como referencia. Dicho número se incluirá como parte de la firma digital del mensaje, y será calculado nuevamente por el receptor del mensaje; si resulta ser diferente del que figura en la firma del mismo, entonces el mensaje habrá sido modificado en el trayecto entre los equipos.

Las claves a utilizar para codificar y decodificar mensajes pueden ser:

iguales: tanto el emisor como el receptor utilizan la misma clave. Esto implica que la clave sólo es conocida por ellos (es “privada”) y plantea la necesidad de hacerla conocida de manera segura por ambas partes; además, no permite identificar quién es el emisor de un mensaje, ya que la misma clave es utilizada para encriptar y desencriptar en ambos extremos de la comunicación.

distintas: el emisor de un mensaje lo encripta utilizando una clave “pública”, no secreta, perteneciente al receptor, quien es el único que lo puede descifrar con una clave “privada” conocida solamente por él; de esa manera se asegura que

solamente el receptor deseado pueda desencriptarlo. La clave privada y la pública son independientes, no se puede deducir una de la otra.

El nivel de protección que ofrecen las claves es proporcional a su longitud, la cual se mide en bits; a medida que mejora la tecnología y la velocidad de procesamiento, la longitud de las claves aumenta, ya que se hace más sencillo obtener la clave por el método de "fuerza bruta", es decir, prueba y error.

Firma digital y Certificados digitales. Los certificados digitales sirven para verificar la identidad del emisor de un mensaje y para comprobar que éste no haya sido modificado desde que fue enviado. De esta manera se logra asegurar la autenticación e integridad de la información transmitida, además de impedir el repudio de origen de la misma.

El certificado digital se usa para "firmar" mensajes. Para ello el emisor utiliza una función matemática sobre el contenido del mensaje para obtener un número hash único, que luego es utilizado, junto con su clave privada, para generar la firma digital. Luego, el mensaje es transmitido junto con la firma. Cuando el receptor lo recibe, calcula el número hash y toma esa firma y la clave pública del emisor y las utiliza para obtener el número hash nuevamente. Si ambos números hash son distintos, el mensaje habrá sido modificado desde que fue enviado, y se rompió su integridad.

Cualquier persona puede crear un certificado digital para sí. Además, una persona malintencionada podrían generar y utilizar un certificado diciendo ser otra persona.

Para evitar eso existen las denominadas “Autoridades de Certificación”, las cuales se supone que son confiables. Dichas autoridades, empresas privadas, pueden certificar otras firmas digitales por una tarifa. Los certificados que están avalados por una autoridad certificante “heredan” su nivel de confianza.

Seguridad en las comunicaciones

Firewalls. Aunque es imposible controlar el transporte de un mensaje en Internet, sí se puede impedir que usuarios hostiles se puedan conectar a la red de una empresa que ofrece servicios de e-commerce y copiar, modificar o eliminar información importante y confidencial.

La manera más común de impedir el acceso a una red es mediante el uso de un “firewall”. Éste es un equipo cuya función es filtrar los posibles accesos desde Internet a la red de la empresa, permitiendo sólo ciertas conexiones o la utilización de ciertos servicios únicamente.

Protocolos seguros

La información transmitida a través de Internet puede ser codificada mediante protocolos seguros que aprovechen algunas de las técnicas de encriptación descritas anteriormente.

Para realizar conexiones seguras a equipos remotos se puede utilizar algunos de los siguientes protocolos:

SSL (Secure Sockets Layer): es un protocolo que utiliza claves públicas y privadas para la autenticación, encriptación de mensajes e integridad de los mismos. Para cada una de estas funciones se usan pares de claves distintas, lo que le da seguridad adicional; sin embargo, esto también ocasiona que las comunicaciones se vuelvan más lentas por el tiempo adicional que requiere codificar y decodificar los mensajes.

SHTTP (Secure Hypertext Transfer Protocol): este protocolo es una derivación del HTTP, un protocolo utilizado para navegar por Internet, que tiene características de seguridad adicionales.

SOCKS5: es un protocolo que reside en la capa de sesión del modelo OSI. Todas las conexiones hechas con este protocolo pasan por un servidor central SOCKS5 de la empresa. Soporta claves públicas y privadas.

Los mensajes de correo también pueden ser codificados utilizando alguno de estos protocolos:

PGP (Pretty Good Privacy): Utiliza claves públicas y privadas para encriptar la información. A diferencia de las otras implementaciones, las claves PGP no tienen

fecha de vencimiento, por lo que, si se descubre la clave de una persona, se podrá utilizar la misma por tiempo indefinido.

S/MIME (Secure Multipurpose Internet Mail Extensions): Este protocolo es una extensión del MIME, y al igual que PGP utiliza claves públicas y privadas.

Seguridad en los servidores

Los servidores, es decir, los equipos que proveen los servicios de e-commerce, deben ser protegidos contra ataques externos e internos y contra caídas en el sistema. Los sistemas críticos que hay que proteger son:

- ✓ los servidores de Internet
- ✓ las aplicaciones propiamente dichas
- ✓ las bases de datos

Cada uno de estos puntos daría para escribir un libro entero, por lo que nos dedicaremos a destacarlos puntos más importantes a tener en cuenta:

Es muy importante impedir el acceso no autorizado a recursos internos. Esto se logra mediante firewalls (ver más arriba), permisos de usuario y especialmente, la correcta configuración de los servicios.

Constantemente se están descubriendo nuevas fallas de seguridad en servidores web, aplicaciones y motores de bases de datos; es conveniente tener siempre al día el software que se utilice, instalando todos los parches necesarios.

En el caso de las aplicaciones desarrolladas internamente por la empresa, se debe tener mucho cuidado de realizar las verificaciones necesarias para impedir la

presencia de errores en los programas que provoquen brechas de seguridad o fallas en los servicios.

Percepción por parte del usuario y confianza

Un negocio debe implementar políticas de seguridad para proteger contra riesgos sus iniciativas. Existen mecanismos robustos que soportan los requerimientos de seguridad, pero todavía hay un desafío que falta cubrir para el comercio electrónico. El elemento faltante es la confianza. En el mundo de los negocios más allá del comercio electrónico, los niveles de confianza están implícitos en actividades y transacciones de forma tan obvia que no son siquiera tomados en cuenta, y los mecanismos utilizados se presentan de forma casi transparente; éstos no lo están necesariamente en el comercio electrónico, siendo muy importantes la percepción del usuario y su confianza para el futuro del e-commerce.

Crear y mantener esta confianza implica más que definir requerimientos de seguridad y verificar que todos los componentes de la parte técnica cumplan con los requerimientos. En un ambiente digital, definir los elementos que caractericen la confianza puede ser muy complejo.

La confianza en un ambiente digital está muy relacionada con requisitos de autorización; la falta de confianza puede tener como consecuencia la denegación de la autorización recesaria. Sin embargo, establecer la confianza puede ser más complicado aún, ya que una percepción individual de confianza sobre un problema en particular puede depender de cómo la situación se desenvuelva. Para un ambiente de comercio electrónico, es imperativo crear un sistema que otorgue los servicios de autorización basados en un análisis de decisión en el momento. La

confianza en un sistema solamente puede ser determinada adecuadamente analizando al sistema como un todo en lugar de hacerlo en partes individuales. Ford y Baum recomiendan una lista de medidas de seguridad que un sistema debe implementar para maximizar la confianza, las cuales son:

- ✓ Comparar el software sin costo o de bajo costo con los riesgos que su uso involucra. Utilizar productos de empresas confiables que implementen los controles de calidad apropiados puede reducir los riesgos.
- ✓ Prestar especial atención a la protección en ambientes que contengan software crítico. La captura de información es de suma importancia para un análisis posterior de problemas de seguridad y para las auditorías de los sistemas.
- ✓ El software es generalmente más susceptible a ser poco confiable que el hardware, ya que es más fácil de modificar y más propenso a las fallas. Por ésta razón, se debería utilizar componentes de hardware para funciones críticas.

La confianza en los sistemas de comercio electrónico está estrechamente relacionada con la la privacidad. Los negocios que definen sus políticas de seguridad y las publican en sus sitios web se ven recompensados con un mayor nivel de confianza por parte de los usuarios, que saben qué información se está obteniendo de ellos y qué uso se le está dando.

Bibliografía

- ✓ Electronic Commerce – Technical, Business and Legal Issues (N. R. Adam, O. Dogramaci, A. Gangopadhyay, Y. Yesha – Ed. Prentice Hall, 1999)
- ✓ E-Commerce Security – Weak links, best defenses (A. Ghosh – E. Wiley Computer Publishing, 1998)
- ✓ http://www.minproduccion.gov.ar/comercioe/
- ✓ http://alarcos.inf-cr.uclm.es/doc/Auditoria/auditoria.htm
- ✓ http://www.delitosinformaticos.com
- ✓ http://www.cace.org.ar (Cámara Argentina de Comercio Electrónico)