CARM
NEGOCIO ELECTRÓNICO
REGIÓN DE MURCIA

SEGURIDAD EN EL COMERCIO ELECTRÓNICO

SEGURIDAD EN EL COMERCIO ELECTRÓNICO

Febrero 2010

Proyecto CECARM

Región de Murcia

www.cecarm.com

cecarm@cecarm.com

Índice

1. Presentación

La guía **Seguridad en el comercio electrónico** permitirá orientar al empresario sobre los elementos necesarios para mantener la seguridad en sus transacciones de comercio electrónico.

2. Introducción

La principal barrera que se encuentran las empresas que desean realizar comercio electrónico reside en una pregunta: **¿cómo puedo solventar los problemas de seguridad?** Asimismo, éste es el mayor inconveniente que se plantean los clientes a la hora de comprar a través de Internet.

En el comercio electrónico **la seguridad** no es un elemento opcional más, sino un **elemento clave e imprescindible** para la puesta en marcha de cualquier proyecto de compra o venta por Internet.

Además, la seguridad es el factor más importante en el comercio electrónico, ya que, según demuestran numerosos estudios, la preocupación por la seguridad es la principal barrera a la hora de realizar una compra online.

La seguridad no solo afecta a la tranquilidad de los consumidores, sino especialmente a la **imagen y credibilidad** de la empresa que decide ofrecer sus productos o servicios por Internet.

Para tratar la seguridad en el comercio electrónico plantearemos diferentes aspectos a considerar:

- Seguridad en las transacciones y medios de pago
- Relaciones seguras en el intercambio de información
- Seguridad en las redes internas de la empresa

3. Requisitos para mantener la seguridad

Mantener la seguridad es un aspecto fundamental para cualquier empresa que trabaje con las nuevas tecnologías, ya sea en Internet o no. Cuando hablamos de seguridad en el comercio electrónico destacamos **cuatro aspectos** básicos:

- **Autentificación.** Consiste en verificar la identidad de los agentes participantes en una comunicación o intercambio de información. Las formas más comunes de autentificarse son las basadas en claves, las basadas en direcciones y la criptografía. Esta última es la más segura, ya que, en las otras dos, existe la posibilidad de que alguien intercepte la información y pueda suplantar la identidad del emisor.
- **Confidencialidad.** Este aspecto de la seguridad permite mantener en secreto la información y que sólo los usuarios autorizados puedan manipularla. Para mantener la confidencialidad se utilizan técnicas de encriptación o codificación de datos.
- **Integridad.** Esta capacidad de la seguridad evita que la información emitida sea modificada por una persona ajena a la transmisión. Se consigue mediante el uso de firmas digitales.
- **No repudio.** Este aspecto consiste en comprobar que los participantes en la transmisión de información realmente han participado en ella. Con esto conseguimos, a ambos lados de la comunicación, que quien ha mandado el mensaje no pueda renegar de él.

4. Tipos de fraudes más frecuentes en el comercio electrónico

Según la Comisión Federal de Comercio de Estados Unidos, los fraudes más frecuentes en el comercio electrónico son:

- **Subastas.** Algunos mercados virtuales ofrecen una amplia selección de productos a precios muy bajos. Una vez que el consumidor ha enviado el dinero puede ocurrir que reciban algo con menor valor de lo que creían, o peor todavía, que no reciban nada.
- **Acceso a servicios de Internet.** El consumidor recibe una oferta de servicios gratuitos. La aceptación lleva implícita el compromiso de contrato a largo plazo con altas penalizaciones en caso de cancelación.
- **Tarjetas de crédito.** En algunos sitios de Internet, especialmente para adultos, se pide el número de la tarjeta de crédito con la excusa de comprobar que el usuario es mayor de 18 años. El verdadero objetivo es cobrar cargos no solicitados.
- **Servicios gratuitos.** Se ofrece una página personalizada y gratuita durante un período de 30 días. Los consumidores descubren que se les ha cargado facturas a pesar de no haber pedido una prórroga en el servicio.
- **Ventas piramidales.** Consiste en ofrecer a los usuarios falsas promesas de ganar dinero de manera fácil sólo por vender determinados productos a nuevos compradores que estos deben buscar.
- **Viajes y vacaciones.** Determinadas páginas de Internet ofrecen destinos maravillosos de vacaciones a precios de ganga, que a menudo encubren una realidad completamente diferente o inexistente.
- **Oportunidades de negocio.** En la Red abundan las ofertas para ganar fortunas invirtiendo en una aparente oportunidad de negocio que acaba convirtiéndose en una estafa.
- **Inversiones.** Las promesas de inversiones que rápidamente se convierten en grandes beneficios no suelen cumplirse y comportan grandes riesgos para los usuarios. Como norma general, no es

recomendable fiarse de las páginas que garantizan inversiones con seguridad del 100%.

- **Productos y servicios milagro.** Algunas páginas de Internet ofrecen productos y servicios que aseguran curar todo tipo de dolencias. Hay quienes ponen todas sus esperanzas en estas ofertas que normalmente están lejos de ofrecer garantías de curación.

5. Seguridad en las transacciones y los medios de pago. Servidores seguros

Por **servidor seguro** entendemos un servidor de páginas web que establece una **conexión cifrada** con el cliente que ha solicitado la conexión, de manera que nadie, salvo el servidor y el cliente, puedan tener acceso a la información transmitida de forma útil.

El **funcionamiento** de un servidor seguro es el siguiente: un cliente accede a un sitio web a través de la dirección y, una vez establecida la conexión, solicita una conexión segura. Entonces, si se trata de un servidor seguro, éste responderá a la solicitud enviándole un certificado electrónico, en el cual vendrá integrada una clave de la autoridad de certificación. Después, el cliente generará una clave encriptada y se la enviará al servidor. A partir de aquí, ambos podrán establecer una comunicación segura basada en las claves que sólo ellos conocen.

El uso de servidores seguros es un elemento imprescindible en todos aquellos servicios que utilicen **información confidencial**, como **operaciones bancarias** en línea, compras por Internet, acceso a servidores de datos sensibles, etc.

Los clientes sabrán que se encuentra en un servidor seguro porqué la dirección de la página web comenzará por "**https**", en vez por "**http**". Además, en la parte inferior derecha de la ventana del navegador aparecerá un **candado cerrado**.

6. Seguridad en las transacciones y los medios de pago. Transacciones EDI

El Intercambio Electrónico de Datos (EDI) es el **intercambio de datos** en un formato normalizado entre los sistemas informáticos de quienes participan en transacciones comerciales.

Las transacciones EDI ofrecen una alta **integridad** y **seguridad**, y ofrecen la posibilidad de escalar hasta grandes procesos por lotes.

En EDI, las interacciones entre las partes tienen lugar por medio de aplicaciones informáticas que actúan a modo de interfaz con los datos locales y pueden intercambiar información comercial estructurada. **EDI establece cómo se estructuran**, para su posterior transmisión, los datos de los documentos electrónicos y define el significado comercial de cada elemento de datos. Para transmitir la información necesita un servicio de transporte adicional (por ejemplo, un sistema de tratamiento de mensajes o de transferencia de ficheros).

Los principales **campos de aplicación** del EDI son el intercambio de información **industrial, comercial, financiera, médica, administrativa** o cualquier otro tipo similar de información estructurada. Esta información, con independencia de su tipo concreto, se estructura en unos formatos que pueden ser procesados por las aplicaciones informáticas. Ejemplos de datos EDI son las facturas, órdenes de compra, declaraciones de aduanas, etc.

Además, EDI **respeta la autonomía de las partes involucradas**, no impone restricción alguna en el procesamiento interno de la información intercambiada ni en los mecanismos de transmisión.

Sin embargo, la tecnología clásica del EDI, basada en centros de compensación y estaciones de usuario, supone para las empresas pequeñas con muy poco volumen de documentos susceptibles de intercambiar por EDI, una barrera económica y tecnológica notable.

Para salvar esta barrera, la Asociación Española de Codificación Comercial (AECOC) desarrolló **EDIWEB**, un sistema que permite a las **pequeñas y medianas empresas** no usuarias de sistemas EDI, las relaciones comerciales telemáticas con empresas que sí tienen el EDI integrado.

El sistema EDIWEB permite a las PYMES usuarias recibir en formato HTML los mensajes en EDI nativo (mensajes pedido y texto libre), así como rellenar un formulario cuyos campos se traducen a mensajes en formato EDI nativo (mensajes factura, viso de expedición, catálogo de producto, relación de facturas y texto libre).

7. Seguridad en las transacciones y los medios de pago. Protocolos de seguridad

Para asegurar las transacciones en línea, fundamentalmente se utilizan dos protocolos de seguridad: SSL y SET.

El **SSL (Secure Sockets Layer)** es un protocolo de intercambio de información que permite asegurar la autentificación, confidencialidad e integridad de los datos que se transmiten a través de Internet. Consiste en encriptar los datos con un sistema de cifrado cuando está ubicado en una zona segura de un navegador.

Las características de SSL son:

- Protege el envío de datos de compra
- Autentifica al comercio, no al cliente
- Fácil de implementar y de bajo coste
- El comercio recibe los datos de pago

El **SET (Secure Electronic Transaction)** es un conjunto de especificaciones de seguridad desarrollado por Visa y MasterCard, junto con empresas líderes en tecnología, que asegura la confidencialidad e integridad de la información transmitida. Además, ni el emisor ni el receptor pueden negar su participación en la transacción. Este protocolo necesita la instalación de un software específico tanto por el vendedor como por el comprador.

Las características de SET son:

- Su principal objetivo es la transferencia segura de números de tarjetas de crédito.
- Realiza una autenticación de todas las partes participantes en la transacción usando certificados digitales.
- Permite la conexión a través de cualquier tipo de red.

8. Seguridad en las transacciones y los medios de pago. Certificados de seguridad

Los certificados de seguridad son sellos emitidos por empresas denominadas **entidades certificadoras** de seguridad. Estas entidades conceden su certificado después de comprobar el correcto funcionamiento del proceso de encriptación y los datos de la empresa solicitante. Los sellos de certificaciones de seguridad más significativos son:

- Verisign
- Thawte
- Entrust
- Bureau Veritas

9. Autentificación. Firma digital

La **firma digital** se define como una secuencia de datos electrónicos que se obtienen como consecuencia de aplicar a un mensaje determinado un **algoritmo de cifrado asimétrico**.

Estos sistemas de **criptografía asimétrica** están basados en el cifrado de la información a partir de un par de **claves** diferentes, denominadas **pública** y **privada**, que se atribuyen a una persona determinada. El proceso se fundamenta en que la clave privada sólo es conocida por la persona a la que se han atribuido el par de claves. En cambio, la clave pública puede ser conocida por cualquier persona que el emisor desee.

10. Autentificación. Certificado digital.

El **certificado digital** es un **archivo electrónico** que contiene los **datos de identificación personal** del emisor, su **clave pública** y la **firma privada** del propio prestador de la certificación. Por lo tanto, a través del certificado digital, podemos conocer la identidad de la persona poseedora del par de claves, es decir, del emisor de la información. Además, incluye, sólo para el titular del certificado, su clave privada.

Los certificados digitales son emitidos por entidades denominadas **Autoridades de Certificación**, que funcionan como agentes ajenos a la transacción garantizando la validez de las partes.

11. Autentificación. Seguridad en el intercambio de información. Virus

Aunque existen muchas definiciones, un **virus** es sencillamente un programa con capacidad de reproducirse por sí mismo, cuyo objetivo es propagarse.

Una de las principales formas de **propagación de los virus** consiste en la utilización del **correo electrónico**, generalmente en forma de archivos anexos al mensaje de correo. El virus infecta un archivo, y cuando éste es enviado por correo y el destinatario lo abre, el virus se empieza a extender por su equipo.

Una modalidad más inteligente de este tipo de contagio es cuando el virus es capaz de **acceder a la libreta de direcciones del programa de correo,** ya que entonces, la mayor parte de las veces sin necesidad de intervención del usuario, el virus empieza a enviar e-mails a las direcciones presentes en la libreta, enviando a la vez el archivo infectado, con lo que el proceso de contaminación continúa.

Para evitar que un virus infecte nuestro ordenador, es necesario utilizar un **antivirus**. Los antivirus son programas que analizan los archivos, localizando los virus y eliminándolos. Sin embargo, aparecen virus nuevos todos los días, por lo que resulta imprescindible actualizar permanentemente nuestro antivirus.

12. Autentificación. Seguridad en redes.

Para mantener la seguridad en las redes, es decir, impedir el acceso no autorizado, existen los denominados **cortafuegos** o **firewalls**.

Un cortafuegos es un sistema diseñado para **impedir el acceso no autorizado** a una red interna o desde una red interna. Lo que hace un cortafuegos es **controlar la información que circula por las redes**, de manera que cada paquete de datos vaya donde tenga que ir, desde la red Internet a nuestra red privada y viceversa, al mismo tiempo que contiene la política de seguridad especificada por el administrador del sistema.

La política de seguridad de un cortafuegos es una parte esencial de su efectividad y permiten definir la manera en que cada organización ve la seguridad de la red interna.

El administrador del sistema puede, a través del cortafuegos:

- Definir qué usuarios tienen la palabra clave de acceso autorizada
- Definir a qué aplicaciones y datos tiene acceso cada usuario
- Llevar un registro de los accesos realizados por cada usuario autorizado
- Evitar que la intrusión pueda cambiar la configuración de la aplicación residente
- Controlar los accesos entre la red privada y el servidor como punto de entrada
- Llevar un registro de todas las incidencias que se produzcan

13. Consejos para aumentar y transmitir seguridad

1) Ofrecer información clara y concisa sobre los productos y sus condiciones.
2) Usar un servidor seguro para alojar las páginas del comercio.
3) Añadir políticas de seguridad al servidor del comercio para aumentar la confianza de los clientes en las compras.
4) Cuidar la privacidad de los datos del cliente. Solicitar sólo los datos necesarios.
5) Aportar a los clientes información sobre la política de privacidad de la empresa.
6) Ofrecer varias alternativas de pago.

Región de Murcia

fundación integra
integración de recursos y nuevas tecnologías para la modernización de la Región de Murcia

Región de Murcia
Crecemos con Europa

UNIÓN EUROPEA
Fondo Europeo de Desarrollo Regional