LA PROTECCIÓN DE DATOS EN TERMINALES Y ORDENADORES DE USO PÚBLICO

Autores:

Jaime Lloret Mauri
Javier Martínez Nohalés
Fernando Boronat Seguí

Dpto. de Comunicaciones Universidad Politécnica de Valencia

Resumen indicativo

En este trabajo se realiza un análisis, búsqueda de soluciones y posterior uso de éstas para implantar una política de seguridad que garantice la protección de datos de los usuarios de terminales u ordenadores de uso público con conexión a Internet. Como ejemplo de éstos, existen los terminales de automatrícula de las universidades, los cybercafés, aulas de acceso a Internet de bibliotecas, aulas de libre acceso en universidades, puntos de acceso a Internet en aeropuertos, etc., algunos de estos ejemplos son muy utilizados actualmente en Europa.

Para realizar esta investigación, se ha estudiado las Directivas vigentes del Parlamento Europeo y del Consejo 95/46/CE y 2002/58/CE y la Ley Orgánica de 10/1995 y 15/1999 del Código Penal Español.

Este tipo de entornos carecen de una legislación explícita que abarque todas las características de éstos y que asegure una privacidad de los ciudadanos que los utilizan. Para su desarrollo se han analizado los inconvenientes que tienen algunos medios telemáticos en lo referente a la intimidad de un usuario y a los datos que por dichos medios circula.

Seguidamente, se ha realizado un estudio de las deficiencias en la configuración inicial que tienen algunos de los sistemas operativos instalados en este tipo de terminales u ordenadores, atendiendo al requisito de ser utilizados por múltiples usuarios. Asimismo, también se han estudiado las configuraciones realizadas por los administradores de red en este tipo de entornos con tal de elaborar una serie de propuestas y recomendaciones, de protección de la privacidad de los datos, a las empresas u organismos que dispongan de dichos terminales u ordenadores de uso público para no vulnerar dicha privacidad, sin el consentimiento del propietario.

Ante el estudio realizado se examina la incidencia de las Directivas 95/46/CE y 2002/58/CE del Parlamento Europeo y del Consejo en las inseguridades observadas.

Posteriormente, se exponen varias políticas de seguridad implantadas en algunas empresas u organismos que poseen dispositivos de estas características con tal de ofrecer diferentes soluciones adoptadas todas ellas independientes del hardware, el sistema operativo y las aplicaciones utilizadas.

Finalmente, se elaboran una serie de conclusiones que nos indican la necesidad de directivas y leyes que regulen la protección de datos personales en estos entornos.

Abstract

In this work it is carried out an analysis, search of solutions and later use to introduce a security policy to guarantee users data protection in public terminals or computers with Internet connection. As an example of these there are, terminals placed in universities, cybercafes, Internet access in libraries, free access classrooms in universities, etc., some of them are very extended in Europe.

To carry out this investigation, the directives 95/46/CE and 2002/58/EC of European Parliament and of the Council and the Organic Laws 10/1995 and 15/1999 of the Spanish Penal Code have been studied.

This kind of environments does not have an explicit legislation with its all characteristics that assures the users privacy. For this development the inconveniences in a transmission medium has been analysed due to the unprotected users data circulation in the local network medium.

Subsequently, a study of the deficiencies in the initial configuration in some terminals or computers operating systems, according to the request of being used by multiple users has been carried out.

Likewise, the administrator configurations in this kind of environments have also been studied in order to develop some proposals and recommendations, in data privacy and protection. These proposals and recommendations should be adopted in organisms or companies with public terminals or computers to avoid harming this privacy, without the proprietor's consent.

It is examined the directives 95/46/CE and 2002/58/CE of the European Parliament and of the Council, taking care of its repercussion in these kind of insecurities.

Later, several implanted security policies are exposed to offer different adopted solutions. All of these solutions should be accomplished in every system independently of the hardware, the operating system or the used applications.

Finally, it is elaborated some conclusions to indicate the necessity of a directive and laws to regulate the personal data protection in these environments.

Palabras clave

Protección de datos, privacidad, intimidad, acceso público

1.- Introducción

En 1990, la Comisión Europea, consciente de la necesidad de una directiva sobre la protección de datos, debido al movimiento de datos que se produciría en un mercado único, propuso un borrador de directiva donde una de las seis propuestas existentes era la protección de datos. Después de un largo proceso de negociación, se adoptó la Directiva 95/46/CE del Parlamento Europeo y del Consejo, de 24 de octubre de 1995, relativa a la protección de datos de las personas físicas en lo que respecta al tratamiento de datos personales y a la libre circulación de estos datos [1]. Con esta Directiva se pretende poner en armonía las distintas legislaciones nacionales (en algunos casos inexistentes) concernientes al tratamiento de datos personales automatizados total o parcialmente así como los datos contenidos en un fichero o que vayan a figurar en él, protegiendo las libertades de las personas y el derecho a la intimidad, y la no prohibición ni restricción de la circulación de dichos datos de manera libre entre los estados miembros.

El 14 de septiembre de 1999, se creó un comunicado, COM(1999) 0337, relativo a la Propuesta de Reglamento del Parlamento Europeo y del Consejo sobre la protección de las personas físicas en lo que respecta al tratamiento de datos personales por las instituciones y los organismos de la Comunidad y sobre la libre circulación de estos datos [2]. Al final de las negociaciones, el Tratado firmado en Amsterdam inserta en el Tratado constitutivo de la Comunidad Europea una disposición específica sobre el tema y se establece en el artículo 286 que *"a partir del 1 de enero de 1999, los actos comunitarios relativos a la protección de las personas respecto del tratamiento de datos personales y a la libre circulación de dichos datos serán de aplicación a las instituciones y organismos establecidos por el presente Tratado o sobre la base del mismo"* y *"con anterioridad al 1 de enero de 1999, el Consejo establecerá, con arreglo al procedimiento previsto en el artículo 251, un organismo de vigilancia independiente, responsable de controlar la aplicación de dichos actos comunitarios a las instituciones y organismos de la Comunidad y adoptará, en su caso, cualesquiera otras disposiciones pertinentes".* Finalmente esto se plasmó en el Reglamento (CE) n° 45/2001 del Parlamento Europeo y del Consejo, de 18 de diciembre de 2000 [3].

Como complemento a la Directiva 95/46/CE la comisión dispuso la Directiva 97/66/CE que establece la armonización de las disposiciones de los Estados miembros necesarias para garantizar un nivel equivalente de protección de las libertades y de los derechos fundamentales y, en particular, del derecho a la intimidad, en lo que respecta al tratamiento de los datos personales en el sector de las telecomunicaciones, así como la libre circulación de tales datos y de los equipos y servicios de telecomunicación en la Comunidad. Aplicándose esta Directiva al tratamiento de datos personales en relación con la prestación de servicios públicos de telecomunicación en las redes públicas de telecomunicación en la Comunidad y, especialmente, a través de la red digital de servicios integrados (RDSI) y las redes móviles digitales públicas"[4].

Posteriormente la Directiva 97/66/CE fue derrogada por la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, de 12 de julio de 2002, relativa al tratamiento de los datos personales y a la protección de la intimidad en el sector de las comunicaciones electrónicas (Directiva sobre la privacidad y las comunicaciones electrónicas) [5].

La Directiva 95/46/CE, se transpuso en España con la Ley Orgánica 15/1999, 13 de diciembre de 1999, de Protección de Datos de Carácter Personal (LOPD) y la 97/66/CE como Real Decreto 994/1999 de 11 de junio por el que se aprueba el Reglamento de Medidas de Seguridad de los Ficheros Automatizados que contengan Datos de Carácter Personal.

Tanto la Directiva 95/46/CE como la Directiva 2002/58/CE tienen como objetivo, en el marco del tratamiento de los datos personales, proteger el derecho a la intimidad, pero en ninguna de éstas directivas se tiene en cuenta la existencia de otros entornos donde sí que se puede atentar contra el derecho a ésta.

Estos entornos son los terminales de acceso o grupos de terminales u ordenadores de acceso público, con conexión a Internet, como ejemplo de las redes

de terminales de acceso tenemos los terminales de automatrícula de las universidades, los cybercafés [6], aulas de acceso a Internet de bibliotecas, aulas de libre acceso en universidades, terrminales de conexiones a Internet en aueropuertos, etc., que cada vez están más extendidas a nivel europeo. Los terminales u ordenadores de dichos entornos son utilizados por múltiples usuarios durante todo el día y en numerosas ocasiones dichos usuarios tienen conversaciones personales (mediante chats), envían datos personales (como es la matriculación en la universidad), correos electrónicos con datos personales (como currículums a empresas o compra por correo) o incluso se realizan transacciones bancarias.

Dichos tipos de terminales y redes de ordenadores de acceso público no garantizan la protección de los datos personales, ni en éstos se protege el derecho a la intimidad, pues en ellos suelen estar presentes dos tipos de inseguridades principales que atentan contra este derecho:

- Inseguridad en la red porque en numerosas ocasiones se trata de una red ethernet o inalámbrica (según las últimas tendencias), donde el medio es compartido utilizando un mismo dominio de colisión (todos los terminales u ordenadores acceden a todos los datos que se han enviado al medio por cualquier equipo, pero sólo aquel dispositivo que sea el destino de los datos será el que los tratará) y por tanto cualquiera, dentro de ese mismo medio de red, puede “escuchar” las conversaciones privadas de otros o capturar archivos, contraseñas, etc. Si el medio de red sobre el que un usuario está conectado no es seguro, se puede estar atentando contra la privacidad en las comunicaciones electrónicas, no del proveedor de servicios de Internet, sino de la empresa u organismo que presta dicho servicio, pues en la red de ésta, se establece parte de la comunicación.

- Inseguridad en el terminal de red u ordenador porque cualquiera puede acceder a la información que ha sido almacenada en el ordenador local sin el conocimiento del propio usuario. Si no existe una correcta configuración del sistema operativo de dichos equipos de telecomunicación para evitar la extracción de los datos anteriormente introducidos en caso de utilizar posteriormente el mismo ordenador, se podría acceder parcial o totalmente a los datos escritos en todos los usos anteriores.

En la Legislación Española, la Ley Orgánica de 10/1995, de 23 de noviembre, del Código Penal, desde el artículo 197 al 201[7],se hace referencia a ataques que se producen contra el derecho a la intimidad, pudiéndose aplicar a algunos de los casos que se van a tratar a continuación.

2.- Inseguridad de los datos en la red

Los medios de red utilizados en los lugares de acceso público son en su gran mayoría ethernet, con un único dominio de colisión, o redes inalámbricas cuyo medio de transmisión es el aire. Ambos tipos de redes se caracterizan porque cualquier dato enviado por un componente de la red, es escuchado por todos los dispositivos de la red, sin embargo, sólo aquel dispositivo que es el receptor (la puerta de enlace, pasarela o router de acceso a Internet), debería ser el único que tratara dicha información. Por el contrario, si en cualquier otro dispositivo de red, se configura la

tarjeta de red (tanto cableada como inalámbrica) en modo promiscuo (utilizando un sniffer o programa similar), también puede ser el receptor de dichos datos y por lo tanto podría visualizarlos sin el consentimiento del propietario.

Para evitar este tipo de acciones en las redes de ordenadores de acceso público es necesario que:

- Para el caso de una red cableada, la red diseñada debe ser conmutada, utilizando dispositivos de conmutación, como por ejemplo switches, donde la información enviada por un terminal de red no es transmitida a todos los dispositivos, sino únicamente al dispositivo destino. Por otra parte, se tienen que tener perfectamente controlados los puntos desde donde se puede acceder a la red pues cualquier extraño podría conectar un dispositivo propio que permitiera intrusión.

- Para el caso de una red inalámbrica, la red debe tener algún sistema de seguridad que impida decodificar fácilmente la información transmitida sobre ésta, como por ejemplo deben estar activados los algoritmos de encriptación pertinentes (WEP, WAP, etc.) así como algún mecanismo que impida el acceso a esta red sin el previo consentimiento del administrador de la red o de la empresa u organismo que sean las responsables de las redes con estas características, mediante por ejemplo listas de acceso a la red, garantizando de esta manera una red más segura que permita mayor privacidad en los datos transmitidos.

3.- Inseguridad de los datos en el terminal de red u ordenador

La protección de los datos locales en un terminal de red u ordenador depende unívocamente del sistema operativo que utiliza. Entre este tipo de sistemas operativos nos podemos encontrar con MS-DOS, Microsoft Windows con sus diferentes versiones, Linux, Unix, BeOs, etc., cada uno con sus propiedades particulares en cuanto a sistema de funcionamiento y seguridad de usuarios. Pero en un entorno de acceso público nos encontramos con algunas configuraciones comunes, que en su mayoría se instalan por defecto en el propio sistema operativo, y hacen peligrar la privacidad de los datos. Estas configuraciones, en algunos casos, son idóneas para un ordenador con un único usuario, pues hacen más fácil y práctica la utilización del terminal u ordenador, pero cuando se trata de un equipo que va a ser utilizado por múltiples usuarios, los datos y las contraseñas introducidas durante los accesos, al ser almacenadas, podrán ser extraídas de manera fácil y rápida por usuarios posteriores [8][9][10].

Realizando un análisis detallado, se pueden encontrar los siguientes problemas en las configuraciones que tienen varios sistemas operativos y algunas de sus aplicaciones cuando todas sus opciones son las que están “por defecto”:

1.- Dado el modo de funcionamiento del protocolo http, cuando un usuario se conecta a una página web de un servidor con el navegador, la página web es almacenada en la caché del navegador para poder visualizarse, y permitir que la conexión entre el navegador y el servidor web se libere. Esto provoca que cada vez que visitamos una página web, ésta será almacenada en el disco duro y por tanto si

no se borra una vez hemos abandonado el equipo, cualquier usuario posterior podría visualizar todas las páginas visitadas, archivos descargados o incluso las conversaciones mantenidas (dependiendo del servidor chat utilizado).

2.- Para poder acceder a cuentas de correo vía web, páginas de acceso restringido, bancas a través de Internet, etc., se debe introducir un usuario y contraseña. Existe algún explorador de Internet que “por defecto” tiene habilitada la opción de almacenamiento de los nombres de usuarios y contraseñas en formularios. Esto puede ser de gran utilidad para un ordenador monousuario, pues se evitaría la introducción del usuario y la contraseña cada vez que accediera a dicha página web, pero si el ordenador es multiusuario, dicho usuario y contraseña están a merced de cualquier visitante posterior.

3.- En ocasiones, los archivos que se utilizan (word, pdf, etc) están comprimidos, para poder visualizar el contenido, el descompresor almacena en un directorio temporal dichos datos. Una vez se descomprime el archivo para visualizar la información, si se cierra la aplicación de descompresión, se puede observar que en el directorio temporal, sigue almacenado después de haber cerrado la aplicación con la que se abrió el archivo en cuestión. Esto mismo también ocurre cuando la aplicación de descompresión o el sistema se ha quedado inestable y deja de responder, quedando el archivo descomprimido a merced de cualquier usuario posterior.

4.- Cuando se edita con una aplicación, como por ejemplo al editar un documento con un editor de textos, se crea un archivo temporal con el contenido de dicho archivo. Si durante la ejecución de la aplicación o programa, éste se vuelve inestable y se cierra automáticamente o es necesario cerrarlo de forma brusca, el archivo temporal creado permanecerá en el sistema.

5.- En varios de los sistemas operativos anteriormente mencionados, se tiene la posibilidad de acceder remotamente con alguno de los usuarios que existen creados en el sistema, y en algún caso este usuario puede ser anónimo, esto provocaría que todo lo que en ese momento se estuviera realizando (copia de archivos, introducción de datos, etc.) un usuario local, pudiera ser observado por un usuario remoto.

A estos inconvenientes, se le puede añadir otros tipos de configuración creadas, o no tenidas en cuenta, por el administrador de red o el encargado para tal efecto por la empresa u organización, para facilitar el mantenimiento del terminal u ordenador que provocan que exista mayor inseguridad en el propio equipo. Entre estas configuraciones se pueden citar las siguientes:

1.- Compartición de recursos en red que faciliten la administración remota de los dispositivos. Esto permite el acceso al terminal u ordenador de manera sencilla a todos los datos almacenados.

2.- Tener una combinación de teclas o una puerta trasera que permita entrar como administrador en el terminal u ordenador de manera fácil. Esta es una técnica utilizada por algunos administradores para poder solucionar cualquier problema que exista en el equipo.

3.- No utilizar antivirus o antitroyanos en los equipos de la red porque ralentizan los terminales, quedando, por tanto, expuestos a infecciones de virus o troyanos no deseadas.

4.- No tener actualizado el sistema operativo ni las aplicaciones que sobre éste corren, quedando expuestos a posibles fallos o bugs que estos tengan. Es necesario que el/los encargado/s de los terminales u ordenadores de acceso público estén informados por medio del soporte de las empresas de aplicaciones o de sistemas operativos, o por medio de noticias o foros en caso de ser una aplicación de código libre.

Ante las razones analizadas, las empresas u organismos que dispongan de dichos terminales u ordenadores de uso público, deben garantizar al ciudadano privacidad e intimidad en sus datos durante la utilización de estos entornos.

5.- Incidencia de las Directivas 95/46/CE y 2002/58/CE del Parlamento Europeo y del Consejo en las inseguridades observadas

Las consideraciones que se tienen en cuenta en la Directiva 95/46/CE del Parlamento Europeo y del Consejo y que afectan a lo anteriormente tratado son: 10, 11, 25, 47, 53 y 68.

Dado que el caso que tratamos es el efectuado por una persona física en un entorno público donde se introducen datos como datos personales para realizar la matrícula en la universidad mediante los puntos de acceso o aula habilitadas para tal efecto, envío de correos electrónicos de carácter profesional, etc., esta Directiva se puede aplicar a tal efecto. Por lo tanto en el artículo 17 se expone que los Estados deberán velar por dicha seguridad.

La Directiva 2002/58/CE del Parlamento Europeo y del Consejo incide más que la anterior en la protección de datos en terminales u ordenadores de uso público como podemos comprobar en las consideraciones: 3, 5, 6, 7, 8, 10, 15, 20, 21, 22, 23, 24, 25, 28 y 46.

En cuanto a los artículos de la presente Directiva que repercuten sobre el tema tratado en este comunicado, nos encontramos con:

Artículo 4: Seguridad
Artículo 5: Confidencialidad de las comunicaciones
Artículo 14: Características técnicas y normalización

6.- Propuestas

Se debe elaborar una serie de propuestas de protección de la privacidad de los datos que no vulnere la intimidad de los usuarios de este tipo de entornos ya que los equipos utilizados no son ordenadores personales en el ámbito estrictamente privado, y no deben permitir una fácil extracción de datos personales sin el consentimiento del usuario:

- Los terminales u ordenadores deben ser configurados para que al finalizar la sesión de un usuario, se borren automáticamente todos los archivos que se hayan descargado en la caché del explorador utilizado.

- Los login de usuario y contraseñas utilizadas durante una sesión para acceder a páginas web, correo electrónico o cualquier otra aplicación de esta índole, no deben ser almacenadas en disco por ninguna aplicación del sistema operativo utilizado.

- Los archivos temporales utilizados durante la sesión de un usuario, deben ser borrados al finalizar ésta, evitando por tanto la visualización o la fácil recuperación de éstos.

- El sistema no debe permitir el acceso de un usuario remoto mientras exista una sesión iniciada por otro.

- No debe existir ningún recurso compartido de ningún dispositivo del terminal u ordenador mientras exista una sesión iniciada por un usuario, con el fin de evitar copias no autorizadas de los datos compartidos.

- No debe permitirse la existencia de “puerta traseras” de aplicaciones creadas con conocimiento de causa por parte de los creadores de la aplicación o por el propio encargado de los terminales, que permitan tomar el control total del dispositivo de manera fácil y accesible por un usuario.

- Se debe tener el sistema operativo y las aplicaciones actualizadas con los últimos parches y paquetes que publica el fabricante

- Se debe tener un antivirus o antitroyano instalado en el sistema operativo para detectar y eliminar troyanos o programas “spyware” en caso de este sistema necesitarlo.

7.- Políticas de seguridad utilizadas

Dado que varios de los sistemas operativos utilizados en estos entornos son configurables por el usuario, las medidas a tomar deben ser fuertes, pues no es permisivo que un usuario deje una configuración errónea y sea utilizada por otro posterior. Ante esto, se comprueba que en el cambio de un usuario a otro se debe configurar el terminal u ordenador con los parámetros correctos.

Entre las políticas de seguridad utilizadas en estos entornos nos encontramos:

1.- En el terminal u ordenador existe una única aplicación específica que permite acceder a Internet, enviar correo, realizar la automatrícula, etc. no permitiendo así, salir de la propia aplicación ni variar los parámetros de configuración del sistema.

Esta opción es válida siempre y cuando dicha aplicación no tenga ningún bug o fallo y esté perfectamente integrada con el sistema operativo, no permitiendo el

acceso a éste. Esta solución es comúnmente optada por puntos de acceso a la red (información, automatrículas, etc.).

2.- La creación de un script que al iniciar el sistema o al finalizarlo, elimine los archivos temporales, la caché de los exploradores, elimine las contraseñas introducidas, desabilite la conexión remota, descomparta los recursos compartidos y testee el equipo en busca de troyanos o “spyware”.

Esta opción es útil si el usuario no puede acceder de alguna forma al script y eliminarlo, ante esta opción, los administradores de red optan por almacenar dicho script en un servidor y lanzarlo desde el propio terminal u ordenador.

3.- Uso de discos de sólo lectura que no permitan escribir sobre éstos y en caso de necesitar almacenar algún dato, deberá realizarse en un dispositivo de almacenamiento removible propiedad del usuario.

4.- Existe software de carga de imágenes de disco en red. Esta solución es adoptada por muchos administradores. Cada vez que se inicia el ordenador, se carga la imagen en el disco duro desde un servidor central, pudiendo tardar esta operación entre 3 y 5 minutos.

Es la solución más segura de las tratadas, el problema es que cada vez que accede un usuario nuevo, se tendrá que reiniciar el sistema con la consecuente perdida de tiempo. Por lo tanto esta alternativa sólo sería válida para aulas de libre acceso, cybercafés, etc.

8.- Conclusiones

Tras revisar las consideraciones y artículos de las Directivas 95/46/CE y 2002/58/CE del Parlamento Europeo y del Consejo, se puede observar cuales de éstas son aplicables a estos entornos y qué observaciones de las anteriormente consideradas no se tienen en cuenta, y por tanto, deberían ser tratadas en posteriores comunicados al Parlamento y al Consejo.

En ambas directivas se pretende que haya confidencialidad en las comunicaciones y garantizar los derechos humanos y las libertades fundamentales evitando poner en peligro los datos y la intimidad del usuario. Esto implicará que el administrador o encargado de la red debería tomar las medidas oportunas para que los datos transmitidos por el medio de red no puedan ser escuchados o decodificados fácilmente por otros usuarios de la red. Para ello deberá ser necesaria la utilización de redes conmutadas en el caso de utilización de cableado y la utilización de protocolos de encriptación en redes locales inalámbricas.

Tanto la Directiva 95/46/CE como la 2002/58/CE del Parlamento Europeo y del Consejo tienen en cuenta la seguridad de la red por donde deben transmitirse los datos contemplando la red del proveedor de servicios pero no la red corporativa de la empresa u organismo que ofrece el servicio de conexión pública como son los cibercafés, aulas de bibliotecas, etc. Esto implica que se debería extender las consideraciones y los artículos tratados a este tipo de entornos.

En cuanto a la seguridad en los equipos terminales, en todas las consideraciones y artículos, siempre se hace referencia al hardware del propio terminal, relegando a un segundo plano el software que se utiliza para navegar, enviar y/o recibir correo, programa para realizar la matrícula, etc. En la consideración 24 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, se tienen en cuenta los programas espía “spyware” y web bugs, y la ilegitimidad de éstos sin el consentimiento del usuario. Igualmente deberían ser considerados los troyanos, pues estos permiten el control total o parcial del terminal u ordenador remotamente. Así pues, el administrador o encargado designado por la empresa u organismo que disponga de terminales u ordenadores de acceso público deben velar por que estos terminales estén libres de troyanos.

Al igual que en la consideración 46 de la Directiva 2002/58/CE del Parlamento Europeo y del Consejo, se exige a los fabricantes de determinados tipos de equipos de comunicaciones electrónicas, que fabriquen sus productos de manera que garanticen la protección de los datos personales y la intimidad del usuario y el abonado. También debería exigirse esta garantía a las empresas que creen o desarrollen los sistemas operativos que se instalan en este tipo de entornos, pues la protección de los datos del usuario dependerá en gran medida de éste. Estos sistemas operativos pueden ser de uso exclusivo (sólo realizan la acción para la cual están programados, por ejemplo, se inicia el terminal y con el sistema sólo se puede navegar, o enviar o recibir correo, o realizar una transferencia o movimiento bancario) o de uso general (sobre éste pueden funcionar uno o varios programas que permitan las acciones anteriormente mencionadas).

Ninguna de las directivas que se han estudiado para el presente documento, establece ningún tipo de consideración en cuanto al deber de los administradores de configurar los sistemas operativos, que se usan en los terminales de estos entornos, sin la existencia de recursos compartidos ni la posibilidad de acceso remoto. De esta manera se evitará la copia de archivos directa desde un sistema remoto.

En este tipo de entornos, los sistemas operativos deben estar configurados para evitar que los datos o información personal de un usuario no puedan observados por usuarios posteriores, para ello se debería adoptar una serie de consideraciones que eviten que los datos personales se guarden en la caché del explorador, las contraseñas y usuarios utilizados en formularios no deben guardarse y los archivos temporales de un usuario deben ser eliminados tras el uso del terminal u ordenador de acceso público.

A modo de establecer unas analogías, una persona que utiliza un ordenador de acceso público administrado sin unas medidas de seguridad correctas y anteriormente utilizado por otra, se podría comparar a la posibilidad de acceder a una cabina telefónica de uso público y existir una opción de rebobinado de grabaciones de llamadas telefónicas realizadas o a la posibilidad de que hubiera una tecla de “ir hacia atrás” para ver todas las transacciones bancarias realizadas anteriormente en un cajero automático. El usuario posterior no debería hacerlo, pero mejor es que no se pueda...

Por último es importante señalar la repercusión que tienen los administradores de la red y los terminales y su empeño en mantener actualizado el

sistema operativo y las aplicaciones que sobre éste funcionan, evitando posibles bugs o errores que permitan accesos malintencionados.

Referencias

[1]http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexplus!prod!DocNumber&type_doc=Directive&an_doc=1995&nu_doc=0046&lg=ES
[2]http://europa.eu.int/smartapi/cgi/sga_doc?smartapi!celexplus!prod!CELEXnumdoc&numdoc=599PC0337&lg=ES
[3]http://europa.eu.int/eur-ex/pri/es/oj/dat/2001/l_008/l_00820010112es00010022.pdf
[4]http://europa.eu.int/eur-ex/pri/es/oj/dat/1998/l_024/l_02419980130es00010008.pdf
[5]http://europa.eu.int/eur-ex/pri/es/oj/dat/2002/l_201/l_20120020731es00370047.pdf
[6]http://www.cybercafes.com/continent.asp?continent=Europe
[7]http://www.mir.es/policia/bit/197cp.htm
[8]Seguridad en Redes Corporativas. Jaime Lloret, Carlos Palau
ISBN:84-9705-455-5
[9]Seguridad en Unix y Redes. Antonio Villalón Huerta.
http://bernia.disca.upv.es/~iripoll/seguridad/Documentos/unixsec.pdf.gz
[10] La protección de Datos Personales: Soluciones en entornos Microsoft. *Rosa García.Consejera Delegada de Microsoft ibérica SRL*
http://www.microsoft.com/spain/technet/seguridad/otros/libro_lopd.asp
[11]Guia de protección de datos en España:
http://europa.eu.int/comm/internal_market/privacy/docs/guide/guide_es.pdf