**Tampering Over Data**

Esta categoría se refiere a la modificación desautorizada a los datos, o al software instalado en un sistema, incluyendo borrado de archivos. Este tipo de ataques son particularmente serios cuando el que lo realiza ha obtenido derechos de administrador o supervisor, con la capacidad de disparar cualquier comando y por ende alterar o borrar cualquier información que puede incluso terminar en la baja total del sistema en forma deliberada. O aún si no hubo intenciones de ello, el administrador posiblemente necesite dar de baja por horas o días hasta chequear y tratar de recuperar aquella información que ha sido alterada o borrada.

Como siempre, esto puede ser realizado por insiders or outsiders, generalmente con el propósito de fraude o dejar fuera de servicio un competidor.

Son innumerables los casos de este tipo como empleados (o externos) bancarios que crean falsas cuentas para derivar fondos de otras cuentas, estudiantes que modifican calificaciones de exámenes, o contribuyentes que pagan para que se les anule la deuda por impuestos en el sistema municipal.

Múltiples web sites han sido víctimas del cambio de sus home page por imágenes terroristas o humorísticas, o el reemplazo de versiones de software para download por otros con el mismo nombre pero que incorporan código malicioso (virus, troyanos).

La utilización de programas troyanos está dentro de esta categoría, y refiere a falsas versiones de un software con el objetivo de averiguar información, borrar archivos y hasta tomar control remoto de una computadora a través de Internet como el caso de Back Orifice y NetBus.

Parámetros de la aplicación web

El protocolo HTTP, es un protocolo de comunicación en la red, hace que sea posible transmitir parámetros de la forma de las solicitudes; puede hacerlo de varias maneras:

* [Cookies](http://ccm.net/contents/securite/cookies.php3);
* [Form](http://ccm.net/contents/html/htmlform.php3) fields;
* [URLs](http://ccm.net/contents/internet/url.php3);
* [HTTP headers](http://ccm.net/contents/internet/http.php3).

Es crucial entender que todos estos métodos de transmisión de datos pueden ser fácilmente manipulados por un usuario y que, como resultado, los datos de usuario no deben considerarse como fiable. A este respecto, la seguridad no se puede basar en las verificaciones de cliente (valores propuestos por un formulario HTML o códigos Javascript verificar la exactitud de los datos).

Además, el establecimiento de una conexión SSL no significa en absoluto a proteger contra la la manipulación de los datos enviados, sino simplemente certifica la confidencialidad de la información transportada entre el usuario final y el sitio Web.

Como tal, todos los diseñadores de aplicaciones Web deben verificar necesariamente los datos, en relación tanto a su valor (Mínimo y máximo para los datos numéricos, de verificación de caracteres para una cadena), y su tipo ylongitud.