



Videovigilancia segura

LA PROTECCIÓN CONTRA EL ACCESO NO AUTORIZADO A LA PROPIA CÁMARA DEBE CONSIDERARSE EXTREMADAMENTE IMPORTANTE Y DEBE GARANTIZAR LA PRIVACIDAD DE LAS PERSONAS



Jesús Garzón

**DIRECTOR REGIONAL
IBERIA, ORIENTE MEDIO Y
ÁFRICA**

Mobotix AG

La videovigilancia es un tema en constante debate cuyos detractores establecen como primer elemento en contra la falta de privacidad y seguridad de la transmisión de las imágenes de los sistemas IP. Pero, ¿y si tomamos las medidas oportunas para que esas imágenes sólo sean accesibles por el personal autorizado? De esta manera eliminamos uno de los principales inconvenientes de los sistemas IP, a los que debemos exigir ciertas características que comentamos a continuación.

Cada vez se discute más sobre los agujeros de seguridad de Internet, teniendo en cuenta el gran crecimiento experimentado por los sistemas de cámaras IP para transmitir datos desde áreas locales a la red. La protección contra ataques de virus, malware, uso no autorizado de los datos, así como el acceso no autorizado a la propia cámara debe considerarse extremadamente importante y debe garantizar la privacidad de las personas. Es decir,

hay que mantener la red del Circuito Cerrado de Televisión (CCTV) como un auténtico "Circuito Cerrado".

Para ello, debemos concienciar a los usuarios de la necesidad de utilizar

La videovigilancia es un tema en constante debate cuyos detractores establecen como primer elemento en contra la falta de privacidad

vídeo cámaras IP que cumplan con todas las medidas de seguridad necesarias para evitar intromisión en los datos o en las imágenes.

Las características que debe cumplir una cámara IP para bloquear el sistema, proteger al usuario de ataques y encriptar los datos es tener un sistema que esté bloqueado y que no dé opción a que ningún software de terceros pueda introducirse en la cámara e influir de manera negativa en el sistema. Básicamente una red IP es comparable a un pequeño PC: una unidad con un procesador interno y con capacidad para el procesamiento

de imágenes. Al igual que ocurre con un PC normal, hay que maximizar la seguridad de la red de cada cámara. El sistema operativo, que es la plataforma básica para las operaciones de este software es **Linux** embebido, que ofrece ventajas y herramientas básicas para proteger los sistemas TI de accesos no autorizados. En nuestro caso concreto, se utilizan exclusivamente módulos de software desarrollado por la propia compañía así que no existen componentes de software de terceros, algo que a priori también podría suponer un riesgo.

Por otro lado, es muy importante tener el nivel de acceso IP activado ya que si está desactivado, cualquier PC en la red puede ser aceptado como cliente para la cámara IP. Esto significa que se puede acceder a los procesos desde cualquier dirección IP que se encuentre en la red. Si se activa el control de accesos sólo será posible acceder desde ciertas direcciones, ya que se reduce el número de posibles clientes. La cámara comparará la dirección IP del PC que demande el acceso con la lista blanca de direcciones IP autorizadas que ella tenga y bloqueará o no ese requerimiento dependiendo del resultado de esa comparación.

Si la dirección IP del PC que solicita la petición de acceso está en la lista de direcciones autorizadas, habrá que **autenticar al usuario** vía **login** y



password. Hay diferentes niveles de usuarios y grupos para distintos derechos de acceso. Algo que, dependiendo de la compañía, se puede adaptar de forma dinámica a sus requerimientos. Si el usuario es autenticado y puede acceder a la cámara, se debe llevar a cabo después una verificación automática para asegurar que ese usuario tiene los permisos correctos para el acceso a las funciones que así estén estipuladas.

Otra de las características que previene de los llamados "ataques de fuerza bruta" es la **detección de intrusión**, ya que ofrece un mecanismo adicional de protección. Normalmente se habla de un ataque de fuerza bruta, si el acceso al sistema se realiza intentando combinar distintos **login y password** de forma automática mediante un programa de algoritmos que trata de conseguir los caracteres de la contraseña de manera sistemática o incluso manual.

La función de detección de intrusión no permitirá la demanda de acceso no autorizada y tomará medidas para mantener al operador del sistema informado mediante email, llamadas telefónicas o mensajes IP sobre la solicitud de acceso infructuosa, y bloqueará las direcciones IP de donde ha procedido la solicitud después de una cierta cantidad de accesos denegados.

Con el fin de ofrecer acceso a la secuencia de imágenes mediante el navegador, se ha integrado un servidor web en la cámara. Sin embargo, la transmisión de datos desde un servidor web a un cliente se realiza normalmente de forma transparente mediante http, transmitiendo lo no encriptado. De esta forma, utilizando un rastreador web se puede acceder a todo el tráfico y ver las secuencias rastreadas de la imagen.

Otra medida de acceso es la **huella o firma digital**. Este mecanismo de protección previene la manipulación

de los datos de los archivos de imagen. Como resultado, es posible confirmar la veracidad de cada imagen y se puede utilizar como material probatorio.

La utilización del **protocolo Radius** para la autorización, autenticación y contabilización de los clientes ligados a la cámara mediante WLAN, VPN, o conexión vía Modem, RDSI, DSL. Radius permite al operador del sistema establecer varios parámetros para controlar el grupo de clientes y prohibir el acceso a la red a clientes no autorizados.

Con estas características se minimiza el esfuerzo y se maximiza el efecto. Asimismo, se recomienda proteger el sistema de accesos no autorizados con accesorios externos como un túnel VPN. Además si se dispone de componentes WLAN en la red es preferible utilizar métodos de encriptación como WEP o WPA. Y, por último, sugerimos el uso de firewalls y software antivirus. ♦