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".

En el caso del fabricante Mobotix, sus cámaras ofrecen un amplio rango de características que permiten bloquear el sistema, proteger al usuario de ataques y encriptar los datos. En estas líneas se realiza una pequeña introducción de estas características de seguridad.

Básicamente una red IP de Mobotix 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.

Sistema operativo y plataforma básicos

Las cámaras IP de Mobotix trabajan con un software basado en el procesamiento de imagen. El sistema operativo, que es la plataforma básica para las operaciones de este software es Linux embebido. Es de todos sabido que los sistemas basados en Linux ofrecen ventajas y herramientas básicas para proteger los sistemas TI de accesos no autorizados.

El sistema está bloqueado y no da la opción para que ningún software de terceros pueda introducirse en la cámara e influir de manera negativa en el sistema. Además, Mobotix utiliza exclusivamente módulos de un software desarrollado por la propia compañía así que no existen componentes de software de terceros en el software de la cámara, algo que a priori también podría suponer un riesgo. El acceso a las funciones de la cámara o a las imágenes se divide en tres secciones:

1) Control de nivel de acceso IP

Con la función de control de nivel de acceso IP desactivada, cualquier PC en la red es 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. Al activar el control de nivel de accesos IP, sólo será posible acceder desde ciertas direcciones IP, 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.

2) Autentificación de usuario

Si la dirección IP del PC que solicita la petición de acceso está en la lista de direcciones autorizadas, habrá que autentificar ahora 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.

3) Autentificación de acceso a funcionalidades

Si el usuario es autentificado y puede acceder a la cámara, se llevará a cabo ahora una verificación automática para asegurar que ese usuario tiene los permisos correctos para el acceso a las funciones que así estén estipuladas.

Detección de intrusión

Otra de las características que completa la arquitectura descrita y que previene de los llamadas ataques de fuerza bruta es la detección de intrusión, ya que ofrecer 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 PASSWORDs de forma automática mediante un programa de algoritmos que trata de conseguir los caracteres del password 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 esta solicitud de acceso infructuosa
- Bloquear las direcciones IP de donde ha procedido la solicitud después de una cierta cantidad de accesos denegados

Encriptación de datos

Con el fin de ofrecer acceso a la secuencia de imágenes mediante el navegador, Mobotix 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.

El protocolo HTTPS/SSL que está integrado en las cámaras Mobotix actúa como autentificador entre el navegador y el servidor Web, ofreciendo de esta forma:

- Verificación de la identidad del servidor de envío (certificado)
- Transmitir el contenido encriptado
- Garantizar que los datos de entrada no fueron modificados

Huella/Firma digital de las imágenes

Cada archivo de imagen Mobotix incluye información de huella 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.

RADIUS (Remote Authentication Dial-In User Service, IEEE 8021.x)

Las cámaras Mobotix también cuentan con el 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. Se pueden incluir diversos atributos de autorización en una relación acceso-aceptado:

- Se puede asignar una dirección IP específica al usuario
- Se puede elegir el rango de direcciones del usuario IP
- El usuario puede permanecer conectado con la máxima longitud

Con estas características se minimiza el esfuerzo y se maximiza el efecto.

Otras medidas adicionales para proteger los sistemas:

Asimismo, Mobotix 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, finalmente, la compañía sugiere el uso de Firewalls y software Antivirus