EAGLE EYE NETWORKS

Las 12 mejores prácticas para sistemas de cámaras de seguridad – Ciberseguridad

Libro blanco técnico de Dean Drako, CEO de Eagle Eye Networks

¿Alguna pregunta?

+34 518 889 442
EMEAsales@een.com-
www.een.com/es

Introducción

Los sistemas de cámaras de seguridad están cada vez más conectados a Internet, impulsados en gran parte por la demanda del cliente por acceso remoto a vídeo. Los sistemas van desde sistemas de vigilancia administrados en la nube, los tradicionales DVR/VMS/NVRs conectados a Internet, y sistemas tradicionales conectados a una red local que a su vez está conectada a Internet.

Con la aceleración de ciberataques, los integradores de seguridad física y el personal de soporte interno deben mantenerse actualizados en los vectores de ataques de ciberseguridad que pueden afectar a los sistemas de gestión de video de la cámara que venden y/o administran. Estos sistemas requieren el mismo nivel de protección contra las vulnerabilidades de ciberseguridad otorgadas a sistemas de TI tradicionales.

Este libro blanco se enfoca en las mejores prácticas para los sistemas de cámaras de seguridad conectadas a Internet. Muchas de estas prácticas también pueden aplicarse a otros sistemas de seguridad física.

1. Seguridad física en una puerta peligrosa para ciberataques

Los sistemas de cámaras de seguridad están cada vez más conectados a Internet, impulsados por el deseo por acceso remoto y control, integración y costes drásticamente reducidos de almacenamiento en la nube.

En adición al número cada vez mayor de sistemas de vigilancia gestionados en la nube, la mayor parte de los sistemas de cámaras de seguridad tradicionales están conectados a Internet para obtener acceso remoto, soporte y mantenimiento, o están conectados a una red local, la cual a su vez está conectada a Internet.

En paralelo, los ataques cibernéticos continúan aumentando. Se vuelve común leer acerca de millones de brechas en los titulares de noticias. Las responsabilidades por daños son un enorme riesgo para las empresas.

Es entonces imprescindible que los sistemas de cámaras de seguridad obtengan el mismo nivel de atención para, y la misma protección de, vulnerabilidades de ciberseguridad que otros sistemas de TI tradicionales.

Los integradores de seguridad física y el equipo interno de soporte deben mantenerse actualizados en los vectores de ataques de ciberseguridad que pueden afectar a los sistemas de gestión de video de la cámara que venden y/o administran.

Este libro blanco se enfoca en las mejores prácticas para los sistemas de cámaras de seguridad conectadas a Internet. Muchas de estas prácticas también pueden aplicarse a otros sistemas de seguridad física.

2. Principales vectores de ataque para sistemas de cámaras de seguridad

Los cinco mayores vectores de ciberataques para sistemas de cámaras de vigilancia son:

1. Windows OS
2. Linux OS
3. DVRs (grabadores de vídeo digitales), NVRs (grabadores de vídeo de red), VMS (sistemas de gestión de vídeo)
4. Puntos finales (cámaras)
5. Puertos de cortafuegos

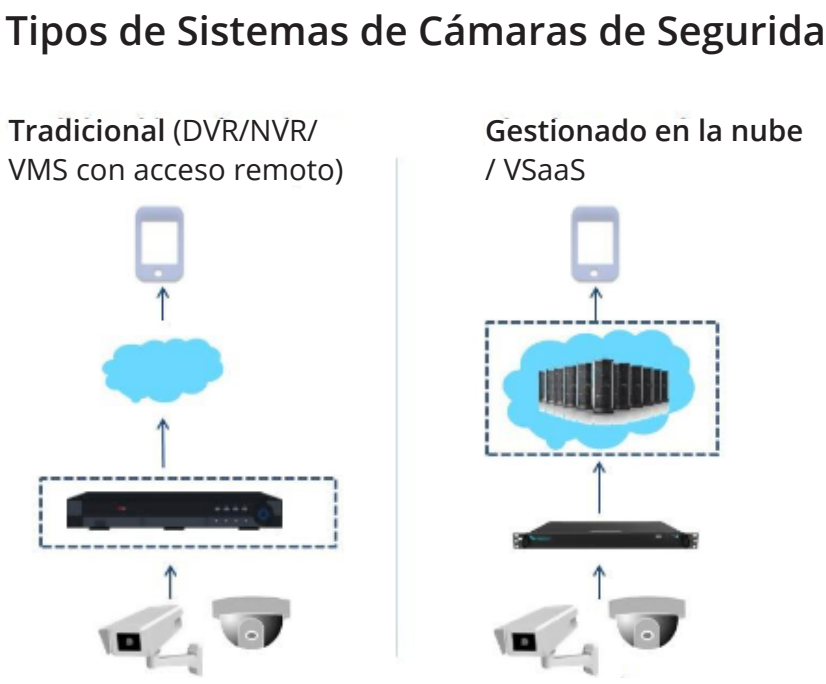
Discutiremos estos vectores de ataques en el contexto de mejores prácticas aplicables que pueden ser destruidas para proteger a su sistema de vigilancia contra ellos.

3. Tipos de sistemas de videovigilancia: tradicional y Cloud/VSaaS

Los términos 'videovigilancia en la nube' y 'sistema en la nube' se usan de inconsistentemente. Es entonces importante revisar con su proveedor para ver exactamente cómo obtienen acceso a Internet debido a que afectará los pasos que debe tomar para asegurarse de que su sistema sea seguro.

Para los propósitos de este libro blanco, distinguiré entre los tipos de sistemas de la siguiente manera:

- **Sistema tradicional**: un DVR, NVR, o VMS con una conexión a Internet, generalmente con el propósito de acceso a vídeo remoto
- **Sistema gestionado en la nube**: (también conocido como VSaaS) con un sistema gestionado en la nube, aunque puede haber un dispositivo físico, el vídeo es grabado y gestionado en la nube.



4. Doce mejores prácticas para la ciberseguridad de sistemas de cámara de seguridad

4.1 Contraseñas de camara

Vulnerabilidad

Se estima que uno de cada 5 usuarios de web todavía usan contraseñas fáciles de vulnerar. Las siguientes son las 10 contraseñas más usadas del 2018, según Splash Data:

1. 123456
2. Password
3. 12345678
4. qwerty
5. abc123
6. 123456789
7. 111111
8. 1234567
9. iloveyou
10. adobe123

Casi todas las cámaras vendidas hoy en día tienen una interfaz de usuario basada en web (GUI), y vienen con un usuario y contraseña por defecto que es publicada en Internet.

Algunos instaladores nunca cambian la contraseña y dejan la misma contraseña por defecto en todas las cámaras.

Solo pocas cámaras tienen una manera de desactivar el GUI, así que la vulnerabilidad de seguridad es que alguien puede intentar acceder a la cámara vía la GUI en línea para adivinar la contraseña. El 'hacker' necesita acceso a la red para hacer esto, pero las cámaras se encuentran usualmente en una red compartida, no en una red separada físicamente o una VLAN.

Mejor práctica:

Ambos: sistema tradicional y sistema gestionado en la nube

La práctica ideal es asignar una contraseña única, larga y no obvia para cada cámara. Un proceso meticuloso como tal toma más tiempo en preparar, es más difícil de administrar y muy difícil de seguir. Es por ello que, lamentablemente, muchos instaladores usan una única contraseña para todas las cámaras en una cuenta.

Para permitir este desafío, una mejor práctica aceptable es:

- Red pública: contraseña fuerte diferente para cada cámara
- VLAN o red física privada: la misma contraseña fuerte para todas las cámaras

Mejor práctica:

Sistema tradicional

Idealmente, NO conecte su servidor desprotegido a Internet. Si expone su sistema a Internet, entonces "redireccione el puerto" a la menor cantidad de puertos posible y utilice un cortafuegos de nueva generación que analice el protocolo y bloquee protocolos incorrectos enviados al puerto equivocado. En una situación ideal, despliegue además un IDS/IPS para mayor protección.

Sistema gestionado en la nube

Los sistemas basados en la nube más seguros no tienen redirección de puertos, así que no existe esta vulnerabilidad y no es necesario incrementar las acciones de protección. Solicite a su integrador o proveedor que verifique esto para cualquier sistema que tenga o considere adquirir.

4.2 Redirección de puertos

Vulnerabilidad

La mayoría de los usuarios finales ahora demandan y esperan acceso remoto a vídeos desde dispositivos móviles.

Esta función es normalmente entregada al exponer el DVR, NVR o VMS a Internet de alguna manera.

La exposición típica a Internet de un servidor HTTP es extremadamente peligrosa debido a que existe un gran número de posibilidades maliciosas que pueden ser usadas para obtener acceso. Las máquinas abiertas a Internet son usualmente escaneadas más de 10.000 veces al día.

Un ejemplo de esta vulnerabilidad fue la explotación Heartbleed de OpenSSL en el 2014; muchos fabricantes tuvieron que pedir a sus usuarios que restablezcan sus contraseñas.

4.3 Cortafuegos

Vulnerabilidad

Como se menciona arriba, cualquier DVR/NVR/VMS en el sistema debe tener un cortafuegos para protección, específicamente si va a exponerlo a Internet para cualquier tipo de acceso remoto.

Los cortafuegos pueden ser muy complejos, con miles de reglas. Los cortafuegos de nueva generación son incluso más complejos porque analizan los protocolos que pasan por los puertos y verifican que protocolos apropiados sean usados.

.

Mejor práctica:

Sistema tradicional

Es mejor asignar a un profesional experto en seguridad de redes para verificar y configurar un cortafuegos moderno.
Es imprescindible tener documentación clara de la configuración del cortafuegos, y monitorizar e implementar regularmente cualquier cambio necesario a la misma.

Sistema gestionado en la nube

Para una solución basada en la nube sin redirección de puertos, una configuración de cortafuegos en el sistema no es necesaria. Contacte con su integrador o fabricante de sistema para confirmar esto.

4.4 Topología de red (cámaras separadas)

Vulnerabilidad

Mezclar cámaras en una red estándar sin separación es una receta para el desastre.

Si su sistema de cámaras de seguridad está conectada a su red principal, está creando una puerta para que los hackers puedan ingresar a su red principal a través de su sistema de vigilancia, o entrar a su sistema de seguridad física a través de su red principal

Algunos DVRs pueden ser incluso ser enviados con un virus.

Mejor práctica:

Ambos: sistema tradicional y sistema basado en la nube

Idealmente, ubique su sistema de cámaras de seguridad en una red separada físicamente del resto de su red.
Si está integrando con un ambiente informático sofisitcado, no siempre es posible separar los dos sistemas físicamente. En dicho caso, debe utilizar una VLAN.

4.5 Sistemas operativos

Vulnerabilidad

Su VMS, DVR, NVR o sistema de grabación tendrá un sistema operativo. Todas las cámaras tienen un sistema operativo.

Todos los sistemas operativos tienen vulnerabilidades, tanto los basados en Windows como los basados en Linux.

Las vulnerabilidades de Windows están tan bien aceptadas que los equipos de TI las monitorizan regularmente. Recientemente, se ha vuelto más y más aparente que Linux tiene también muchas vulnerabilidades, como Shellshock (2014) y Ghost (2015), lo cual ha hecho vulnerables a millones de sistemas.

En teoría, su fabricante de sistema tendrá un equipo de seguridad de alta gama que esté disponible para ofrecerle actualizaciones de seguridad. La realidad es que muchos proveedores no hacen esto de una manera predecible.

Mejor práctica:

Sistema tradicional

Para asegurarse de que su sistema y red estén protegidas de brechas maliciosas, debe seguir y monitorizar las vulnerabilidades conocidas del sistema operativo, y después debe asegurarse de que su sistema operativo esté actualizado con todos los parches de seguridad.

Si es un sistema basado en Windows, existen muchas vulnerabilidades y muchas actualizaciones a ser aplicadas. Aunque son menos frecuentes, las vulnerabilidades de Linux deben también ser rastreadas y atendidas rápidamente.

Los profesionales de seguridad informática típicamente entienden cuáles son relevantes y cuáles debería ignorar, pero esta es una tarea extremadamente intimidante sin el entrenamiento y experiencia apropiadas.

También puede contactar con su proveedor de DVR/NVR para averiguar qué sistema operativo usa su NVR/DVR (Linux, Windows) y también qué versiones de sistema y qué versiones de módulos adicionales están implementados (por ejemplo, el servidor de páginas web Microsoft ISS) para que pueda entender qué vulnerabilidades de seguridad van a impactarle.

Después, rastree las vulnerabilidades de ese sistema operativo y contacte con su proveedor para ver qué parches son necesarios.

Las mejores prácticas para un VMS es asegurarse de que las máquinas están bajo el dominio de un departamento de TI y que este departamento tenga las responsabilidades y equipo asignado para realizar los parches, actualizaciones, modificaciones y procesos apropiados para asegurar que las máquinas sean seguras.

Además, asegúrese de que su proveedor de cámara ofrezca parches para problemas de seguridad y de que esté actualizando el firmware de su cámara en cuanto las nuevas versiones estén disponibles.

Sistema basado en la nube

La mejor práctica aquí es preguntar a su integrador o proveedor en la nube si se tiene un equipo de seguridad dedicado y experimentado que monitoree vulnerabilidades.

También confirme si su proveedor en la nube enviará automáticamente parches/actualizaciones de seguridad a través de la nube a cualquier terminal en las instalaciones. Si es así, no es necesario tomar acción de parte del usuario final para realizar operaciones de monitorización, parches o actualizaciones.

4.6 Contraseñas de sistemas operativos

Vulnerabilidad

Como sucede con las contraseñas de cámaras, una contraseña de sistema débil puede crear una oportunidad para ciberataques a su sistema de vigilancia y a su red.

Desafortunadamente, en muchos ambientes de sistemas operativos, la contraseña de raíz o de administrador es compartida entre todos los administradores, extendiendo el riesgo de seguridad. La rotación de empleados, ya sea por desgaste o por un cambio de roles, puede crear agujeros de seguridad inesperados.

Mejor práctica:

Sistema tradicional

Establezca contraseñas largas y de alta calidad para su sistema operativo.

Adicionalmente, establezca políticas y procedimientos para cambiar contraseñas. Por ejemplo, la contraseña de administrador debe ser cambiado cada vez que un empleado con acceso a la contraseña deja la empresa o cambia de roles.

Sistemas gestionados en la nube

No se requiere acción. Los verdaderos sistemas en la nube no tienen contraseñas separadas para acceso al sistema operativo. Solo tienen contraseñas de sistemas que son para cuentas individuales (mire más abajo) que pueden ser eliminadas explícitamente cuando los empleados se van o cambian de roles.

4.7 Contraseñas de sistemas de videovigilancia

Vulnerabilidad

El acceso no autorizado a su sistema de cámaras de seguridad deja vulnerable tanto a su sistema de vigilancia como a la red conectada a la misma.

Mejor práctica:

Ambos: sistema tradicional y sistema gestionado en la nube

Cambie las contraseñas de su sistema de vigilancia siguiendo un calendario. Refuerce la calidad de seguridad con el mismo rigor que su estándar de empresa. Las contraseñas largas y fuertes son las mejores.

4.8 Cifrado de conexión

Vulnerabilidad

Un número sorprendente de DVR/NVR/VMSs usan conexiones que no están cifradas con SSL o equivalentes.

Este riesgo es idéntico al de iniciar sesión en un banco o realizar compras en líneas sin https. Crea una vulnerabilidad de contraseña y abre la posibilidad a brechas de privacidad y espionaje.

Mejor práctica:

Sistema tradicional

Es imprescindible que su conexión sea cifrada con SSL o equivalente.

Pregunte a su proveedor cómo manejar esto. Solo elija proveedores que cifren sus conexiones.

Sistema gestionado en la nube

Es imprescindible que su conexión sea cifrada con SSL o equivalente.

Muchos proveedores en la nube ofrecen cifrado de conexión, pero esto es variable. Confirme con su proveedor en la nube como su sistema maneja esto.

4.9 Cifrado de vídeo

Vulnerabilidad

Además de conexiones inseguras debido a una falta de cifrado, los mismos riesgos de privacidad se aplican cuando el vídeo no es cifrado al ser guardado en un disco o en tránsito.

Mejor práctica:

Ambos: sistema tradicional y sistema gestionado en la nube

Para un sistema verdaderamente seguro, el vídeo debe ser cifrado, tanto cuando es guardado en un disco como cuando está en tránsito.

4.10 Acceso móvil

Vulnerabilidad

Las vulnerabilidades de contraseña, eliminación de cuenta y de cifrado se aplican doblemente a terminales móviles.

Mejor práctica:

Ambos: sistema tradicional y sistema gestionado en la nube

Al momento de ejecutar la aplicación en su ordenador personal, asegúrese de que tenga una conexión cifrada para la aplicación móvil en el dispositivo iPhone o Android conectado al VMS o NVR/DVR.

Establezca contraseñas de alta calidad y realice un reforzamiento de contraseñas y eliminación de cuentas cuando el equipo técnico cambie.

4.11 Acceso físico al equipo y almacenamiento

Vulnerabilidad

Las recompensas económicas por robar datos de empresa son lo suficientemente altas como para que los intrusos busquen también acceder a su red mediante un ataque directo a su equipo físico en sus instalaciones.

Mejor práctica:

Sistema tradicional

Mantenga seguro: sus gabinetes, cables y la habitación donde guarda los DVR/NVR/VMS, interruptores y servidores de almacenamiento de vídeo. Proporcione un control de acceso seguro a la habitación, incluyendo vídeos de seguridad para monitorizarlo. Esta práctica no solo protege su red, sino que también previene robos violentos en sus instalaciones, aquellos donde el DVR/NVR de grabación es robado junto a otros artículos.

Sistema gestionado en la nube

Aunque los mismos principios claramente se aplican a un sistema basado en la nube, existen muchos menos equipos en las instalaciones que proteger. La grabación inmediata en la nube también protege ante ataques violentos al equipo de grabación en sitio.

Es importante preguntar a su integrador o proveedor por medidas de seguridad generales que toman para sus servidores en la nube.

4.12 Software de grabación de vídeo

Vulnerabilidad

Los programas de gestión de vídeo usan muchos componentes más allá del sistema operativo, como aplicaciones de bases de datos de Microsoft. Como con el sistema operativo, estos componentes debe ser mantenerse actualizados y seguros.

Muchos VMS, por ejemplo, usan Microsoft Access, bibliotecas, así como el software que tienen instalados. Nuevas vulnerabilidades de sistema pueden ser introducidas si el software en el que se apoya no está actualizado, incluyendo parches de seguridad.

Si es pasivo en este aspecto, dependerá completamente de que el proveedor envíe parches para actualizar el sistema ante dichas vulnerabilidades.

Mejor práctica:

Sistema tradicional

Pregunte a su proveedor de VMS sobre su política para mantener los componentes que usan actualizados y seguros. Asegúrese de instalar actualizaciones regularmente. Sea proactivo al monitorizar las vulnerabilidades de sistema conocidas en la industria y contacte con su integrador o proveedor cuando sepa de nuevas brechas.

Es importante asegurarse de que su proveedor de VMS disponga de un equipo enfocado en esto y de que esté enviando actualizaciones regularmente.

Sistema gestionado en la nube

Los verdaderos sistemas gestionados en la nube no tienen un software en sitio, así que no existe vulnerabilidad en este aspecto.

Sin embargo, es muy importante confirmar si el sistema está verdaderamente “gestionado en la nube” en lugar de estar “conectado a Internet” antes de asumir aquello, o correrá el riesgo de exponerse a una vulnerabilidad potencial.

Conclusión - Mezcla de referencias de mejores prácticas

Las brechas de seguridad continúan acelerando alrededor del mundo. Con mayor conexión a Internet, los sistemas de seguridad física son muy vulnerables a los ciberataques, tanto a ataques directos como a intrusiones al resto de la red. Las responsabilidades por estos ataques todavía se están definiendo.

Para maximizar su seguridad, es imprescindible definir mejores prácticas para su propia empresa como parte de la evaluación del sistema de su cámara de seguridad, así como su implementación y mantenimiento.

Es recomendable proteger a su empresa y clientes con medidas de prevención.

¿BUSCANDO CÓMO MOVERSE A LA NUBE?

Aprenda más sobre la plataforma de gestión de vídeo de Eagle Eye Networks.

Eagle Eye Networks fue creado para facilitar la seguridad de los vídeos. Los sistemas de cámaras tradicionalmente han sido complejos y difíciles de manejar para todo el mundo. El VMS de Eagle Eye Cloud, puede implementar múltiples cámaras en múltiples ubicaciones, sin instalar software ni comprar servidores grandes.

Obtenga más información sobre VMS en la nube, explore la plataforma que ofrecemos, o hable con uno de nuestros especialistas hoy.

Reserve una demo

Eagle Eye Networks EMEA
Hogehilweg 19
1101 CB Amsterdam
The Netherlands

Contact Us
+31 20 26 10 460
EMEAsales@een.com
www.een.com

Support Desk
+31 20 26 10 461
support@een.com
www.een.com/support