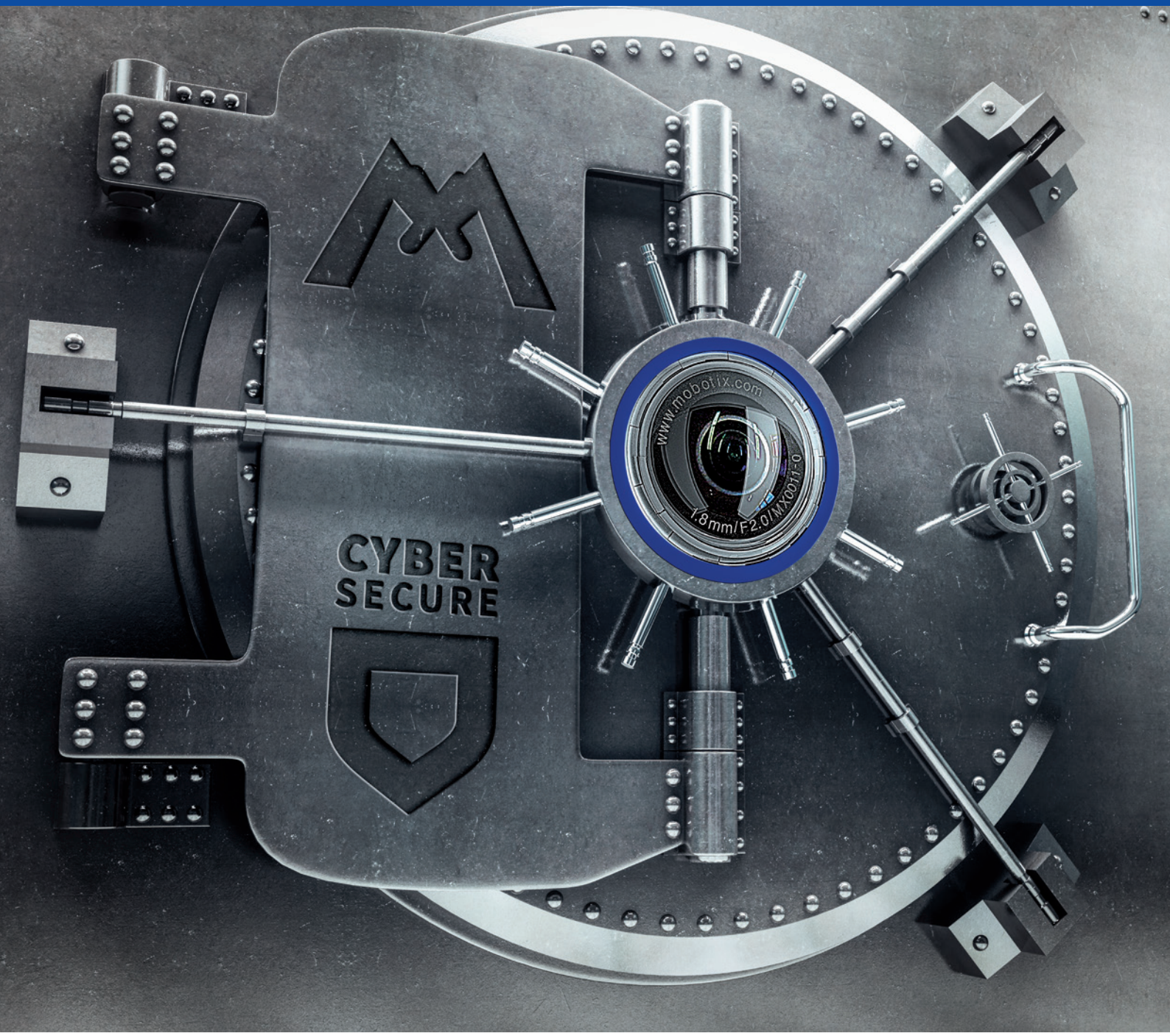
La importancia de la ciberseguridad en los sistemas de videovigilancia

Documento técnico



BeyondHumanVision

MOBOTIX

Introducción

El uso del vídeo para la seguridad, el control industrial y la salud tiene un impacto beneficioso en las vidas de miles de millones de personas cada día. Desde una familia paseando por un centro comercial seguro bajo la atenta mirada de un sistema CCTV hasta el vídeo remoto que ayuda a los gerentes a detectar defectos en una cadena de producción, o incluso padres preocupados por monitorizar a un bebé dormido; la videovigilancia afecta a todas nuestras vidas.

¿Cuáles son los principales motores del crecimiento?		
1	Aumento de las preocupaciones de seguridad	58 %
2	Mejora en análisis de vídeo	51 %
3	Disponibilidad de redes IP	50 %

El aumento del uso del vídeo para vigilancia y otras aplicaciones se ha visto acelerado por los sectores más amplios de la información, comunicación y tecnología. Anteriormente, una imagen de videovigilancia precisaba que un operador humano viera una situación para tomar una decisión. Sin embargo, cada vez más, las imágenes de vídeo están vinculadas a otros tipos de datos sensoriales como temperatura, sonido, movimiento y sistemas de inteligencia artificial, que pueden activar alarmas o acciones automáticamente. El vídeo ha pasado de ser un medio de recepción pasiva a una situación en la que una inteligencia más automatizada puede realizar tareas en función de lo observado.

Sencillos ejemplos como el reconocimiento de matrículas en sistemas automáticos de peajes en autopistas a sistemas más potentes capaces de detectar visualmente fallos menores en las máquinas antes de que se averíen son sólo la punta del iceberg. Incluso en aplicaciones convencionales como la vigilancia de pequeños comercios, las tecnologías más recientes están incorporando elementos como el recuento de personas y el análisis de patrones de compra para ayudar en la distribución de las tiendas e incluso el diseño de nuevos centros comerciales.

La demanda crece y, según la estimación de Cisco, el vídeo con fines comerciales y de entretenimiento consumirá el 79 % del tráfico de Internet para 2020[1]. Y cada vez resulta más fácil generar vídeo con cámaras más pequeñas, más económicas y menores requisitos energéticos. La transferencia de vídeo desde el origen al destino también está resultando menos compleja gracias a la expansión de la conectividad de Internet y las redes móviles más rápidas. La percepción del vídeo, y especialmente de la videovigilancia, se considera en gran medida un importante beneficio social ya que se cuenta con entornos más seguros con menos delitos y más libertad personal. Sin embargo, a medida que el uso del vídeo está más generalizado, también resulta más expuesto a ataques de delincuentes, terroristas y otros grupos que pretenden perjudicar o aprovechar las plataformas de videovigilancia para realizar acciones negativas.

Riesgos de seguridad en la videovigilancia y los dispositivos IOT

Hasta ahora, los ataques contra las redes de videovigilancia eran poco frecuentes debido a la naturaleza cerrada de los sistemas, que a menudo se conectaban mediante redes privadas cableadas directamente a las salas de control in situ. Además, las cámaras de vídeo heredadas estaban cableadas de forma eficiente y contaban con un firmware simplista que hacía poco más que enviar vídeo a través de un cable coaxial, lo que dejaba pocas oportunidades a los ataques. Sin embargo, los tiempos cambian y las cámaras de vídeo actuales ejecutan de forma eficiente software de ordenadores conectado a un sensor de imagen digital. Con el auge de Internet y las cámaras de bajo coste, los sistemas de videovigilancia son cada vez más accesibles a través de cualquier red IP.

Al igual que los ataques de seguridad contra comercios minoristas y proveedores de servicios, y a menudo con el objetivo de recopilar tarjetas de crédito u otra información valiosa, la complejidad y la naturaleza cambiante de los procesos, los protocolos de software y los mecanismos de autenticación implican que surgirán vulnerabilidades. Este problema no es nuevo. Durante más de una década, los investigadores de seguridad[2] han descubierto vulnerabilidades en las cámaras que han afectado tanto a los principales proveedores internacionales como a pequeñas marcas regionales con una creciente lista de problemas que incluye:

- Ataques que obtienen la contraseña del administrador del dispositivo vulnerando el control de seguridad de una cuenta de usuario predeterminada
- Acciones que omiten la autenticación del usuario mediante el uso de credenciales con codificación fija que el fabricante del dispositivo ha instalado en el dispositivo como puerta trasera
- Ejecución de código arbitrario en el dispositivo sin autenticación mediante el aprovechamiento de vulnerabilidades del controlador de paquetes del Protocolo de transmisión en tiempo real
- Vulnerabilidad de seguridad que omite la autenticación de operador de cámara, permitiendo así a un atacante acceder directamente a los archivos de configuración
- Acciones que permiten a un atacante restablecer la contraseña del dispositivo y posteriormente habilitar la modificación no autorizada de archivos de configuración para proporcionar acceso a un atacante a las funciones principales de la cámara
- Ataque contra cámaras que permiten a terceros interceptar transmisiones de vídeo en vivo enviadas a través de una red privada o conexión a Internet

Muchos de estos problemas que afectan a diversas marcas secundarias que otorgan licencias de tecnología de grandes proveedores han generado puntos débiles en millones de dispositivos. Aunque los mayores proveedores con reputaciones importantes a menudo han publicado revisiones para solucionar el

problema, muchas de las empresas de menor tamaño simplemente han ignorado el problema. Incluso cuando hay una solución disponible, las actualizaciones son procesos manuales y muchos propietarios de plataformas de videovigilancia no son conscientes del problema. El problema también se extiende a los usuarios particulares con gran cantidad de sistemas de videovigilancia de consumo adquiridos a comercios minoristas que en gran medida siguen sin actualizar.

Ataques dirigidos y botnets

Aunque parezca el guion de una película de Hollywood, la capacidad de desactivar sistemáticamente todo un sistema de videovigilancia que brinda protección a un centro, una zona o incluso una ciudad de gran valor no es ciertamente imposible. Con un gran número de proveedores de videovigilancia que reutilizan las mismas bibliotecas de software que administran elementos como la transmisión, la autenticación de usuarios y la transferencia de vídeo a medios de almacenamiento, es casi seguro que los adversarios expertos pueden planificar sus ataques para cometer delitos, pero también como forma de causar terror y pánico.

Otro problema para la red son los atacantes que se apoderan de un dispositivo conectado, por ejemplo, una cámara, y posteriormente utilizan su situación autenticada para obtener acceso a otros recursos conectados. Aunque esto se ha detenido en gran medida a través de defensas de red bien diseñadas, a medida que las cámaras y otros dispositivos del Internet de las cosas (IoT) comienzan a prevalecer e integrarse en los procesos centrales, el requisito de ofrecer acceso a dispositivos de IoT puede crear más riesgos. Pero el ataque a las cámaras no es el único problema. En casos recientes, las propias cámaras han sido tomadas y utilizadas como arma para ataques distribuidos de denegación de servicio (DDoS).

En octubre de 2016 se produjo un ataque DDoS a gran escala que afectó a Twitter, Amazon, Tumblr, Reddit, Spotify y Netflix y que fue provocado, en parte, por el botnet basado en Mirai. Según informa la experta en seguridad Allison Nixon, directora de investigación de Flashpoint, los botnets resultan comprometidos principalmente por las grabadoras de vídeo digital (DVR) y las cámaras IP fabricadas por la empresa china de alta tecnología XiongMai Technologies. Los componentes que fabrica XiongMai se venden a proveedores que posteriormente los utilizan en sus propios productos, lo que conlleva que varias decenas de miles se hayan incorporado a estas peligrosas armas cibernéticas.[3]

Gobierno, organismos reguladores y legislación

La explosión de los dispositivos conectados a Internet, según estimaciones de Gartner, Cisco y otros, se encontrará entre 25 y 50 mil millones[4] para 2020, lo que provoca dolores de cabeza a gobiernos nacionales y otros organismos reguladores transnacionales. A diferencia de los transmisores de radio, las emisoras de televisión o los vehículos de motor, apenas existe legislación sobre lo que se puede conectar a Internet. No hay estándares obligatorios sobre el nivel de seguridad que debe ofrece un dispositivo. ¿Qué ocurre si ese dispositivo es pirateado o se utiliza para atacar a un tercero? El derecho penal de la mayoría de las regiones puede afrontar los delitos informáticos en los que exista un infractor y una víctima, pero a medida que la tecnología se vuelve más autónoma, existe el riesgo de que los dispositivos no seguros atraigan virus como las epidemias que solían inundar los ordenadores de escritorio, que podrían reaparecer en dispositivos como las redes de cámaras de videovigilancia para las que se disponen de escasas formas de detectar o de solucionar rápidamente el problema.

Posibles responsabilidades financiera y penal

También existe el espinoso problema de la responsabilidad. La instalación de sistemas de videovigilancia puede reducir los costes de seguros y aumentar la probabilidad de detención de los delincuentes. Sin embargo, si un sistema de videovigilancia se vuelve inoperativo debido a un punto débil de la seguridad y se comete un delito pero no se registra con cámara, los aseguradores podrían reclamar la cancelación del pago de indemnizaciones debido al incumplimiento de las condiciones de la cobertura. En este caso, ¿demandaría la víctima al fabricante de la cámara? ¿Al proveedor de cualquier contrato de mantenimiento de CCTV? O, en el caso de un incidente de seguridad pública, ¿asumiría la responsabilidad el organismo oficial local? Hay tantas preguntas sobre el impacto de una infracción de seguridad en un sistema como la videovigilancia y tan pocos casos de prueba que la incertidumbre en el mercado es considerable.

Preocupaciones sobre la privacidad

Aunque las cuestiones de responsabilidad financiera y penal relacionadas con la piratería de dispositivos de videovigilancia aún están abiertas a debate, la legislación sobre la privacidad de los ciudadanos se ha consolidado en la mayoría de las naciones desarrolladas. Aunque los detalles pueden cambiar ligeramente, en general todos los datos personales privados sobre salud, finanzas, orientación sexual, afiliación política y una serie de criterios adicionales deben recopilarse y guardarse de manera segura. Esto también se aplica a los datos de vídeo; por ejemplo, los pacientes que acuden a consultas de salud mental o las personas que asisten a eventos políticos esperan que cualquier vídeo de videovigilancia se conserve de forma segura y fuera del dominio público. En el caso de un ciberataque contra un dispositivo o red de videovigilancia, existe un

riesgo muy elevado de que la información personal buscada, como imágenes y otros datos, sea la concerniente a determinadas personas y pueda ser robada y filtrada sin autorización. Esto supondría una violación de los derechos de privacidad de los usuarios monitorizados por el sistema y podría tener consecuencias legales para el responsable del procesamiento de datos personales.

Acciones gubernamentales

Los gobiernos de todo el mundo piden más explicaciones sobre la forma de asegurar la nueva generación de dispositivos IoT. En Europa, los altos funcionarios de la Comisión han discutido abiertamente la creación de un proceso de homologación para los dispositivos de Internet de las cosas (IoT) que garantizaría la protección de los usuarios. La Comisión también ha contribuido a establecer el grupo Alianza para la innovación del Internet de las cosas, que incluye a varios líderes de importantes proveedores de tecnología de los sectores de energía, automotriz y sanitario para comenzar el proceso de creación de una serie de guías de prácticas adecuadas. En EE. UU., el Departamento de Seguridad Nacional ha publicado una guía sobre los Principios estratégicos para asegurar el Internet de las cosas[5], que incluye algunos conceptos clave como la incorporación de la seguridad en la fase de diseño, la promoción de actualizaciones de seguridad y la gestión de vulnerabilidades con un enfoque en la priorización de las medidas de seguridad en consonancia con posibles impactos. Sin embargo, no existe un consenso mundial o respaldado por la industria, como los estándares PCI-DSS de los sectores crediticios. El resultado final es que la seguridad de los dispositivos IoT ahora se basa en lo estipulado en cada país y en una regulación tibia, que varía considerablemente en su ámbito y efectividad.

¿Cómo se enfrenta MOBOTIX a estos problemas?

Como líder del sector de la videovigilancia digital, MOBOTIX no es un fabricante común ya que desarrolla todo su software internamente. Esto nos permite ofrecer no sólo productos altamente avanzados, sino también una ventaja considerable en lo que respecta a la seguridad. Al controlar el desarrollo del software, MOBOTIX es menos vulnerable a los problemas de seguridad que pueden surgir al combinar hardware y software de terceros con un diseño deficiente. En las áreas en que utilizamos estándares del sector que gozan de un gran respaldo, como ONVIF, contamos con políticas que permiten publicar de inmediato cualquier actualización a medida que están disponibles. Al utilizar el mismo software para todos los modelos de cámaras MOBOTIX, este proceso de garantizar continuamente que el firmware de la cámara sea actual y seguro hace que sea mucho más sencillo para nuestros clientes internacionales.

El espíritu de seguridad en el diseño lleva en la empresa desde el primer día y resulta evidente en varias áreas:

Sistema operativo seguro y actualizaciones

El comienzo del enfoque de seguridad de MOBOTIX comienza con su integración en el diseño del sistema operativo de la cámara y la pila de aplicaciones. Todos los dispositivos MOBOTIX se diseñan sobre la base de un sistema operativo Linux modificado y protegido que elimina los servicios y módulos estándar. Los módulos de Linux críticos, como la autenticación, son completamente rediseñados por los ingenieros de MOBOTIX para garantizar que no ofrezcan vulnerabilidades estándar ni estén expuestos a técnicas de inyección de código. Este software operativo no es de código abierto y está protegido por técnicas de seguridad de software adicionales. Además, cada actualización del firmware del dispositivo y los elementos del software se cifra y firma digitalmente para evitar su manipulación.

Configuración segura de la cámara

Sólo los usuarios autorizados pueden acceder a la interfaz de configuración de la cámara y, para garantizar la seguridad interna, todos los sistemas permiten la creación y aplicación de diferentes derechos para grupos de usuarios distintos. En la práctica, esto significa que las cámaras MOBOTIX nunca guardan las contraseñas de los usuarios con texto de forma explícita, sino que se crean con un avanzado algoritmo de control unidireccional (SHA-512) para que, incluso si el archivo de configuración termina en malas manos, sea extremadamente difícil recuperar el texto explícito de la contraseña. Los servicios de Linux no esenciales están desactivados, lo que limita las posibles vulnerabilidades y evita ataques. Además, no existe telnet o una "contraseña maestra" sin documentar: se puede acceder y configurar una cámara MOBOTIX a través de su GUI (interfaz gráfica de usuario) web. Las contraseñas se pueden conservar en sistemas de administración de acceso privilegiado como BeyondTrust y CyberArk, que se pueden proteger con sistemas de un mayor nivel de autenticación de dos factores.

Comunicación segura de red y dispositivos

Todos los datos intercambiados entre cada cámara MOBOTIX y otros hosts de la red se pueden cifrar para garantizar la confidencialidad e integridad de los datos en tránsito. HTTPS (SSL/TLS) y los certificados son compatibles de forma estándar para cumplir con las prácticas adecuadas aplicadas en los principales marcos de seguridad por expertos, como el Instituto SANS. MOBOTIX también ofrece compatibilidad con la administración de certificados exclusivos X.509 en cada cámara y autoridades de certificados raíz para permitir a las organizaciones ampliar la seguridad de sus dispositivos a fin de incluir cámaras y videoporteros autenticados a través de sistemas como OpenVPN. Esto significa que, si se roba o piratea una cámara, un atacante no puede usar las credenciales que residen en dicha cámara para atacar al resto de la red de cámaras.

Grabación interna segura y antisabotaje

Todas las grabaciones registradas por la cámara se pueden cifrar antes de ser almacenadas, comenzando por el búfer circular que utiliza la tarjeta SD incluida en cada cámara. MOBOTIX ha construido un sistema de archivos seguro mediante el cual, si se piratea o roba una cámara, el vídeo grabado que aún se encuentra en la cámara no se puede recuperar sin antes obtener derechos administrativos

que están protegidos mediante los procesos de configuración segura descritos anteriormente. Cada imagen generada por una cámara MOBOTIX puede firmarse digitalmente con certificados personalizados para evitar manipulaciones, lo que garantiza la admisibilidad de las grabaciones como prueba en un tribunal.

Características especiales	Cámaras IP estándar	MOBOTIX
HTTPS (SSL/TLS) y certificados	✓	✓
Síntesis de autenticación para HTTP	✓	✓
Listas de control de acceso	✓	✓
Usuarios y grupos con derechos personalizados	⚠	✓
Detección de intrusos	✗	✓
Protección contra botnets	✗	✓
Grabaciones cifradas	✗	✓
Vídeo y mensajes cifrados	✗	✓
Cliente VPN	✗	✓

Detección de intrusos

Incluso con la aplicación de diversos sistemas y procesos de seguridad, sería temerario suponer que no se intentará atacar las cámaras MOBOTIX, razón por la cual MOBOTIX ha invertido en medidas adicionales para detectar dichos intentos. Mediante la implementación de diversos elementos de detección de intrusos, cada cámara o dispositivo de videoportero informa a través de un canal cifrado sobre cualquier inicio de sesión no autorizado y ataques de fuerza bruta; asimismo, se pueden enviar notificaciones en caso de repetidos intentos fallidos de inicio de sesión y la dirección IP infractora se puede bloquear automáticamente.

Resumen

El aumento de la popularidad de la videovigilancia y como parte de otros procesos de salud, seguridad e industriales no muestra signos de desaceleración. Con la creciente importancia de estos elementos, los procesos adicionales como el control de acceso, la monitorización del clima, y los procesos analíticos como el reconocimiento facial, se convertirán cada vez más en objetivos para el ciberataque.

Los prescriptores de los sistemas de videovigilancia junto con los proveedores de servicios e incluso los organismos reguladores deberán ampliar el control de la seguridad tanto como un deber de atención al público como para cumplir las futuras obligaciones legales. Como sector, líderes como MOBOTIX han reconocido estos problemas y están trabajando de forma activa para integrar la seguridad en el hardware y software de los dispositivos en las fases iniciales del diseño.

No obstante, la seguridad de los dispositivos sólo es tan buena como lo sea el nivel de protección del entorno general. Cerrar la puerta con llave no tiene sentido si se deja abierta la ventana. Así pues, descriptores y operadores de videovigilancia y redes IoT más amplias deben evaluar otras partes, como la red subyacente, la infraestructura de almacenamiento y, de forma crucial, el elemento humano, que a menudo es un eslabón débil. Varios grupos del sector, como el Instituto SANS, han creado pautas de gran utilidad como los controles de seguridad críticos del Centro de Seguridad de Internet (CIS), que ofrecen un conjunto de acciones recomendadas para la defensa cibernética que proporcionan formas específicas y aplicables para detener los ataques más penetrantes y peligrosos de hoy en día.[6]

Mirando hacia el futuro, resulta evidente que la seguridad de los dispositivos y plataformas se convertirá en un factor clave en los principales proyectos de vídeo y, a medida que se amplía el alcance de la concienciación sobre los desafíos de IoT, MOBOTIX espera trabajar con sus homólogos del sector, los clientes y los organismos gubernamentales para proteger las mismas tecnologías y sistemas que contribuyen a que la sociedad sea más segura para todos.

Referencias

https://www.coresecurity.com/system/files/publications/2016/05/corelabs-ipcams-research-falcon-riva.pdf

https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

Fuentes:

[1]https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/mobile-white-paper-c11-520862.

[2]html https://www.coresecurity.com/advisories/hikvision-ip-cameras-multiple-vulnerabilities

[3]https://krebsonsecurity.com/2016/10/hacked-cameras-dvrs-powered-todays-massive-internet-outage/

[4]http://www.telecomtv.com/articles/iot/internet-of-things-to-reach-25-billion-devices-within-five-years-11931/

[5]https://www.dhs.gov/sites/default/files/publications/Strategic_Principles_for_Securing_the_Internet_of_Things-2016-1115-FINAL....pdf

[6]https://uk.sans.org/critical-security-controls

MOBOTIX desarrolla y fabrica sistemas de vídeo IP, gestión de vídeo y software de análisis en Alemania desde 2000.

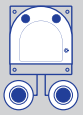
MOBOTIX destaca por su **elevado nivel de fiabilidad**. Todas las cámaras de exterior se someten a una prueba de esfuerzo a temperaturas comprendidas entre -30 °C y +60 °C (-22 °F y +140 °F). Sin componentes adicionales, sin calefacción ni refrigeración, y sin piezas móviles (por ejemplo, autoiris), prácticamente no requieren mantenimiento alguno.

MOBOTIX entrega un **paquete perfectamente adaptado**, desde la tarjeta microSD para la gestión del almacenamiento y el audio HD (micrófono y altavoz) con telefonía VoIP hasta el análisis de vídeo, el sistema de gestión de vídeo profesional y el software de detección de movimiento para reducir las falsas alarmas.

La **arquitectura descentralizada** implica que no se requiere un ordenador central y que la carga de la red es mínima. Las cámaras inteligentes de MOBOTIX procesan y almacenan los datos de imagen por sí mismas, desencadenan eventos y, en caso de acceso remoto, gestionan la frecuencia de vídeo y la resolución en función del ancho de banda disponible.

Los **sensores Moonlight 6 MP** y la **tecnología de imagen térmica** complementaria garantizan una detección fiable de objetos en movimiento, incluso en las condiciones de iluminación más complicadas y a gran distancia. Por consiguiente, es posible cubrir grandes superficies con tan solo unas pocas cámaras. Se necesitan menos cableado de alimentación, menos infraestructura de TI y menos fuentes de luz adicionales. Las cámaras MOBOTIX se alimentan vía PoE estándar y no requieren más de 4-5 W.

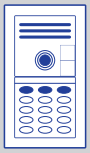
Un sistema de vídeo IP inteligente de MOBOTIX le permite **reducir los costes totales**. La inversión se paga sola al cabo de un breve periodo de tiempo, y el software y las actualizaciones gratuitas garantizan que su inversión sea a prueba de futuro.

Lente doble de exterior			Térmicas	
M16 AllroundDual	S16 FlexMount	D16 DualDome	M16 Thermal	S16 DualThermal
				
Resistente para condiciones extremas	Cámara dual flexible	Cámara dual modular	Térmica dual	Térmica dual

Lente sencilla de exterior			
M26 Allround	S26 FlexMount	Q26 Hemispheric	D26 Domo
			
Resistente en condiciones extremas	Discreta, análisis de vídeo	Discreta, análisis de vídeo	Domo fijo modular

Interior			
i26 Panorama	c26 Hemispheric	p26 Allround	v26 MiniDome
			
180° Hemispheric	Discreta, análisis de vídeo	Techo modular cámara	Vandalismo cámara

Módulos de puerta			MxDisplay+
Cámara	BellRFID	Teclado	Unidad remota
			

Kits de puerta			
Marco doble		Marco triple	
			

ES_11/17

MOBOTIX AG
Kaiserstrasse
D-67722 Langmeil (Alemania)
Tel.: +49 6302 9816-103
Fax: +49 6302 9816-190
sales@mobotix.com
www.mobotix.com

MOBOTIX