La importancia de conocer la seguridad de nuestros sistemas "closed-circuit television" (CCTV)

Gil V. Camareno Mendrell
Maestría en Ciencias de Computadoras
Nelliud Torres
Departamento de Ciencias de Computadoras
Universidad Politécnica de Puerto Rico

Resumen *— Este documento explora cómo las compañías manufactureras de cámaras y programas de seguridad aplican el concepto* seguridad *en sus programas y dispositivos. Se exploró cuáles son las normativas existentes que pueden aplicarse a la tecnología y el diseño de un sistema de seguridad de circuito cerrado de televisión (*closed-circuit television*, o CCTV). Se buscó información sobre esta normativa o estándar en la página de ISO, pero no se pudo encontrar un estándar que nos lleve a realizar un proceso evaluativo sobre cómo debe estar diseñado, configurado y protegido un sistema de seguridad CCTV que esté fuera de cualquier riesgo cibernético.*

No obstante, se encontraron otros estándares relacionados al tema de la seguridad, como el ISO 22311:2012, orientado a la definición de un perfil de interoperabilidad de exportación de datos digitales; el ISO 30137-1:2019, que aunque se indica que es para sistemas CCTV, su uso está orientado a los equipos de biometría utilizados para controles de acceso; el ISO/IEC 27037:2012, que contiene pautas para actividades específicas en el manejo de evidencia digital; y el ISO/IEC 24745:2022, que está dirigido estrictamente a la protección de los datos de la información capturada por un sistema biométrico. Existen otros estándares que tratan directamente el tema de la ciberseguridad: ISO/IEC TR 27103:2018, ISO/IEC 27102:2019, ISO/IEC TS 27100:2020 e ISO/IEC TS 27110:2021, pero ninguno de ellos está orientado a sistemas de video de vigilancia electrónica.

Palabras clave *— CCTV, ISO, riesgo cibernético, vigilancia electrónica*

INTRODUCCIÓN

Un sistema de televisión de circuito cerrado (*closed-circuit television*, o CCTV) opera de forma independiente o conectado a un sistema de información. Las funcionalidades pueden variar de acuerdo con el propósito y la aplicación del sistema. Estos sistemas permiten en todas sus versiones supervisar el funcionamiento o la condición de los equipos desde cualquier lugar donde se encuentre su usuario o administrador.

El campo de la seguridad ha aumentado de forma exponencial en los últimos años, ya que la tecnología actual ha permitido la integración de Internet y diversos dispositivos inteligentes. Las aplicaciones utilizadas y sus propósitos son variados y están presentes en aplicaciones corporativas y del hogar. Al igual que la evolución de la tecnología, y antes de la existencia de Internet, la mayor cantidad de funciones estaban basadas en redes cerradas en las cuales el acceso a los equipos se hacía de forma directa por cables coaxiales a un grabador. Las pocas conexiones remotas se realizaban a través de una línea de teléfono con una conexión de 28, 56 y 128 K, que se utilizaba para otros propósitos. La seguridad de estos equipos no era una prioridad, ya que todo estaba en un solo lugar, dada la tecnología existente en sus comienzos.

Los cambios tecnológicos como la integración de Internet como medio de interconexión de redes y los cambios de los equipos de coaxial a tecnología IP revolucionaron la industria de la seguridad. Luego de estos cambios, la seguridad comenzó a ser una preocupación para todos los manufactureros y usuarios de la tecnología CCTV. Cuando observamos una nueva configuración en la cual existen equipos como cámaras IP, conmutadores, servidores o sistemas de almacenamiento

conectados a una red externa, la seguridad se vuelve el tema principal. Al tener una cámara IP conectada a una red externa, existe un riesgo de seguridad y nos convertimos en blanco vulnerable de un ataque cibernético. Por esta razón, las cámaras conectadas a Internet necesitan atención adicional en cuanto a seguridad y configuración.

Una de las técnicas más fáciles mediante las cuales se pueden *hackear* las cámaras de seguridad es ingresando sus credenciales; así se tiene acceso a la red en la cual se encuentran sus cámaras y sistema informático. Los *hackers* utilizan nombres de usuario y contraseñas robadas que se pueden bajar de lugares como project-rainbowcrack.com o utilizando herramientas como John the Ripper o Brutus, entre muchas otras. Con esto se logra tener acceso al *hash* (figura 1), o sea, el algoritmo matemático o criptográfico que protege las contraseñas de los usuarios, el cual se usa para entrar de forma ilegal a los sistemas.

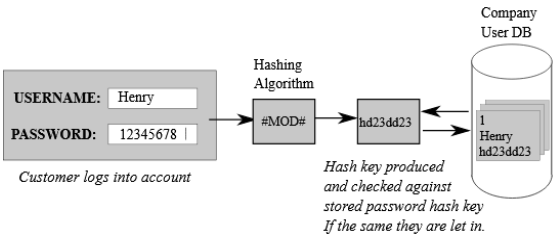

Figura 1
Cómo se usa el *hashing* al iniciar una sesión en los sitios

Con esto en mente, debemos ser conscientes de que cada día se encuentran nuevas vulnerabilidades. Por ello, nos toca investigar cuál es nuestro nivel de riesgo, teniendo presente que los ciberpiratas están atentos y se aprovechan de una vulnerabilidad para hacer daño no quizás a nuestro sistema de cámaras, pero quizás a algún otro equipo utilizando como entrada una cámara de seguridad. Al investigar sobre los temas de seguridad en los sistemas CCTV, no encontramos un estándar que indique cómo proteger nuestros sistemas de circuito cerrado. Entonces, esto crea una brecha de seguridad importante, ya que queda en manos del diseñador e instalador de los sistemas protegerlos de ataques cibernéticos. Tener acceso a una red no requiere de mucho conocimiento técnico, lo cual expone el sistema CCTV a que un ciberpirata tenga acceso al suyo. Una brecha de seguridad de este tipo puede exponer videos del interior de una tienda o de un banco, que pueden venderse para alguna actividad criminal. Una exposición de este tipo en una tienda o en un banco implicaría que se puede obtener acceso a la información de horarios, personal, dinero, personal y (lo más importante) la logística de operaciones del negocio. Este agujero no solo expone el sistema CCTV, sino que, si este está en el mismo segmento de la red interna de una empresa, por ejemplo, también podrían tener acceso a cualquier equipo dentro de la red.

Cada una de las compañías manufactureras de este tipo de producto o solución analizadas expone las mejores prácticas para los sistemas CCTV para manejar los temas de ciberseguridad. La mayoría presenta diferentes formas de proteger sus sistemas mediante políticas de seguridad en redes, criptografía, restricciones en los protocolos y métodos de autenticación. Los ciberpiratas están en constante monitoreo, buscando vulnerabilidades para acceder y poder adquirir información que puedan vender, usar en un secuestro para solicitar dinero o simplemente por hacer daño y acreditarse un evento de crimen cibernético.

Todo profesional del campo de la tecnología y sistemas CCTV debe proporcionar a sus usuarios el conocimiento suficiente para garantizar que su privacidad no se vea comprometida o expuesta. Además, con el concepto de traer su propio dispositivo (*bring-your-own-device*, o BYOD), se debe orientar a los usuarios sobre cómo interactuar con los equipos existentes y sacar el máximo de beneficios a la tecnología. El primer punto de entrada de cualquier sistema es una computadora física, remota o una página web, por lo que el uso de un nombre de usuario y una contraseña es mandatorio para acceder a cualquier sistema. Los administradores deben crear contraseñas extremadamente seguras que puedan complementarse con un sistema de doble autenticación. Asimismo, un dispositivo como una cámara de seguridad se debe proteger mediante una contraseña que contenga más de ocho dígitos

mínimos con una complejidad de caracteres que sea difícil de deducir. Si la configuración inicial de nuestro sistema de cámaras se queda tal como sale de la caja o se queda en su forma predeterminada por el manufacturero, estamos poniendo en riesgo nuestros dispositivos y la privacidad de nuestra información.

ANTECEDENTES

Un factor importante al seleccionar la tecnología CCTV como tema de investigación para este proyecto fue el aumento en la demanda de individuos y compañías preocupadas por su seguridad personal y la de su entorno. Hay compañías que se especializan en el sector corporativo y otras, en clientes residenciales. Entonces, de acuerdo con el sector del mercado de ese proveedor de servicios, usualmente se determina qué tipo de seguridad debe implementarse.

Según avanzaba la investigación, se encontró que el presupuesto asignado para este tipo de sistemas es muy bajo, por lo que se opta por adquirir equipos de seguridad en una megatienda. Son los mismos clientes quienes, a través de la experiencia y el conocimiento, se aventuran a instalar ellos mismo el equipo. Esta práctica es más común en ambientes residenciales y de pequeños negocios (*small and mid-sized businesses*, o SMB). En otros casos, los clientes buscan ayuda de compañías que realicen este tipo de instalación, pero, al informárseles del costo, recurren a otro tipo de profesional sin capacidad ni experiencia para realizar estas instalaciones. Esta práctica de contratar de personal sin conocimientos técnicos sobre tecnología crea un problema de seguridad y vulnerabilidad.

Esta investigación se enfoca en compañías manufactureras de tecnología CCTV: Hanwha Techwin; Axis Communications; GeoVision, con su afiliada en EE. UU. Vision Systems, Inc; Bosch; y Hikvision. Estas son empresas que llevan mucho tiempo en el campo de la seguridad y, al igual que otras empresas, han tenido situaciones de seguridad, como veremos. Se explicará cuáles son las mejores prácticas de estas empresas y qué problemas de seguridad han tenido en diferentes niveles y productos.

Ahora bien, a nivel residencial y de SMB, hay una cantidad de marcas genéricas que están por un corto periodo de tiempo.

Este es un posible escenario: una persona compra un sistema como un grabador de video de red (*network video recorder*, o NVR) en una megatienda y lo instala por su cuenta o lo hace un contratista sin experiencia. Surge una situación técnica con el equipo y no consiguen cómo resolverla. Solicitan el servicio de un profesional de sistemas de seguridad, quien encuentra que no hay documentación sobre cómo se configuró el sistema. El técnico de seguridad encuentra que la contraseña y el IP estaban configurados tal y como salieron de fábrica. Este NVR estaba publicado en Internet, ya que su contenido se accedía desde varios dispositivos remotos. Dejar el equipo como salió de la fábrica pudo haber comprometido la información de esa persona o comercio. Como método de validación de cómo su red podría estar expuesta, se puede utilizar un programa de escaneo de redes como Free IP Scanner 3.x.

La incertidumbre de la tecnología CCTV

El 68.4% de las cámaras de seguridad funcionan con una versión de *firmware* desactualizada, o sea, siete de cada diez cámaras están desactualizadas. [5] El *firmware* es un programa que trabaja directamente en una pieza de equipo y su sistema operativo proporciona instrucciones para que el dispositivo se comunique con otros dispositivos y realicen tareas y funciones previstas.

Una de cada cuatro empresas le deja al equipo la contraseña que vino del fabricante, lo que crea un problema de vulnerabilidad que los ciberpiratas conocen. Además, los fabricantes publican estas contraseñas en sus páginas web o en algún documento técnico, por lo que no hay que pasar mucho trabajo para tener acceso a esta información. Casi todos los dispositivos están conectados a una

red cableada o inalámbrica, lo que significa que tienen un *MAC address* y/o un IP por el cual los piratas pueden escanear y encontrar una brecha de seguridad para entrar en los sistemas. En [6] publican cámaras de diferentes partes del mundo en las que acceden sin la necesidad de utilizar algún programa maligno, demostrando el riesgo de utilizar los nombres de usuario y contraseñas proveídos por el manufacturero. Puede que algunas se hayan publicado a propósito y algunas que simplemente se instalaron sin utilizar las mejores prácticas al momento de diseñar e instalar este tipo de tecnología.

Tomando todo esto en consideración, las acciones de sabotaje a gobiernos, empresas comerciales o cualquier tipo de institución pueden ser objetivos de un ataque cibernético. En la actualidad, cualquier individuo con un conocimiento limitado sobre sistemas de información puede adquirir equipo y programas que se pueden descargar de Internet para *hackear* un sistema. En Internet se consigue todo tipo de herramientas de piratería, foros en la *dark web*, videos y adiestramientos en línea para entender y ejecutar las herramientas que se utilizan para *hackear*.

NORMATIVAS DE LAS COMPAÑÍAS

Hikvision

Esta compañía tiene en su página de Internet un área dedicada a la ciberseguridad donde incluye varios enlaces donde se encuentran sus mejores prácticas. En una búsqueda de los documentos relacionados al tema, solo se encontraron cinco artículos, todos de 2018 y ninguno actualizado desde esa fecha. Existen tres enlaces adicionales que están directamente relacionados al tema de los equipos necesarios para que un sistema de seguridad funcione como solución, como el equipo NVR, el programa de manejo y las cámaras de seguridad. El documento que está relacionado al programa de manejo solo tiene cuatro secciones. Las primeras dos secciones son reglas básicas del sistema operativo y redes.

El capítulo 3 de [7] se refiere al concepto HikCentral Security Configuration. [8] En esta sección, se refieren a la utilización de puertos *gateways* específicos del manufacturero y recomendaciones para cambiar ciertos parámetros *default*. Referencias relacionadas a puertos de redes tema suelen estar disponibles en Internet. Se pueden aplican reglas a nivel del directorio activo (*active directory*, o AD). Entre las reglas que se pueden ejercer, se encuentran bloquear la cuenta después de varios intentos de acceder a la cuenta, complejidad de contraseña y tiempo de validez. El capítulo 4 del mismo documento habla de recomendaciones adicionales de seguridad que son básicas en cualquier red corporativa regular.

En el documento que define las mejores prácticas sobre eel dispositivo de la cámara, las reglas son muy similares a las del programa. Las únicas excepciones son la parametrización de las cámaras y que se recomienda que se actualice el equipo regularmente con la última versión de *firmware*. Sobre el NVR, las políticas de seguridad son repetitivas a las anteriormente descritas, con excepción de la sección 2.6, donde se incluyen instrucciones para proteger los videos. Es un proceso, al parecer, bien general, ya que trabaja con un *file management*, mismo concepto del *file explorer* de Windows, pero dentro de un aplicativo propietario de Hikvision.

Geovision

La compañía tiene una página que hace referencia a ciberseguridad, pero con muy poca información relacionada al tema. En esta página solo se encuentran una breve explicación de las políticas relacionadas a vulnerabilidades y unas advertencias de seguridad que datan de julio de 2021 a abril de 2022. De los únicos seis documentos, cuatro están asociados a vulnerabilidades; uno, a un incidente de seguridad en sus plataformas de GV-Cloud Center y myGVcloud; y el artículo más reciente, de abril de 2022, detalla cómo deben generarse las contraseñas. El documento no detalla si el artículo se debe a que hubiese alguna exposición. En la

sección de preguntas frecuentes, bajo la categoría *Security*, no se pudieron identificar documentos relacionados a seguridad.

La compañía provee un correo electrónico para que los usuarios reporten anomalías con sus productos. Muchas otras compañías utilizan de manera similar el apoyo de los usuarios para identificar errores o vulnerabilidades en sus sistemas o equipos.

Axis

Esta compañía tiene un área dedicada a la ciberseguridad donde provee la información necesaria para entender su misión y visión sobre la ciberseguridad. Al final de su página tienen dos guías dirigidas al tema de ciberseguridad.

El documento *Hardening Guide* [9], fechado junio de 2020, contiene los fundamentos básicos de seguridad. A diferencia de los dos manufactureros anteriores, este documento menciona que las cámaras de esta marca no funcionarán hasta que se configure la contraseña administrativa. Además, indica cuáles servicios están disponibles pero deshabilitados, como los servicios de FTP, SSH, Audio QoS y ONVIF. Estos equipos tienen un módulo de almacenamiento seguro para las llaves de seguridad (TPM) y menciona los puertos TCP y UDP que están abiertos de fábrica.

El documento *Best Practices eMagazine* [10] da consejos de un marco sólido para la protección de su sistema. Desarrollaron un concepto de *framework* de diez pasos que detallan conceptos generales de seguridad.

Encontramos artículos adicionales, como un blog sobre ciberseguridad, una página de seguridad de productos y una página con un archivo de datos sobre vulnerabilidades. En el blog hay mucha información de diversos temas, creados y publicados por diversas fuentes colaborativas. La página de seguridad de productos provee información sobre ataques y vulnerabilidades encontradas por la empresa como externas. Este manufacturero provee un servicio llamado Axis Security Notification Service con el cual envían a sus suscriptores correos electrónicos relacionados a productos, programas y servicios. La página relacionada a las vulnerabilidades detalla cómo surgió el evento y cómo se mitigó. Proveen suficiente información para mitigar cualquier riesgo cibernético.

Bosch

Esta compañía, fundada en 1886, es la más longeva y tiene una cartera de productos de tecnología. Algunos de los mercados e industrias donde tiene presencia son aeropuertos, estaciones de trenes, integración de plataformas como detección de incendios, sistemas de instrucción, videovigilancia y sistemas de acceso. No se encontró un área en su portal que esté directamente orientada a la ciberseguridad. En su lugar, tiene dos páginas que cubren los temas de seguridad de productos y seguridad de datos. En la página de seguridad de productos, se incluyen datos relacionados a vulnerabilidades que han tenido, específicamente una relacionada a Apache Log4j. En caso de que surja alguna situación con alguno de sus productos, ofrecen consultas mediante correo electrónico con su Product Security Incident Response Team. En su página del área de seguridad de datos solo hay datos generales y de un concepto llamado seguridad de extremo a extremo (*end-to-end security*), y enfatizan en cómo ellos aseguran las cámaras, dispositivos de almacenamiento y redes, y cómo apoyan la *public key infrastructure*. Solo se encontró un documento de dos páginas que explica los cuatro conceptos mencionados anteriormente.

Además de la página principal, se encontraron otras dos referencias con información adicional. En esta área, se encontró una política que consiste en ingresar una contraseña desde la inicialización del equipo. Si la cámara es nueva, se ingresa una contraseña y se continúa el proceso de instalación. De otro lado, si el equipo tiene que ser reconfigurado, hay que realizar una configuración predeterminada de fábrica. El procedimiento a seguir es el siguiente: el usuario se comunica con su división de apoyo técnico, que le solicitarán la orden de compra con la cual se adquirieron los

equipos. Una vez validada la información de compra, ellos le proveen al usuario un código que se ingresa en un campo del equipo. Este código desbloquea la cámara que había quedado completamente deshabilitada. Este es un procedimiento que garantiza que el equipo está siendo reiniciado por el verdadero dueño autorizado a realizar este proceso.

Hanwha Techwin

Está compañía, fundada en 1977, es la segunda en antigüedad de las empresas seleccionadas. Tiene un área dedicada a la ciberseguridad. Muestra más información que las compañías evaluadas hasta el momento. Sus prácticas están basadas en políticas y reglas de seguridad como conexión en formato https://, servicios web como Telnet/SSH, encriptación de *firmware* y bases de datos. Tienen un equipo se seguridad llamado S-CERT [10] que está dedicado a la revisión de intrusiones proactivas y a su vez el usuario se puede comunicar a un chat de soporte para servicio en línea o fuera de horas laborables. Incluyen servicios de educación de ciberseguridad de sus equipos, que pueden ser presenciales o en línea, orientados a las mejores prácticas disponibles. Tienen dos áreas de soporte: un área para visitas generales y otra para socios de negocio. En su página tienen publicados *white papers* relacionados a vulnerabilidades reportadas, pruebas de penetración y guías de ciberseguridad, así como documentos sobre cómo mejorar la red, el NVR y servicios de Simple Network Management Protocol (SNMP).

Dos documentos (*Network Hardening Guide* [12] y *Network Hardening Guide (NVR)* [13]) contienen información sobre cómo deben configurarse los equipos utilizando las mejores prácticas. No obstante, las mejores prácticas a las cuales se refieren son de *networking*. Explican cómo estas prácticas minimizan que usuarios malintencionados ingresen a sus equipos**.** Estos equipos, como cualquier dispositivo de red, tienen opciones para realizar múltiples funciones. Sin embargo, Hanwha Techwin documenta que se debe deshabilitar como medio de prevención, ya que la mayoría de los ciberataques se basan en información pública que se puede conseguir en Intenet. También, como parte de su esfuerzo por crear un ambiente seguro utilizando protocolos existentes, generaron unas guías de uso seguro de SNMP. Este documento le indica al usuario la manera de implementar el servicio de SNMP, que es un estándar de las comunicaciones definido por la Junta de Arquitectura de Internet (IAB) en RFC1157 para el intercambio de información de gestión entre dispositivos de red. En este documento, se recomienda el realizar un *firmware update* a los equipos e implementar el uso del SNMP v3, ya que esta versión tiene tecnología de autenticación y encriptación.

Seguridad de dispositivos

Se buscó y se analizó información relacionada a la vulnerabilidad de los equipos de videoseguridad. Se desprende de los hallazgos que el dispositivo con mayor vulnerabilidad es la cámara de seguridad. Este equipo se ha vuelto muy popular; la necesidad de sentir seguridad ha obligado a compañías y a personas a adquirir diversos tipos de sistemas de seguridad.

Los equipos están conectados a la red a través de un cable de Ethernet o conexión inalámbrica. Como parte del análisis y de validar cuán seguras son nuestras cámaras, se analizaron varios programas para el escaneo de redes, entre los cuales se seleccionó la herramienta Shodan. [14]

Esta aplicación es un buscador de dispositivos que están conectados a la red, como computadoras, servidores, enrutadores o cualquier equipo que tenga un puerto de red, incluida una cámara de seguridad. Hay artículos en los que se comenta que es un buscador orientado al *hacking*. Una vez registrado en el aplicativo, se observó que no había muchas funcionalidades que se pudieran llevar a cabo con la versión gratuita. Se procedió a revisar las opciones adicionales y se seleccionó una que nos fuera útil para el propósito investigativo.

Comenzamos a realizar búsquedas relacionadas a cámaras de seguridad. En nuestra primera búsqueda, con las palabras “ip camera”, se encontró

una cantidad considerable de dispositivos a lo largo del mundo. Se identificó el área geográfica de Puerto Rico y se analizaron las incidencias encontradas, identificadas en rojo en la figura 2.

Figura 2
Incidencias encontradas en Puerto Rico

Localizamos un área en la zona metropolitana donde se encontraron dispositivos con puertos abiertos. Se seleccionó un dispositivo que estaba conectado a la red de Internet local. Se identificaron dos puertos abiertos: puerto 80 y puerto 554 (figura 3). El puerto 80 se utilizaba para la navegación en la web no segura a través de *Hypertext Transfer Protocol* (HTTP). El puerto 554 era utilizado por un protocolo de transmisión en tiempo real (*Real-Time Streaming Protocol*, o RTSP). Este protocolo permite a un usuario obtener una transmisión de video en vivo desde su cámara y verla desde diferentes dispositivos y programas. Sus usos son variados, pero a nivel de CCTV, su principal uso es obtener una transmisión de video de una cámara a un NVR, *software* de visualización o incluso soluciones de automatización del hogar.

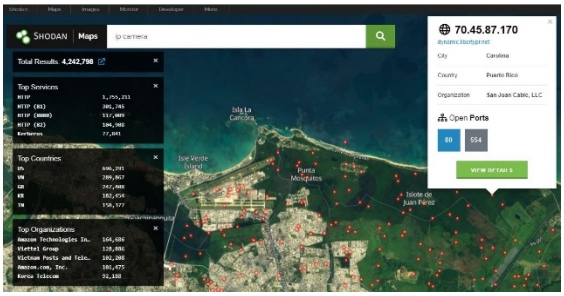

Figura 3
Puertos abiertos en dispositivo conectado a red local

En el detalle de los puertos, podemos ver que se identifica el equipo como una cámara IP de la marca Hikvision (figura 4). Se nos provee información sobre las versiones, la estructura y los archivos ActiveX, aplicaciones en los sitios web que proporcionan contenido de video. Esta información es importante, ya que un *hacker* puede identificar información sobre vulnerabilidades de alguno de estos componentes que se encuentran aquí listados. Esto, a su vez, le serviría para realizar un *exploit* para ingresar en el equipo.

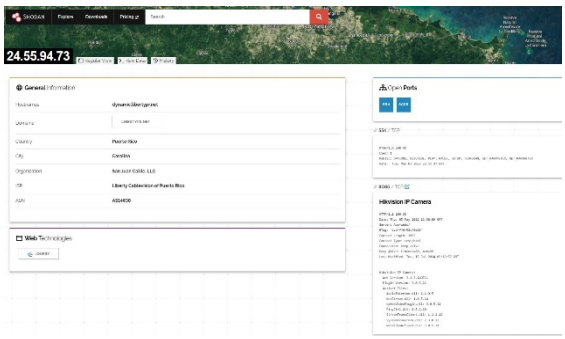

Figura 4
Información sobre cámara IP Hikvision

La versión básica de este aplicativo nos provee mucha información. Con ella se encontraron imágenes de cámaras que están expuestas. En el buscador del aplicativo, se realizó una búsqueda con las palabras “ip camera”, y se identificaron varias imágenes en diversas localizaciones (figura 5).

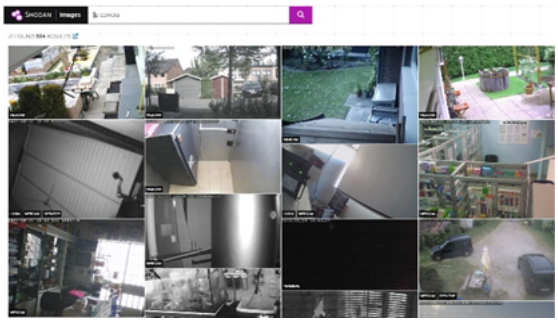

Figura 5
Imágenes identificadas en cámaras expuestas

Para conocer más información sobre las imágenes, se seleccionó la primera imagen de las cámaras que se encontraron (figura 6). Esta cámara resultó estar en Alemania y pertenecer a una compañía llamada Arcor AG, con oficinas en Barcelona. El dispositivo es una cámara modelo Apexis APM-H602-MPC. En este caso, se encontraba abierto el puerto 5060, que se utiliza en comunicaciones para enlaces VoIP y PBX y que

también se usa para conectarse a servidores. El puerto 8001 estaba abierto también. El uso de este puerto podría estar relacionado a acceder videos a través de un teléfono inteligente para conectarse al servidor de grabaciones.

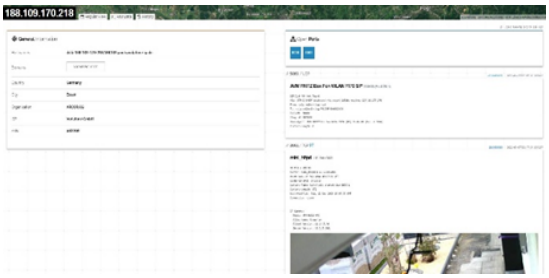

Figura 6
Imagen de cámara

El análisis realizado nos muestra ejemplos reales de la problemática y gravedad de un sistema de videovigilancia mal configurado. Esta aplicación nos puede ayudar o nos puede perjudicar, según el uso y las circunstancias. Para un usuario de seguridad, nos ayuda a identificar vulnerabilidades, y a un ciberpirata le ayuda a identificar una puerta o vulnerabilidad expuesta para ingresar a nuestros sistemas. Este aplicativo tiene la capacidad de buscar todo tipo de puertos. Se realizó una búsqueda del puerto 3389, protocolo de control de transferencia (*Transfer Control Protocol*, o TCP), que se utiliza para acceso remoto mediante la plataforma Windows. Se encontró una máquina con sistema operativo Windows 11 con información detallada del usuario. Una estación como esta puede tener acceso a nuestra red de cámaras, creando un riesgo adicional si estuviera en el mismo rango o segmento de IP corporativo.

RESULTADOS

Según los datos recopilados, observamos que existe una problemática de seguridad y vulnerabilidad en los sistemas de videovigilancia. Cuando se describe un sistema de videovigilancia a nivel de componentes, nos referimos a un NVR, un *digital video recorder* (DVR), un servidor de grabaciones, un *firewall* o un enrutador *switch* y una cámara. El uso del sistema dependerá de la combinación de los dispositivos anteriormente mencionados. Regularmente, si el equipo es corporativo, los equipos están dentro de un centro de cómputos donde están protegidos físicamente. Además, los equipos están respaldados y hay personal que los monitorea constantemente. En un ambiente corporativo, el equipo está seguro, pero no así en otros entornos. Al analizar los dispositivos, se pudo determinar que la cámara de seguridad es la de mayor riesgo. En un ambiente de videoseguridad, este dispositivo está en el interior o exterior de una estructura o instalada en un poste.

Según la información y el análisis realizado, la mayor incidencia de riesgo cibernético es doméstica. La aplicación Shodan mostró una cantidad considerable de cámaras en todo el mundo que tienen su nombre de usuario y contraseña *default*. Esta información puede ser fácilmente localizada en Internet con poco conocimiento del tema. Si agregamos la falta de controles por dejar un equipo en modo *default*, las convierte en un objetivo probable.

Cambios en la seguridad

Preocupados por las incidencias de intrusiones a los sistemas tecnológicos, los manufactureros de sistemas de videovigilancia realizaron cambios en sus políticas de seguridad. El cambio más significativo fue la modificación en las credenciales de la cámara de seguridad. Originalmente, en las versiones de *firmware* de las cámaras que formaron parte de este estudio venían con su nombre de usuario y contraseña *default*. Estas versiones se podían dejar tal cual, pero esto hace las cámaras vulnerables a un ataque cibernético. Aunque las cámaras siguen viniendo con un nombre de usuario y contraseña *default*, ahora es requisito cambiar la contraseña de la cámara, de modo que el proceso de instalación no pueda continuar hasta que se cambie. Esto añade una capa de seguridad a nivel del *endpoint*, o sea, la cámara de seguridad, que no existía cuando se lanzó esta tecnología. Las compañías que fueron ejes de este trabajo investigativo implementaron el cambio. El nuevo procedimiento requiere que la contraseña contenga letras minúsculas, letras mayúsculas, números y

caracteres especiales, con la excepción de una de las compañías que no permite la incorporación de caracteres especiales en la contraseña.

Nuevos desafíos de la tecnología

El establecimiento de este nuevo proceso para la construcción de la contraseña con mayor complejidad por parte de estos manufactureros adelanta los problemas existentes de seguridad que implicaba la contraseña *default.* Existe un nuevo desafío con relación al nuevo procedimiento de las contraseñas. Debido a la falta de una normativa o estándar para este proceso, debemos hacer referencia al manual del usuario de cada manufacturero para entender cómo ellos aplican este nuevo procedimiento. Hasta ahora, cada compañía ha implementado el cambio del requisito de la contraseña al momento de iniciar el equipo, pero de forma distinta. Las variaciones en los cambios son en estructura; largo del campo; y la cantidad de números, letras y caracteres especiales que se pueden utilizar. En la industria existe un concepto que se llama "ser o no ser" (*to be or not to be*) y las reglas básicas de cómo generar una buena contraseña utilizando aplicativos para la autogeneración de contraseñas. Esto sería una buena práctica, debido a que así se pueden autogenerar las contraseñas para nuestras cámaras y asignarlas a cada dispositivo. Esta funcionalidad reduciría el riesgo de que nuestro equipo se comprometa.

RECOMENDACIONES

Existen varios mercados y aplicaciones en los que se pueden utilizar los sistemas CCTV, como lugares públicos como centros comerciales, cascos urbanos, carreteras, transportación, corporaciones gubernamentales y privadas, y aplicaciones en el hogar. Nuestra recomendación inicial es localizar una escuela o universidad que tenga un currículo dirigido a los profesionales de la seguridad CCTV. Este currículo podría incluir temas sobre sistemas de seguridad, redes, seguridad y ética. Nuestra segunda recomendación sería crear un comité de profesionales en esas áreas para la creación de una colegiatura con un examen teórico, mediante la cual se pueda emitir una licencia. Como parte de la colegiatura, los profesionales de seguridad deberían realizar estudios continuos para mantenerse actualizados con la tecnología. Como última recomendación, el técnico debería tener conocimientos sobre ciberseguridad, debido a que el tema crece constantemente y los ciberpiratas buscan constantemente oportunidades para lograr sus objetivos.

CONCLUSIÓN

Según va avanzando la tecnología, la seguridad informática debe evolucionar con ella. La información es un activo que transciende individuos y compañías, ya que salvaguardar los datos es de suma importancia. Los sistemas de videoseguridad no están excluidos de ser blancos de ataques cibernético. La investigación demuestra que estos riesgos surgen debido a individuos que desconocen el riesgo de la exposición de sus datos y cómo se puede exponer su privacidad. Este estudio muestra los cambios en los procedimientos para instalar cámaras de videovigilancia, en los que se obliga a cambiar la contraseña que viene de fábrica. Este cambio ha resuelto el tema de la contraseña por defecto, pero al no existir un estándar, cada manufacturero lo ha diseñado en base a sus mejores prácticas. Para lograr uniformidad en el patrón para la creación de la contraseña, sugiero un modelo estandarizado o de autogestión que sea más robusto. En un modelo estandarizado, la sugerencia sería una contraseña no menor de doce caracteres que incluya números, letras mayúsculas, letras minúsculas y caracteres especiales.

Los manufactureros pueden integrar la funcionalidad de autogestión de contraseñas aleatorias como un módulo dentro de su sistema de manejo. Este algoritmo podría ser una combinación del número de serie de la cámara y el *MAC address* de la tarjeta de red del grabador. Cuando estos dos

campos se unen, le aplicaríamos el método de encriptación Ceasar Cipher (figura 7).

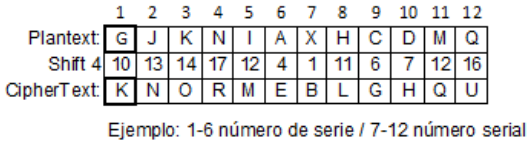

Figura 7
Método de encriptación Ceasar Cipher

Los caracteres identificados como CipherText en la figura 7, KNORMEBLGHQU, serían la contraseña que aplicaríamos a la cámara de seguridad y sincronizando con el sistema de manejo del sistema de cámaras de seguridad. Este algoritmo se puede desarrollar fuera del entorno de los manufactureros. La implementación y el costo de implementar funcionalidades efectivas son costosas, pero el costo de la pérdida o robo de la información puede ser más oneroso que la propia solución.

REFERENCIAS

[1] *Societal Security — Video-surveillance — Export Interoperability*, ISO 22311:2012, nov. 2011 [En línea]. Disponible: https://www.iso.org/standard/53467.html

[2] *Information Technology — Use of Biometrics in Video Surveillance Systems — Part 1: System Design and Specification*, ISO/IEC 30137-1:2019, mayo 2019 [En línea]. Disponible: https://www.iso.org/standard/64935.html

[3] *Information Technology – Security Techniques – Guidelines for Identification, Collection, Acquisition, and Preservation of Digital Evidence*, ISO/IEC 27037:2012, nov. 2012 [En línea]. Disponible: https://www.iso.org/standard/44381.html

[4] *Information security, cybersecurity and Privacy Protection — Biometric Information Protection*, ISO/IEC 24745:2022, feb. 2022 [En línea]. Disponible: https://www.iso.org/standard/75302.html

[5] D. Chaverra Agudelo, "Aumenta el riesgo de ataques cibernéticos en cámaras de seguridad", *Ventas de Seguridad*, 10 de dic 2019 [En línea]. Disponible: https://www.ventasdeseguridad.com/2019121011816/noticias/empresas/aumenta-el-riesgo-de-ataques-ciberneticos-en-camaras-de-seguridad.html

[6] Insecam, "Live cameras directory." Accedido el 17 de mayo de 2022 [En línea]. Disponible: http://www.insecam.org/

[7] *HikCentral V1.1.x for Windows Hardening Guide*, Hikvision. Accedido el 17 de mayo de 2011 [En línea]. Disponible: https://www.hikvision.com/es-la/support/cybersecurity/best-practices/hikcentral-v1-1-x-for-windows-hardening-guide/

[8] *HikCentral Security Configuration*, Hikvision. Accedido el 17 de mayo de 2011 [En línea]. Disponible: https://www.hikvision.com/content/dam/hikvision/en/support/download/vms/hikcentral-v2-0/HikCentral-V2.0-Hardening-Guide_20210118.pdf

[9] *AXIS OS Hardening Guide*, Axis. Accedido el 17 de mayo de 2011 [En línea]. Disponible: https://help.axis.com/axis-os-hardening-guide

[10] *Best Practices eMagazine*, Axis. Accedido el 17 de mayo de 2011 [En línea]. Disponible: https://www.axis.com/dam/public/8d/71/65/partners-in-protection:-insights--inspiration-from-the-world-of-cybersecurity-emagazine-en-US-334194.pdf

[11] *Hanwha Techwin's S-CERT*, Hanwha. Accedido el 17 de mayo de 2011 [En línea]. Disponible: https://www.hanwhasecurity.com/wp-content/uploads/Graphics/Whitepapers/Cybersecurity_Whitepapers/hanwha_techwin_cyber_security_enhancement_activity_20180808.pdf

[12] *Network Hardening Guide*, Hanwha. Accedido el 17 de mayo de 2011 [En línea]. Disponible: https://www.hanwhasecurity.com/cybersecurity/

[13] *Network Hardening Guide NVR*, Hanwha. Accedido el 17 de mayo de 2011 [En línea]. Disponible: https://www.hanwhasecurity.com/cybersecurity/

[14] Shodan, "Homepage." Accedido el 17 de mayo de 2011 [En línea]. Disponible: https://www.shodan.io/explore