La importancia de conocer la seguridad de nuestros sistemas "Closed-Circuit Televisión – CCTV"

Autor: Gil V. Camareno Mendrell
Mentor: Dr. Nelliud D. Torres Batista
Department of Computer Science

Resumen

Este documento está orientado a como las compañías manufactureras de cámaras y programas de seguridad aplican el concepto de seguridad en sus programas y dispositivos. Para conocer como es aplicado este concepto se comenzó con la exploración de cuáles son las normativas existentes que puede ser aplicadas a la tecnología y diseño de un sistema de seguridad de Circuito Cerrado de Televisión "CCTV – Close-Circuit Television" (Figura 1), como comúnmente se le llama en el campo de la seguridad. Se iniciaron los trabajos buscando información de esta normativa o estándar en la página www.iso.org. En esta búsqueda no se pudo encontrar información sobre un estándar que nos lleve a realizar un proceso evaluativo relacionado a cómo debe estar diseñado, configurado y protegido un sistema de seguridad CCTV que este fuera de cualquier riesgo cibernético. Durante el proceso se encontraron otros estándares relacionados al tema de seguridad, pero ninguno de ellos está orientados a sistemas de video vigilancia electrónica.

Figura 1
Componentes básicos de un Sistema de Video Seguridad

Introducción

Un sistema de televisión de circuito cerrado "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 uso que se le vaya a dar al sistema. Estos sistemas en todas sus versiones permiten supervisar el funcionamiento o la condición de los equipos desde cualquier punto donde se encuentre su usuario o administrador. El campo de la seguridad a aumentado de forma exponencial en los últimos años, ya que la tecnología actual ha permitido la integración de la Internet y diversos dispositivos inteligentes. Las aplicaciones utilizadas y su propósito son variados y están presentes en aplicaciones corporativas, así como aplicaciones de hogar. Al igual que la evolución de la tecnología y previo a la existencia de la Internet la inmensa cantidad de funciones estaban basadas en redes cerradas donde el acceso a los equipos se hacía de forma directa en cables coaxiales directamente a un grabador. Los cambios tecnológicos como la integración de la Internet como medio de interconexión de redes y los cambios de los equipos de coaxial a tecnología IP revolucionó 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 de CCTV. Cuando observamos una nueva configuración donde existen equipos como cámaras IP, conmutadores, servidores, sistema de almacenamiento conectados a una red externa, la seguridad se torna el tema principal. Al tener una cámara IP conectada a una red externa, existe un riesgo de seguridad y nos convertimos en un blanco vulnerable para un ataque cibernético. Por esta razón, las cámaras conectadas a la Internet necesitan una atención adicional en cuanto a seguridad y configuración. Un sistema de cámaras de seguridad donde la comunicación esta codificada (Figura 2) y, aunque estén espiando la red capturando los paquetes que pasan por el "router" o "switch", según sea el caso el usuario no autorizado es incapaz de descifrarla.

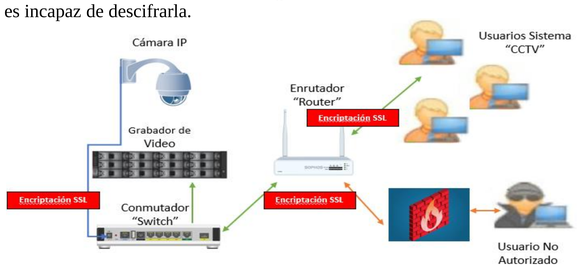

Figura 2
Diagrama de comunicación codificada.

Incertidumbre de la tecnología CCTV

Según un artículo publicado por la compañía Genetec [1] dedicada a la innovación de nuevos productos en el área de seguridad física, servicios y soluciones informo en diciembre 2019 que se encontró que el 68.4% [1] de las cámaras de seguridad funcionan con una versión de "firmware" desactualizada lo que se traduce a siete de cada diez cámaras están desactualizadas. El firmware es programa que trabaja directamente en una pieza de equipo y su sistema operativo proporciona instrucciones para que el dispositivo se comunique con otros dispositivos realicen tareas y funciones previstas. En este mismo estudio he de indicar que uno de cada cuatro empresas conservan la contraseña que vino del fabricante lo que crea un problema de vulnerabilidad que los piratas cibernéticos conocen. Entonces, podemos deducir que los objetivos de los piratas informáticos son muy distintos de lo que es hoy día. La razón es sencilla, casi todos los dispositivos están conectados a una red cableada o inalámbrica lo que significa que tienen una MAC Address y/o una IP por el cual los piratas puede escanear y encontrar una brecha de seguridad para entrar a los sistemas. Tomando en consideración los datos presentados, las acciones de sabotaje a gobiernos, empresas comerciales o cualquier tipo de institución pueden ser objetivos de un ataque cibernético.

Normativas de las compañías

Los fabricantes para ajustarse a la nueva tecnología realizaron cambios en su forma de aplicar la seguridad a sus sistemas de video vigilancia. Las compañías que fueron integrantes de este estudio Hikvision, Geovision, Axis, Bosch y Hanwha Techwin realizaron cambios orientados a la ciberseguridad. Sus prácticas se enfocaron en políticas y reglas de seguridad como conexión en formato https://, servicios web como Telnet/SSH, encriptación de "firmware" y bases de datos. Crearon páginas con diferentes tipos de contenidos como guías de Ciberseguridad, "White Papers" relacionados a temas de seguridad y documentos de cómo mejorar la red, el NVR y servicios de SNMP. Además, crearon equipos de soporte técnico en línea o por correo electrónico donde se pueden reportar, preguntar y resolver todo tipo de temas relacionados una situación o problema con su sistema.

Seguridad a nivel de dispositivos

Como parte de este trabajo investigativo se analizó y se buscó información relacionada a la vulnerabilidad de los equipos de video seguridad. Se desprende de los hallazgos encontrados que el dispositivo con mayor probabilidad de vulnerabilidad es la cámara de seguridad. La popularidad de este equipo se ha vuelto muy popular, basado en la necesidad personal de sentirse seguros ha obligado a las compañías y personas a adquirir diversos tipos de sistemas de seguridad. Los equipos están conectados a la red a través de un cable "Ethernet" o conexión inalámbrica. Como parte de análisis y validar cuan seguro son nuestras cámaras, se analizaron varios programas para el escaneo de redes y para este trabajo se seleccionó la herramienta "Shodan". [2] (Figura 3)

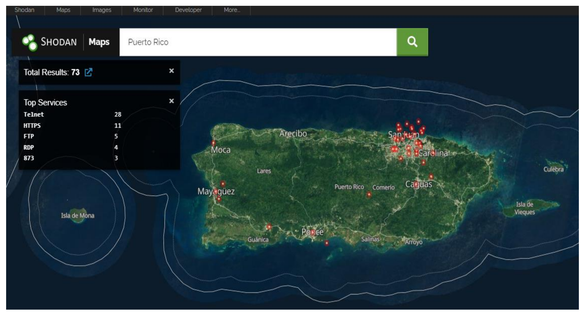

Figura 3
Pantalla de búsqueda de programa Shodan

Se realizó una búsqueda por cámaras "IP" (Figura 4) en el cual se encontró una cantidad considerable de dispositivos a través del mundo. Se identifico el área geográfica de Puerto Rico y se analizaron las incidencias encontradas que se identifican en color rojo.

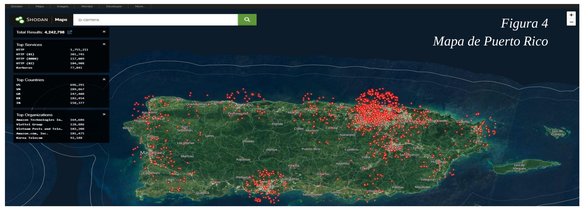

Figura 4
Mapa de Puerto Rico

Se seleccionó un dispositivo (Figura 5) el cual está conectado a la red de Internet local identificando dos puertos abiertos; puerto 80 y puerto 554.

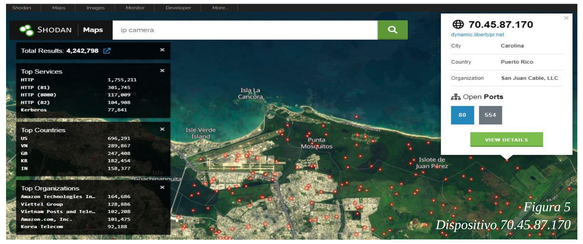

Figura 5
Dispositivo 70.45.87.170

Identificamos el equipo (Figura 6) como una cámara IP de la marca Hikvision donde nos provee información de las versiones, estructura y los archivos "ActiveX".

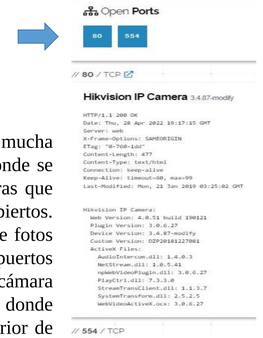

Figura 6
Descripción de dispositivo 70.45.87.170

Este aplicativo nos provee de mucha información con una versión básica donde se pudieron encontrar imágenes de cámaras que están expuestas y otros puertos abiertos. Realizamos otra búsqueda en el área de fotos y se identificó una cámara con los puertos 5060 y 8001. (Figura 7) Esta cámara pertenece una compañía en Alemania donde se puede observar una imagen del interior de alguna área de su propiedad.

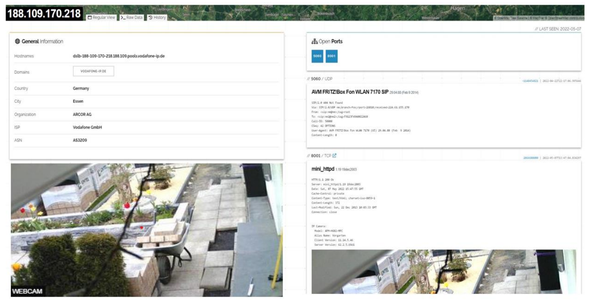

Figura 7
Ejemplo de cámara con Puerto 5060 y 8001 abiertos

El análisis realizado nos muestra ejemplos reales de la problemática y gravedad de un sistema de video vigilancia mal configurado. Esta aplicación nos puede ayudar o nos pudiera perjudicar, según el uso y las circunstancias de para que se esté utilizando. Para un usuario de seguridad, nos ayuda a identificar vulnerabilidades y para un pirata cibernético le ayuda a identificar una puerta o vulnerabilidad expuesta para ingresar a nuestros sistemas.

Resultados

Según los datos recopilados en la sección de "seguridad a nivel de dispositivos" observamos que existe una problemática de seguridad y vulnerabilidad en los sistemas de video vigilancia. El uso de estos sistemas dependerá del mercado vertical donde será instalado. Regularmente si es uno corporativo, los equipos están dentro del centro de cómputos donde están protegidos físicamente, respaldados y personal monitoreándolos constantemente. En un ambiente corporativo el equipo está seguro, pero no así en otros entornos. Concluido es trabajo se pudo determinar que la cámara de seguridad es la de mayor riesgo.

Cambios en la Seguridad

Los manufactureros de sistemas de video vigilancia preocupados por las incidencias de intrusiones a los sistemas tecnológicos, realizaron cambios en sus políticas de seguridad. El cambio más significativo fue la modificación en las credenciales de la cámara de seguridad. Las versiones de "firmware" de las cámaras salían de fabrica con su usuario y contraseña "default". Esto era una práctica que dejaba vulnerable la cámara para un ataque cibernético. Ahora, se sustituyó el usuario y contraseña "default" y ahora es requisito cambiar la contraseña de la cámara. Este cambio se implemento con el propósito de no continuar el proceso de instalación hasta que se cambie el mismo y no permite que se deje la contraseña de fábrica.

Nuevos desafíos de la tecnología

El establecimiento de este nuevo proceso para la construcción de la contraseña con mayor complejidad por parte de los manufactureros adelanta los problemas existentes de seguridad que implicaba la contraseña "default". Debido a la falta de una normativa o "standard" para este proceso, tenemos que hacer referencia al manual del usuario del manufacturero para entender cómo aplicaron este nuevo procedimiento. Las compañías evaluadas implementaron el cambio de la contraseña al momento de iniciar el equipo, pero de forma distinta. Las variaciones fueron en estructura, largo del campo y la cantidad de números, letras y caracteres especiales que pueden ser utilizados. En la industria existe un concepto que se llama ser o no ser y las reglas básicas de como generar una buena contraseña utilizando aplicativos para la autogeneración de contraseñas que pidieron ser implementadas como parte de los cambios.

Agradecimientos

Quiero agradecer al Dr. Nelliud D. Torres Batista por guiarme en esta investigación. Además, agradezco a todos los profesores del Departamento de Ciencias de Computadoras que me han brindado el conocimiento y las oportunidades de aprendizaje ofrecidas durante todos mis cursos.

Conclusión

La seguridad informática según va avanzando la tecnología, esta tiene que evolucionar con ella. La información es un activo que transciende individuos como compañías ya que la importancia de proteger y salvaguardar sus datos es de suma importancia. Los sistemas de video seguridad no están excluidos de ser un blanco para un ataque cibernético. Este cambio resolvió el tema de la contraseña por defecto, pero al no existir un estándar cada manufacturero lo diseño distinto. Una sugerencia para lograr una uniformidad en el patrón para la creación de la contraseña se pude modelo estandarizado definiendo su estructura, largo y contenido. Un modelo de autogestión de contraseñas aleatorias pudiera 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 aplicáramos el método de encriptación "Ceasar Cipher". (Figura 8)

	1	2	3	4	5	6	7	8	9	10	11	12
Plantext:	G	J	K	N	I	A	X	H	C	D	M	Q
Shift 4	10	13	14	17	12	4	1	11	6	7	12	16
CipherText:	K	N	O	R	M	E	B	L	G	H	Q	U

Ejemplo: 1-6 número de serie / 7-12 número serial

Figura 8
Ejemplo de cómo pudiera implementarse el método combinado de estos campos.

El texto identificado como "CipherText" en la figura # "KNORMEBLGHQU" sería la contraseña que estaríamos aplicando a la cámara de seguridad. Este algoritmo puede ser desarrollado integrado el sistema o como una herramienta externa.

Referencias

[1] Aumenta el riesgo de ataques cibernéticos en cámaras de seguridad [En línea]. Disponible: https://www.ventasdeseguridad.com/2019121011816/noticias/empresas/aumenta-el-riesgo-de-ataques-ciberneticos-en-camaras-de-seguridad.html

[2] Shodan Web Page [En línea]. Disponible: https://www.shodan.io/explore