CASO DE ESTUDIO:

6 Medidas a tomar para reducir los riesgos de ataques Cibernéticos

razberi™ technologies

Hace unos meses un ataque masivo de Denegación de Servicio (DDoS por sus siglas en Ingles) causó cortes en los sistemas de empresas como Amazon y Twitter. Los Hackers tomaron posesión de un estimado de 100,000 dispositivos que incluyeron cámaras de video vigilancia para hacer el ataque vía "botnet". Estos dispositivos fueron infectados con el virus "Mirai" que ingresó a las cámaras usando una de las 61 contraseñas simples o de fábrica. Una vez dentro, el virus colma la web mientras continuá su operación de video vigilancia de manera normal.

Estos dispositivos quedaron abiertos al internet, aún las cámaras en redes privadas son vulnerables a este tipo de ataques. Las disrupciones de estos sitios web durante este ataque produjeron pérdidas cuantiosas a las empresas, la economía y los consumidores.

A principios del 2015, un centro de seguridad de China fue hakeado empleando técnicas similares con un virus que atacó sus cámaras de seguridad.[1] Las cámaras habían sido programadas para escanear la red interna y encontrar vulnerabilidades.

Estos son solo dos de los ataques de alto perfil que han llamado la atención sobre las potenciales brechas de seguridad y su impacto en las redes de seguridad. En la industria de la seguridad física, somos relativamente buenos en anticipar las amenazas e implementar capas adicionales de seguridad para nuestra protección lo que hace curioso que en este tipo de situaciones hayamos sido lentos en reaccionar. Todos sabemos que las redes son plataformas poderosas para la conexión de nuestros sistemas de seguridad, pero aún así no pensamos mucho en los riesgos existentes si estas caen en manos equivocadas.

¿Por qué me debe importar?

La seguridad de toda organización requiere de una atención inmediata. Esto no es una táctica para asustar, estas son amenazas reales que tienen que ser tomadas en serio. En una encuesta reciente de más de 100 profesionales de seguridad uno de los temas de mayor preocupación es la falta de cooperación a través de los distintos departamentos para abordar temas de seguridad cibernética. Los l deres de las áreas de seguridad física y lógica (TI) tienen que trabajar juntos. Por los motivos que comentamos en este documento, sus equipos de TI seguramente han de darle la bienvenida a una estrategia de seguridad lógica para los equipos de seguridad.

1. https://translate.google.com/translate?sl=zh-CN&tl=en&js=y&prev=_t&hl=en&ie=UTF-8&u=http%3A%2F%2Fwww1.hikvision.com%2Fcn%2Fnews_detail_63_i1273.html&edit-text=&act=url

"Pero las cámaras siguen operando"

Debido a que las cámaras continúan operando durante estos ataques, la primera reacción generalmente es "¿Por qué ha de importarme?" en realidad hay tres escenarios importantes a considerar

1. Si a la cámara se le pide que bombardee un sitio web con tráfico, también se le puede pedir que comprometa el Sistema de producción o ventas de la empresa. ¿Tenemos su atención ahora?

2. Si alguien puede programar la cámara para generar tráfico, esta persona puede programarla para realizar otras funciones como por ejemplo hacer un "loop" de video o apagarla por completo.

3. Si las cámaras participan en el ataque y este es amplio, su proveedor de servicios de red puede cortarle el servicio mientras se investiga el hecho cosa que no es buena para su organización pues la mayoría de empresas dependen del internet para su supervivencia.

Tener un buen Firewall no es siempre la solución

Si Uds. Piensan que esto no aplica debido a que tienen un buen firewall, piensen de nuevo. En el reporte de Meritalk del 2015, "The Inside Job" donde se encuestaron a más de 150 gerentes de TI del gobierno federal, casi la mitad de ellos (45%) reportaron ataques cibernéticos internos en los 12 meses previos y 29% de estos resultaron en pérdidas de información.[2] La amenaza más grande a su organización puede ser interna.

Muchas veces las "amenazas internas" vienen del exterior. La violación de datos de Target® del 2013 ocurrió debido a que un contratista externo con clave de ingreso válido usó el portal de la empresa para presentar facturas y sus credenciales fueron robadas en un hackeo de su servidor de emails.[3] Los hackers usaron esta información para acceder a la red corporativa de Target y luego a los sistemas de punto de ventas. Esto resultó en una sustracción de información de 70 millones de tarjetas de crédito y una pérdida de $3000 millones de dólares.[4] De haber infectado sus cámaras durante ese ataque Target hubiese tenido una perdida adicional.

Lo que no ha pasado, aún

Lo que es obvio es que dispositivos simples como cámaras deben ser instaladas y administradas con políticas de seguridad cibernética. Si no, se convertirán en riesgos importantes para las empresas que se suponen se protegen con estas.

A la fecha, los ataques a cámaras se enfocan en perturbar empresas distintas a las que tienen las cámaras instaladas. Con códigos flotando en el internet ¿cuánto tiempo tenemos antes que alguien modifique los ataques para hacerle daño a la empresa que es dueña de las cámaras?

Personalice el riesgo

Pensamos en una empresa que pierde uno o dos días de ventas debido a un ataque cibernético de sus propias cámaras. ¿Sobrevirá el departamento de seguridad? ¿el Integrador? Con tanta información publica sobre las vulnerabilidades de las cámaras y las técnicas de instalación, ¿su empresa sobreviviría los juicios que siguen a estos eventos?

Lo que es obvio es que dispositivos simples como cámaras deben ser instaladas y administradas con políticas de seguridad cibernética. Si no, se convertirán en riesgos importantes para las empresas que se suponen se protegen con estas.

2. https://www.meritalk.com/study/inside-job/
3. https://krebsonsecurity.com/2015/09/inside-target-corp-days-after-2013-breach/
4. http://www.lavasoft.com/mylavasoft/company/blog/cost-of-target%E2%80%99s-holiday-season-data-breach-300-million

Protegiendo sus activos

Una definición simple de seguridad cibernética es mantener malos elementos fuera de sus redes. En términos más técnicos, es la protección de los sistemas de cómputo contra robo y pérdidas al hardware, software y a la información al igual que la disrupción del servicio.

Las 6 medidas a tomar

Afortunadamente, aun cuando los riesgos son reales, hay acciones simples que pueden disminuir estos a niveles razonables, acá van algunas medidas a tomar para minimizar los riesgos de ataques cibernéticos:

1. LAS CONTRASEÑAS SON IMPORTANTES

El punto más importante en la lista es el no ignorar las contraseñas de las cámaras. Muchas cámaras instaladas aún tienen los valores de fábrica y otras cuentan con contraseñas débiles que son fáciles de adivinar. De una u otra forma esto deja una gran puerta para los hackers que escriben programas con listas de contraseñas de fábrica o simples. El virus "Mirai" opera exactamente así usando las 61 contraseñas de fábrica y las débiles como "admin" y "54321" y el hecho que este virus haya infectado más de 400,000 dispositivos indica que estas prácticas son prevalentes y deben ser cambiadas.

2. AÍSLEN SUS CÁMARAS

Si las malas personas no pueden conectarse a sus cámaras no podrán hackearlas. No cometa el error de ponerlas en redes corporativas con otras PC's. Aíslen estas mediante el uso de redes virtuales (VLAN) o en redes separadas. Las cámaras deberán poder comunicarse únicamente con los sistemas de VMS.

3. CIERRE SU RED

Por naturaleza, muchas cámaras se encuentran fuera del área segura del local, generalmente en el exterior de este. Esto representa un riesgo importante pues al desconectar una cámara esta puede ser reemplazada por una laptop u otro dispositivo que accese su red. La solución es asegurarse que la red este configurada de tal manera que solo los dispositivos permitidos puedan comunicarse a través de esta. Cada cámara cuenta con una dirección MAC única la cual debe ser programada en un puerto específico de la red impidiendo así que dispositivos con direcciones MAC distintas no tengan acceso a la red.

4. DOS OPERADORES = MENOR RIESGO

Los departamentos de TI descubrieron hace mucho que los computadores deben usar doble tipo de autenticación, uno básico para usuarios y otro para administradores con privilegios completos. Esta separación de tipo de usuario minimiza el impacto de que las credenciales caigan en manos equivocadas. Las cámaras deben de también contar con dos tipos de usuarios uno para programar estas en el VMS y otra para los administradores para cuando haya que hacerles actualizaciones a los equipos.

5. NO IGNORE EVENTOS INUSUALES

Cuando alguien esta hackeando sus cámaras, generalmente dejan huellas. Las cámaras saldrán de línea y pérdidas de conectividad por más cortas que sean tienen que ser investigadas. El virus en las cámaras generalmente tiene un impacto negativo en el rendimiento de estas.

Puede ser que tenga suerte y vean estos hechos durante la normal operación de sus sistemas, pero buenas prácticas de seguridad dictan tener métodos de monitorear este tipo de eventos.

6. ADQUIERA CÁMARAS DE EMPRESAS CON BUENA REPUTACIÓN DE SEGURIDAD

Ha habido gran consideración sobre la seguridad de ciertas marcas de cámaras (notablemente las de fabricación China) y la preocupación ha llegado a un punto donde algunos proveedores de VMS están dejando de soportar estas marcas.[5] Adicionalmente el gobierno de EEUU ha manifestado su preocupación al punto de remover estas de las embajadas.[6] Chequear la reputación de seguridad cibernética de los sistemas a ser instalados debe ser una prioridad previa a la compra e instalación de estos sistemas. Busquen proveedores que tengan una buena reputación y que cuenten con respuestas apropiadas a este tipo de incidentes.

Si cuenta con una inversión importante de cámaras de reputación dudosa siga las recomendaciones antes mencionadas y reducirá el riesgo de manera significativa.

Herramientas y arquitectura que ayudan

Desafortunadamente hay un problema con estas recomendaciones: requieren de un nivel de dedicación y esfuerzo para ser efectivas. Los líderes de seguridad tienen que afrontar muchas situaciones con limitantes de tiempo y presupuesto; como resultado, en muchas ocasiones ignoran la seguridad cibernética y las empresas instaladoras no mencionan estas amenazas a sus clientes. No es necesario contar con certificaciones CCNA para ser proactivo en el desarrollo de políticas de seguridad cibernética, pero si se requiere tener las herramientas necesarias para implementar estas.

Los profesionales de seguridad necesitan herramientas para la administración de estas prácticas que sean escalables y automatizadas. Adicionalmente, hay oportunidades de crear arquitecturas de sistemas que minimicen el impacto de las amenazas e incrementen el nivel de seguridad y la facilidad de administración de estos sistemas.

Razberi Technologies está al frente de este movimiento con su línea de productos Razberi ServerSwitchIQ™. Esta es una suite de productos con características específicamente diseñadas para facilitar la implementación de políticas de seguridad cibernética. Adicionalmente, estos sistemas minimizan el impacto de las cámaras megapíxel en las redes, incrementan la redundancia y permiten la creación de redes virtuales, VLAN's, para proteger de ataques externos y hackeos. Estos sistemas incluyen Razberi CameraDefense ™ para el endurecimiento automátizado de la cámara y Razberi VyneWatch ™ para proporcionar monitoreo de amenazas cibernéticas.

Hay tres pilares de la solución que proporcionan capas de seguridad proactiva:

- Endurecimiento automátizado de la cámara
- Arquitectura de dispositivos seguros
- Supervisión de amenazas cibernéticas

"Los líderes de seguridad tienen que lidiar muchas situaciones con limitantes de tiempo y presupuesto"

5. https://ipvm.com/reports/genetec-hikvision
6. http://www.voanews.com/a/hikvision-surveillance-cameras-us-embassy-kabuk/3605715.html

Abordemos estas de una en una:

ENDURECIMIENTO AUTOMATIZADO DE LA CAMARA

La plataforma Razberi ServerSwitchIQ es compatible con Razberi CamaraDefense ™, que automatiza el endurecimiento de la cámara. Sirve para:

- Bloquear dispositivos IoT no autorizados: enlaza las cámaras y otros dispositivos de seguridad IoT a la red y evita que los dispositivos no autorizados utilicen conexiones Ethernet.

- Acceso seguro a las cámaras: Restringe el acceso de la cámara a las direcciones IP de la lista blanca, bloquea el tráfico de la cámara a la Internet pública, señala las contraseñas débiles.

- Proteger contra ataques cibernéticos: niega servicios de cámara no necesarios y potencialmente peligrosos con un firewall de próxima generación.

ARQUITECTURA DE SISTEMAS SEGUROS

Un diferenciador importante del uso de una arquitectura de sistemas seguros en lugar de un servidor centralizado, es la capacidad de mantener las cámaras aisladas de la red. Hay tres aspectos clave de la arquitectura:

- Proporciona una red de cámara aislada: Separa la red de la cámara de la empresa con interfaces de red independientes y en una VLAN configurable.

- Viene con un hardware listo para el cifrado: Soporta el cifrado de video y el inicio del sistema de confianza con un TPM (Trusted Platform Module) incorporado.

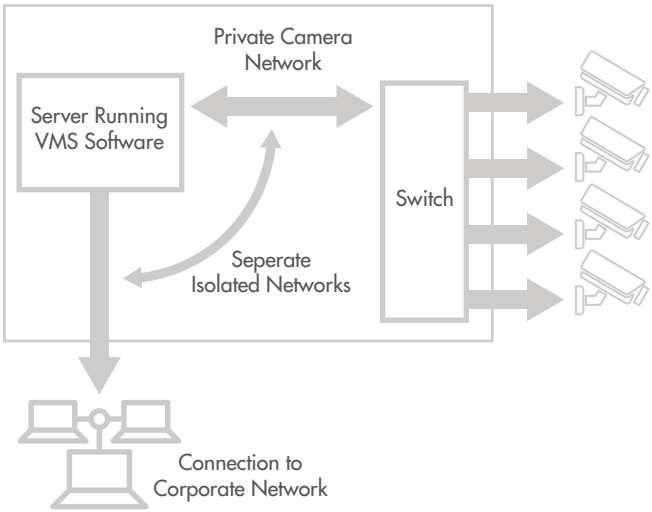
- Protección integrada contra virus y programas maliciosos: protege el sistema de gestión de vídeo mediante la predicción de ataques conocidos y desconocidos para prevenir proactivamente el malware. Los equipos Razberi son alimentados por Cylance PROTECT, que utiliza inteligencia artificial (AI) para predecir, prevenir y proteger el sistema más eficazmente que los productos anti-virus tradicionales.

SUPERVISIÓN DE AMENAZAS CIBERNÉTICAS

El último pilar de un enfoque efectivo de ciberseguridad es la capacidad de supervisar lo que está sucediendo dentro del sistema y los dispositivos que están conectados a él. Cada vez más, las herramientas basadas en la nube se utilizan para automatizar la supervisión y los servicios de TI.

Los sistemas inteligentes de Razberi incluyen un monitoreo de salud basado en la nube denominada VyneWatch ™ y la capacidad de integrarse con los provedadores mas conocidos de VMS para las notificaciones de supervisión y amenazas ciberneticas.

Razberi ServerSwitchIQ en una arquitectura VLAN



PROPORCIONA:

- Alertas de seguridad en tiempo real: genera mensajes de texto SMS, correo electrónico y alertas de seguridad en tiempo real para la respuesta a incidentes.

- Gestión flexible de alertas: gestiona alertas de seguridad con Razberi VyneWatch ™, Milestone XProtect® y otros productos VMS certificados.

- Protección dinámica contra amenazas: la protección evoluciona con nuevas amenazas para mantenerse a la vanguardia de los hackers a través del aprendizaje automático y la inteligencia artificial (AI). En comparación con los proveedores tradicionales de antivirus / malware que requieren una conexión de internet para actualizaciones periódicas.

MAÑANA ES TARDE

La seguridad es más compleja que nunca y la convergencia de la seguridad física y de TI está sobre nosotros. Hay esfuerzos pragmáticos que las organizaciones deben tomar de inmediato. Las soluciones de Razberi hacen el trabajo más fácil y rentable. Los sistemas inteligentes de Razberi con CameraDefense y VyneWatch reducen la carga del video megapíxel en la red, automatizan el endurecimiento de la cámara, proporcionan una arquitectura segura del sistema y ofrecen un monitoreo proactivo de amenazas cibernéticas. Esto significa que puede regresar a su labor diaria más importante: mantener la organización físicamente segura sin abrirla a nuevas amenazas de ataque cibernético.

Contacte a Razberi Technologies para solicitar una demonstración y descubra lo que un equipo de vigilancia inteligente puede hacer por usted a: www.razberi.net

Razberi Technologies ofrece una infraestructura de vigilancia confiable, segura y amigable a la red que registra los ajustes de calidad de vídeo más altos a la vez que reduce los costos, el ancho de banda y los espacios necesarios. Los sistemas Razberi ServerSwitchIQ ™ combinan de forma única un firewall, un switch administrativo de PoE, servidor, almacenamiento e inteligencia. La plataforma, que se implementa en una arquitectura escalable cerca del borde de la red, permite a las organizaciones reducir la utilización de la red por un 95 por ciento y proteger las cámaras de ataques cibernéticos. El software Razberi CameraDefense ™ automatiza las protecciones de seguridad cibernética con el endurecimiento de la cámara y el monitoreo de amenazas cibernéticas. El software de monitoreo de salud Razberi VyneWatch ™ ofrece alertas 24x7 a los profesionales de seguridad. Los equipos Razberi son compatibles con los proveedores de sistemas de gestión de vídeo (VMS) y cualquier cámara de red. Para más información, visítenos en razberi.net.

razberi technologies

salesinfo@razberi.net