Asegurar sistemas de automatización y control de edificios contra ataques cibernéticos

Ferdinand Meléndez Torres
Maestría en Ciencias de Computadoras
Dr. Nelliud Torres
Departamento de Ingeniería Eléctrica y de Computadoras y de Ciencias de Computadoras
Universidad Politécnica de Puerto Rico

Abstracto *— Los ataques cibernéticos a sistemas de IT o tecnologías de la información son comunes y generalmente se originan en la Internet. Los sistemas de automatización y control de edificios (SACE) a menudo están conectados a la Internet, pero carecen de una protección sólida contra estos ataques: contraseñas débiles y / o predeterminadas, comunicación no encriptada, falta de protección contra cambios no autorizados en los datos y utilización de programación básica o de conocimiento público, por mencionar algunos. En este artículo discutimos cómo los SACE pueden protegerse contra ataques cibernéticos. Esto incluye una evaluación de las características de seguridad en sistemas de información según estándares como ISA/IEC-62443 y ASHRAE 135 (BACnet) entre otros.*

Palabras clave *— botnet, hackers, legacy, ransomware*

INTRODUCCIÓN

Los edificios más modernos contienen tecnologías para regular automáticamente la temperatura, controlar la entrada de luz y la intensidad de la iluminación. La recopilación de datos en medidores permite la optimización del consumo energético; sensores adicionales como los detectores de movimiento pueden apagar la luz cuando el cuarto, oficina o área de trabajo no esta siendo utilizada, maximiza la vida útil de los equipos, reducen costo asociados a mantenimiento, entre otros. Una alternativa adicional que proveen estas tecnologías es ayudar a mantener el edificio seguro de intrusos o acceso a personas no autorizadas con la intención de hacer daño a la operación del negocio. La seguridad se garantiza mediante el uso de dispositivos electrónicos, p. ej., enrutadores, “firewalls”, “switches”, controladores, etc. La operación automática en general funciona cuando los sensores recopilan datos y los actuadores (dispositivo mecánico cuya función es proporcionar fuerza para mover o “actuar” otro dispositivo mecánico), permiten el cambio de posición según datos obtenidos de los sensores, accionando y regulando piezas móviles como válvulas o interruptores. Estos sensores y actuadores se controlan mediante controladores que se utilizan para la automatización de edificios; juntos forman un sistema de automatización y control de edificios (SACE) (figura 1).

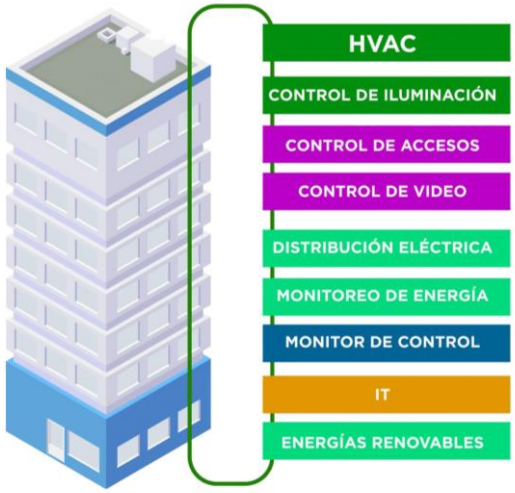

Figura 1
Diagrama típico de un Sistema de Automatización y Control de Edificios

Los equipos que componen un SACE generalmente se agrupan en tres niveles. La automatización en el nivel de campo (nivel donde se encuentran los equipos mecánicos, eléctricos), es el más bajo y se logra mediante la comunicación directa entre los sensores, interruptores y actuadores como, por ejemplo, el interruptor de control de la luz o pasando por un elemento del CPU como un controlador lógico programable (PLC) o control digital directo (DDC). Los tres

niveles pueden incluir equipos de la siguiente manera:

- **Nivel de campo:** sensores, actuadores interruptores, etc.
- **Nivel de automatización:** los controladores (PLC o DDC) permiten el control de los sistemas de calentamiento, ventilación y aire acondicionado (HVAC); control para funciones como iluminación de pasillo y control de luz para fachadas. Una funcionalidad de control simple son los controladores de luz de las oficinas que regulan la intensidad de la iluminación, así como los aspectos de las unidades de aire (HVAC) de un área de trabajo. Estos controladores pueden hacer uso de equipos de nivel de campo para recopilar datos p. ej. medidores de uso, y poder utilizar dicha información para evaluaciones de la gerencia para futuras mejoras en eficiencia energética.
- **Nivel de monitoreo:** aquí es donde los datos se recopilan, se almacenan en bases de datos y se muestran a los usuarios que operan estos equipos a través de pantallas (HMI) o estaciones de trabajo (WS), incluyendo alarmas, historial de condiciones, reportes, etc. Aquí también encontrará interfaces de configuración y programación para el sistema.

Las comunicaciones de datos entre equipos de campo y desde equipos de campo a equipos de automatización se implementan utilizando transportación de datos (data bus) o señales análogas/digitales directa. Las señales análogas de medición/control a menudo tienen rangos como 0-10V, 1-10V, 0-20mA y 4-20mA, mientras que las digitales usan señales 0/5V, 0/24V que permite la detección de fallas. Algunas tecnologías que se utilizan para sistemas de automatización y control de edificios son productos de compañías tales como Siemens, Honeywell, Rockwell, entre otros.

Los niveles de automatización y monitoreo se comunican usando estándares basados en IP, BACnet/IP [1] siendo este último el más seguro, moderno y con mayor cantidad de funciones. También se utiliza Modbus/IP y Ethernet/IP. Las interfaces web para equipos de nivel de automatización y nivel de monitoreo también se están volviendo cada vez más comunes en implementaciones en la industria.

En este artículo analizaremos algunos ataques cibernéticos comunes en la Internet a los SACE y un análisis de herramientas de seguridad y canales de comunicación para proteger estos sistemas del ataque. También se incluye una discusión de los estándares sugeridos sobre seguridad cibernética de SACE como el BACnet Anexo g e ISA/IEC-62443.

ATAQUES CIBERNÉTICOS

Desarrollos en el campo del hacker

En el pasado, la intención del hacker era de naturaleza diferente a la que presentan hoy en día. Se escuchaban historias acerca de personas jóvenes e inteligentes que pirateaban por diversión, para demostrar que podían exponer a las empresas que no aseguran sus sistemas, y a menudo no para obtener recompensas económicas. El ataque a sistemas del gobierno e industrias privadas no solía aparecer en los medios.

Hoy en día las actividades de sabotaje por parte de gobiernos, compañías privadas o instituciones asociadas a estas son ampliamente conocidas y comentadas en los medios y redes sociales; incluso sus herramientas de hacking han sido expuestas. Cualquier delincuente con poca experiencia en sistemas de información puede adquirir equipos o programas, descargar herramientas de piratería en la Internet como, por ejemplo, en foros como la "dark web" o áreas ocultas en la Internet y convertirse en un “hacker” sin entender mucho sobre las herramientas que utilizan.

Tipos de ataques

Los ataques comunes en los sistemas de información se enfocan en servidores y computadoras, así como en la infraestructura de la red o equipos IoT (Internet of Things).

Los servidores son atacados por su presencia en la web; estar expuestos a la Internet por diseño significa que tienen una "superficie de ataque" o

punto de vulnerabilidad. Los hackers en sistemas de información intentan penetrar en la red y acceder a los servidores o cuentas individuales o de administradores para obtener información de mucho valor en el mercado y así obtener algún tipo de compensación económica. Logran realizar todo este engaño a través del uso de emails y/o espacios en redes para enviar spams (emails con virus). Los ataques generalmente funcionan probando contraseñas “brute force", lo que le permite al hacker intentar varias contraseñas en una sesión de correo electrónico (emails) o “website logins” hasta lograr obtener la correcta. También utilizan debilidades en páginas de la internet creados por ejemplo con CMS (Content Management System), es una aplicación de software que permite manejar, crear y desarrollar el contenido digital en los websites. Aplicaciones de CMS que se utilizan con frecuencia son WordPress, Joomla, Drupal y Squarespce entre otros [2]. Otro ataque muy frecuente y de mayor impacto para las compañías y agencias de gobierno es el ataque a las bases de datos. En las bases de datos se encuentra toda la información crítica de agencias de gobierno y compañías privadas y es de gran valor en el mercado negro. Uno de los más conocido ataque cibernéticos de este tipo lo fue el de Yahoo en agosto de 2013 donde se comprometieron 3.000 millones de cuentas de usuarios y sus datos se vendieron en la “dark web” [3]. Computadoras conectadas a la Internet generalmente son puntos de ataque para sacarle dinero al usuario. Este tipo de ataque se puede lograr robando datos personales como tarjetas de crédito y datos bancarios, números de seguro social y contraseñas. Otro método popular es instalar un virus que encripta o elimina archivos importantes del usuario y luego muestra un mensaje de “ransom” o de pagar para recuperarlo. Para recuperar los archivos (que puede o no que realmente los recuperes), el usuario debe pagar dinero al hacker a través de la Internet. Programación o software malicioso que utiliza los hackers en este tipo de ataques se conoce como "malware" o "ransomware", y en la mayoría de los casos, se distribuye por correo electrónico en un archivo adjunto que utiliza vulnerabilidades en la seguridad de aplicaciones como MS Office o Acrobat Reader. Estos ataques también son posibles a través de los websites utilizando vulnerabilidades en el navegador (web browser) o sus complementos (plugins). Los ataques son más fáciles cuando se instalan los “plugins”, p. ej., Adobe, Java y web browsers como Internet Explorer, Chrome o Firefox. Estos plugins son componentes de software que añaden una característica específica a un programa de computadora existente. Cuando un programa admite estas extensiones o complementos, permite personalizar la experiencia que el usuario tiene durante el uso de la aplicación o durante la navegación en un website. Plugins permiten realizar funciones adicionales además de las funciones predeterminadas por las cuales fue diseñado originalmente. Una vez dentro de una red local (LAN), el malware a menudo puede propagarse fácilmente, aprovechándose de las vulnerabilidades en la seguridad o políticas de acceso en los sistemas operativos.

Se ha demostrado que los ataques más frecuentes de ransomware han sido en la industria médica, comercial y de educación. Los mecanismos utilizados en dichos ataques han sido emails (phishing), descargas de archivos en la Internet, equipos con protocolos de seguridad no actualizados conectados a la red y ataques internos dentro de la red a través de equipos como USB, memoria externa o equipos con puerto abiertos [4].

La mayoría de los ataques contra Internet of Things (IoT) y equipos dentro de una infraestructura de una red se enfocan en enrutadores de cable o DSL y cámaras con IP. Estos equipos están conectados a la Internet 24 horas al día. A menudo carecen de la configuración de seguridad adecuada, no tienen, o tienen una contraseña predeterminada de fácil acceso, o tienen otras vulnerabilidades de seguridad. Suplidores de hardware no solucionan problemas de seguridad en equipos actualmente en uso, específicamente en equipos legacy si modelos recientes salieron al mercado. Incluso si estos suplidores publican actualizaciones de firmware, muchos equipos

legacy no se actualizan automáticamente porque no tienen esa función. En muchas ocasiones los usuarios desconocen de la necesidad de nuevos firmwares, creando una vulnerabilidad en la seguridad estos equipos. Una vez el hacker tiene acceso, utiliza estos equipos para acceder a otros equipos o sistemas en la red implantando un gusano "*worm*" y poder crear un botnet.

Un botnet es un número de equipos conectados a la Internet, cada uno de los cuales ejecuta uno o más bots (aplicaciones de software que corren instrucciones automáticamente en la Internet). Botnets se pueden utilizar para realizar ataques de negación de servicio distribuida (DDoS), robar datos, enviar spam y permitir que el hacker acceda a otros equipos y sistemas. El hacker puede controlar el botnet utilizando el software de comando y control (C&C) (figura 2). La palabra "botnet" es un acrónimo de las palabras "robot" y "network" [5]. El término generalmente se usa con una connotación negativa o maliciosa.

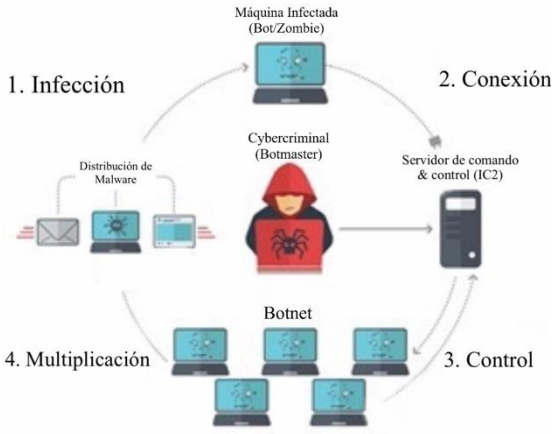

Figura 2
Cómo funciona un botnet

ATAQUES A SISTEMAS DE AUTOMATIZACIÓN Y CONTROL DE EDIFICIOS (SACE)

Riesgos

La incidencia de eventos como estos y las posibles ganancias económicas que se obtienen al operar IoT botnets hacen que los ataques a SACE sean cada vez más atractivos desde el punto de vista de un hacker. El espionaje industrial y el sabotaje de SACE u otros sistemas de automatización pueden provocar pérdidas de gran impacto a empresas y agencias de gobierno. Las empresas gastan miles de millones de dólares cada año en investigación y desarrollo. La información descubierta vale al menos la cantidad de recursos tomados para obtener la información más el beneficio económico producido por la información. Por ejemplo, si una empresa gasta $200,000 investigando un proceso que a su vez generará $1 millón en ingresos, entonces esos datos valen al menos $1.2 millones [6].

Es por esta razón que proteger los SACE de los ataques cibernéticos es importante y crítico, más aún cuando las tecnologías de la información avanzan a gran escala.

Asegurar un SACE de ataques cibernéticos es costoso y complicado por varias razones:

- Estos sistemas operan cerca del público, por ejemplo, en empresas privadas, hospitales, agencias de gobierno, etc.
- Están diseñados para un funcionamiento independiente, lo que significa que los operadores no suelen comprobar la presencia de ataques cibernéticos en los equipos ni instalar actualizaciones de seguridad.
- Las actualizaciones de seguridad pueden resultar en aprobaciones adicionales por parte de la gerencia o certificación final del sistema en general por parte del proveedor, lo que a veces representa un costo adicional y por ende una razón para no instalarlas, incluso si existieran.
- Las garantías de los equipos que se utilizan en los SACE son de 10 años o más, lo que es un periodo muy largo en comparación con los componentes, equipos y softwares que se utilizan en IT.
- En la práctica no existen diseños seguros que consideren hardware y software para SACE; están protegidos por una contraseña en el mejor de los casos y la data es enviada a través de líneas no encriptadas.

Objetivos

Cuando se protegen sistemas en general de ataques cibernéticos, se deben analizar los tipos de ataques que se pueden esperar, posible entrada o punto vulnerable y establecer cuál será el objetivo para salvaguardar ese activo.

Los siguientes aspectos son los tres pilares de la seguridad y generalmente considerados durante el análisis [6]:

- **Confidencialidad:** restringir el acceso a la información y los sistemas, por ejemplo, mediante encriptación de datos y protección con contraseña.
- **Integridad:** garantizar que no se modifiquen los datos (al menos no sin detección), por ejemplo, al navegar en una página de banca por internet o de comercios en línea.
- **Disponibilidad:** los sistemas y los datos deben estar accesibles cuando es necesario; Los ataques DDoS y ransomware (ambos mencionados anteriormente) son ataques típicos a la disponibilidad de datos y sistemas.

A veces se consideran otros aspectos, como la autenticidad, p. ej. autenticidad del origen de los datos, lo que implica que la persona que recibe el mensaje puede verificar si los datos provienen de una fuente legitima.

Aplicando los aspectos C-I-D a un SACE, podemos determinar los siguientes objetivos de seguridad:

- **Confidencialidad:** solo personal con privilegios de acceso a la información está autorizado a leer los datos que se puedan intercambiar entre sistemas o entre un usuario y un sistema. Esto incluye la protección para cualquier mantenimiento remoto, se deben utilizar canales seguros, p. ej., VPN (Virtual Private Network) con mecanismos de autenticación, p. ej. contraseñas. Si un hacker obtiene acceso a las facilidades donde está localizado el Data Center o la base de datos, los datos almacenados y canales de comunicación pudieran ser encriptados.
- **Integridad:** los datos, configuraciones, programación y actualizaciones de firmware, no pueden ser cambiados sin la aprobación de un control de cambio.
- **Disponibilidad:** Acceso a los datos, sistemas y equipos deben estar listos en todo momento cuando se requiera por razones de trabajo. Es vital que se protejan contra ataques DDoS, fallas en los equipos o sistemas, eliminación de datos y programación, fallas en la red y pérdida de comunicación y energía. Los servidores de base de datos, webserver, servidores de aplicaciones, servidores de email deben estar disponibles en todo momento.

Puntos vulnerables de ataque

Los posibles puntos de ataque dependen mucho del sistema y de la industria que se esté considerando. Por ejemplo, un SACE en una prisión puede estar en peligro de ser manipulado por los mismos reclusos para abrir puertas o provocar un motín. Esto podría incluir la manipulación de alarmas de incendio en el nivel de campo o crear fallas en la comunicación entre equipos. Eventos como estos podrían desencadenar situaciones no deseadas, p. ej. cuando no hay personal de seguridad disponible para garantizar el orden y un funcionamiento normal de las operaciones sin mayores problemas.

En el caso de un SACE de un hospital pudiera estar en peligro la salud y la seguridad de los pacientes y familiares o amigos que los visitan. Una vez dentro del sistema el hacker puede activar alarmas intencionalmente para que el personal desaloje y poder tener acceso algún paciente que este custodio por agencias de gobierno local o federales o algún cuarto con medicamentos controlados o equipos especializados. Pudiera robar información personal de los pacientes registrados en el hospital para luego robarles la identidad. Lo mismo pudiera pasar en instituciones de educación. Otro caso interesante sería el SACE de las instituciones financieras, el cual tienen que cumplir con un sinnúmero de regulaciones federales

haciendo la implementación de un SACE más compleja y costosa.

Ataques de personas con acceso físico son difíciles de defender. Esto puede incluir a trabajadores o extrabajadores que desean causar daños, por ejemplo, como un tipo de represalia después de ser despedido o haberle rechazado algún ascenso. Por supuesto, también se les puede pagar por realizar trabajos destructivos o de sabotaje y espionaje, como recopilar datos para un competidor.

Digamos que para un SACE de un hospital se considera la instalación de equipos basados en IPs. Sería un gran reto poder evitar que cualquier persona acceda a la red, debido a que hay equipos electrónicos, p. ej., impresoras, teléfonos VoIP, computadoras, etc. conectados a la red y hay salidas (outlets) de network en todo el hospital, incluyendo en las habitaciones de los pacientes. La mayoría de las personas que visitan hospitales, buscan acceso a Internet a través de Wifi o ethernet (cable) para pasar el tiempo, evitando cargos adicionales en sus tarifas móviles o una reducción de velocidad en el plan de datos. Sin embargo, inadvertidamente pueden propagar un virus desde sus computadoras portátiles a través de vulnerabilidades en el sistema operativo y saturar la red creando un problema de disponibilidad (DDoS).

En general, se pueden distinguir otros puntos de ataque donde sea posible el acceso:

- Acceso físico a equipos o sistemas en la red (con pocas posibilidades de defensa)
- Componentes de un SACE que comparten una red, generalmente con IP, p. ej. PC de oficina con acceso a emails y navegación en la Internet.
- SACE expuestos a Internet, p. ej., para mantenimiento remoto o monitoreo energía [7][8].
- Laptops, tabletas y otros dispositivos de personal de mantenimiento que comparten la red temporalmente.

Las superficies de ataque o puntos de vulnerabilidad deben considerarse durante la vida útil de todos los componentes del sistema. Esto puede comenzar en el momento en que los controladores de edificios, p. ej. controladores de parámetros de proceso o DDC, se instalan en el techo de un edificio sin terminar (donde es difícil monitorear quién accede a él) hasta un análisis de posibles ataques a computadoras portátiles utilizadas durante el mantenimiento de componentes de un SACE mucho más tarde durante su ciclo de vida.

Seguridad por oscuridad

Seguridad por oscuridad es la confianza en el diseño o el secreto de implementación en la ingeniería de seguridad como el método principal para proporcionar seguridad a un sistema o equipo.

A menudo, el acceso a la información y los sistemas está oculto en lugar de estar encriptado o protegido de otra manera tecnológicamente, p. ej., mediante el uso de un número de puerto IP no estándar para conectarse a una interfaz de administración, o un URL "secreto" que permite que solo las personas que lo conocen ejecuten un comando del sistema. Incluso solía haber casos en el que la contraseña de inicio de sesión estaba escrita en el código fuente de la página HTML de inicio de sesión, generalmente invisible, pero claramente visible para las personas que miraban el código fuente.

La aparente seguridad obtenida de la oscuridad simplemente ocultando información no funciona en absoluto contra los hackers que poseen una computadora y menos con los avances en la tecnología de hoy. Las computadoras pueden probar todos los números de puerto IP posibles, pueden probar URL populares y generar automáticamente aún más. Mirar el código fuente de una página HTML es parte del análisis estándar de un hacker.

Si realizas una búsqueda en línea exclusivamente para sistemas de automatización, incluyendo los SACE, encontraras decenas de miles de estos sistemas, algunos conectados a la Internet para mantenimiento remoto. Muchos de estos no ocultan datos confidenciales sobre el edificio o del

sistema de automatización que utilizan y algunos inclusive permiten el acceso remoto parcial sin una contraseña.

CÓMO ASEGURAR UN SISTEMA DE AUTOMATIZACIÓN Y CONTROL DE EDIFICIOS

Para que los SACE sean más seguros contra los ataques cibernéticos, es necesario establecer un proceso que rija la producción, cadena de suministro, instalación, configuración/programación, operación y mantenimiento. Los estándares internacionales como el ASHRAE 135 (BACnet) anexo g [9] e ISA/IEC 62443 [10] pueden ayudar a cubrir muchos aspectos de seguridad y hacer que los sistemas sean operables conforme a estos estándares de seguridad.

BACnet

BACnet [9] es un protocolo de comunicación de datos que estandariza las comunicaciones entre equipos electrónicos de automatización de edificios de diferentes fabricantes, lo que permite compartir datos y que los equipos trabajen juntos fácilmente. BACnet define los objetos de datos, sus propiedades y los servicios para la comunicación. A diferencia de otros estándares (como Modbus), este se ha escrito específicamente para sistemas de automatización de edificios, no para sistemas de automatización y control en general. Esto significa que tiene todas las definiciones y tipos de datos necesario facilitando también la documentación y análisis.

Su comunicación basada en IP (BACnet/IP) se basa en UDP/IP, mientras que la mayoría de los estándares más seguros de comunicación y autenticación (como TLS y SSH) (en su forma estándar) se basan en TCP/IP. ASHRAE 135g define sus propios mecanismos de protección, lo que hace que su implementación sea más compleja.

El estándar define, entre otras cosas:

- Confidencialidad e integridad de los datos.
- Autenticación peer to peer, origen de datos y acceso administrativo.

La seguridad se realiza en la capa de network y se define para todos los medios, como MS/TP, BACnet/IP, etc. y todos los tipos de equipos. También funciona para todos los servicios/paquetes, incluyendo mensajes confirmados y no confirmados, difusión uno a uno (unicast), uno a todos (broadcast) y uno a varios (multicast) (figura 3).

Figura 3
Tipos de difusiones de mensajes

Características y evaluación

ASHRAE 135g permite el uso de hash MD5 y SHA-256 (SHA2 con 256 bits). Para la confidencialidad mediante encriptación, permite encriptación simétrica con el estándar AES-128, que también es bueno según los estándares de seguridad actuales. ASHRAE 135g requiere un manejo de claves o llaves algo complejo, por lo que permite la protección de capas del acceso al bus (comunicación), datos (confidencialidad) y configuración del equipo.

AES también se utiliza para firmas digitales como prueba de autenticidad de datos y acceso. Un equipo puede verificar si la comunicación recibida es auténtica o si es un hacker: un ataque de hombre en el medio. La autenticación normalmente se realizaría con un algoritmo de encriptación con clave o llave pública (es decir, asimétrico) como RSA, como se usa en estándares como HTTPS, PGP, etc. En comparación con los algoritmos asimétricos modernos y seguros, AES tiene la

ventaja de ser mucho menos exigente computacionalmente y su ejecución es más acelerada debido a instrucciones especiales integradas en los CPU modernos. Esta ventaja de la velocidad puede haber sido la razón para elegir AES para las firmas digitales.

La verificación de autenticidad, así como la protección de acceso mediante claves o llaves, también pueden evitar el cambio no autorizado de datos, programación y firmware, que es una característica importante.

En general, ASHRAE 135g parece cubrir todos los aspectos importantes necesarios para la seguridad cibernética en los sistemas BAC (excepto quizás el aspecto de disponibilidad que exige otras técnicas que no encajan en este contexto de todos modos). Existen varios equipos y sistemas de diferentes compañías alrededor del mundo que implementan el estándar, p. ej., Siemens, Honeywell, Rockwell, Allen Bradley, Schneider, entre muchos otros.

IEC 62443

El estándar fue creado originalmente como ISA-99 por la Sociedad Internacional de Automatización (ISA), pero ahora es desarrollado por la Comisión Electrotécnica Internacional (IEC) [10]. Actualmente el desarrollo del estándar sigue en progreso.

IEC 62443 está organizado en las siguientes cuatro categorías: General, Políticas y Procedimientos, Sistema y Componentes:

- **General:** proporcionan una visión general del proceso de seguridad industrial e introduce conceptos esenciales.
- **Políticas y procedimientos:** destacan la importancia de las políticas: incluso la mejor seguridad es inútil si las personas no están capacitadas y comprometidas a apoyarla.
- **Sistemas:** debido a que la seguridad solo puede entenderse como un sistema integrado, los documentos del sistema proporcionan una guía esencial para diseñar e implementar sistemas seguros.
- **Componentes:** los documentos de componentes describen los requisitos que deben cumplirse para componentes industriales seguros.

IEC 62443 cubre un área amplia, que incluye muchas recomendaciones para procesos comerciales según las mejores prácticas en la industria, desde infraestructura y control de acceso hasta copias de seguridad para garantizar la disponibilidad.

Uno de los requisitos es la seguridad de hardware para los niveles de seguridad 3 y 4.

Los chips de seguridad de hardware discretos son mucho más seguros que la seguridad de software. Los atacantes pueden analizar fácilmente el software para encontrar vulnerabilidades y desarrollar vulnerabilidades que socaven la seguridad. Tales ataques aparecen todos los días. Los chips de seguridad de hardware a prueba de manipulaciones evitan eficazmente tales ataques.

La mayoría de los chips de seguridad de hardware son evaluados y certificados por laboratorios de pruebas de seguridad independientes. Estas certificaciones demuestran las barreras más altas para penetrar las defensas del chip. Cualquiera puede afirmar que proporciona seguridad, pero para aplicaciones críticas, se requiere una evaluación experta independiente.

La seguridad del hardware reduce los costos de ingeniería y soporte. La seguridad personalizada es costosa de construir y requiere un mantenimiento constante. Elegir un chip de seguridad en su lugar toma ventajas de décadas de experiencia y pruebas en seguridad.

El estándar fue escrito para sistemas de automatización y control en general, no específicamente para la construcción de aplicaciones. Sin embargo, aplicarlo al entorno del edificio es posible. Es posible que no se introduzcan nuevos estándares de comunicación para estos sistemas, por lo que una combinación con ASHRAE 135g (que no cubre tantos aspectos de monitoreo) podría ser una buena alternativa.

Como un estándar relativamente nuevo y aún no final, evaluar IEC 62443 en su totalidad sería complicado. Es bastante extenso y tendrá que ser revisado y probado en el mundo real. Sin embargo, se ve bastante prometedor.

Otros aspectos en la seguridad cibernética

Al considerar la seguridad de un SACE, las técnicas presentadas en los estándares y las mejores prácticas en la industria del mundo de IT deben implementarse.

Por ejemplo, si se necesita acceder a un SACE remotamente, ya sea para mantenimiento, acceso a datos o control, se puede usar VPN (Red Privada Virtual). Se puede implementar un acceso VPN en un enrutador de la red instalado en sitio. Los equipos del SACE se configurarían y conectarían de manera tal que no fuera posible el acceso externo directo, sin embargo, se conectarían al router (o por medio de él). Entonces, se podría usar VPN para acceder al router desde el exterior utilizando un canal encriptado y seguro. Una vez obtenido este acceso a un equipo o sistema, el router prácticamente lo convierte en parte de la red local, lo que permite la comunicación con todos los componentes del SACE.

También se pueden usar técnicas de endurecimiento “hardening” como las utilizadas en servidores y redes, por ejemplo:

- Reducir el acceso físico y electrónico al mínimo requerido para un funcionamiento adecuado.
- Cierre, deshabilitación y eliminación de puertos no utilizados en la red, software y servicios no necesarios, incluyendo, pero no limitado a telnet, Modbus y servicios de configuración/programación y controladores de puertos
- Elegir buenas contraseñas de acceso individual y distintos niveles de usuario, p. ej., para visualización, configuración/control y reprogramación
- Inhabilitar la posibilidad de adivinar las contraseñas rápidamente mediante el uso de la fuerza bruta, limitando la cantidad de intentos cuando se inicia una de sesión y activando bloqueos automáticos después de cierta cantidad de intentos.
- Separar partes de la red que no necesitan comunicarse, p. ej., redes de oficinas, redes de invitados, redes de WiFi, SACE, etc. mediante el uso de VLANs, y utilizando DMZ (zonas desmilitarizadas) para restringir el acceso en línea
- Utilizar firewalls buenos y bien configurados para filtrar el tráfico entrante y saliente
- Mantener seguras otras computadoras en el mismo sitio, así como las computadoras portátiles que se usan para mantenimiento.

CONCLUSIÓN

La seguridad cibernética para los edificios es cada vez más importante a medida que avanza la tecnología, dándole más recursos a los hackers, por lo tanto, aumentando los ataques a estos sistemas. Las soluciones y tecnologías de seguridad presentadas son las que se incluyen en los estándares actuales de seguridad de redes y las más utilizadas en la industria. Se pueden utilizar equipos/sistemas más robustos como los que se adaptan al estándar de BACnet g. y tener como complemento la implementación de los aspectos de seguridad para monitoreo y control según IEC 62443. Implementar una seguridad eficiente y efectiva contra los ataques cibernéticos es difícil y costosa, pero es un activo si lo comparas con la posible pérdida de información o interrupción de operaciones de una manufactura o negocio.

REFERENCIAS

[1] M. Nast, B. Butzin, F. Golatowski y D. Timmermann, "Performance Analysis of a Secured BACnet/IP Network", *15th IEEE International Workshop on Factory Communication Systems (WFCS)*, Sundsvall, Suecia, 2019, pp. 1-8, doi: 10.1109/WFCS.2019.8758009.

[2] N. A. Khan y H. Ahangar, "Use of Open Content Management Systems in Government Sector," *5th International Symposium on Emerging Trends and Technologies in Libraries and Information Services*

(ETTLIS), Noida, 2018, pp. 183-187, doi: 10.1109/ETTLIS.2018.8485191.

[3] C. Easttom, *Computer Security Fundamentals*, 3ª ed. Indiana: Pearson, 2016.

[4] *Energy management systems – Requirements with guidance for use*, ISO 50001, 2018.

[5] Building Automation And Control Systems (BACS) – Part 5: Data Communication Protocol, ISO 16484-5, 2017.

[6] *BACnet: A Data Communication Protocol for Building Automation and Control Networks*, ANSI/ASHRAE 135, 2016.

[7] *Network and System Security for Industrial Process Measurement and Control*, ISA/IEC 62443, 2020.