NOTAS TÉCNICAS

Importancia del control de acceso electrónico a nivel de gabinete para la seguridad de los datos y el cumplimiento normativo

Por David Knapp
Gerente de Marketing de productos
Chatsworth Products (CPI)

Ashish Moondra
Gerente de productos sénior, Energía, Electrónica y Software
Chatsworth Products (CPI)

Raissa Carey
Especialista en Relaciones Públicas y escritora técnica
Chatsworth Products (CPI)

Publicado en: 03/19; v2 06/20

EE. UU
Agoura Hills, CA
800-834-4969
Canadá
Toronto, Ontario, Canada
+905-850-7770
chatswoth.com • techsupport@chatsworth.com

Europa
Buckinghamshire, UK
+441628524834

Oriente Medio y África
Dubái, EAU
+971-4-2602125

Doha, Qatar
+974-4-267422

América Latina
+52-55-5203-7525
Número gratuito en México
800-201-7592
chatsworth.com.co

Asia-Pacífico
+86 21 6880-0266
chatsworth.com.cn

CHATSWORTH PRODUCTS

Introducción

La importancia de la seguridad física para proteger los datos generalmente se comprende bien, pero ¿con qué frecuencia su organización evalúa el nivel de seguridad física para proteger los datos? ¿Y cumple con las normas sobre la seguridad de los datos?

En estas notas técnicas de Chatsworth Products (CPI), encontrará una descripción general de las normas de seguridad de los datos y los requisitos de cumplimiento, el argumento para extender la seguridad física al nivel del bastidor, recomendaciones sobre el uso de sistemas de control de acceso y cierre electrónico a nivel del bastidor y explicaciones sobre cómo el ecosistema de gabinetes de CPI (Figura 1) proporciona una solución más económica y fácil de implementar y usar que otras en el mercado.

Dato útil

eConnect® RFID Electronic Lock Kittienen tecnología de consolidación IP de Secure Array®. Secure Array reduce los costos y los requisitos de redes al vincular hasta 32 EAC a través de una sola dirección IP. Pruebe el Estimador de ahorros de eConnect® Secure Array de CPI chatsworth.com/en-us/resources/configurators-and-estimators/estimator-page p ara ver cuánto podría ahorrar.

Figura 1: El ecosistema de gabinete de CPI es una solución más económica para extender la seguridad física al nivel del bastidor.

Las Normas, los estándares y el cumplimiento

¿Cuáles son las normas y los estándares sobre la privacidad (seguridad) de los datos y qué exigen? Todos los estándares y las normas sobre la privacidad de los datos exigen que se tomen medidas de control de acceso físico a los equipos de almacenamiento y procesamiento de datos, pero, como sucede con la mayoría de las normas, depende de las organizaciones decidir qué método o tecnología específica usar. Debido a inquietudes sobre la privacidad de los datos confidenciales, algunos segmentos de nuestra industria, particularmente, el de la atención médica y el financiero, piensan en el control de acceso a nivel del gabinete de manera más estricta, al requerir un informe detallado de quién, cuándo y por qué accedió al gabinete.

Algunas de las normas y los estándares importantes son la Ley de Portabilidad y Responsabilidad de los Seguros Médicos (HIPAA)[1], la Ley Federal de Gestión de Seguridad de la Información (FISMA)[2], el Reglamento General de Protección de Datos (GDPR)[3], la Norma de Seguridad de Datos de la Industria de Tarjetas de Pago (PCI-DSS)[4] y el marco del Sistema AICPA y el Control de Organización (SOC-2)[5]. A continuación, se describen las normas y los requisitos relacionados con el control de acceso.

HIPPA Ley de Portabilidad y Responsabilidad de los Seguros Médicos

FISMA Ley Federal de Gestión de Seguridad de la Información

GDPR Reglamento General de Protección de Datos

PCI-DSS Norma de Seguridad de Datos de la Industria de Tarjetas de Pago

HIPAA: Ley de Portabilidad y Responsabilidad de los Seguros Médicos

Los Centros de Servicios de Medicare y Medicaid (CMS) tienen una regla titulada “Normas de seguridad para la protección de información electrónica de salud protegida”, que exige a las entidades cubiertas que “implementen políticas y procedimientos para limitar el acceso físico a sus sistemas de información electrónicos y a las instalaciones en las que están alojados, mientras se garantice el acceso debidamente autorizado. El acceso al hardware y al software debe estar limitado a las personas debidamente autorizadas”.

Además, las compañías que cumplen con la HIPAA deben documentar los intentos de acceso, incluidas las fechas y el motivo de este. Estas notas pueden variar desde un simple libro de registro hasta una base de datos electrónicos más completa.

Las organizaciones que deben cumplir con la HIPAA son las que gestionan registros de atención médica individuales, incluidos los proveedores de servicios farmacéuticos, dentales, médicos y de la vista, los programas de seguros, facturación y bienestar, las aplicaciones de seguimiento de la salud e incluso los gimnasios.

Algunos de los requisitos relacionados con el control de acceso de la HIPAA son los siguientes:

- Limitar el acceso físico a los sistemas de información electrónicos y a las instalaciones en las que se encuentran.
- Documentar los intentos de acceso, las fechas y el motivo de acceso.

FISMA: Ley Federal de Modernización de Seguridad de la Información

Sobre la base de la Orden Ejecutiva de 2013, "Mejora de la ciberseguridad de la infraestructura crítica", el Instituto Nacional de Normas y Tecnología (NIST) publicó un marco de ciberseguridad para guiar los procesos de gestión de riesgos de ciberseguridad de las compañías.

El control de acceso es un elemento de la función principal del marco, proteger, que recomienda lo siguiente:

- El acceso a los activos y a las instalaciones asociadas está limitado a los usuarios, procesos o dispositivos autorizados, y a las actividades y transacciones autorizadas, en las cuales:
  - Se gestionan las identidades y credenciales de dispositivos y usuarios autorizados.
  - El acceso físico a los activos está gestionado y protegido.
  - Se gestionan el acceso remoto y los permisos de acceso.
  - La integridad de la red está protegida, y se incorpora segregación de redes cuando corresponde.

GDPR: Reglamento General de Protección de Datos

El GDPR forma parte de la reforma de protección de datos de la Unión Europea (UE) y es un conjunto estricto de normas que otorga a las políticas de protección de datos y seguridad un nuevo nivel de prioridad. Aunque el GDPR es un reglamento de la UE, cualquier organización que recopile o procese datos de individuos dentro de la UE también debe contar con una estrategia de cumplimiento.

Los centros de datos deberán poder demostrar ejemplos de "prevención del acceso no autorizado a redes de comunicaciones electrónicas y distribución de códigos maliciosos y detención de ataques de 'denegación de servicio' y daños a los sistemas informáticos y de comunicación electrónica".

PCI DSS: Normas de Seguridad de Datos para la Industria de Tarjetas de Pago

El Consejo de Normas de Seguridad de la PCI (PCI SSC) creó las PCI DSS para proteger los datos de los titulares de tarjetas en la era digital. Las vulnerabilidades están en todas partes en la esfera del procesamiento de tarjetas, incluidos los dispositivos en los puntos de venta, los puntos críticos inalámbricos, el comercio electrónico y la transmisión de datos del titular de la tarjeta al proveedor de servicios.

Las PCI-DSS afecta a las organizaciones que manipulan información de transacciones financieras, incluidas instituciones financieras, comerciantes y proveedores de servicios, desarrolladores de software de sistemas de pago y fabricantes de dispositivos PIN.

Algunos de los requisitos relacionados con el control de acceso de la PCI-DSS son los siguientes:

- Usar los controles de entrada a la instalación adecuados para limitar y monitorear el acceso físico a los sistemas en el entorno de datos del titular de la tarjeta.
- Desarrollar procedimientos para distinguir fácilmente entre el personal del sitio y los visitantes, por ejemplo, mediante la asignación de credenciales de identificación.
- Usar un registro de visitantes para realizar un seguimiento de la información y la actividad del visitante, lo que incluye el nombre del visitante, la compañía y el personal del sitio que autoriza el acceso físico.
- Conservar el registro durante al menos tres meses, a menos que haya restricciones legales.

Saas SOC 2®: marco del Sistema y el Control de Organización (SOC-2)

Desarrollado por el Instituto Estadounidense de Contadores Públicos Certificados (AICPA), SOC 2 es un marco que ayuda a las organizaciones de servicios a aplicar procesos e implementar controles de ciberseguridad. Los criterios incluyen varias consideraciones para garantizar la prevención de eventos de seguridad intencionales o no intencionales, incluidos los siguientes:

- Protección de datos, ya sea en reposo, durante el procesamiento o en tránsito.
- Identificación, autenticación, autorización y gestión de credenciales del usuario.
- Aprovisionamiento y cancelación de acceso físico y lógico, incluido el acceso remoto.
- Seguridad física en el centro operativo y en el centro de datos y protecciones ambientales.

Resumen de requisitos

En cuanto a los requisitos de cumplimiento mencionados anteriormente, los requisitos generales relacionados con la seguridad son los siguientes:

- Debe contar con un método para asegurar físicamente el procesamiento de datos y los equipos de almacenamiento.
- Debe tener un método para identificar y gestionar los descriptores de acceso autorizados.
- Debe tener un método para gestionar el acceso al espacio físicamente seguro.
- Debe mantener los registros de acceso al espacio físicamente seguro.

Rol de la seguridad física a nivel del bastidor

La mayoría de los centros de datos y las salas de computadoras son físicamente seguros. En una instalación especialmente diseñada, hay seguridad perimetral, un sólido control de acceso por la puerta frontal y acceso controlado a las salas de datos. En instalaciones empresariales, el acceso a las salas de datos suele estar más limitado que el acceso estándar al edificio. Entonces, ¿por qué ampliar la seguridad al nivel del bastidor?

Es importante recordar que la intención de las normas de privacidad y seguridad de los datos es evitar la filtración de los datos. Por lo tanto, evitar la filtración de los datos debería impulsar sus decisiones sobre la seguridad física. Reconozca que la última línea de defensa de la seguridad física entre el procesamiento de datos y el equipo de almacenamiento y el acceso de usuarios no autorizados es un gabinete de servidores seguro.

La mayoría de las filtraciones de datos son perpetradas a través de la explotación del software o la red por parte de terceros, ¿verdad? La mayoría de las filtraciones sí, pero de acuerdo con el Índice de inteligencia sobre amenazas X-Force de IBM[6] de 2017, entre el 1 y el 25 por ciento de los intentos de robo de datos son realizados por personas internas con fines maliciosos. El Índice de inteligencia sobre amenazas X-Force de IBM[7] de 2018 también señala que entre los ataques estudiados entre 2015 y 2017, la mayoría de los cuales se originaron a través de explotaciones de redes o software, 19 incidentes de seguridad exitosos se originaron mediante el acceso físico a los datos.

Para un sitio de inquilino único de propiedad empresarial, la seguridad en las salas probablemente sea suficiente. Pero, para los sitios de múltiples inquilinos y los sitios remotos, es mejor controlar el acceso al nivel del bastidor para controlar el acceso a sus activos y a los datos que almacenan. Este es el nivel más granular de la seguridad física y cuenta con un mejor control por parte de los administradores de sistemas de TI y los gerentes de instalaciones que administran el equipo.

Motivos para utilizar un sistema de control de acceso y cierre electrónico a nivel del bastidor

Probablemente, esté de acuerdo y diría que ya cumple con las normas de privacidad. Después de todo, la mayoría de los gabinetes del centro de datos tienen cerraduras codificadas y las claves están cuidadosamente controladas. Bueno, ¿cómo se asegura de que las puertas estén aseguradas? ¿Cómo documenta el acceso a los gabinetes? ¿Cómo recupera las claves de los usuarios? ¿Cuál es su respuesta cuando alguien pierde o le roban una clave? Los sistemas de control de acceso y cierre electrónico automatizan el monitoreo, la documentación y el control de acceso y permiten una rápida reprogramación si cambian los derechos de acceso o si se pierde o se roba una credencial. Tenga en cuenta lo siguiente:

Los tres niveles de seguridad

Los sistemas de control de acceso y cierre electrónico pueden utilizar tres tipos de llaves: tarjetas de acceso, códigos de teclado o biométricas. Estos brindan niveles progresivos de seguridad y recuperación de las cerraduras con clave con algo que usted tiene, algo que sabe y algo que es (Figura 2). La tarjeta de acceso es algo que tiene. Aunque se la pueden robar como una llave física, tiene la ventaja de que permite asignar y cambiar las credenciales rápidamente sin la necesidad de recuperar la credencial ni de cambiar la cerradura. Un código de teclado es algo que sabe. Es más difícil de robar, pero puede adivinarse. Una llave biométrica es algo que es. Salvo en casos poco frecuentes de coacción o fraude, permite asociar de forma única el acceso con un individuo.

Figura 2: Los sistemas de control de acceso y cierre electrónico tienen tres niveles de seguridad: algo que tiene, algo que sabe o algo que es.

Autenticación de factor único frente a factor doble o multifactor

El factor hace referencia al número de claves únicas requeridas para acceder al gabinete (Figura 3). Los sistemas de autenticación de factor único utilizan una sola clave. Las cerraduras con clave son estrictamente un sistema de factor único. Si se usan individualmente, las tarjetas de acceso, los códigos de teclado o los datos biométricos también son de factor único. Sin embargo, las claves de la cerradura electrónica son más fáciles de usar en combinaciones de factor doble y multifactor. Las claves de factor doble y multifactor reducen las probabilidades de acceso de un usuario no autorizado. Los sistemas de factor doble y multifactor pueden requerir una actualización de la cerradura electrónica para incluir un lector.

Figura 3: Las cerraduras con capacidades multifactoriales combinan varios tipos de claves para mejorar la seguridad y conectar las credenciales a usuarios autorizados específicos.

Gestión de claves

Si usa cerraduras con clave para asegurar los gabinetes de los equipos, debe tener un programa de gestión de claves sólido y completamente eficaz. Esto exige acompañar a los visitantes o recuperar las claves cuando los usuarios entran y salen de las instalaciones, recuperar las claves cuando un empleado se va y volver a codificar los gabinetes cuando se pierden o roban las claves. Por el contrario, el cierre electrónico puede reprogramarse con rapidez mediante nuevos códigos de acceso y no es necesario modificar el hardware.

Gestión de derechos

Las cerraduras con clave proporcionan una gestión de derechos limitada. Por lo general, todos los gabinetes están codificados de la misma manera. Puede usar cerraduras de combinación o tener grupos de gabinetes con claves diferentes para limitar el acceso a los gabinetes de grupos o usuarios individuales. Pero esto requiere de un sistema sólido para documentar las combinaciones asignadas o para la gestión de claves.

Por el contrario, el cierre electrónico puede reprogramarse con rapidez mediante nuevos códigos de acceso y no es necesario modificar el hardware. Puede asignar derechos de acceso a usuarios individuales y a gabinetes individuales. Cada usuario puede tener derechos de acceso diferentes y específicos. En la configuración de los derechos en el software se documentan simultáneamente los códigos de acceso asignados (claves).

Informes de registro y auditoría

El hecho de que los usuarios se registren en el acceso frontal controlado del edificio permite documentar la presencia de la persona en el edificio, pero no los gabinetes individuales a los que accede. Para crear un informe de acceso a gabinetes individuales, puede revisar las imágenes del video de seguridad y anotar las fechas y horas, o bien puede asignar escoltas y mantener registros manuales. Luego, puede generar informes de acceso a partir de esos registros.

Sin embargo, los sistemas de control de acceso y cierre electrónico permiten automatizar el registro de acceso a nivel del gabinete y permiten realizar informes automatizados por usuario o gabinete. Esto acelera la preparación para una auditoría y ayuda a limitar el alcance de las investigaciones de eventos.

Respuesta al evento

Cuando se produce una filtración de datos, la respuesta al evento es fundamental. Con un sistema de cierre cifrado, debe verificar manualmente el estado de las puertas y las claves. Si se pierde o se roba una clave, debe volver a programar las cerraduras. Los informes requieren la recolección, la revisión y la preparación manuales de registros.

Los sistemas de control de acceso y cierre electrónico simplifican, acortan y, en algunos casos, automatizan estas respuestas. Puede deshabilitar rápidamente una credencial o reprogramar las cerraduras. Puede recibir una notificación de manera proactiva si una puerta se deja abierta o destrabada (desbloqueada). Puede filtrar y crear informes de acceso rápidamente.

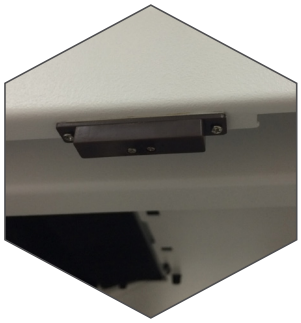
Aspectos básicos de los sistemas de control de acceso y cierre electrónico a nivel del bastidor

A nivel del bastidor, los sistemas de control de acceso y cierre electrónico tienen cinco componentes básicos:

1. Cerraduras electrónicas
2. Sensores de la puerta
3. Cableado y conexiones de red
4. Software de monitoreo
5. Claves

En el diagrama a continuación (Figura 4) se muestra cómo se conectan estos componentes. En la siguiente sección, se brindan más detalles sobre cada uno de estos componentes.

Sensorde la puerta



Key Acess Card

Cerraduras delanteras y traseras

Software de monitoreo

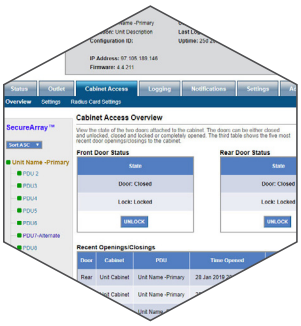


Figura 4: Cableado y conexiones de red

Module with Network Connections

Cerraduras electrónicas

Las cerraduras electrónicas permiten asegurar las puertas de los gabinetes, detectan los intentos de acceso e indican el estado de bloqueo (cierre) o apertura de la puerta. Por lo general, son una manija giratoria con un solenoide integrado que hace funcionar el pestillo para abrir o cerrar la puerta, un sensor de proximidad que indica el estado abierto o cerrado del pestillo y un lector de tarjetas de acceso que detecta y lee los valores de las claves introducidas. Algunos modelos también pueden incluir un teclado integrado o un lector biométrico (Figura 5).

Figura 5: Varios estilos de cerraduras electrónicas integradas con manijas giratorias del gabinete. Las fotos son de las soluciones de cierre de Southco®: www.southco.com.

A diferencia de las cerraduras mecánicas, las cerraduras electrónicas conectadas en red pueden indicar un estado de desbloqueo, registrarán todos los intentos de acceso (autorizados o no autorizados), pueden ser destrabadas (desbloqueadas) remotamente por los administradores de sistemas, se pueden cerrar (bloquearse) automáticamente después de un tiempo de haber estado abiertas, pueden medir el tiempo en el que han estado destrabadas (desbloqueadas) e indicarán si el pestillo ha sido manipulado (forzado mecánicamente o abierto mediante la anulación de la llave física).

Sensores de la puerta

Los sensores de la puerta indican que la puerta del gabinete está abierta o cerrada. Son sensores de proximidad por separado ubicados en el marco y el umbral de la puerta del gabinete, generalmente, del lado de enganche de la puerta (Figura 6).

Los sensores de la puerta se pueden usar para enviar una notificación de advertencia si la puerta se abre y para determinar el tiempo durante el cual la puerta estuvo abierta.

Cableado o conexión de red con un módulo de controlador

Hay dos opciones: instalarlo al sistema de control de acceso al edificio (BACS) existente o conectarlo como un sistema en red por separado. La instalación en el BACS requiere del cableado desde cada cerradura electrónica y sensor de la puerta a un panel centralizado. Por lo general, para esto se necesita que un electricista conecte las manijas, incluida la instalación de los conductos o una estructura de paso para asegurar o aislar el cableado de la cerradura electrónica de la red y los cables de alimentación.

El cableado, como un sistema en red por separado, implica conectar las cerraduras electrónicas y los sensores de la puerta a un pequeño módulo del controlador instalado en un bastidor (Figura 7). El módulo del controlador tiene una conexión de red y una conexión eléctrica. Se conecta a un switch de red con un cable de conexión de red estándar. El personal del sitio puede instalar este sistema o puede instalarse previamente en el gabinete, y necesita un puerto de red y una dirección IP para cada módulo del controlador.

Para garantizar que el módulo del controlador tenga el mayor rango de compatibilidad y seguridad posibles para la red, asegúrese de que admita los protocolos IPv4 e IPv6 para el direccionamiento TCP/IP con asignaciones de direcciones estáticas o dinámicas, y los protocolos SNMP v1, v2c y v3 para la integración del software de Gestión de la infraestructura del centro de datos (DCIM) de terceros. La interfaz web debe admitir sesiones HTTP o HTTP con puertos definibles. Las conexiones de red deben admitir cifrado y certificados. La conexión del servidor de correo electrónico debe ser saliente solo con el protocolo TLS y puertos definibles. Para facilitar el mantenimiento, el módulo del controlador debe admitir la configuración masiva y las actualizaciones de firmware. El firmware debe registrar cada cambio del sistema.

Figura 6: Sensor de puerta instalado en la puerta de un gabinete.

Figura 7: Módulo del controlador y mazo de cables.

Software de monitoreo

El software de monitoreo será específico del sistema de cierre seleccionado y, en sistemas en red por separado, puede integrarse en el firmware del módulo del controlador. Debe proporcionar una sólida seguridad de inicio de sesión, roles de administrador y usuario separados, cuentas de usuario individuales, fácil administración de los derechos de acceso del usuario para una rápida asignación y eliminación de derechos de usuario, registro de eventos, notificaciones de eventos y registro de informes de acceso o exportación.

El acceso debe estar protegido por contraseña con niveles de derechos de usuario separados para administradores y usuarios. Debe admitir la autenticación del usuario desde una base de datos interna, una base de datos LDAP o una base de datos RADIUS. Los administradores deben poder asignar derechos de acceso individuales a la cerradura electrónica (puerta del gabinete) específicos del usuario; deben poder destrabar (desbloquear) las cerraduras electrónicas (puertas del gabinete) de manera remota y establecer un tiempo específico para que las cerraduras (puertas) permanezcan destrabadas (desbloqueadas).

La interfaz del software debe indicar con claridad las condiciones de apertura y cierre; registrar cada intento de acceso y asociar el intento con una clave y un usuario específicos; y determinar condiciones de apertura, desbloqueo y manipulación (Figura 8). Lo ideal es que en los informes figure el acceso por gabinete o por usuario de cualquier período de registro de eventos definido.

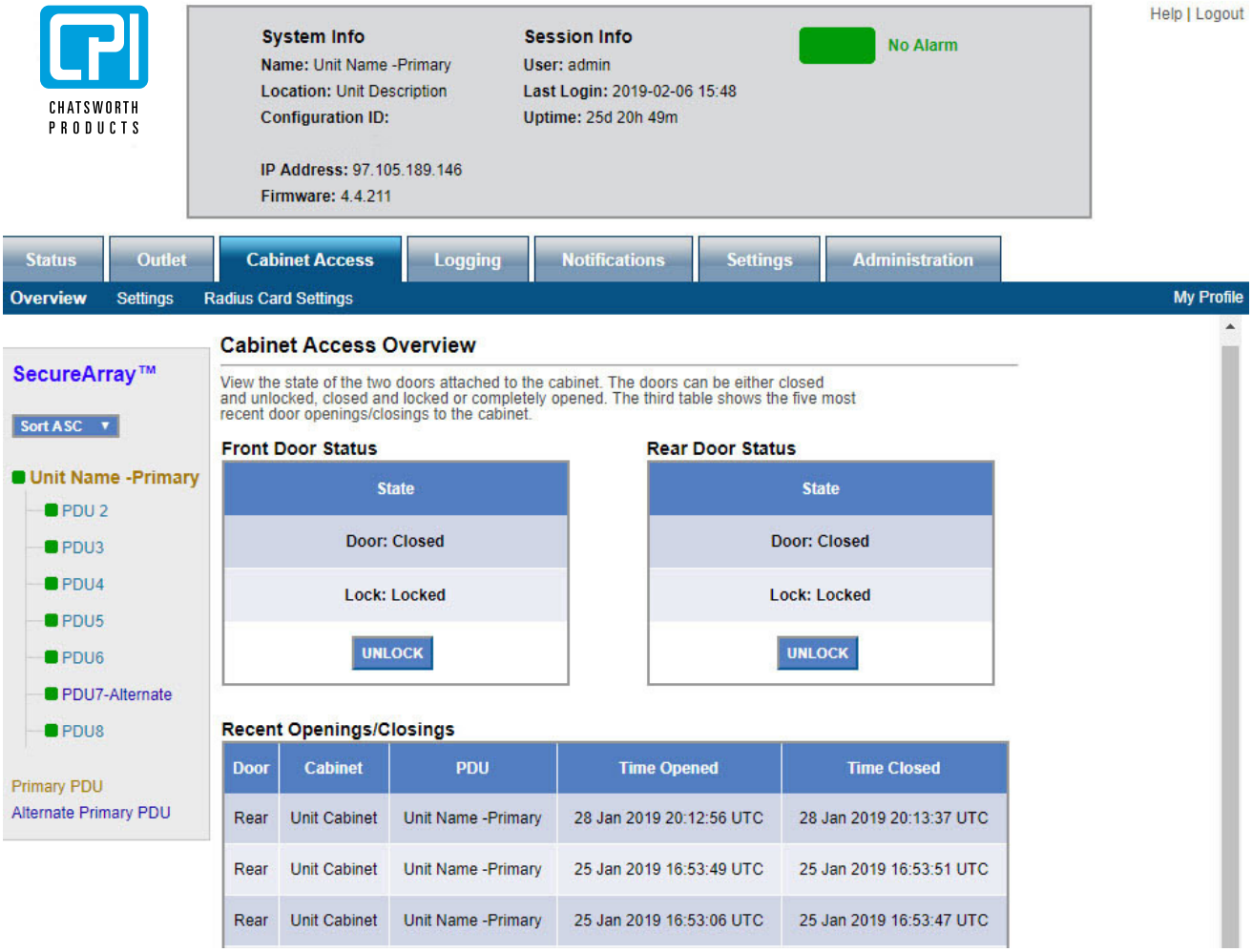


Figura 8: Captura de pantalla del sistema de EAC en red de CPI que muestra las condiciones de bloqueo y la puerta.

Claves

Hay tres tipos de claves para los sistemas de control de acceso y cierre electrónico: tarjetas de acceso, teclado y código, y biométricas. No hay una interfaz mecánica entre la clave y la cerradura. Todos los derechos se asignan en el software. Algunos sistemas utilizan varias claves para proporcionar una mayor seguridad.

En el caso de sistemas biométricos y con tarjeta de acceso, la cerradura electrónica debe tener un lector compatible (Figura 9). El software debe admitir la asignación de códigos clave. Si desea utilizar una tarjeta de acceso existente, como una credencial de empleado emitida por la compañía, deberá asegurarse de contar con estas compatibilidades. De lo contrario, es posible que deba asignar una segunda credencial a los empleados que deberían tener acceso a los gabinetes de ICT.

Figura 9: Tarjeta de acceso utilizada con cerradura electrónica con lector de tarjeta de proximidad integrado.

Principales desafíos de la implementación del cierre electrónico al nivel del bastidor

Las organizaciones que han estudiado la implementación del cierre electrónico a nivel del bastidor, a menudo, se encuentran con dos desafíos principales: el costo del hardware y de la implementación. Además, puede haber algunas preocupaciones a nivel organizativo si TI opta por un sistema por separado fuera del control directo del Departamento de Seguridad. Finalmente, la actualización del sistema puede resultar difícil.

El desafío del costo del hardware

Puede haber un costo inicial significativo de hardware para implementar el cierre electrónico en los bastidores. En primer lugar, debe instalarse en cada manija (pestillo) de la puerta una cerradura electrónica. En segundo lugar, se deben conectar las cerraduras a un panel central o a los módulos del controlador en cada bastidor. Si utiliza módulos del controlador, estos se deberían conectar a la red de TI, para lo que se necesitarían switches de red adicionales. Los módulos del controlador también deben recibir alimentación en cada bastidor. Puede que también haya un contrato de software, licencia y mantenimiento por separado.

El desafío del costo de implementación

El sistema se deberá configurar, y luego, gestionar. Si está conectado a la red de TI, cada módulo del controlador usará un puerto de red y una dirección IP. Estos puertos se agregan a otros puertos y direcciones que se usan para monitorear una unidad de distribución de energía (PDU) inteligente y un sistema de monitoreo ambiental a nivel del bastidor. Es posible que se necesite un servidor para ejecutar el software y almacenar los datos registrados. Estos representan costos continuos de energía, redes y administración de sistemas.

El desafío de la propiedad organizacional

El sistema puede ser un sistema por separado del sistema de seguridad del edificio principal. ¿El Departamento de Seguridad o de TI es propietario del sistema y gestiona el acceso de autorización a los usuarios? Tiene más sentido que TI tenga el control de acceso a nivel del bastidor, incluso si debe ser un sistema por separado. TI es responsable de los equipos y los datos protegidos en los gabinetes y el mantenimiento de esos sistemas. Además, el acceso al gabinete debe estar estrechamente integrado a los sistemas empresariales, como RADIUS y LDAP para la autenticación del usuario.

El desafío de la modernización del hardware

Es posible que el hardware del sistema y los mazos de cables no se ajusten bien a los gabinetes existentes. Las cerraduras electrónicas generalmente tienen un diseño de manija giratoria y el recorte en la puerta del gabinete puede o no coincidir con la cerradura electrónica modificada. Además, deberán conectarse las manijas a un módulo del controlador o a un panel del BACS. Puede resultar difícil conectar los cables a través de un gabinete lleno.

La solución de CPI

La solución de CPI aborda ambos desafíos al reducir los costos de hardware e implementación y al ofrecer un sistema fácil de configurar, usar y mantener. La solución de CPI tiene tres componentes: PDU de eConnect® con RFID Electronic Lock Kits and Temperature and Humidity Sensors y Power IQ® para el software de DCIM

PDU de eConnect con RFID Electronic Lock Kit and Temperature and Humidity Sensors

La PDU de eConnect con RFID Electronic Lock Kit and Temperature and Humidity Sensors resuelven el costo del hardware al consolidar el sistema de control y monitoreo de energía de una PDU con un sistema de monitoreo ambiental y un sistema de control de acceso y cierre electrónico en una sola solución de hardware. Esta solución utiliza un solo firmware, una interfaz web y una conexión de red. La solución eConnect de CPI permite reducir la cantidad de puertos de red necesarios para monitorear el control de la energía, el medio ambiente y el acceso en un solo bastidor de tres a uno. El cierre electrónico y los sensores ambientales se conectan a la PDU y reciben alimentación de esta. Hay una interfaz web para acceder, configurar, monitorear e informar todas las condiciones a nivel del bastidor.

La PDU de eConnect con RFID Electronic Lock Kit resuelve los costos de implementación gracias a la tecnología de consolidación IP Secure Array integrada. Esto permite que hasta 32 PDU con todas las cerraduras y sensores ambientales instalados compartan una sola conexión de red o dos conexiones de red por cuestiones de redundancia (Figura 10). Esto reduce en gran medida el número de puertos de red, direcciones IP y switches de red asociados necesarios para respaldar el sistema. Al igual que la PDU eConnect individual, cada Secure Array puede verse desde una única interfaz web.

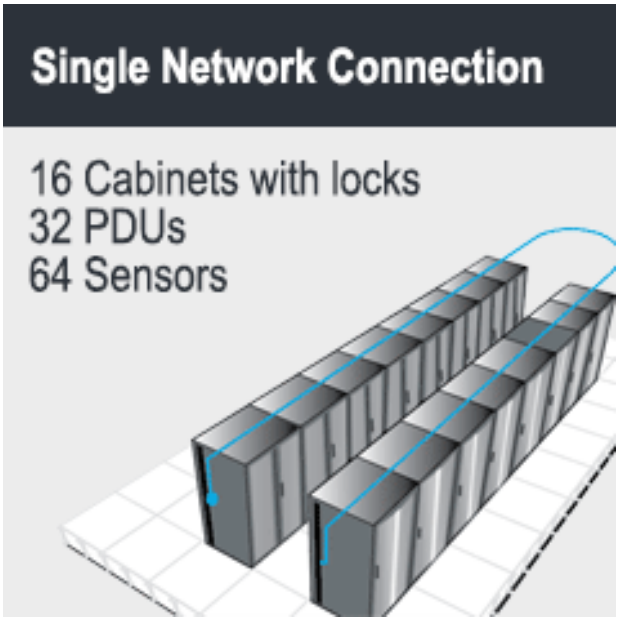


Figura 10: La PDU eConnect de CPI integra el monitoreo de energía, el monitoreo ambiental y el control de acceso en un solo sistema. La tecnología de consolidación IP de Secure Array integrada permite que hasta 32 PDU y todas las cerraduras y los sensores instalados compartan una sola conexión de red.

Dato útil

Si está modernizando una solución existente y no necesita actualizar sus PDU, aún puede reducir los costos de hardware e implementación con el Control de acceso electrónico en rCPI Networked RFID Electronic Lock Kit chatsworth.com/14667-001, que combina el cierre electrónico y el monitoreo ambiental en una sola solución y es compatible con la tecnología de consolidación IP de Secure Array de CPI.

Power IQ para el software de DCIM de la PDU de eConnect

Power IQ para la PDU de eConnect es un software de DCIM que le permite monitorear todas las PDU de eConnect con EAC de la sala, sitio o múltiples sitios desde una sola pantalla. Power IQ reconoce la tecnología de consolidación IP de Secure Array IP e identifica todos los dispositivos en la red, por lo que tiene la ventaja de contar con menos conexiones de red, pero aún sigue viendo cada dispositivo individual en la interfaz del software.

Power IQ usa tableros gráficos para mostrar las condiciones inmediatas en los bastidores, lo que le permite identificar rápidamente los problemas que deben abordarse (Figura 11). Analiza las tendencias de los datos de energía y ambientales para que pueda monitorear y optimizar la capacidad. Proporciona un solo lugar para asignar derechos de acceso a todos los gabinetes de la red, y también genera informes sobre intentos de acceso por gabinete y usuario.

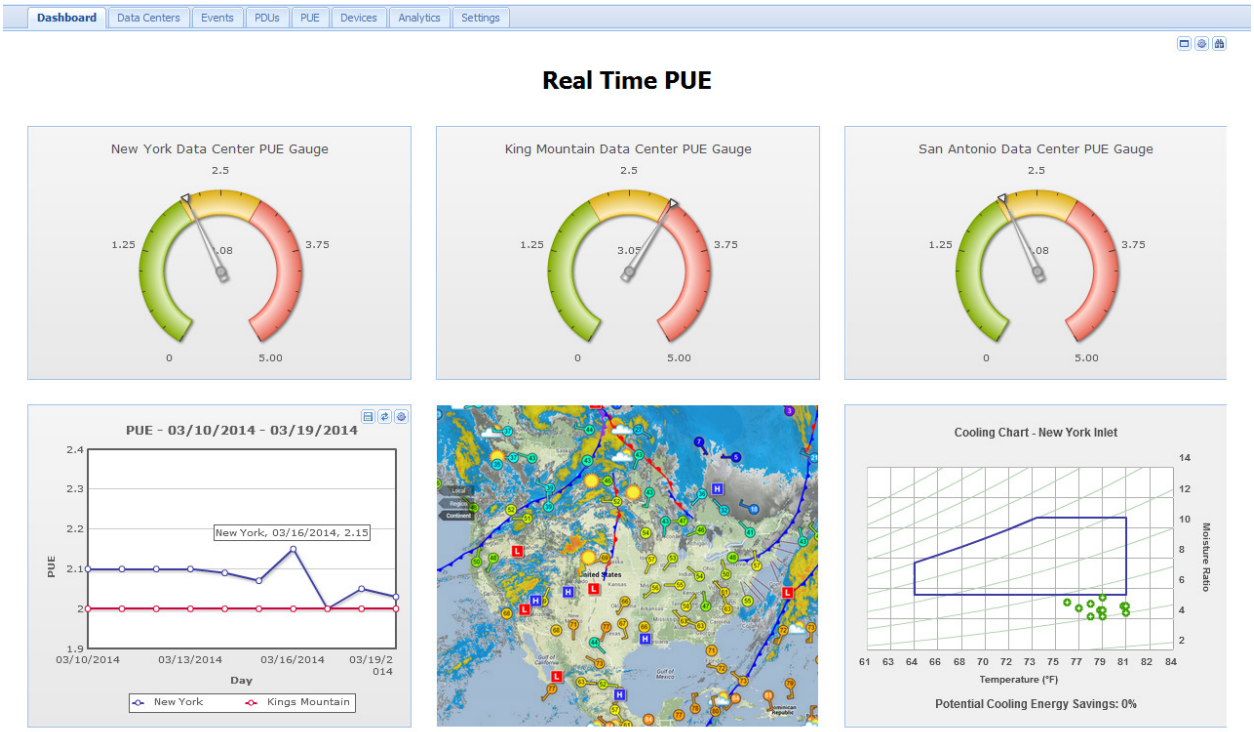


Figura 11: Power IQ para la PDU de eConnect permite monitorear las condiciones del sitio desde una sola pantalla. Los diales y cuadros fáciles de leer lo ayudan a identificar problemas y tendencias con rapidez.

Comparación de la solución de CPI con la solución tradicional

En la (Tabla 1) a continuación se comparan los costos estimados de una solución tradicional y la solución del ecosistema de CPI para obtener una solución completa de monitoreo a nivel del bastidor. La solución tradicional tiene dos PDU inteligentes para el monitoreo de la energía, un sistema de monitoreo ambiental por separado y un sistema de control de acceso electrónico por separado. Cada uno tiene una conexión de red y un software de monitoreo por separado. La solución del ecosistema de CPI es la PDU de eConnect con RFID Electronic Lock Kit and Temperature and Humidity Sensors.

Comparación de costos estimados de un NUEVO sistema de monitoreo para 16 gabinetes							
	Sistema tradicional PDU separada, ambiental, y Control de acceso electrónico			Ecosistema de CPI PDU integrada, ambiental, y Control de acceso electrónico			Ahorro con CPI
Componente (estimaciones)	**CANTIDAD**	**Cada**	**Total**	**CANTIDAD**	**Cada**	**Total**	
Juego de manijas de gabinete	16	$1000,00	$16 000,00	16	$300,00	$4800,00	$11 200,00
Fuente de alimentación para el juego de manijas	16	$25,00	$400,00	0	$-	$-	$400,00
Tarjeta de acceso	5	$5,00	$25,00	5	$5,00	$25,00	$-
Software de control de acceso	1	$1000,00	$1000,00	0	$-	$-	$1000,00
Aparato de monitoreo ambiental	16	$750,00	$12 000,00	0	$-	$-	$12 000,00
Suministro eléctrico para electrodomésticos	16	$25,00	$400,00	0	$-	$-	$400,00
Sensores ambientales	32	$5,00	$160,00	32	$5,00	$160,00	$-
Software de monitoreo ambiental	1	$1000,00	$1000,00	0	$-	$-	$1000,00
PDU inteligentes	32	$1000,00	$32 000,00	32	$1000,00	$32 000,00	$-
Software de monitoreo de PDU	1	$1000,00	$1000,00	0	$-	$-	$1000,00
Software DCIM	1	$5000,00	$5000,00	1	$5000,00	$5000,00	$-
Subtotales			**$68 985,00**			**$41 985,00**	**$27 000,00**
Servicio (estimaciones)	**CANTIDAD**	**Cada**	**Total**	**CANTIDAD**	**Cada**	**Total**	
Instalación de la manija	16	$25,00	$400,00	16	$25,00	$400,00	$-
Instalación ambiental	16	$25,00	$400,00	16	$25,00	$400,00	$-
Instalación de PDU inteligente	32	$25,00	$800,00	32	$25,00	$800,00	$-
Nueva conexión de red	64	$250,00	$16 000,00	1	$250,00	$250,00	$15 750,00
Nueva conexión eléctrica	64	$250,00	$16 000,00	32	$250,00	$8000,00	$8000,00
Gestión de TI, configuración del sistema	4	$500,00	$2000,00	1	$500,00	$500,00	$1500,00
Contrato de mantenimiento de software	4	$100,00	$400,00	1	$100,00	$100,00	$300,00
Subtotales			**$36 000,00**			**$10 450,00**	**$25 550,00**
Total			**$104 985,00**			**$52 435,00**	**$52 550,00**
Ahorros estimados con CPI					**50 %**	**$(52 550,00)**	

Tabla 1: Comparación de los costos estimados para los componentes y la instalación de una solución completa de monitoreo a nivel de gabinete que incluye PDU inteligentes, monitoreo ambiental y ecosistema de gabinete. El sistema tradicional utiliza sistemas de hardware separados, conexiones de red y software de monitoreo. El ecosistema de CPI utiliza hardware y firmware integrados, y la tecnología de consolidación IP de Secure Array.

Nota: El precio es estrictamente una estimación. La comparación muestra las diferencias relativas en las cantidades de componentes y servicios para los sistemas dados, pero los precios unitarios reales variarán según los sistemas seleccionados.

La solución de ecosistema de gabinete de CPI consolida el sistema de control y monitoreo de energía (PDU), el sistema de monitoreo ambiental y el sistema de control de acceso y cierre electrónico en una sola plataforma de hardware con una sola conexión de red. Por lo tanto, solo necesita una conexión de red por bastidor en lugar de cuatro con una solución estándar. Además, la tecnología de consolidación IP de Secure Array de CPI permite que se conecten 32 PDU y todas las cerraduras electrónicas y sondas ambientales asociadas a través de una sola conexión de red. El resultado es una reducción significativa de los puertos de red necesarios para implementar el monitoreo y el control de acceso a nivel del bastidor, y la reducción de los costos de redes correspondientes (Figura 12).

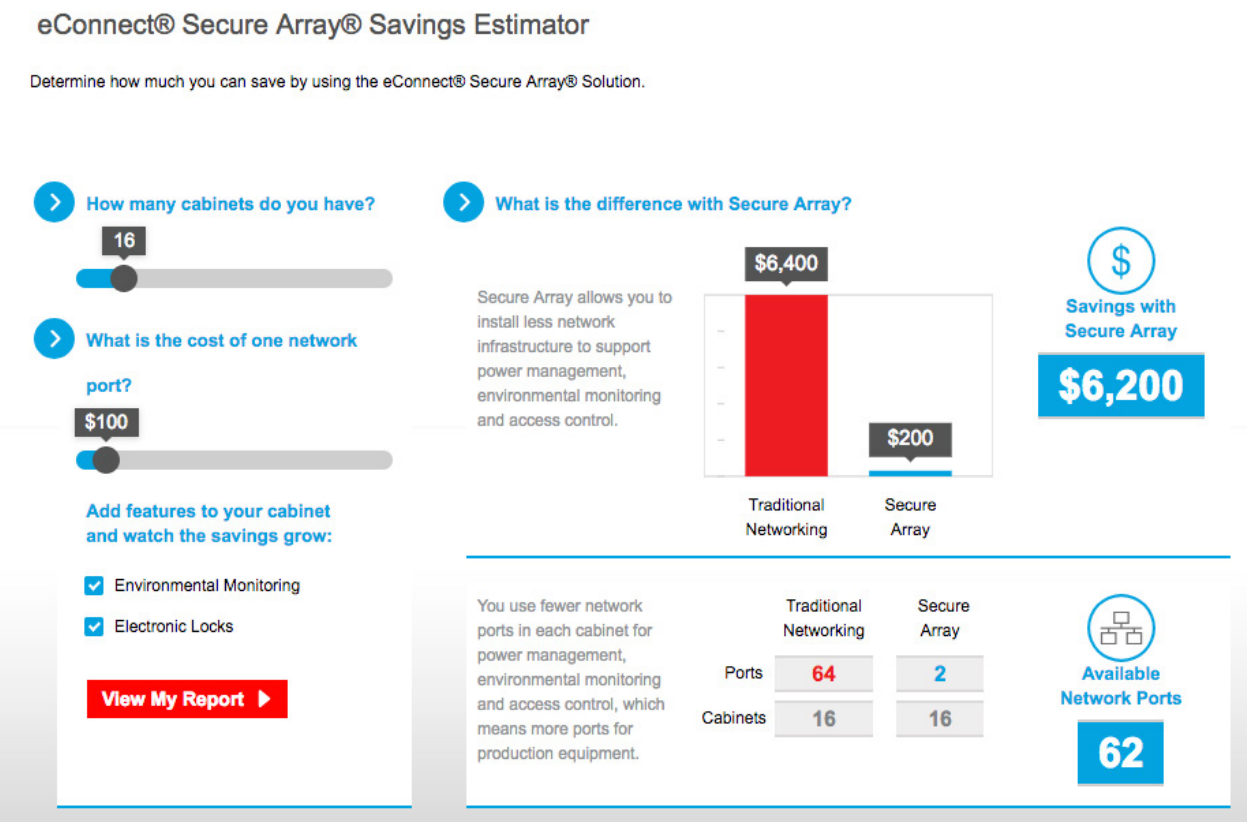


Figura 12: Captura de pantalla de la herramienta en línea Estimador de ahorros Secure Array eConnect de CPI, que le permite comparar el costo relativo de la red de un sistema tradicional con el sistema de CPI con Secure Array.

Dato útil

Pruebe el Estimador de ahorros Secure Array eConnect de CPI chatsworth.com/en-us/resources/configurators-and-estimators/estimator-page para ver cuánto puede ahorrar con la PDU eConnect de CPI con EAC y Secure Array.

¿Qué sucede con las actualizaciones?

Si está actualizando un sitio existente y ya ha implementado PDU inteligentes, la consolidación IP de Secure Array eConnect aún reducirá el costo frente a un sistema tradicional, pero el hardware consolidado ofrece menos beneficios porque está implementando un hardware por separado. En la (Tabla 2) a continuación, se comparan los costos estimados de una solución tradicional y la solución del ecosistema de gabinetes de CPI para obtener una solución de actualización del sistema de control de acceso y cierre electrónico.

Comparación de costos estimados de un NUEVO sistema de control de acceso para 16 gabinetes							
	Sistema tradicional Control de acceso electrónico			CPI en red Control de acceso electrónico			Ahorro con CPI
Componente (estimaciones)	**CANTIDAD**	**Cada**	**Total**	**CANTIDAD**	**Cada**	**Total**	
Juego de manijas de gabinete	16	$1000,00	$16 000,00	16	$1000,00	$16 000,00	$-
Fuente de alimentación para el juego de manijas	16	$25,00	$400,00	16	$25,00	$400,00	$-
Tarjeta de acceso	5	$5,00	$25,00	5	$5,00	$25,00	$-
Software de control de acceso	1	$1000,00	$1000,00	0	$-	$-	$1000,00
Subtotales			**$17 425,00**			**$16 425,00**	**$1000,00**
Servicio (estimaciones)	**CANTIDAD**	**Cada**	**Total**	**CANTIDAD**	**Cada**	**Total**	
Instalación de la manija	16	$25,00	$400,00	16	$25,00	$400,00	$-
Nueva conexión de red	16	$250,00	$4000,00	2	$250,00	$500,00	$3500,00
Nueva conexión eléctrica	16	$250,00	$4000,00	16	$250,00	$4000,00	$-
Gestión de TI, configuración del sistema	1	$500,00	$500,00	1	$500,00	$500,00	$-
Contrato de mantenimiento de software	1	$100,00	$100,00	0	$-	$-	$100,00
Subtotales			**$9000,00**			**$5400,00**	**$3600,00**
Total			**$26 425,00**			**$21 825,00**	**$4600,00**
Ahorros estimados con Networked Electronic Locks de CPI					**17 %**	**$(4600,00)**	

Tabla 2: Comparación de los costos estimados para los componentes y la instalación de un sistema de control de acceso y cierre electrónico a nivel del bastidor actualizado. Ambos sistemas requieren de un módulo del controlador en cada gabinete y una fuente de alimentación para el módulo (juego de manija), pero el ecosistema de gabinete de CPI tiene un firmware integrado (software) y una tecnología de consolidación IP Secure Array, lo que reduce los costos de red.

Nota: El precio es estrictamente una estimación. La comparación muestra las diferencias relativas en las cantidades de componentes y servicios para los sistemas dados, pero los precios unitarios reales variarán según los sistemas seleccionados.

Conclusión

La extensión de la seguridad física al nivel del bastidor con un sistema de control de acceso y cierre electrónico proporciona la solución más segura físicamente para la protección de datos. Este enfoque permite ubicar el monitoreo y el registro de cada intento de acceso en el punto más cercano al equipo. Simplifica la gestión de claves y credenciales, documenta automáticamente cada intento de acceso, proporciona a TI una notificación inmediata de las condiciones de apertura de la puerta y permite una respuesta a los eventos mucho más rápida.

Sin embargo, a menudo, las organizaciones que están considerando la adopción de estos sistemas han descubierto que tienen altos costos de hardware e implementación. CPI aborda ambas inquietudes gracias a la PDU eConnect con sistema de control de acceso electrónico. La PDU eConnect de RFID Electronic Locking Kit combina el sistema de control y monitoreo de energía a nivel del bastidor, el sistema de monitoreo ambiental y el sistema de control de acceso y cierre electrónico en una sola solución, lo que reduce los costos de hardware y los requisitos de red.

Además, CPI puede ser la única fuente de gabinetes, cierre electrónico, PDU inteligentes, monitoreo ambiental y software de DCIM, e instalará previamente las cerraduras y las PDU en los gabinetes, lo que acelerará su implementación. Lo llamamos el ecosistema del gabinete de CPI. Comuníquese con el Soporte Técnico de CPI (techsupport@chatsworth.com) para obtener más detalles.

Referencias

[1] 1104.° Congreso de los Estados Unidos. Ley Pública 104-191. Estatuto 110, 1936. Ley de Portabilidad y Responsabilidad de los Seguros Médicos (HIPAA). Promulgada el 21 de agosto de 1996. www.congress.gov/bill/104th-congress/house-bill/3103?s=10&r=68

[1]Legislación relacionada. Departamento de Salud y Servicios Humanos de los Estados Unidos (HHS). Ley de Tecnología de la Información de la Salud para la Salud Económica y Clínica (Ley HITECH) de 2009. www.healthit.gov/topic/laws-regulation-and-policy/health-it-legislation.

[2]113.° Congreso de los Estados Unidos. Ley Pública 113-283. Estatuto 113, 2521. Ley Federal de Modernización de Seguridad de la Información (FISMA) de 2014. Promulgada el domingo, 14 de diciembre de 2014. www.congress.gov/bill/113th-congress/senate-bill/2521?q=%7B%22search%22%3A%5B%22FISMA%22%5D%7D&s=7&r=2.
www.dhs.gov/fisma.

[3]Unión Europea. Parlamento Europeo. Norma (UE) 2016/679. Reglamento General de Protección de Datos (GDPR). Promulgado el 27 de abril de 2016.eur-lex.europa.eu/eli/reg/2016/679/oj.

[4]Consejo de Normas de Seguridad de la Industria de Tarjetas de Pago. Normas de Seguridad de Datos para la Industria de Tarjetas de Pago (PCI-DSS v3.2.1). Publicada en mayo de 2018. www.pcisecuritystandards.org/document_library.

[5]Instituto Estadounidense de Contadores Públicos Certificados (AICPA). Sistema y el Control de Organización (SOC-2), Reporting on Controls at a Service Organization Relevant to Security, Availability, Processing Integrity, Confidentiality or Privacy Guide (Guía de informe de controles en una organización de servicios respecto de la seguridad, la disponibilidad, la integridad de procesamiento, la confidencialidad o la privacidad). Publicado en 2011. www.aicpa.org/interestareas/frc/assuranceadvisoryservices/sorhome.html
www.aicpa.org/interestareas/frc/assuranceadvisoryservices/cybersecurityforcpas.html.

[5]Instituto Estadounidense de Contadores Públicos Certificados (AICPA). Comité Ejecutivo de Servicios de Aseguramiento (ASEC). Criterios de servicios de confianza. Publicado en 2017.
www.aicpa.org/content/dam/aicpa/interestareas/frc/assuranceadvisoryservices/downloadabledocuments/trust-services-criteria.pdf.

[6]IBM. IBM Security. Índice de inteligencia sobre amenazas X-Force de IBM de 2017. Publicadoen marzo de 2017.
www.ibm.com/security/data-breach/threat-intelligence.

[7]IBM. IBM Security. Índice de inteligencia sobre amenazas X-Force de IBM de 2018. Publicado en marzo de 2018.
www.ibm.com/security/data-breach/threat-intelligence.

Colaboradores

David Knapp | Gerente de Marketing de productos

David Knapp es el gerente de Marketing de productos en Chatsworth Products (CPI), un fabricante global de productos y soluciones de servicio que optimiza, almacena y asegura equipos de tecnología. David tiene más de 18 años de experiencia en la industria de las telecomunicaciones como experto en aplicaciones de productos y comunicador técnico. Actualmente, se concentra en soluciones de centros de datos, redes empresariales y gestión de la energía.

Ashish Moondra | Gerente de productos sénior, Energía, Electrónica y Software

Ashish Moondra es gerente de productos sénior de Energía, Electrónica y Software en Chatsworth Products (CPI). Tiene 20 años de experiencia en el desarrollo, la venta y la gestión de soluciones de distribución de energía en bastidores, suministro de energía ininterrumpida, almacenamiento de energía y gestión de DCIM. Ashish trabajó anteriormente en American Power Conversion, Emerson Network Power y Active Power.

Raissa Carey | Especialista en Relaciones Públicas y escritora técnica

Raissa Carey es periodista con más de 20 años de experiencia en la producción, el desarrollo y la gestión de una variedad de artículos de noticias y marketing de contenido en varias industrias en los Estados Unidos e internacionalmente. Desde 2013, Carey ha sido escritora creativa y técnica en Chatsworth Products, y ha contribuido en gran medida con el liderazgo de pensamiento y el contenido basado en soluciones globalmente.

CHATSWORTH PRODUCTS