Cinco buenas prácticas para mejorar la ciberseguridad de los sistemas de gestión de edificios (BMS)

Por Gregory Strass, CISSP, CEH
Jon Williamson

Resumen del artículo

Las filtraciones de datos y otros ciberdelitos cuestan a las empresas miles de millones cada año en todo en todo el mundo, y el daño causado a la reputación de la marca puede ser incalculable. Dado que los *hackers* buscan sistemas poco protegidos para dirigir sus ataques, el propósito de este documento es presentar cinco "buenas prácticas" en el ámbito de la ciberseguridad para mitigar las vulnerabilidades de los sistemas. En algunos casos se trata de medidas de sentido común, tales como una gestión efectiva de las contraseñas; otras consisten en proteger puertos abiertos y otros puntos de acceso, actualizaciones de software, gestión de usuarios y planes de vulnerabilidad.

998-2095-07-29-14AR0

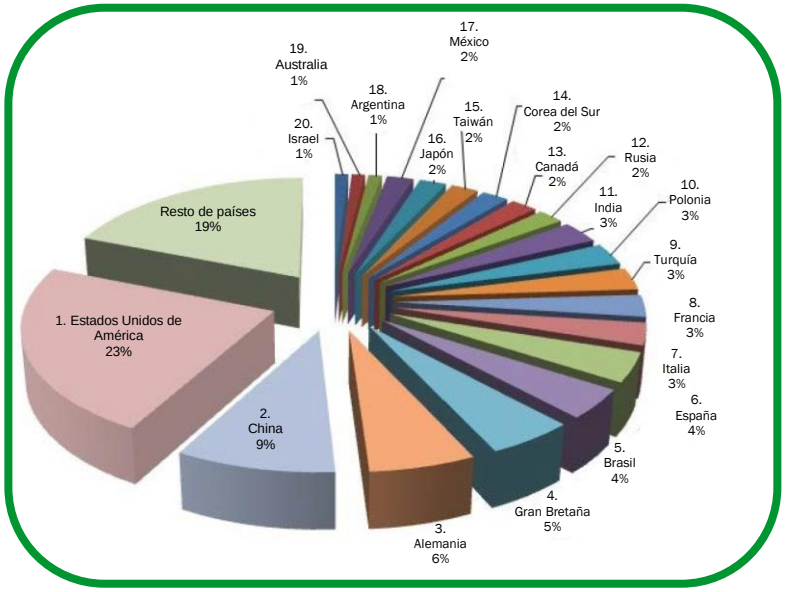
Schneider Electric

Introducción

Los ataques y las amenazas en el campo de la ciberseguridad se han convertido en un hecho común y constituyen un problema global. Los ciberdelincuentes tienen como objetivo de sus ataques a personas y empresas, y los llevan a cabo cada vez con más frecuencia, con un mayor grado de sofisticación y de forma más coordinada. Solo en Estados Unidos los ciberataques se multiplicaron por 17 entre 2009 y 2011.[1] El Centro Europeo de Ciberdelincuencia de la Europol ha identificado los 20 principales países por ciberdelitos **(Figura 1),** y no existe ninguna región del mundo que sea inmune. No es de sorprender que los países con infraestructuras de Internet más avanzadas y que han incorporado más tecnologías digitales on-line a sus operaciones empresariales diarias sufran más incidentes relacionados con ciberataques.

Figura 1

Los 20 principales países que sufren ciberdelitos

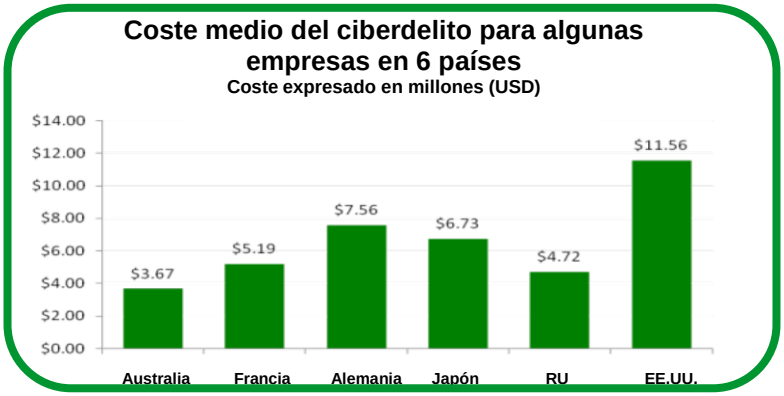


"La delincuencia cibernética es una empresa criminal de ámbito mundial de 400.000 millones de dólares, por lo que supera al tráfico de drogas global".

El ciberdelito cuesta literalmente a las empresas cientos de miles de millones de dólares cada año. Una agencia policial internacional estima que las víctimas pierden alrededor de 400.000 millones de dólares cada año en todo el mundo, lo que lo convierte en una empresa criminal mayor que el comercio global de marihuana, cocaína y heroína juntas.[2] Otro informe arroja la misma conclusión: estima que el coste de las actividades cibernéticas maliciosas mueve, en el ámbito mundial, entre 300.000 millones y un billón de dólares.[3] El impacto financiero para las empresas varía de un país a otro **(Figura 2)** y según sectores, pero una característica común es que los ciberataques cuestan cada año más dinero a las empresas **(Figura 3).**[44]

Figura 2

Coste medio del ciberdelito según una encuesta realizada a 234 empresas en seis países.[4]



[1] "The Economic Benefits from Improved Cyber Security Infrastructure", Gary Anderson y Gregory Tassey. NIST Economic Analysis Office Economic & Policy Analysis Brief 13-3

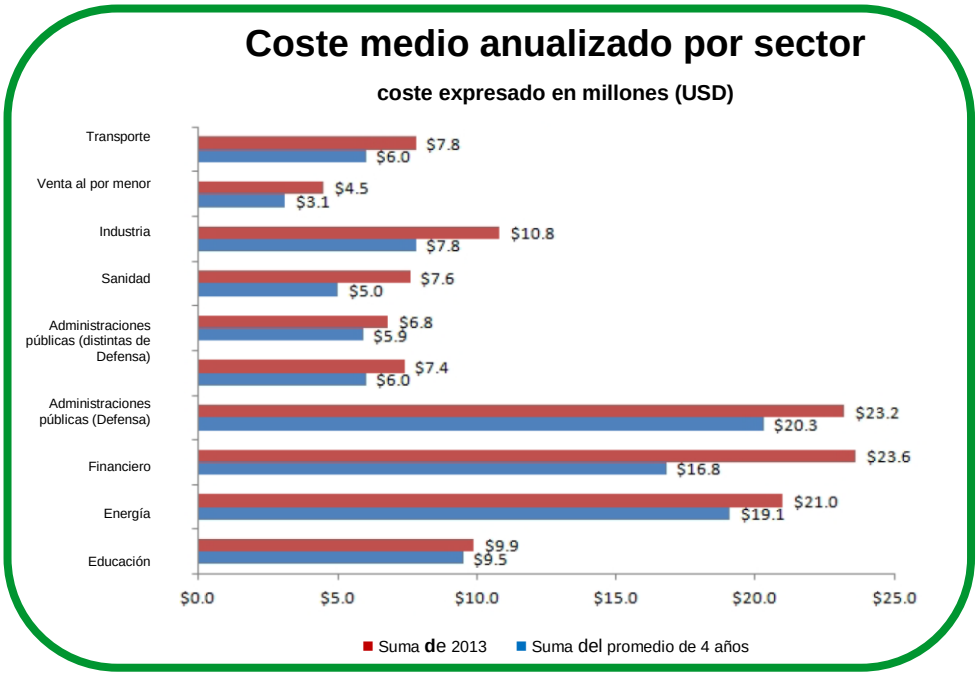
[2] "Cybercrime: A growing global problem", Centro Europeo de Ciberdelincuencia.

[3] "The Economic Impact of Cybercrime and Cyber Espionage", McAfee y Centro de Estudios Estratégicos e Internacionales, julio de 2013.

[4] "2013 Cost of Cyber Crime: Global Report", Ponemon Institute, octubre de 2013.

Figura 3

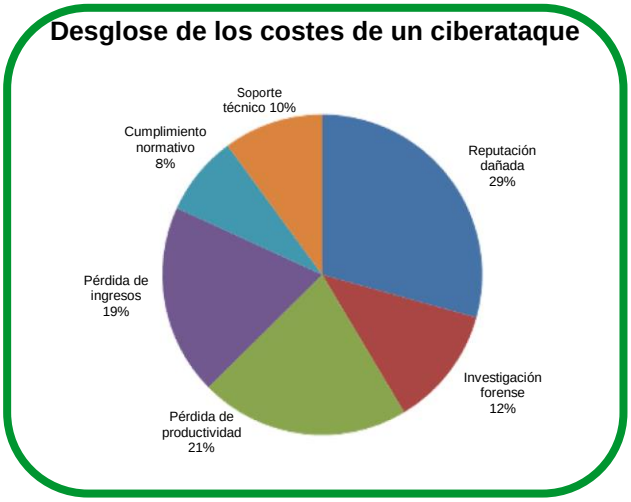
Coste medio en 2013 del ciberdelito por sector frente al promedio de los 4 años anteriores



Las consecuencias económicas de un ataque de ciberseguridad incluyen costes directos, como son la investigación forense de la filtración, el soporte técnico, la pérdida de ingresos, la actualización de actividades y tecnologías de ciberseguridad y, también, costes indirectos, tales como pérdida de productividad, incumplimiento normativo, pérdida de propiedad intelectual, degradación de la calidad del producto o servicio y, lo más difícil de cuantificar pero quizás lo más costoso de todo, el daño a la reputación de la empresa y/o la pérdida de clientes **(Figura 4)**[5]**.**

Figura 4

Consecuencias económicas de un ciberataque desglosadas en 6 categorías.



Los sistemas de gestión de edificios (BMS), antaño propietarios e independientes, están integrados en la actualidad con otros sistemas. Los sistemas de gestión inteligente de edificios (iBMS) actuales están conectados en red con data centers de IT, servidores de acceso remoto y empresas de servicios públicos mediante protocolos abiertos. Si bien

5 "Understanding the economics of IT risk and reputation," IBM, noviembre de 2013.

estos iBMS ofrecen ventajas significativas, también exponen a las empresas a mayores vulnerabilidades de ciberseguridad.

Este documento analiza prácticas y procedimientos para hacer que los iBMS sean más seguros sobre el terreno. Muchas de las medidas puedan resultar sonar conocidas y de sentido común, pero se explican los motivos por los que son tan importantes. Estas buenas prácticas giran en torno a los siguientes 5 aspectos de ciberseguridad, así como de otras actividades que deben tenerse en cuenta:

1. Gestión de contraseñas
2. Gestión de la red
3. Gestión de usuarios
4. Gestión de software
5. Gestión de vulnerabilidades

La consecución de mejoras en estos 5 campos ofrece grandes réditos y aporta sistemas reforzados y sólidos, menos vulnerables a los ataques.

Gestión de contraseñas

Una gestión adecuada de usuarios y contraseñas resulta vital para proteger cualquier sistema de gestión de edificios (BMS). La mayoría de los ataques a dispositivos de BMS tienen éxito gracias a la consecución de una contraseña. Podríamos abordar muchos temas relacionados con las contraseñas. Pero nos centraremos en este documento en los dos más importantes:

- Cambio de las contraseñas predeterminadas
- Complejidad de las contraseñas

Credenciales y acreditación

A menudo se utiliza el término "credencial" al hablar del nombre de usuario y la contraseña con un único elemento. El proceso de gestionar nombres de usuarios y contraseñas puede denominarse "acreditación".

Cambio de las contraseñas predeterminadas

No debe subestimarse la importancia de cambiar las contraseñas predeterminadas en cada instalación. **Es lo primero que debe hacerse al poner en marcha un nuevo dispositivo.**

Los productos se entregan con unas credenciales mínimas para permitir la puesta en marcha del sistema. Desde el punto de vista de la seguridad, cuanto más tiempo esté en funcionamiento el dispositivo con las credenciales predeterminadas desde que se desembala, mayor es el riesgo de uso fraudulento.

Muchos piensan que el cambio de las credenciales predeterminadas es innecesario porque a nadie le va a interesar su dispositivo, por no hablar de que alguien sea capaz de encontrarlo en Internet. Por desgracia, la realidad es todo lo contrario. Los dispositivos que mantienen las credenciales predeterminadas hacen que piratear un BMS sea un juego de niños.

Aunque el fabricante no lo pretenda, los valores predeterminados de las credenciales de los dispositivos acaban siendo de dominio público o apareciendo en Internet. Basta con hacer una consulta en Google para encontrarlos. Existen motores de búsqueda que analizan de forma rutinaria todos los dispositivos accesibles conectados a Internet, incluidos los dispositivos BMS. Una cantidad considerable de información acerca de los dispositivos se almacena en la base de datos del servicio. Por lo tanto, esos datos están disponibles para todos los suscriptores del sitio, sean usuarios legítimos, o *hackers*.

"Cuanto más tiempo esté en funcionamiento el dispositivo con las credenciales predeterminadas, mayor es el riesgo de uso fraudulento".

Esta información acerca de los dispositivos es valiosa para un *hacker*. Para un *hacker* que dispone de la información de la red, es muy fácil acceder al dispositivo y averiguar si está utilizando credenciales predeterminadas o fáciles de adivinar. Cuando consigue el acceso, recopila información del dispositivo y la guarda para su uso posterior. También es posible que el *hacker* se limite a vender esa información a terceros en el mercado pirata. Este proceso está siempre en marcha y ningún dispositivo conectado a Internet está a salvo.

Como muy tarde, las credenciales predeterminadas del dispositivo deben cambiarse antes de que se haya conectado a Internet. Una "buena práctica" sería cambiar las credenciales predeterminadas tras sacar el dispositivo por primera vez de la caja.

Tabla 1

Cuatro buenas prácticas en la gestión de contraseñas

Vulnerabilidad	Motivo	Buena práctica
Credenciales predeterminadas	Disponible en bases de datos on-line	Cambiar los valores predeterminados antes de su conexión
Contraseñas sencillas	Fáciles de *crackear*	Contraseñas de 10 a 15 caracteres de diferentes tipos
Sistemas de demostración	Credenciales codificadas	Cambiar los valores predeterminados antes de su conexión
Mismas credenciales para todos los sitios	Se pone en riesgo todos los sitios si se *hackean* las credenciales	Credenciales diferentes para cada sitio
Credenciales compartidas por un grupo de usuarios	Falta de trazabilidad y rendición de cuentas	Solicitar credenciales diferentes para cada usuario

Otra práctica común es la conexión de una "unidad de demostración" a Internet cuando aún mantiene las credenciales predeterminadas. Aunque no haya información útil en la base de datos, supone un riesgo real. El mero hecho de tener acceso al dispositivo proporciona al *hacker* gran cantidad de información.

Una vez que los *hackers* "entran" en un dispositivo de demostración, pueden analizarlo para encontrar deficiencias. Pueden descubrir credenciales codificadas que pondrían en riesgo todos los dispositivos de este tipo, aunque se cambiaran las credenciales predeterminadas. Por ejemplo, muchos dispositivos BMS antiguos tienen credenciales codificadas integradas en el código. El motivo de integrarlas era que los equipos de soporte de las fábricas pudieran restablecer contraseñas perdidas u olvidadas. Los fabricantes siempre intentaban que esta información fuera confidencial. Pero si las credenciales están en el código, en general resulta sencillo para un *hacker* encontrarlas y aprovechar esa información para poner en riesgo a todos los dispositivos similares.

Otra buena práctica es tener credenciales diferentes en cada sitio. El uso de un único conjunto de credenciales para todos los sitios hace más fácil la gestión de dispositivos, pero si un *hacker* lo obtiene, todos los sitios estarán en peligro.

Las buenas prácticas dictan que cada sito tenga credenciales propias y únicas.

"Los ordenadores actuales pueden probar hasta 348 mil millones de contraseñas por segundo".

Complejidad de las contraseñas

Las contraseñas sencillas con entre 6 y 8 caracteres alfabéticos son cosa del pasado. Actualmente, existen ordenadores baratos que pueden probar fácilmente hasta *348 mil millones de contraseñas por segundo.* Para conseguir un nivel de protección real, solo deben usarse contraseñas complejas o lo suficientemente largas.

Crear una contraseña compleja es fácil. El aumento del número de tipos de caracteres utilizados (mayúsculas y minúsculas, números y caracteres especiales) incrementa de forma exponencial el tiempo necesario para *crackear* una contraseña.

Habida cuenta de la potencia del software existente para *crackear* contraseñas, es importante que no resulte sencillo adivinarlas y que sean lo suficientemente complejas. Las normas siguientes, que se resumen en la **Figura 5,** son los requisitos mínimos para la creación de contraseñas seguras:

- Longitud mínima de 10 caracteres
- Al menos un carácter numérico, un carácter alfabético en minúscula y un carácter alfabético en mayúscula en cada contraseña

Figura 5

"Normas" para crear una contraseña compleja y segura.

¿Qué hace que una contraseña sea segura?	
Longitud	Al menos 10 caracteres 15 caracteres para sistemas de acceso poco frecuente
Conjunto de caracteres	Incluir una combinación de números, letras en mayúsculas y minúsculas y caracteres especiales

"Recordar una frase larga suele ser más fácil que recordar una contraseña larga y compleja".

En teoría, es necesario cambiar las contraseñas cada cierto tiempo para no dar lugar a que sean *crackeadas*. Dado que la vida útil de muchos dispositivos BMS es de entre 15 y 30 años y es posible que no se acceda a ellos con frecuencia, el uso de una contraseña más compleja es la única manera efectiva de proteger de forma adecuada estos sistemas. Cuando el intervalo entre accesos puede ser de años, se recomienda usar contraseñas de 15 caracteres o más.

Cuando las contraseñas son muy largas, suele ser mejor emplear "frases de paso". En lugar de intentar modificar (o "decorar") las contraseñas existentes con caracteres especiales y una combinación de mayúsculas y minúsculas, plantéese crear una frase secreta. Pueden ser muy eficaces porque, por lo general, están formadas por más de 15 caracteres. Recordar una frase larga suele ser más fácil que recordar una contraseña larga y compleja.

¡Atención!

Históricamente, las funciones de gestión de contraseñas de los dispositivos BMS han sido muy básicas. Intentar utilizar contraseñas o frases de paso lo suficientemente complejas puede conllevar problemas operativos e, incluso, provocar que el sistema se bloquee. Se recomienda encarecidamente que antes de convertir las contraseñas existentes de los dispositivos en contraseñas más complejas se consulte en el manual de usuario qué se considera una contraseña válida en lo que a longitud y los conjuntos de caracteres se refiere. Otra opción es probar antes contraseñas nuevas complejas en dispositivos que no sean de producción y ver qué tipos de contraseñas admite el dispositivo.

Gestión de la red

Una vez que todos los dispositivos tienen credenciales lo bastante seguras, el siguiente paso es proteger otras formas de acceso al sistema que tiene un *hacker*. Entre estos otros "puntos de entrada" encontramos la interfaz web, los puertos USB, los puertos IP abiertos y dispositivos de automatización de edificios que se comunican a través de protocolos abiertos.

Protección de la interfaz web

"La 'inyección SQL' fue el medio utilizado en el 83 % de las filtraciones de datos realizadas con éxito por hackers entre 2005 y 2011".

Fuente: Privacyrights.org

Los dispositivos que contienen interfaces web requieren una atención especial. Cualquier interfaz web accesible desde Internet es el primer punto de ataque, y el más susceptible. Existen diversos ciberataques que pueden superar con facilidad una autorización basada en una interfaz web mal codificada. Uno se denomina "inyección SQL" y podría permitir a un atacante cambiar todas las contraseñas de un dispositivo por un solo valor "debidamente formateado" introducido en el campo "Nombre".

Puede resultar complicado determinar los tipos de vulnerabilidades existentes en la interfaz web de un dispositivo. Una buena práctica es acceder al sitio web del fabricante del BMS para conseguir información acerca de la seguridad de la interfaz web. Los dispositivos con interfaces web vulnerables nunca deben situarse directamente en Internet. Si es necesario tener acceso a Internet, una buena práctica para mitigar el riesgo es colocar un cortafuegos entre el dispositivo e Internet y bloquear el puerto 80 y el puerto 443 y cualquier otro puerto que sea compatible con los protocolos HTTP/HTTPS. (el 8080 es un puerto HTTP alternativo habitual).

Protección de todos los puntos de acceso

A menudo los dispositivos BMS tienen varios canales de comunicación no basados en IP. Además del conector de Internet RJ-45, suelen tener conexiones RS-232 o RS-485, así como bucles de corriente. Deben evaluarse las deficiencias de todas estas interfaces que pudieran suponer una amenaza para el funcionamiento seguro del dispositivo. Siempre que se posible, se deberán deshabilitar las interfaces que no se utilicen.

*"Desde el punto de vista de la seguridad, el puerto USB supone un **elevado riesgo**".*

Un punto de acceso habitual, que suele desatenderse, es el puerto USB. Desde el punto de vista de la seguridad, el puerto USB supone un **elevado riesgo para** el dispositivo. Los controladores de software asociados a los puertos USB se diseñaron para ejecutar de forma automática programas guardados en el dispositivo en cuanto se inserta. Si el dispositivo USB está contaminado con *malware*, esta función "autoejecutable" puede provocar que el *malware* se cargue en el dispositivo sin ninguna advertencia.

Una buena práctica supone deshabilitar la función "autoejecutable" de todos los puertos USB. Si no es posible, al menos debe limitarse el acceso físico a los puertos USB.

Otras recomendaciones

Muchos sitios web ofrecen recomendaciones acerca de cómo gestionar mejor la ciberseguridad. Muchos de ellos se basan en el documento del Instituto Nacional de Estándares y Tecnología (NIST) Generally Accepted Principles and Practices for Securing Information Technology Systems (Principios y prácticas generalmente aceptados para la protección de sistemas de tecnología de la información).

Otro riesgo de seguridad importante es que los *hackers* distribuyan memorias USB a personas con posibilidades de acceder a los dispositivos que les interesan. Los *hackers* pueden poner en circulación los USB de distintas formas: solo tienen que tirar al suelo una memoria infectada en el aparcamiento de un edificio o enviarla por correo como si se tratara de un "premio". El objetivo es conseguir que una memoria infectada llegue a manos de una persona con acceso y que pueda utilizarla para transferir datos al dispositivo.

Una vez que se inserta la memoria infectada en el puerto USB sin protección, el sistema está "autoinfectado" y el *hacker* tiene acceso sin restricciones al dispositivo comprometido.

Por ello, para transferir datos a un dispositivo, las buenas prácticas exigen que se utilicen exclusivamente dispositivos "manifiestamente seguros", de un proveedor de calidad y extraídos de un paquete sellado.

Habilitar solamente los menos puertos necesarios

Con frecuencia, los dispositivos se distribuyen con muchos puertos TCP/IP abiertos. Y, por lo general, no se necesitan todos estos puertos para que el sistema funcione

correctamente. Algunos puertos como FTP, SMTP, SNMP y otros pueden ser necesarios en instalaciones de gran tamaño, pero no en sitios pequeños.

Analice las funciones requeridas en cada segmento de la red y ajuste el acceso a los puertos en consecuencia. En el caso de dispositivos que no ofrecen la posibilidad de cerrar los puertos no utilizados, debe instalarse y configurarse un cortafuegos para permitir comunicaciones exclusivamente mediante los puertos necesarios.

Segmentos seguros que ejecutan protocolos BMS abiertos

La mayoría de las redes de bus de campo que se ejecutan en un iBMS utilizan protocolos que son inherentemente poco seguros. En algunos casos estos protocolos presentan vulnerabilidades que permiten a los usuarios insertar comandos en el dispositivo controlador. Si bien se han tomado medidas para mejorar los protocolos como BACnet con características de seguridad, estos cambios en los protocolos todavía no han llegado a los nuevos dispositivos.

Finalmente, debe realizarse una evaluación de los riesgos para determinar el riesgo relativo de cada red de este tipo. La mayoría de protocolos iBMS son administrados por comités o grupos activos y tienen sitios web a los que pueden hacer referencia al iniciar un análisis de riesgos. En el caso de que se determine que algún segmento contiene elementos críticos de control, debe plantearse la protección física de todos los aspectos de este segmento.

Tabla 2

Cuatro buenas prácticas en la gestión de la red

Vulnerabilidad	Motivo	Buena práctica
Interfaz web	Inyección SQL	Instalar un cortafuegos
Puerto USB	Acceso a todo el sistema	Deshabilitar autoejecutable Deshabilitar / proteger puertos
Puertos TCP/IP	Acceso a todo el sistema	Cerrar puertos Instalar cortafuegos
Redes con protocolos abiertos	Permite a los *hackers* introducir comandos	Realizar una evaluación de riesgos Proteger físicamente los segmentos

Gestión de usuarios

Tras haber "ciberprotegido" el BMS frente a amenazas externas, la siguiente cuestión que se debe abordar es proteger el sistema desde dentro. Durante los últimos años, los BMS han pasado de ser sistemas de línea de comandos para un único usuario a ser sistemas avanzados con interfaz gráfica para múltiples usuarios. El aumento de las funciones ha ido acompañado de un aumento significativo en los tipos de operaciones que puede realizar un usuario.

Concesión de los permisos mínimos imprescindibles para cada trabajo

Aunque resulta más sencillo conceder privilegios de "súper usuario" a todo el mundo, esta práctica está totalmente desaconsejada. Una de las principales amenazas para todos los sistemas es el empleado "insatisfecho". Los daños que pueden causar los empleados insatisfechos pueden controlarse mediante el nivel de acceso concedido. Si, por simplificar, se les ha concedido a todos privilegios de "súper usuario", los daños pueden ser catastróficos.

Una buena práctica es seguir el principio del mínimo privilegio y dar a cada usuario únicamente los privilegios de acceso que requieran para llevar a cabo su trabajo.

Gestión de cuentas de usuario

La gestión de usuarios es un componente importante a la hora de salvaguardar la seguridad de un dispositivo. Algunos dispositivos disponen de servicios para ayudar a automatizar este proceso, o se basan en servicios de directorio externos (Microsoft Active Directory o LDAP en Linux) para esta funcionalidad. En el caso de sitios en los que las cuentas de usuario solo se controlan dentro del dispositivo, deben implementarse las prácticas siguientes:

"Una de las principales amenazas para todos los sistemas es el empleado 'insatisfecho'".

Caducidad automática de todas las cuentas

En aquellos dispositivos que ofrecen la función de caducidad de contraseñas, todas las cuentas distintas de las del administrador deben configurarse de forma que sus contraseñas caduquen en una fecha concreta o después de un cierto número de días. Esto significa que los usuarios habituales tendrán que restablecer periódicamente sus contraseñas. Las cuentas a las que no se acceda en un plazo concreto de tiempo deben deshabilitarse automáticamente y requerir la intervención del administrador del sistema para volver a habilitar la cuenta.

Deshabilitar de inmediato las cuentas de los empleados que dejen la empresa

Un riesgo de seguridad que suele pasarse por alto pero que es significativo reside en no deshabilitar las cuentas de aquellos empleados que hayan abandonado la empresa. Esta medida tiene especial importancia cuando se rescinde la relación laboral, ya sea temporal o definitivamente. Una buena práctica es deshabilitar estas cuentas tan pronto como el empleado deja su trabajo o antes de que se les notifique la rescisión.

En el caso de aquellos empleados que presentan su dimisión, es importante evaluar el riesgo asociado a permitirles que tengan acceso a los dispositivos de forma continuada hasta la fecha de su salida.

Cambiar las cuentas cuando el empleado cambie de funciones

Del mismo modo, revise las autorizaciones y el acceso de los empleados cuando se produzcan cambios en sus funciones en la empresa. Es importante que su acceso y sus autorizaciones se mantengan en niveles adecuados para sus nuevas funciones.

Gestión de software

Aplicar siempre los parches de seguridad de software

Cuando van a atacar un dispositivo, lo primero que miran los *hackers* es si se han instalado todos los parches de seguridad. Cuando las funciones de seguridad no están actualizadas, suelen existir áreas que pueden explotarse para comprometer los

dispositivos. Una buena práctica es aplicar de forma regular todos los parches de seguridad en todos los dispositivos.

Asegurarse de que solo los usuarios autorizados pueden instalar software

Únicamente los usuarios que gocen de un alto grado de confianza deben contar con privilegios que les permitan instalar software. A menudo, la instalación requiere ejecutar un sistema de host en modo administrador. En otros casos, las herramientas utilizadas para instalar software exponen al dispositivo a un riesgo mayor de ataques. Una buena práctica es limitar este papel a un grupo reducido de empleados de mucha confianza.

Instalar únicamente software autorizado

Un ciberataque cada vez más común consiste en la distribución de paquetes de instalación de software manipulados que pueden contener aplicaciones modificadas o aplicaciones adicionales que ponen en riesgo la integridad del dispositivo.

Cada dispositivo ofrece métodos diferentes para comprobar que un paquete de instalación es válido antes de proceder a la instalación. Algunos paquetes ofrecen códigos de verificación para autenticar la integridad del software. Muchos instaladores comprueban estos códigos de forma automática; otros requieren verificación manual (se trata de un proceso sencillo que consiste en comparar dos cadenas). Otros instaladores usan certificados digitales, y hay quienes emplean canales seguros de comunicación entre hosts de confianza.

Le recomendamos familiarizarse con todas las funciones de seguridad de los sistemas de instalación e implementar procedimientos para garantizar que se cumplen los procesos de autenticación de paquetes de software antes de la instalación.

Gestión de vulnerabilidades

El parcheo de dispositivos con vulnerabilidades requiere planificación. Cada compañía tiene una política diferente a la hora de realizar actualizaciones en los BMS. Es importante entender estos requisitos y determinar el impacto operativo causado por la interrupción temporal del servicio necesario para llevar a cabo el proceso de actualización. Un plan de gestión de vulnerabilidades debe tener en cuenta todos los aspectos de la actualización de vulnerabilidades.

Una clasificación de la gravedad de las vulnerabilidades ayuda a determinar la velocidad a la que debe darse respuesta a cada incidente. Consiste en asignar una puntuación cualitativa a cada vulnerabilidad conocida. Algunos sistemas de puntuación utilizan "Crítica", "Elevada", "Media", "Baja"; otros utilizan un sistema de puntuación de 1 a 10. En general, las vulnerabilidades consideradas Críticas (9-10) y Elevadas (7-8) deben abordarse lo antes posible. Normalmente, las vulnerabilidades menos graves pueden tratarse durante el mantenimiento habitual.

Entre los problemas a tener en cuenta al crear un plan de gestión de vulnerabilidades se encuentran:

- ¿Cómo afecta una vulnerabilidad en concreto a una instalación determinada?
- ¿Cuál es el proceso para acceder y actualizar rápidamente el dispositivo?
- ¿Existen factores que afectarán a la capacidad de acceder o actualizar el dispositivo?
- ¿Hay riesgos asociados a la actualización?

Una buena práctica es contar con un documento formal de gestión de vulnerabilidades en cada instalación.

Conclusión

A lo largo de los últimos años, las filtraciones de datos han ocupado titulares en todo el mundo. Entidades muy diversas, desde estados hasta redes avanzadas de *hackers*, han convertido la búsqueda y la explotación de las vulnerabilidades en armas de los países y en un lucrativo negocio.

Los ciberataques cuestan miles de millones a las empresas cada año en ingresos perdidos, actualizaciones de seguridad, pérdida de productividad y daños a su reputación. Cualquier empresa con una infraestructura conectada a Internet es vulnerable. Los actuales sistemas de gestión de edificios informatizados, con redes de comunicaciones IP integradas, no son una excepción. Un *hacker* puede utilizar un único dispositivo BMS como punto de entrada para acceder a todo el sistema.

"Una formación eficaz y periódica en ciberseguridad consigue que todos sean conscientes de las vulnerabilidades".

Es un hecho reconocido que los *hackers* son más propensos a atacar sistemas mal protegidos y dejar de lado aquellos sistemas que requieren demasiado esfuerzo. Existen ciertas "buenas prácticas" comunes para frustrar estos ataques o, al menos, poner las cosas mucho más difíciles a los *hackers*. Algunas son tácticas sencillas de sentido común, como cambiar las credenciales predeterminadas de fábrica, usar contraseñas más complejas, o cambiarlas periódicamente. Otras medidas son bloquear el acceso externo: proteger las interfaces web, deshabilitar puertos IP y USB o instalar cortafuegos. Algunas prácticas se centran en vulnerabilidades de acceso interno, como definir de forma más estricta el nivel de autorización de cada empleado, deshabilitar cuentas inactivas, asegurarse de que se instalan los parches de seguridad y limitar quién puede instalar actualizaciones.

Si bien no es necesario que todos los empleados sean expertos en todos los campos, algunas prácticas son de aplicación a todos los empleados. Una formación eficaz y periódica en ciberseguridad consigue que todos sean conscientes de las vulnerabilidades. En definitiva, el nivel de ciberseguridad está directamente relacionado con el esfuerzo dedicado a dificultar a los *hackers* el acceso a valiosos sistemas.

Acerca de los autores

Gregory Strass es Jefe de Ciberseguridad de IT para Sistemas de Edificios de Schneider Electric. Es graduado en Ingeniería Eléctrica y Ciencias Informáticas por la Universidad de Illinois en Urbana. Además, cuenta con las certificaciones CISSP y CEH. Lleva más de 35 años trabajando en el campo de los sistemas integrados.

Jon Williamson es el Responsable de Comunicación de Sistemas de Edificios de Schneider Electric. Es graduado en Ingeniería Mecánica por la Universidad de New Hampshire en Durham. Trabaja en el mercado de los BMS desde hace 19 años y cuenta con experiencia práctica y de gestión de productos en implementación de sistemas, redes y protocolos. En su función actual como Responsable de Comunicación, está al cargo de la arquitectura de sistemas, protocolos de comunicaciones y requisitos de ciberseguridad.