Estudio de Seguridad de IBM i 2017

Todos los días un caso de filtraciones de datos llega a las noticias. Ataques de softwares maliciosos a hospitales, un caso de phishing en Snapchat, y más. Sin embargo, usted no suele preocuparse por esta información, ya que sus datos y aplicaciones corporativas se encuentran a salvo en los servidores IBM i que su equipo de IT configuró hace algunos años.

De repente, su nuevo administrador de sistemas se da cuenta de que en su red hay una actividad inusual y que su sistema tuvo una filtración 10 meses atrás. Al parecer, ese servidor tenía algunos problemas de seguridad que nunca fueron identificados.

Recuperarse de los costos legales y la mala prensa que conlleva un caso de robo de información podría llevarle mucho tiempo.

RESUMEN EJECUTIVO

Desde hace 14 años, este estudio muestra las vulnerabilidades de seguridad que afectan a muchos de los sistemas IBM i que suelen almacenar datos críticos de la empresa como, por ejemplo, información sobre tarjetas de crédito o información de identificación personal (PII).

El Estudio de Seguridad de IBM i 2017, analizó 332 servidores y particiones de la industria financiera, manufacturera y de salud, entre otras.

Este estudio no analiza los mismos sistemas año tras año, sino que describe las tendencias generales. En esta oportunidad, demostró que para las compañías consultadas, **la seguridad informática se está convirtiendo en una de las prioridades más altas,** de modo que en los últimos años se realizaron mejoras graduales con controles básicos de la seguridad del sistema y las contraseñas.

A pesar de las mejoras realizadas, el estudio demuestra que algunos servidores no están configurados de manera adecuada y, por lo tanto, dan a los usuarios un mayor acceso al sistema del que realmente necesitan y dejan sin monitorizar el tráfico en la red. Este descuido en la seguridad informática provoca que muchas organizaciones estén en riesgo de sufrir una filtración de datos.

EL ALCANCE DE ESTE RIESGO ESTÁ RESUMIDO EN LAS SIGUIENTES SIETE ÁREAS CRÍTICAS DE SEGURIDAD DE IBM I:

Preparando el terreno: Niveles de seguridad básica del sistema

Casi un 20% de los sistemas analizados no aplican las mejores prácticas en seguridad general de sistemas, según las recomendaciones de IBM y de expertos en la materia.

Usuarios avanzados

La gran mayoría de los servidores IBM i analizados tienen demasiados usuarios con permisos especiales, lo cual podría provocar la pérdida, la alteración o el robo de datos a manos de empleados negligentes o insatisfechos. En cualquier auditoría estándar de IBM i, los auditores se focalizan en encontrar casos de uso indebido de permisos especiales. Incluso aquellos auditores que no están muy familiarizados con el entorno IBM i saben que este problema se repite también en otras plataformas.

Contraseñas defectuosas y seguridad de perfiles de usuarios

En IBM i, los perfiles de usuarios tienen, por defecto, su nombre de usuario como contraseña. El 24% de los sistemas incluidos en el estudio tenía más de 100 perfiles de usuarios con contraseñas por defecto, e incluso uno de los sistemas tenía un total de 4153 perfiles de usuarios con contraseñas por defecto.

Acceso a los datos

Casi todos los usuarios del sistema tienen acceso de lectura a los datos, lo cual excede en gran medida las necesidades de su perfil. En general, los auditores buscan garantizar que la compañía cuente con una división de funciones adecuada y controles apropiados para aplicar la división de funciones.

Control y auditoría de acceso a redes

En la mayoría de los centros de datos con IBM i no se lleva ningún tipo de control ni se audita el acceso hacia y desde redes. Es por eso que el acceso autorizado como el no autorizado no pueden coexistir sin ningún tipo de control de responsabilidades ni trazabilidad. La tecnología de puntos de salida (exit points) de IBM permite controlar y monitorizar el acceso a los datos desde y hacia la red. Sin embargo, el estudio demuestra que no se han adoptado exit points al mismo ritmo que las utilidades de acceso a datos desde y hacia la red.

Auditoría del sistema

En la mayoría de los sistemas analizados, se pueden producir violaciones de seguridad sin ni siquiera ser detectadas. Casi el 15% de las organizaciones no registra los eventos de seguridad en un lugar seguro, y aproximadamente el 83% no cuenta con una estrategia eficiente para monitorizar e interpretar los datos de seguridad.

Susceptible a ataques de virus y malware

Al revisar los servidores para realizar controles anti-virus, se encontró que solamente el 6% estaba analizando los archivos antes de abrirlos. Esto significa que el 94% restante está en riesgo, ya sea por verse afectados sus objetos internos o por propagar algún virus a otro servidor en su red. Con el reciente aumento de malware y ataques de software maliciosos, el peligro es mayor que nunca.

ÍNDICE DE CONTENIDOS

Introducción

Por cada caso de filtración de datos que llega a las noticias, docenas de organizaciones sufren robos por parte de hackers, o incluso por parte de sus propios usuarios. Las amenazas de seguridad informática son cada vez más sofisticadas y aplicar los controles adecuados es cada vez más importante.

UNA VEZ MÁS, EL ESTUDIO DE SEGURIDAD DE IBM I 2017 DEMUESTRA QUE MUCHAS DE LAS ORGANIZACIONES QUE UTILIZAN IBM I CONFÍAN EN TIPOS DE CONFIGURACIONES DEL SISTEMA OPERATIVO QUE DEJAN LOS DATOS EN UN ESTADO DE VULNERABILIDAD. ESTO SUCEDE EN TODAS LAS INDUSTRIAS, EN EMPRESAS GRANDES Y PEQUEÑAS.

El uso de contraseñas simples, sistemas de auditoría laxos y perfiles de usuarios con demasiados privilegios hacen que su servidor sea vulnerable a amenazas internas y externas. La filtración de datos provocada por un hacker o por una persona negligente vinculada a la empresa, puede provocar daños irreparables a organizaciones de cualquier tamaño.

La intención del Estudio Anual de Seguridad de IBM i es ayudar a los ejecutivos, gerentes de sistemas, administradores de sistemas y auditores, a comprender el alcance de los riesgos de seguridad de IBM i y cómo corregirlos en forma rápida y efectiva.

¿Por qué este estudio es importante para usted?

En los últimos 14 años, el Estudio de Seguridad de IBM i ha aportado información invaluable sobre seguridad, en relación a más de 2.500 participantes en todo el mundo. Los resultados del estudio de 2017 y la naturaleza de las vulnerabilidades de IBM i nos permiten concluir que **si usted tiene sistemas IBM i en su datacenter, su organización podría sufrir fallas de control interno similares.**

Seguramente su servidor IBM i ejecute aplicaciones críticas para su empresa, y lo ha hecho durante años. A esta altura, es posible que el personal que configuró la seguridad de ese servidor ya no esté en su organización.

Para complicar las cosas, la naturaleza integrada de muchos de los controles de seguridad de IBM i genera confusión sobre quién es finalmente el responsable de la configuración de seguridad: IBM, el cliente o los proveedores de la aplicación. De hecho, muchos de los sistemas funcionan con la configuración predeterminada por falta de un responsable.

Usted sabe que, hace tiempo, debería haberse realizado la auditoría al sistema IBM i, pero está muy ocupado lidiando con:

- Falta de conocimiento
- Personal desbordado de trabajo
- Presupuestos limitados de IT

Como las plataformas Windows y UNIX suelen requerir más recursos de seguridad, resulta mucho más sencillo dejar que los proyectos de seguridad relacionados con IBM pasen a segundo plano.

En consecuencia, la administración de los controles de seguridad de IBM i ha caducado y el sistema de protección está desactivado, a pesar de que las amenazas a su sistema aumentan.

Sin embargo, la buena noticia es que las debilidades detectadas mediante escaneos y documentadas en este estudio se originan debido a configuraciones deficientes o ausentes, lo cual puede y debe ser corregido.

Este estudio muestra cuáles son los riesgos de seguridad de IBM i más frecuentes y más peligrosos, también detalla las mejores prácticas que se deben llevar a cabo para lograr mejoras y explica cómo se relaciona todo esto con el cumplimiento de leyes aplicables, de normas de la industria y de estándares y lineamientos de IT.

El entorno de Power Systems

La comunidad de IBM i es grande y leal. IBM estima que aproximadamente 120 mil clientes alrededor del mundo utilizan IBM i y que más del 70% de estas organizaciones ejecutan más de la mitad de su actividad principal en esta plataforma, según los resultados del Estudio de Mercado IBM i 2017.

En general, las empresas dedicadas a la venta minorista, la actividad financiera, la manufactura y la distribución adquieren servidores Power Systems como parte de un sistema de negocios integrado. En la actualidad, aproximadamente 16 mil bancos ejecutan sus aplicaciones principales de actividad bancaria y financiera en un servidor IBM i.

Más allá de la industria en la que operan, las organizaciones almacenan una gran cantidad de información crítica en IBM i, que incluye:

- Datos financieros
- Información de identificación personal para empleados y clientes
- Datos de nómina de sueldos
- Niveles de inventario
- Información sobre precios
- Listados de clientes
- Propiedad intelectual
- Procesos de fabricación
- Estrategias comerciales

Muchas de las organizaciones que utilizan IBM i deben cumplir con normas gubernamentales y de la industria, como la Ley Sarbanes-Oxley, HIPAA para la industria de salud en Estados Unidos, PCI DSS para organizaciones que operan con tarjetas de crédito, y otras normas equivalentes en todo el mundo. Para poder mantener el cumplimiento normativo se debe dar prioridad a establecer una configuración segura.

El cumplimiento y la seguridad cobran cada vez mayor importancia, a medida que se añaden nuevos requisitos y se aprueban más normas. En 2015, PCI DSS comenzó a requerir el análisis de penetración; en 2018, la autenticación multifactorial será obligatoria. La Regulación General de Protección de Datos de la Unión Europea (GDPR) entrará en vigencia en mayo de 2018, mientras que la ley de seguridad informática para instituciones financieras del estado de Nueva York entró en vigencia en marzo de 2017.

Las normativas de seguridad no cubren todos los tipos de datos, y no afectan a todas las organizaciones, pero debe considerar las consecuencias que puede traer una filtración de aquella información que le da a su organización una ventaja competitiva, como datos relativos a precios o niveles de inventario. Las empresas que pertenecen a industrias altamente reguladas no son las únicas que deben preocuparse por la seguridad del sistema IBM i.

Nuestra metodología

Para llevar a cabo este estudio, los expertos en seguridad de HelpSystems auditan los sistemas IBM i con la herramienta Powertech Security Scan. Se trata de un software gratuito, que funciona directamente en una PC conectada a la red sin modificar las configuraciones del sistema IBM i (System i, iSeries y AS/400) y que lo evalúa en **siete áreas críticas de control:**

- Control de seguridad del servidor
- Configuración de perfiles y contraseñas
- Privilegios de administración
- Comandos iniciados en la red y acceso a datos
- Acceso público a datos de la organización
- Auditoría de eventos del sistema
- Escaneo de virus

Una vez finalizado el análisis, se envían las estadísticas de seguridad en forma anónima y directa a uno de nuestros servidores. El software no recopila datos específicos de aplicaciones; por lo tanto, tampoco recopila información sobre la finalidad del servidor. La participación en el estudio es opcional.

El estudio de este año incluye 332 servidores y particiones de IBM i que fueron auditados entre enero y diciembre de 2016. El tamaño de esta muestra casi duplica la del año pasado, lo que sugiere que **más organizaciones están preocupadas por encontrar y corregir de manera proactiva las vulnerabilidades en sus sistemas.** Esta muestra incluye sistemas de diversos tamaños, donde el modelo más común es el E4D, que comprende el 15% de los servidores analizados.

Las organizaciones pueden aportar información demográfica al estudio de forma voluntaria. Aquellas que eligieron hacerlo, clasificaron a sus industrias del siguiente modo:

- Finanzas
- Seguros
- Venta minorista
- Salud
- Manufactura
- Tecnología
- Gobierno
- Otras

Al igual que en los años anteriores, las organizaciones participantes abarcaron un amplio rango de tamaños, pero la muestra no es aleatoria. Los administradores de seguridad de estas compañías estaban lo suficientemente preocupados sobre la seguridad de IBM i como para solicitar un escaneo. Esto podría haber tenido como resultado una muestra que fuera excepcionalmente consciente en cuanto a la seguridad, o por el contrario, deliberadamente deficiente.

Por último, este no es un estudio que analice los mismos sistemas año tras año. No se pueden realizar comparaciones directas de un año a otro, pero algunas tendencias generales resultan evidentes.

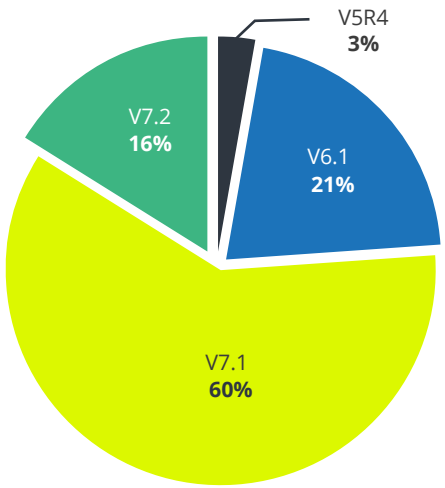
El sistema promedio escaneado en el estudio de 2017 incluye 1146 usuarios y 447 bibliotecas. Estos números son un poco más altos que la media, ya que la muestra de datos incluyó varios servidores grandes (Tabla 1).

Tabla 1: Tamaño promedio del sistema

Tamaño del sistema	Promedio	Media
Cantidad de usuarios	1146	443
Cantidad de bibliotecas	447	332

La mayoría de los servidores escaneados funcionan con versiones compatibles del sistema operativo. Solo el 3% todavía funciona con la versión V5R4 y el 21% con la versión V6.1. IBM dejó de dar soporte a ambas versiones en septiembre de 2015. Mientras tanto, el 60% funciona con V7.1 y el 16% con V7.2 (Imagen 1).

Imagen 1: Versiones instaladas de IBM i



Preparando el terreno: niveles de seguridad básica del sistema

Las mejores prácticas de seguridad de IBM i comienzan con la configuración de los valores del sistema que regulan la facilidad o la dificultad con la que un tercero puede utilizar o hacer uso indebido del sistema. Cuando esos valores están mal configurados o no son controlados, se genera un riesgo de seguridad inaceptable.

Nivel QSECURITY

¿De qué se trata y cuál es el riesgo?

El nivel de seguridad del sistema (QSECURTY) marca la pauta general. Sin embargo, muchas veces puede verse debilitado por otras configuraciones. IBM recomienda y ofrece sistemas con nivel de seguridad 40 como mínimo, debido a la vulnerabilidad registrada en los niveles 30 e inferiores. Cabe destacar que, a pesar de los cambios en la configuración predeterminada, si se realiza una migración del servidor, por lo general, se restablecerán los mismos valores de la generación anterior del servidor.

Los servidores Power Systems se pueden configurar en cualquiera de estos cinco niveles de seguridad:

- **Nivel 10** — Sin seguridad. No se requiere contraseña. Los ID de usuario son creados por cualquier usuario que intente iniciar sesión. IBM ya no brinda soporte para el nivel 10.
- **Nivel 20** — Seguridad con contraseña. Todo usuario debe tener un ID y una contraseña válidos, con los que tendrá privilegios de administrador (*ALLOBJ) por defecto.
- **Nivel 30** — Seguridad por recurso. Como los usuarios no tienen privilegios de administrador por defecto, se otorga un permiso a nivel del objeto. Un programador u operador con conocimientos avanzados puede sortear la seguridad por recurso y tomar privilegios de administrador fácilmente.
- **Nivel 40** — Seguridad del sistema operativo. Incluye la protección del nivel 30 más la integridad adicional del sistema operativo. Es posible que un programador experto con acceso al sistema pueda subir su nivel de privilegio y tomar privilegios de administrador.
- **Nivel 50** — Seguridad del sistema operativo mejorada. Incluye la protección de nivel 40 más la integridad del sistema operativo mejorada. Un sistema con seguridad de nivel 50 tendrá la mejor defensa. Sin embargo, incluso en el nivel 50 se deben abordar otros temas de configuración del sistema.

¿Cuáles son los resultados?

La Imagen 2 muestra el uso de los distintos tipos de configuración de seguridad de los sistemas incluidos en el estudio del año 2017. De los 332 sistemas analizados, el 16% funciona con nivel de seguridad 30 y el 3% con nivel de seguridad 20. En líneas generales, el 19% no satisface el nivel mínimo recomendado por IBM (Imagen 2A). Si bien es un número significativo, se trata de un área de la seguridad de IBM i que ha mejorado gradualmente en los últimos años.

Imagen 2: Nivel de seguridad del sistema

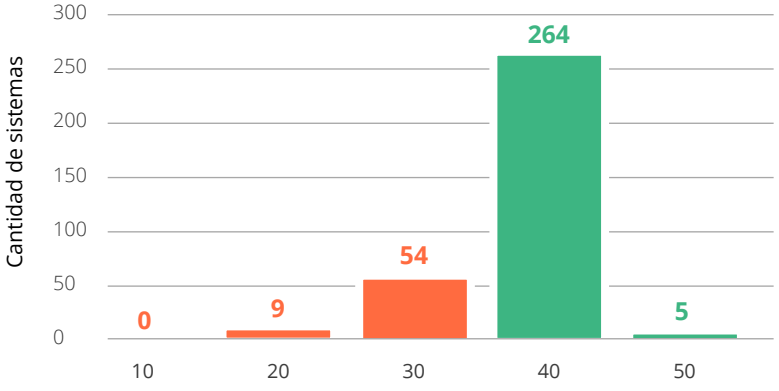
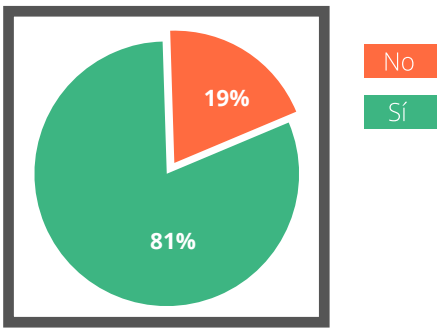


Imagen 2A: Sistemas que satisfacen el nivel de seguridad recomendado



Próximos pasos

Llevar su sistema al nivel 40 de QSECURITY o superior es un paso fundamental para protegerlo. Las organizaciones que no estén seguras sobre el impacto potencial de los cambios en los valores del sistema, podrán consultar a los profesionales de seguridad de IBM i, pero es importante que implementen una solución con rapidez. Tercerizar esta tarea y dejarla en manos de profesionales de seguridad como el equipo de HelpSystems es una forma rápida de eliminar todas las conjeturas del proceso.

Valores claves del sistema para restaurar objetos

¿De qué se trata y cuál es el riesgo?

Muchos otros valores del sistema relacionados con la restauración de objetos suelen quedar en su nivel por defecto, reflejando la configuración típica de "carga y ejecución" de IBM i.

Esos valores del sistema están diseñados para funcionar en conjunto como un filtro que evita la restauración de objetos maliciosos o corrompidos, pero los valores por defecto de IBM i no ofrecen esta protección y, por lo tanto, el sistema podría quedar vulnerable.

¿Cuáles son los resultados?

A continuación, se muestran los valores del sistema que operan en forma consecutiva para determinar si un objeto puede ser restaurado o debe ser convertido durante la restauración:

- **Verificar objeto al restaurar** (QVFYOBJRST)): el 63% de los servidores operan por debajo del nivel de seguridad mínimo recomendado, el nivel 3.

  Este valor está configurado por defecto en el nivel 1 y define si una firma será validada o no al restaurar un objeto con firma digital.

- **Forzar conversión al restaurar** (QFRCCVNRST): el 96% de los servidores operan por debajo del nivel de seguridad mínimo recomendado, el nivel 3.

  Este valor está configurado por defecto en el nivel 1 y define si se convierten o no ciertos tipos de objetos durante la restauración.

- **Permitir restauración de objeto** (QALWOBJRST)): solamente en 20 servidores se había modificado la configuración por defecto *ALL de este valor del sistema.

  Este valor define si se pueden restaurar programas con ciertos atributos de seguridad, como el estado del sistema o el otorgamiento de permisos de acceso.

¿Cuál es la solución?

Las configuraciones por defecto no suelen ofrecer el grado de seguridad que las organizaciones necesitan, y los valores por defecto para la restauración de objetos son un buen ejemplo de ello. Un enfoque proactivo es definir e implementar una política de seguridad que detalle cuál es la configuración de los valores del sistema más segura para su entorno. (Busque asesoramiento profesional si no está seguro acerca del impacto que pueden tener ciertas configuraciones). La Política de Seguridad gratuita IBM i Security Standard de HelpSystems puede ayudarlo a comenzar a definir su propia política.

Para estar seguro de que la configuración de su sistema cumple con los lineamientos de su política de seguridad, la solución Powertech Policy Minder para IBM i puede ayudarlo a definir esa política e informar las excepciones.

LAS CONFIGURACIONES POR DEFECTO NO SUELEN OFRECER EL GRADO DE SEGURIDAD QUE LAS ORGANIZACIONES NECESITAN, Y LOS VALORES POR DEFECTO PARA LA RESTAURACIÓN DE OBJETOS SON UN BUEN EJEMPLO DE ELLO.

Usuarios poderosos

¿De qué se trata y cuál es el riesgo?

Los profesionales de IT necesitan permisos especiales para administrar servidores. Además de cambiar la configuración del sistema, estos permisos podrían habilitar la capacidad de lectura o modificación de aplicaciones financieras, datos sobre tarjetas de crédito de los clientes y archivos confidenciales de los empleados.

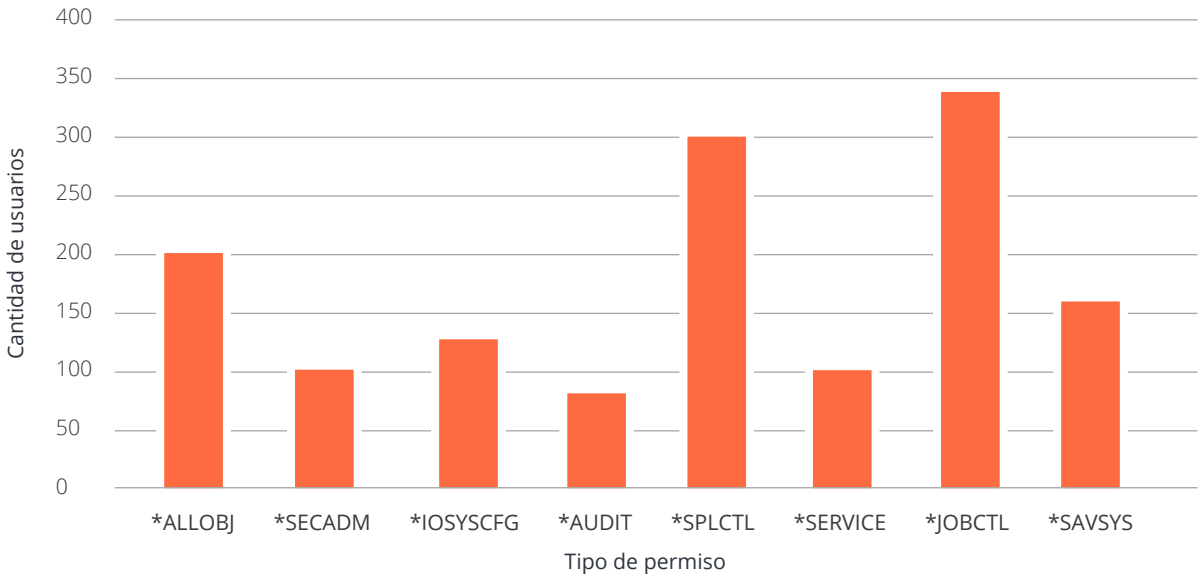
Estos permisos especiales pueden ser muy peligrosos en manos de un usuario descuidado, negligente o malintencionado. Dos tercios de las empresas han sufrido el robo o la corrupción de datos originada dentro de sus organizaciones. La filtración de datos en Boeing, en noviembre de 2016, es un caso clásico de un usuario descuidado que expuso datos confidenciales: un empleado de recursos humanos tenía problemas para dar formato a una planilla que contenía los números de seguro social de los empleados, entonces se la envió por correo electrónico a su esposa para que lo ayude.

Los permisos especiales siempre conllevan un riesgo de seguridad; por lo tanto, los auditores siempre piden que se limite la cantidad de usuarios que tienen estos permisos especiales y que se monitorice y audite su uso con atención.

¿Cuáles son los resultados?

Hay ocho tipos de permisos especiales en IBM i. La imagen 3 muestra la cantidad promedio de perfiles de usuario para cada permiso especial.

Imagen 3: Usuarios poderosos (Permisos especiales)



De los permisos especiales, *ALLOBJ es el que ofrece a los usuarios acceso sin restricciones de lectura, modificación y eliminación de archivos y programas del sistema. Como se muestra en la Imagen 3, este permiso se otorga a una cantidad inaceptable de usuarios.

Solo cinco de los sistemas analizados tenía 10 o menos usuarios con permiso de acceso *ALLOBJ. El permiso especial más otorgado fue Job Control (*JOBCTL), el cual superó al primer puesto del año pasado, el Spool Control (*SPLCTL). El permiso especial Job Control (*JOBCTL) fue concedido a casi el 30% de los usuarios, quienes pueden hacer cambios en la prioridad de los trabajos y de las impresiones, o incluso en algunos casos, finalizar subsistemas. Spool Control ofrece al 26% de los usuarios la posibilidad de tener acceso ilimitado a cualquier archivo de SPOOL en cualquier cola de salida, independientemente de las restricciones establecidas de SPOOL.

Muchas organizaciones aprovechan el modelo de control de acceso basado en funciones (RBAC) intentando de ese modo estandarizar la configuración de usuarios. En IBM i, esto se suele implementar mediante un mecanismo conocido como

Perfiles de Grupo (Group Profiles). De acuerdo con este estudio, el 97% de los servidores tenían uno o más perfiles de grupo definidos y el 41% tenía 10 o más. De todos los perfiles de grupo, más del 93% otorgaban permisos especiales a sus miembros, un legado que, a veces, no se tiene en cuenta al momento de llevar a cabo un control de permisos de usuarios.

¿Cuál es la solución?
IBM no publica ninguna documentación sobre las funciones disponibles para cada permiso especial, lo cual hace que el Departamento de IT se abstenga de eliminar permisos por temor a "romper" operaciones existentes.

Como es difícil crear una norma rígida y ágil para todos los entornos, los expertos en seguridad de IBM i sugieren mantener al mínimo posible la cantidad de usuarios con permisos especiales. Esto se conoce como el principio del mínimo privilegio.

En general, una buena práctica de seguridad es mantener en menos de 10 la cantidad de usuarios con permisos especiales.

A continuación, se detallan las mejores prácticas relacionadas con usuarios poderosos:

- Documente y realice la división de tareas de los usuarios poderosos.
- Evite que todos sean usuarios poderosos, todo el tiempo.
- Monitorice, registre e informe la utilización de permisos de usuarios poderosos.
- Piense cómo justificar la utilización de permisos de usuarios poderosos frente a auditores y gerentes.

Para hacer más fácil el trabajo de monitorización y documentación de privilegios de usuarios, la solución Powertech Authority Broker puede monitorizar, controlar y auditar en forma automática a los usuarios que necesitan obtener mayores permisos de acceso. Powertech Command Security es una herramienta efectiva para evitar que usuarios no autorizados ejecuten un comando monitorizado.

LOS EXPERTOS EN SEGURIDAD DE IBM I SUGIEREN MANTENER AL MÍNIMO POSIBLE LA CANTIDAD DE USUARIOS CON PERMISOS ESPECIALES.

Seguridad de usuarios y contraseñas

Los problemas de seguridad relacionados con usuarios y contraseñas son muy importantes porque representan la manera más obvia y sencilla de comprometer a su sistema.

Si no cuenta con medidas de seguridad apropiadas para usuarios y contraseñas, los esfuerzos que pueda realizar para asegurar otras áreas de la red IBM i serán, en su gran mayoría, ineficaces. ¿Cómo puede estar seguro de que el usuario que ingresó al sistema es el mismo usuario al que se le asignó un ID y una contraseña?

Blancos principales: Perfiles inactivos

¿De qué se trata y cuál es el riesgo?
Los perfiles inactivos son perfiles de usuarios que no han sido utilizados en los últimos 30 días o más. Crean una exposición en la seguridad porque estas cuentas no están siendo mantenidas activamente por sus usuarios, lo que las convierte en el blanco principal para el robo de datos.

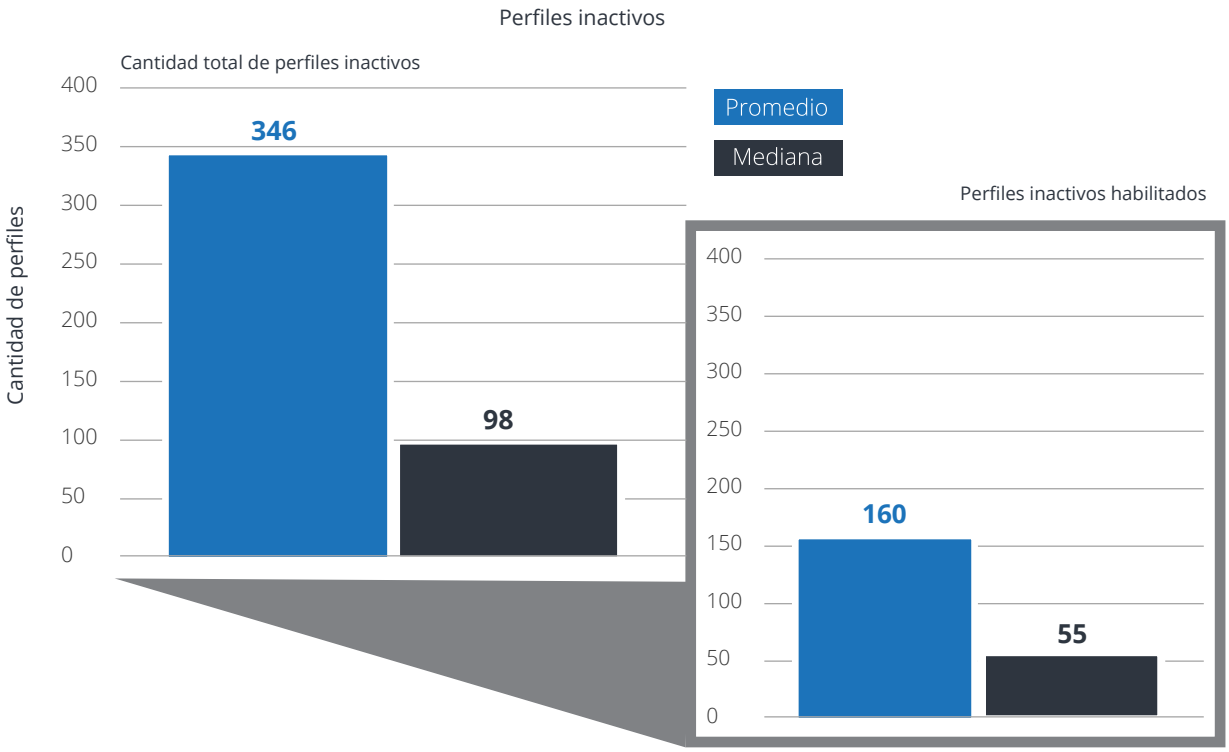
Muchos de estos perfiles inactivos le pertenecen a ex-empleados o contratistas, gente que podría estar resentida con la compañía o a quienes les podría resultar útil tener acceso a los datos de su ex-empleador para utilizarlos en sus nuevas funciones o con la competencia.

La amenaza persiste aún cuando los ex-empleados jamás intenten utilizar esos perfiles. Otros usuarios dentro de la organización podrían conocer, por ejemplo, que el perfil del ex-director de IT aún se encuentra en el sistema. Más allá de que un ex-empleado, un empleado mal intencionado o un hacker hagan uso de un perfil inactivo, el mayor problema es que el uso inusual no será detectado ni informado por el dueño del perfil.

¿Cuáles son los resultados?

La Imagen 4 muestra que un promedio de 346 perfiles (el 30% del total) no ingresaron al sistema en los últimos 30 días o más. De estos, 160 siguen habilitados y listos para ser usados.

Imagen 4: Perfiles inactivos



¿Cuál es la solución?

Establezca un procedimiento para los perfiles inactivos. Comience por definir cuánto tiempo debe estar inactivo un perfil hasta que se tomen medidas (quizás 60 días), luego inhabilite los perfiles inactivos y elimine todos los permisos especiales y asignaciones a perfiles de grupo. Espere otros 30 días para estar seguro de que el perfil está realmente inactivo antes de eliminarlo del sistema, o espere hasta que ese nombre de usuario ya no sea requerido como dato informativo en las pistas de auditoría.

Este proceso se puede llevar a cabo en forma manual o automática, utilizando las herramientas de seguridad incorporadas de IBM i.

El secreto que todos conocen: las contraseñas por defecto

¿De qué se trata y cuál es el riesgo?

En IBM i, los perfiles de usuario con contraseñas por defecto son aquellos con contraseñas idénticas a los nombres de usuarios. Como este es el modo predeterminado para la creación de nuevos perfiles, se lo considera un factor de alto riesgo para los servidores IBM i.

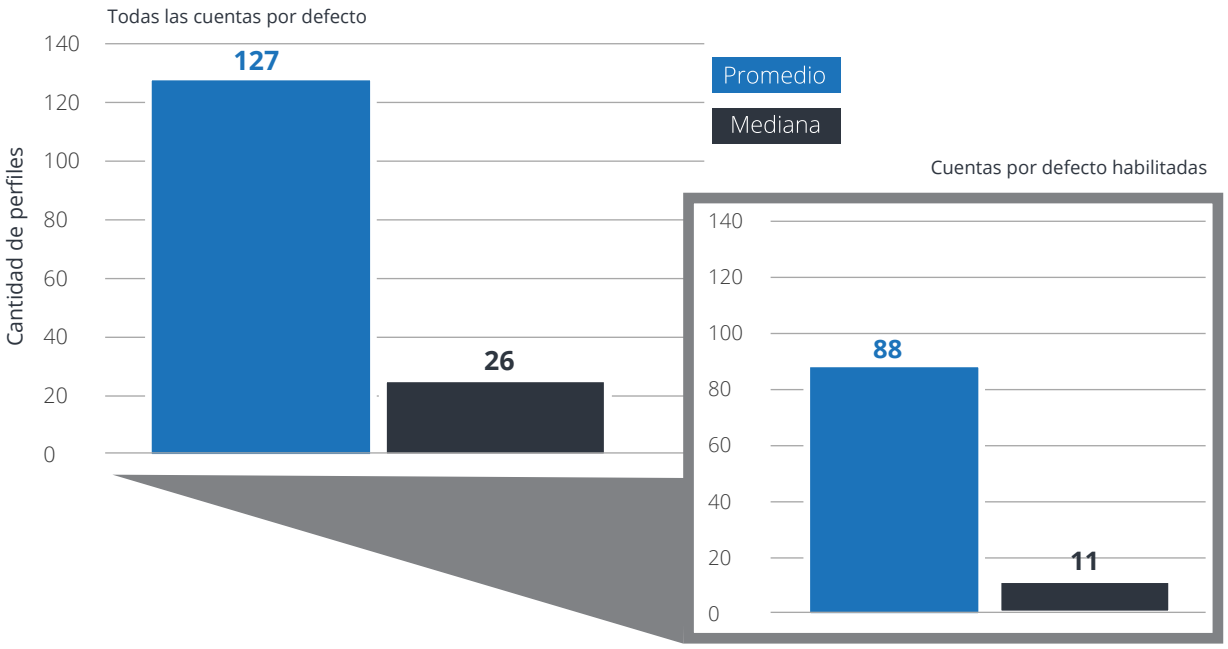
Muchas empresas tienen políticas relacionadas con los nombres que le otorgarán a sus cuentas de usuarios o a sus perfiles mediante la aplicación de un formato estándar, por ejemplo, la inicial del primer nombre seguida por el apellido (por ejemplo: jsmith o tjones). Un hacker puede adivinar nombres de perfiles como "jsmith" e intentar ingresar contraseñas por defecto. Es incluso más fácil para un empleado que entiende la convención interna de los nombres de los perfiles de usuarios adivinar los nombres de las cuentas e intentar ingresar contraseñas por defecto, en especial si ese empleado sabe que las cuentas ya han sido creadas pero que aún no se están utilizando.

En general, las regulaciones y los estándares aplicables establecen que cada usuario debe utilizar credenciales únicas que solo deben ser conocidas por él y, de este modo, asegurar que cada una de las acciones realizadas se pueden vincular con esa persona en particular. Las organizaciones podrían entonces intentar identificar al autor de una actividad ilegal o no autorizada, siempre que fuera evidente que las credenciales identifican inequívocamente al culpable. El predominio de contraseñas por defecto hace increíblemente fácil la tarea de adivinar contraseñas y esto se traduce, en última instancia, en una falta de cumplimiento normativo.

¿Cuáles son los resultados?

En este estudio, más del 10% de los perfiles de usuario tienen contraseñas por defecto (Imagen 5). Casi la mitad (el 47%) de los sistemas incluidos en el estudio tienen más de 30 perfiles de usuario con contraseñas por defecto, mientras que el 24% tiene más de 100. Uno de los sistemas tenía un total de 4153 perfiles de usuario con contraseñas por defecto y 4054 de ellos estaban habilitados.

Imagen 5: Perfiles con contraseñas por defecto



¿Cuál es la solución?

Establezca y haga cumplir políticas de contraseñas que tiendan a reducir la vulnerabilidad de la cuenta del usuario. Desde su versión V7.2, IBM i apoya la prohibición de contraseñas por defecto mediante la aplicación del valor del sistema QPWDRULES, a pesar de que se deben tener en cuenta las aplicaciones o el software de proveedores que generen perfiles durante la instalación.

Las herramientas de reportes como Powertech Compliance Monitor facilitan la tarea de generar reportes de auditoría en forma regular, para comparar la información sobre los nombres y las contraseñas de los usuarios de IBM i con las políticas correspondientes.

Longitud mínima de contraseñas

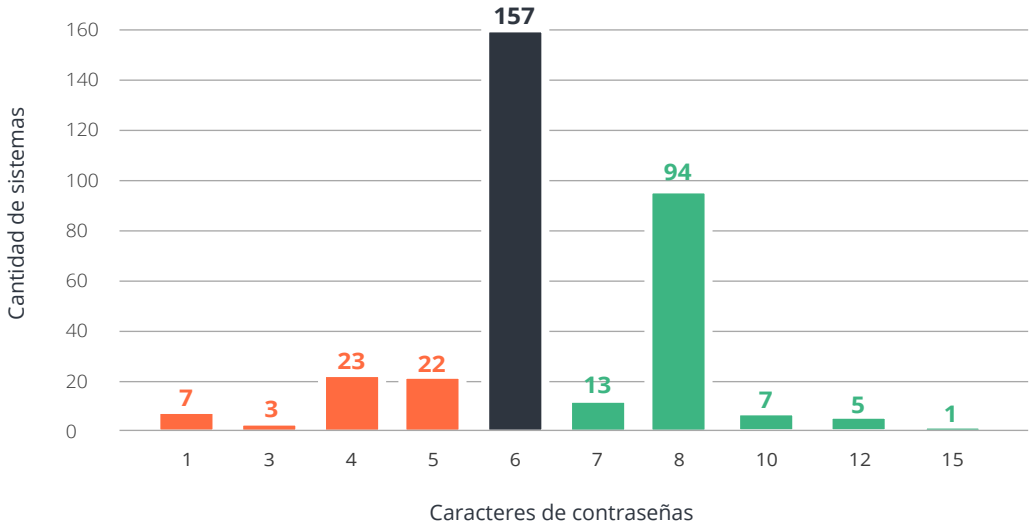
¿De qué se trata y cuál es el riesgo?

IBM i ofrece la posibilidad de requerir una longitud mínima de contraseñas. Las contraseñas más cortas son más fáciles de recordar, pero también son más fáciles de adivinar para los demás. A pesar de que las contraseñas cortas se pueden reforzar mediante el uso de caracteres aleatorios, las probabilidades de adivinar una contraseña de cuatro caracteres son mucho mayores que las de adivinar una contraseña de seis caracteres.

¿Cuáles son los resultados?
La Imagen 6 muestra la configuración del valor de longitud mínima de contraseñas en los sistemas revisados. De acuerdo con nuestros resultados, el 83% alcanza o supera los estándares de mejores prácticas de seis caracteres o más.

Las normas generales de cumplimiento, como el Estándar de Seguridad de Datos para PCI DSS, reconoce el beneficio de una contraseña de mayor longitud. Sin embargo, el 64% de los servidores incluidos en este estudio no cumplieron con el requisito de PCI de contraseñas de siete caracteres. Es increíble que casi el 10% de los sistemas permiten a los usuarios seleccionar una contraseña de menos de cinco caracteres y siete servidores permiten el uso de contraseñas de un solo carácter.

Imagen 6: Longitud mínima de contraseñas



¿Cuál es la solución?
Establezca una política de contraseñas que exija a los usuarios el uso de seis caracteres o más en sus contraseñas; y siete caracteres como mínimo en caso de que su organización deba cumplir con el estándar PCI DSS.

Capitalizar otras configuraciones de contraseñas

¿De qué se trata y cuál es el riesgo?
Además de la longitud, la complejidad de las contraseñas también contribuye a la seguridad. IBM i permite a los administradores del sistema controlar ambos aspectos. Estas configuraciones ayudan a que las contraseñas sean más difíciles de adivinar y aumentan la protección de su sistema. Sin embargo, los administradores de sistemas no siempre usan las funciones de control de contraseñas que se encuentran disponibles.

Las contraseñas simples y fáciles de adivinar como "123456" y la palabra "contraseña" siguen siendo comunes. Imagine qué podría suceder si los usuarios de su organización que tienen contraseñas simples tuvieran permisos especiales o acceso a información confidencial.

¿Cuáles son los resultados?
Algunas de las configuraciones de contraseñas más importantes, y los resultados del estudio en cuanto a su uso, son los siguientes:

- **El 59% de los sistemas no requiere un dígito en las contraseñas,** y esto facilita el cumplir con el deseo de los usuarios de utilizar palabras simples (no muy seguras), tomadas del diccionario.

IMAGINE QUÉ PODRÍA SUCEDER SI LOS USUARIOS DE SU ORGANIZACIÓN QUE TIENEN CONTRASEÑAS SIMPLES TUVIERAN PERMISOS ESPECIALES O ACCESO A INFORMACIÓN CONFIDENCIAL.

- **El 97% de los sistemas no impone ninguna restricción con respecto a los caracteres.** Simplemente limitando el uso de vocales, se podría mejorar la seguridad evitando que los usuarios utilicen palabras simples y fáciles de adivinar.
- **El 30% de los sistemas no establece una fecha de caducidad para las contraseñas** y los usuarios nunca tienen la obligación de modificarlas. Esto también puede controlarse a nivel de usuario pero, en general, queda reservado para ciertos perfiles.
- **El 40% de los sistemas no requiere que las contraseñas sean distintas a la última que se utilizó.** Solo el 33% exige un mínimo de 10 contraseñas únicas y apenas el 8% exige que los usuarios cumplan con la configuración máxima de 32 contraseñas únicas.

La versión V6.1 de IBM i introdujo QPWDRULES, un nuevo valor del sistema que ofrece la posibilidad de establecer varias configuraciones de políticas de contraseñas en un mismo repositorio. Casi todos los sistemas incluidos en el estudio (el 97%) tienen acceso a este valor del sistema, pero solo el 7% lo usa.

Otro valor nuevo en la versión V6.1 es QPWDCHGBLK, que restringe la frecuencia con la cual los usuarios pueden solicitar un cambio de contraseña de forma voluntaria. Esto evita que los usuarios cambien repetidamente sus contraseñas para volver a su favorita. La configuración más común, y por defecto, es *NONE, ya que se encontró en el 91% de los servidores de IBM i versión 6.1 o posterior. Solo el 8% de los sistemas analizados en el estudio establecieron un valor de 1 a 24 horas, que es el rango de configuración recomendado por HelpSystems.

El control de calidad de las contraseñas es tan importante como el establecimiento de una política de caducidad de contraseñas. Las mejores prácticas para la creación de una política de caducidad de contraseñas incluyen determinar un período de caducidad de 90 días como máximo. De acuerdo con los sistemas incluidos en nuestro estudio, el intervalo de caducidad de la contraseña es de 71 días, y el valor más común de los sistemas que configuran un intervalo de caducidad de contraseñas, es de 90.

¿Cuál es la solución?
IBM i incluye configuraciones que permiten a los administradores del sistema exigir el uso de contraseñas más seguras. Asegúrese de que su organización las use.

Evalúe en función de su industria. Si su sistema es utilizado para emitir informes contables o financieros, es mejor establecer períodos de caducidad de contraseñas aún inferiores a 90 días. Trabaje con sus auditores para determinar la mejor política aplicable a su sistema.

Otra opción es eliminar las contraseñas por completo mediante la implementación de la solución de "Inicio de Sesión Único" o Single Sign-On (SSO) basado en la infraestructura Enterprise Identity Mapping (EIM) que está incluida en el sistema operativo.

CASI TODOS LOS SISTEMAS INCLUIDOS EN EL ESTUDIO (EL 97%) TIENEN ACCESO A ESTE VALOR DEL SISTEMA, PERO SOLO EL 7% LO USA.

Contraseñas olvidadas y otros intentos de inicio de sesión no válidos

¿De qué se trata y cuál es el riesgo?
La gente se olvida las contraseñas, las escribe mal o simplemente las confunde con otras contraseñas. Los intentos de inicio de sesión no válidos son algo frecuente y los usuarios de IBM i no son la excepción. El personal de la Mesa de Ayuda que se encarga de restablecer estas contraseñas con frecuencia tiene que ayudar a los mismos usuarios una y otra vez. ¿Cómo se puede controlar quiénes son los usuarios que tienen muchos intentos de inicio de sesión no válidos? ¿Qué pasaría si fueran sus usuarios poderosos?

Un solo intento de inicio de sesión no válido, o incluso unos cuantos intentos fallidos, no deberían ser motivo de preocupación. ¿Pero qué sucedería si su sistema tuviera un perfil de usuario con cientos o quizás miles de intentos de inicio de sesión no válidos?

Una mayor cantidad podría indicar un intento de intrusión mientras que tres, cinco y hasta diez intentos son probablemente indicio del error de un usuario.

También es posible que los miles o hasta cientos de miles de intentos sean una señal de una aplicación dañada; quizás por falta de un mecanismo incorporado de reconocimiento cuando se deniegan los intentos de conexión al servidor. Pero nunca se debería hacer tal suposición sin una investigación. Además, una aplicación dañada sigue siendo una aplicación que no está cumpliendo el objetivo empresarial para el cual fue elaborada.

El nivel de riesgo aumenta significativamente en caso de que el perfil ofensivo sea, por ejemplo, un QSECOFR, y que no sea inhabilitado de forma automática, o en caso de que el equipo de seguridad no tenga forma de ser notificado de los intentos de acceso fallidos de manera oportuna.

¿Cuáles son los resultados?

Más del 95% de los sistemas tiene al menos un perfil con un intento de inicio de sesión no válido, lo cual no es sorprendente. Casi la mitad de los sistemas (160 de 332) tenía un perfil que había experimentado más de 100 intentos denegados. 66 sistemas tenían más de 1000 intentos de inicio de sesión no válidos contra un solo perfil.

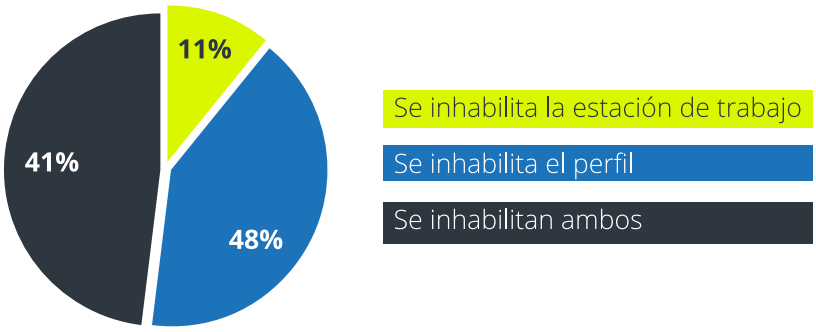
Uno de los sistemas incluidos en nuestro estudio tuvo 619.461 intentos contra un solo perfil. Esa cantidad de intentos puede sonar sorprendente, pero también fuimos testigos de un sistema en el cual un solo perfil había experimentado ¡casi siete millones de intentos!

Vale la pena mencionar que el conteo de la cantidad de intentos sigue corriendo incluso si el perfil es inhabilitado. El administrador no puede hacer nada para evitar los intentos mientras el usuario se conecte con el servidor. Por ese motivo, el elemento más importante es la detección y la notificación oportuna.

La Imagen 7 muestra las medidas tomadas cuando se alcanza la cantidad máxima de intentos de inicio de sesión permitida. En el 89% de los casos, el perfil es inhabilitado y esto es lo que siempre se recomienda hacer. Cuando se utilizan dispositivos explícitamente nombrados (en contraposición a los nombres de dispositivos virtuales), la recomendación se amplía para incluir así la inhabilitación de la descripción del dispositivo. No se recomienda inhabilitar dispositivos virtuales, ya que el sistema suele crear un nuevo dispositivo cuando el usuario se vuelve a conectar. La configuración del dispositivo no es aplicable a todas las conexiones, por ejemplo los servicios ODBC y REXEC.

El otro 11% de los servidores inhabilita el dispositivo, pero deja el perfil habilitado. Esto genera un riesgo en caso de que el usuario vuelva a establecer una conexión, o quizás se conecte a un servicio que no requiera un dispositivo en la estación de trabajo.

Imagen 7: Acción predeterminada en caso de que se excedan los intentos de inicio de sesión no válidos



¿Cuál es la solución?

Notificar e investigar oportunamente la existencia de una gran cantidad inusual de intentos de acceso denegados es la primera fase fundamental para detectar el peligro al que se expone el sistema.

Muy a menudo, las noticias sobre filtraciones de datos están acompañadas por una revelación alarmante sobre el tiempo que se permitió que dure la filtración. Una organización no puede detener la filtración de datos si no sabe que está pasando, y los intentos de inicio de sesión no válidos son uno de los indicadores más obvios.

Para proteger su sistema, asegúrese de que los perfiles sean inhabilitados por defecto después de que se haya excedido la cantidad máxima de intentos de inicio de sesión permitidos.

El acceso a los datos por medio de *Public

¿De qué se trata y cuál es el riesgo?

En general, en los servidores que no son IBM i, los usuarios que no tienen permisos para ciertos objetos o tareas, no pueden tener acceso a ellos. Con IBM i, este no es el caso. Cada objeto cuenta con un permiso por defecto, conocido como *PUBLIC, que se aplica a usuarios no mencionados explícitamente.

Salvo que se le brinde algún otro permiso específico al usuario, otorgando o denegando el acceso, este podrá operar con el permiso predeterminado del objeto. Esto no parece ser un problema hasta que descubrimos que este valor predeterminado lo establece IBM inicialmente y es suficiente como para permitir que un usuario abra un programa y tenga acceso de lectura, modificación o eliminación de datos de un archivo.

En otras palabras, salvo que se tomen medidas preventivas para restringir los permisos de acceso de *PUBLIC, los usuarios a quienes no se les ha otorgado un permiso específico a un objeto o tarea tendrán acceso de lectura, modificación y eliminación de datos.

Esta situación genera un riesgo de modificaciones no autorizadas en programas y cambios en bases de datos; una señal de alerta para los auditores, quienes recomiendan que los usuarios no tengan acceso de lectura ni modificación sobre bases de datos de producción o códigos fuente, a menos que tengan una necesidad de negocios concreta.

¿Cuáles son los resultados?

Este estudio utiliza los permisos de acceso *PUBLIC para bibliotecas como una medición simple que indica qué tan accesible deberían ser los datos de IBM i para el usuario final promedio.

La Imagen 8 muestra el nivel de acceso a las bibliotecas que tiene *PUBLIC en los sistemas incluidos en nuestro estudio. Si *PUBLIC tiene al menos los permisos de *USE para una biblioteca, cualquier persona que ingrese al sistema podrá acceder al catálogo de todos los objetos en esa biblioteca y utilizar o acceder a cualquier objeto de la biblioteca. Si se asume que el usuario o *PUBLIC también tiene el permiso necesario para el objeto específico, entonces hasta podrían borrar objetos de la biblioteca.

***USE** significa que cualquier usuario puede intentar acceder a objetos dentro de la biblioteca. A veces un usuario con acceso FTP puede descargar (leer) cualquier archivo de datos que se encuentre en la biblioteca. La función GET de FTP o las operaciones ODBC en herramientas como Microsoft Excel podrían permitir que hasta un usuario final inexperto tenga acceso a sus datos.

El permiso de acceso a bibliotecas ***CHANGE** le otorga la posibilidad al usuario de agregar nuevos objetos a la biblioteca y modificar algunas de las características de las bibliotecas.

El permiso ***ALL** posibilita a cualquier persona en el sistema administrar, renombrar, establecer permisos y hasta borrar una biblioteca (si tiene permiso para borrar los objetos en la biblioteca).

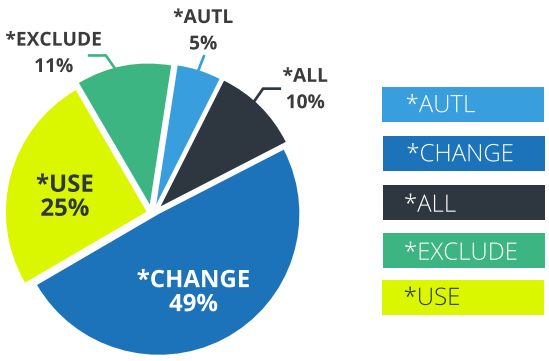


Imagen 8: Permiso de acceso a datos para *PUBLIC

Este estudio demuestra que las compañías con IBM i todavía tienen muchas bibliotecas que son accesibles para el usuario final promedio. Las estadísticas sobre bibliotecas DB2 muestran la falta de un control adecuado sobre los datos, los cuales suelen incluir información financiera corporativa fundamental.

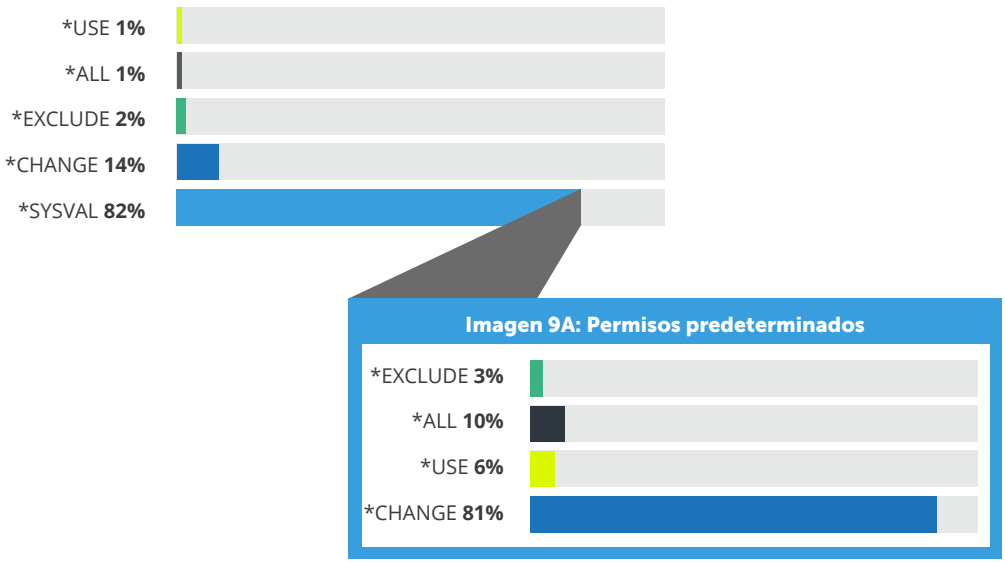
El método que se utiliza para determinar qué permiso tendrá *PUBLIC sobre nuevos archivos y programas proviene en general de los parámetros de los Permisos Predeterminados (Default Create Authority, CRTAUT) para la biblioteca.

La Imagen 9 muestra que el 16% de las bibliotecas revisadas tenían los Permisos Predeterminados *USE, *CHANGE y *ALL. Sin embargo, más del 82% de las bibliotecas dejan la configuración al valor del sistema QCRTAUT (*SYSVAL).

La Imagen 9A muestra la asignación del nivel de bibliotecas de *SYSVAL y refleja que el valor del sistema, en general, se mantiene en el permiso predeterminado de *CHANGE. De hecho, menos del 3% de los servidores han sido configurados para actuar por defecto denegando el acceso por defecto, tal como lo requieren estándares normativos comunes como PCI.

Esto significa que cuando se crean nuevos programas y archivos en estos sistemas, el usuario promedio automáticamente tiene permisos para realizar cambios sobre la gran mayoría de esos objetos nuevos. En estos sistemas, los usuarios no mencionados explícitamente tienen permiso de lectura, adición, modificación y eliminación de datos del archivo. Los mismos usuarios pueden copiar datos desde el archivo o cargar datos al archivo, y hasta modificar algunas de las características del objeto del archivo.

Imagen 9: Permisos predeterminados por biblioteca



La seguridad "adoptada" es una técnica de programación poderosa de IBM i que habilita a un programa a realizar funciones que los usuarios no podrían realizar por cuenta propia. El valor del sistema QUSEADPAUT define cuáles son los usuarios que pueden crear programas con el atributo de ejecución bajo seguridad "adoptada" (USEADPAUT(*YES)). Solo tres sistemas establecen una restricción en la configuración de este valor.

¿Cuál es la solución?

Los administradores de sistemas necesitan contar con procesos de control de acceso a datos de IBM i, ya que casi todos los usuarios de sistemas tienen permisos de acceso a datos mucho más amplios de lo que su perfil realmente requiere.

Primero, utilice las funciones de seguridad del sistema operativo de IBM i. Cuando sea posible, asegure los datos utilizando el recurso "nivel de seguridad" para proteger aplicaciones individuales y objetos de datos.

Cuando no sea posible o práctico asegurar los datos de ese modo, utilice un programa de salida (exit program) para regular el acceso a datos. Powertech Network Security es una solución de programa de salida de IBM i, líder en la industria, que está lista para usar.

Monitorice los cambios que se realizan sobre la información de su base de datos. Powertech Data Thread crea imágenes del antes y el después de los cambios en la base de datos, y exige a los usuarios que firmen los cambios realizados. De este modo, podrá también cumplir con los requerimientos normativos correspondientes.

Investigue el uso que sus proveedores externos de software hacen del recurso de nivel de seguridad en sus sistemas operativos. Busque asistencia del proveedor para proteger los objetos de la aplicación.

Finalmente, asegúrese que las bibliotecas de aplicación queden protegidas del perfil de usuario general del sistema. (Configure el Valor del Sistema y los valores de Bibliotecas para los permisos predeterminados en la configuración más restrictiva [*EXCLUDE].)

Control y auditoría de acceso a redes

¿De qué se trata y cuál es el riesgo?

Con el paso de los años, IBM amplió el poder de IBM i al agregar herramientas que posibilitan el acceso a datos desde otras plataformas, en especial desde PC. Muchos servicios reconocidos, como FTP, ODBC, JDBC y DDM están activos y listos para enviar datos por la red tan pronto como se enciende el ordenador. Cualquier usuario con un perfil en el sistema y permiso sobre los objetos puede tener acceso a datos críticos corporativos en su servidor Power System.

Esto es posible incluso cuando los administradores no instalan deliberadamente herramientas de acceso a datos en las PCs de los usuarios. Los usuarios finales pueden descargar herramientas gratuitas de Internet y hasta usar herramientas incluidas en otro software instalado en sus PCs para tener acceso a datos confidenciales. Por ejemplo, Windows viene con un software de cliente FTP que envía o recupera datos de un servidor IBM i con facilidad.

Lo peor es que los resultados analizados en la sección "El acceso a los datos por medio de *Public" indican que, en muchos de los sistemas analizados, casi no se utilizan permisos a nivel del objeto. La combinación de permisos de acceso abierto a datos, la cantidad excesiva de usuarios poderosos y las herramientas de acceso a datos desde PC constituye un escenario perfecto para una exposición de seguridad de IBM i.

Además del acceso a datos, algunos servicios TCP permiten la ejecución de comandos de servidores. Los servicios FTP de fácil acceso permiten que cualquier usuario pueda ejecutar comandos, hasta quienes no tienen permiso de línea de comando en su perfil. Esto es todavía una sorpresa para muchos administradores de sistemas y es algo desconocido por muchos gerentes y auditores.

¿Cuáles son los resultados?

Las estadísticas en la Imagen 10 muestran que REXEC, una aplicación TCP/IP que permite a los usuarios mandar comandos a un sistema remoto, a menudo, no se inicia de forma automática. El FTP, sin embargo, está siempre activo y alerta. Esto significa que la mayoría de los usuarios están a pocos pasos de poder utilizarlo para enviar datos a través de la red.

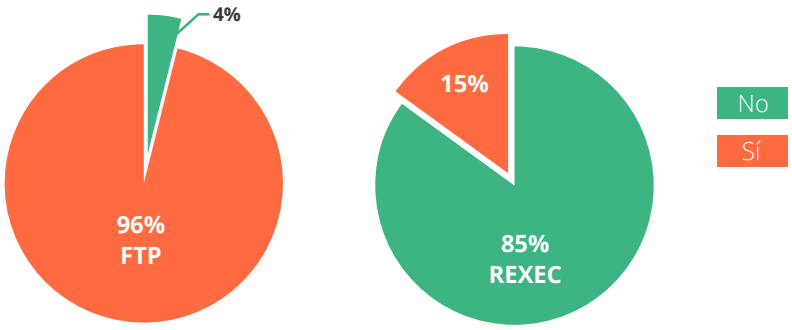


Imagen 10: Inicio automático de REXEC y FTP

Para reducir este riesgo, IBM ofrece interfaces conocidas como *exit points,* que permiten a los administradores asegurar sus sistemas. Un programa de salida unido a un *exit point* puede monitorizar y restringir el acceso de red al sistema.

Un programa de salida debería tener dos funciones principales: auditar solicitudes de acceso y brindar un control de acceso que permita aumentar la seguridad a nivel del objeto de IBM i. El estudio supone que todos los programas de salida designados satisfacen ambos requerimientos mínimos.

HelpSystems revisó 27 interfaces de *exit points* de red diferentes en cada sistema para ver si tenían registrado un programa de salida. Aproximadamente tres cuartos de los sistemas no contaban con programas de salida adecuados que les permitieran registrar y controlar el acceso a redes (Imagen 11).

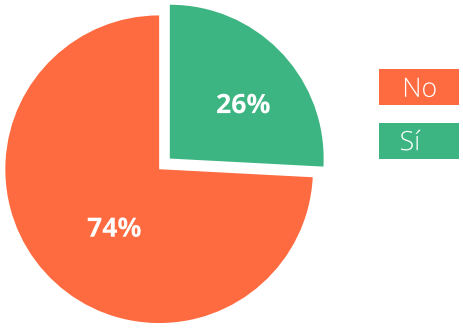
Hasta en los sistemas con programas de salida, la cobertura suele ser incompleta. Entre los sistemas con programas instalados, el 5% tenía solamente uno o dos programas de salida registrados; mientras que menos del 9% tenía programas registrados en todos los *exit points* de acceso a red.

El hecho de tener tan pocos programas de salida registrados es un fuerte indicador de la existencia de desarrollos de políticas propias a través de un cliente que autoriza sus propios programas de salida. Mientras que esto sugiere que el concepto de registrar programas de salida está comprendido, la cobertura suele quedar limitada solo a aquellos servidores que son considerados más destacados o cargados de riesgo.

En este estudio, el 8% de los servidores tienen más de cinco programas de salida, pero menos del 27% muestra la presencia de una solución de programas de salida a nivel comercial. El *exit point* más común cubierto fue FTP Server Request, seguido por FTP Sign-On Request. Las funciones de acceso a datos ODBC/JDBC se mantienen en su mayoría sin ser monitorizadas, exponiendo así al servidor al riesgo de pérdida de datos transparentes.

APROXIMADAMENTE TRES CUARTOS DE LOS SISTEMAS NO CONTABAN CON PROGRAMAS DE SALIDA ADECUADOS QUE LES PERMITIERAN REGISTRAR Y CONTROLAR EL ACCESO A REDES

Imagen 11: Programas de salida instalados



¿Cuál es la solución?

Sin programas de salida instalados, IBM i no ofrece ninguna pista de auditoría con respecto a las actividades de los usuarios que se originen a través de herramientas de acceso de redes comunes, tales como FTP y ODBC. Hasta las empresas que han instalado soluciones de programas de salida para proteger sus datos con frecuencia descuidan algunos de los puntos de acceso críticos.

Pareciera que muchas empresas en la comunidad de IBM i desconocen, de forma peligrosa, el problema que representa la amplia apertura del acceso a la red. La falta de monitorización y control del acceso a la red es una deficiencia importante en muchas empresas.

Las empresas usuarias de IBM i pueden desarrollar sus propios programas de salida o utilizar software de venta comercial para realizar esta tarea. La ventaja de utilizar una solución comercial de programa de salida como Powertech Network Security para monitorizar y controlar el acceso de usuarios por medio de interfaces de red, es que usted obtiene una mayor cobertura, que protege todos los puntos de acceso críticos.

Usuarios con acceso a la línea de comandos

¿De qué se trata y cuál es el riesgo?

La forma tradicional de controlar el acceso a datos confidenciales y comandos poderosos era limitar el acceso a la línea de comandos a los usuarios finales. En el pasado, este método era eficaz.

Además de configurar el perfil de usuario con limitaciones de acceso a la línea de comandos, los menús de aplicaciones controlaban la forma en que los usuarios accedían a los datos y también cuándo tenían acceso a una línea de comandos. Sin embargo, desde que IBM abrió nuevas interfaces que brindan acceso a datos y la oportunidad de ejecutar comandos remotos, este enfoque dejó de ser tan eficaz.

¿Cuáles son los resultados?

De acuerdo con los resultados del año 2017, el 33% de los usuarios tiene acceso a la línea de comandos por medio de las interfaces basadas en menúes tradicionales. De esos usuarios, el estudio reveló que el 52% de los perfiles estaban habilitados.

Varias interfaces de redes no reconocen las limitaciones de la línea de comandos que se configuran en el perfil del usuario y deben ser controladas de otro modo. Esto significa que los usuarios pueden ejecutar comandos remotos, incluso cuando los administradores de sistemas hubieran tomado precauciones deliberadamente para limitarlos en el uso de la línea de comandos.

¿Cuál es la solución?

Tal como se describió en la sección "El acceso a los datos por medio de *Public", el permiso amplio *PUBLIC permite que cualquier persona con acceso a estos sistemas tenga también acceso a los datos, comandos y programas sin que quede registrado en el sistema operativo.

Comience a abordar este problema controlando las transacciones de acceso a datos desde la red para detectar actividad inadecuada o peligrosa. Asegúrese de establecer lineamientos claros para la descarga y permisos de intercambio de archivos. Elimine el acceso predeterminado DB2 en herramientas como Microsoft Excel e IBM i Client Access.

ESTO SIGNIFICA QUE LOS USUARIOS PUEDEN EJECUTAR COMANDOS REMOTOS, INCLUSO CUANDO LOS ADMINISTRADORES DE SISTEMAS HUBIERAN TOMADO PRECAUCIONES DELIBERADAMENTE PARA LIMITARLOS EN EL USO DE LA LÍNEA DE COMANDOS.

Auditoría del sistema

¿De qué se trata y cuál es el riesgo?

Una de las funciones de seguridad más importantes de IBM i es su capacidad de registro de eventos relacionados con la seguridad en un centro de almacenamiento no modificable, o Registro de Auditoría de Seguridad. Esta función permite a las organizaciones determinar la fuente de eventos críticos de seguridad, a saber:

- ¿Quién eliminó este archivo?
- ¿Quién le otorgó a este usuario el permiso *ALLOBJ?

Esta información puede marcar la diferencia entre reaccionar de inmediato ante un evento de seguridad o descubrir una filtración de datos después de que ya se haya producido un daño significativo.

El desafío es que el volumen de datos en el Registro de Auditoría de Seguridad es tan extenso y su contenido es tan enigmático, que la mayor parte del personal de IT no puede monitorizar la actividad registrada con las herramientas disponibles en el sistema operativo.

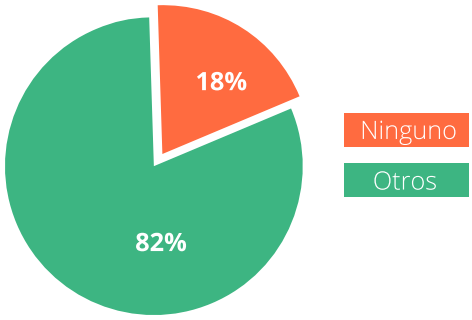
Analizar el significado de los datos de seguridad es la segunda mitad fundamental de la ecuación de auditoría. Sin una forma de convertir los datos en información significativa y factible, las organizaciones corren el riesgo de perder señales de advertencia muy importantes.

¿Cuáles son los resultados?

El 15% de los sistemas revisados no tiene un centro de almacenamiento de registros de auditoría, lo que indica un nivel de control muy bajo.

De acuerdo con una estadística relacionada, casi el 18% de los sistemas está operando con la configuración de valor del sistema QAUDCTL en su valor predeterminado *NONE (Imagen 12). Este es el interruptor principal para dar inicio o finalizar una auditoría y bloquear en forma global el registro de cualquier evento a nivel sistema u objeto, independientemente de la existencia del registro de auditoría del sistema.

Imagen 12: Valor del sistema QAUDCTL



La ausencia del Registro de Auditoría de Seguridad de IBM i (QAUDJRN) indica un nivel muy bajo de control para el sistema en cuestión.

También hay inconsistencia en los tipos de eventos que se auditan. Algunas configuraciones sugieren que la auditoría ha sido activada por aplicaciones de alta disponibilidad (High Availability) que deben replicar eventos para generar backups. Tipos de eventos de auditoría como *AUTFAIL (Fallas de Permisos) no son requeridos en una infraestructura de alta disponibilidad. Cuando *AUTFAIL no está activado, queda en evidencia que los clientes no están usando la herramienta de auditoría para realizar controles de seguridad.

Cuando las organizaciones activan el Registro de Auditoría de Seguridad, no queda claro cuánta información les está proporcionando esa gran cantidad de datos. Algunos proveedores de software proporcionan herramientas de auditoría que informan y revisan los datos de sistemas incorporados al Registro de Auditoría de Seguridad. Sin embargo, solo el 17% de los sistemas incluidos en este estudio cuentan con una herramienta reconocible instalada.

¿Cuál es la solución?

En la mayoría de los sistemas incluidos en este estudio, se pueden producir violaciones de seguridad sin ser detectadas. Las empresas que usan el Registro de Auditoría de Seguridad están en una posición mucho mejor que aquellas que no lo usan, dado que pueden utilizar una herramienta automática para examinar cuidadosamente e interpretar los eventos del registro de auditoría en cualquier momento.

Teniendo en cuenta la gran cantidad de datos sin procesar que son recopilados en el Registro de Auditoría de Seguridad de IBM i, no se puede esperar que los administradores del sistema revisen esos registros en forma manual con regularidad. El trabajo de filtrar y analizar cantidades considerables de datos complejos sin procesar requiere herramientas de software.

Al mismo tiempo, muchas organizaciones están abrumadas por la cantidad de informes requeridos para demostrar el cumplimiento de normas tales como Sarbanes-Oxley (SOX) y el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS); sin embargo, parece que muy pocas de ellas aprovechan las herramientas que están disponibles para automatizar y simplificar tareas de generación de informes.

El uso de una herramienta de auditoría de software, como Powertech Compliance Monitor reduce los costos relacionados con la generación de informes de cumplimiento y aumenta la probabilidad de que se lleve a cabo este trabajo. La implementación de Powertech Interact agregará datos de seguridad de IBM i a sus Soluciones de Seguridad Corporativa, que son compatibles con los formatos de Gestión de Eventos e Información sobre Seguridad (SIEM) o Syslog, lo que le permite identificar eventos de seguridad con rapidez.

Susceptible a ataques de virus y malware

¿De qué se trata y cuál es el riesgo?

Uno de los temas más polémicos de seguridad de IBM i es el riesgo que suponen los virus y otros programas maliciosos. Aunque la infraestructura tradicional de la biblioteca y objetos de IBM i se considera altamente resistente a virus, se sabe que otras estructuras de archivos dentro del Sistema Integrado de Archivos (IFS) son susceptibles de albergar archivos infectados que después pueden propagarse por toda la red.

Conociendo esta realidad, IBM creó valores de sistemas y *exit points* de registros para respaldar el escaneo de virus nativos hace algunos años.

Muchos proveedores de software de IBM i están intentando todavía llegar a un acuerdo respecto de las amenazas de virus. Una empresa escaneó su IBM i para detectar virus por primera vez y se sorprendió al encontrar casi 250.000 archivos infectados por el virus CryptoWall. Si había alguna duda sobre la necesidad de protección contra virus, este ejemplo comprueba que el riesgo es real.

Además, el estándar PCI DSS establece el uso de un software anti-virus y esto probablemente sea cada vez más común.

UNA EMPRESA ESCANEÓ SU IBM I PARA DETECTAR VIRUS POR PRIMERA VEZ Y SE SORPRENDIÓ AL ENCONTRAR CASI 250.000 ARCHIVOS INFECTADOS POR EL VIRUS CRYPTOWALL.

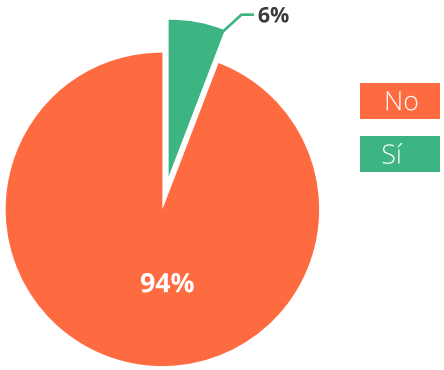
¿Cuáles son los resultados?

En una actualización reciente de la herramienta de recopilación de datos, registramos la configuración de valores de sistema relacionados con el análisis (QSCANFSCTL y QSCANFS), así como también de los exit points QIBM_QP0L_SCAN_OPEN (escaneo con archivos en uso) y QIBM_QP0L_SCAN_CLOSE (escaneo sin archivos en uso).

El *exit point* QIBM_QP0L_SCAN_OPEN permite el registro de un programa de salida que interceptará todos los intentos de apertura de archivos y escaneará el archivo antes de que se pueda abrir. Esto garantiza que no se propagará una infección fuera del entorno de IBM i.

El análisis de servidores respecto de los controles anti-virus demostró que había un 6% que escaneaba archivos en uso. Esto significa que el 94% restante corre el riesgo de afectar objetos internos o de propagar una infección a otro servidor de su red (Imagen 13).

Imagen 13: Escaneo de archivos IFS en uso



Todos los sistemas evaluados respecto de los controles anti-virus, salvo dos, utilizan el valor del sistema por defecto QSCANFS (*ROOTOPNUD) para el sistema operativo. Esta configuración permite que se escaneen archivos de flujo (stream files) en la raíz(/), QOpenSys y sistemas de archivos definidos por el usuario con el fin de detectar amenazas de virus si se instala una aplicación de escaneo.

Además, se puede optimizar el rendimiento en un 6% de los sistemas configurando el valor del sistema QSCANFSCTL para incluir el valor *FSVRONLY. Si los valores incluyen *FSVRONLY, solo se escaneará el acceso a través del servidor del archivo para detectar amenazas maliciosas, y el acceso al archivo desde trabajos locales no generará un escaneo ni afectará el normal funcionamiento del sistema.

¿Cuál es la solución?

A pesar de que IBM i no podrá infectarse con malware de PC o Unix, sí pueden infectarse los objetos almacenados en IFS. Además, los virus activos funcionan con el permiso del usuario que los activó y, por lo tanto, pueden afectar objetos nativos por medio de acciones, como cambiarles el nombre o borrar objetos.

Si utiliza IBM i como servidor de archivos, debe tomar medidas para garantizar que estos objetos infectados no puedan ejecutarse en un servidor Windows. Una defensa anti-virus adecuada detectará, eliminará y evitará la propagación de la infección más allá del entorno actual.

Registre un programa de salida para el *exit point* QIBM_QP0L_SCAN_OPEN a fin de interceptar intentos de apertura de archivos desde la red y escanee sus archivos antes de abrirlos. Esto evitará que los virus se puedan propagar fuera del entorno IBM i.

Instale una aplicación de escaneo de virus para detectar y eliminar infecciones, así como para evitar la propagación de malware más allá del entorno actual.

Implemente una solución de escaneo que se ejecute en forma local en IBM i, como Stand Guard Anti-Virus, para proteger los datos de los virus, gusanos o malware. El uso de un escáner de virus nativo de IBM es más seguro, rápido y confiable que uno de PC.

CONCLUSIÓN

IBM i es reconocida como una de las plataformas más seguras en el mercado. Una de las principales ventajas es que IBM i incluye herramientas sofisticadas de seguridad, monitorización y registro en su sistema operativo. Los expertos concuerdan en que la seguridad de IBM i es tan eficaz como las políticas, los procedimientos y las configuraciones implementadas para su administración.

Este estudio destacó una serie de riesgos de seguridad frecuentes y las prácticas de configuración que deberían llevarse a cabo para proteger los datos en los sistemas de IBM i.

A pesar de que las organizaciones podrían mejorar los controles de IT en su servidor IBM i, la decisión sobre qué controles deben hacerlo primero puede ser todo un desafío. Ningún sistema se ha tornado vulnerable de la noche a la mañana, y tampoco es posible solucionar todos los problemas de seguridad en un solo día. **Lo importante es comenzar por algún lado y lograr un progreso continuo hacia un perfil de seguridad más sólido.**

Cada sistema enfrenta desafíos únicos, pero en general hay tres prioridades principales sobre la seguridad de IBM i. Si no está seguro sobre cómo proceder, comience con esta lista:

- Seguridad del Sistema: Verifique el nivel QSECURITY y asegúrese de que sea 40 o superior.
- Auditoría de Seguridad: Habilite QAUDJRN y busque una herramienta que ayude a interpretarlo.
- Acceso a la red: En principio, registre los *exit points* más comunes, como FTP y ODBC.

La mayoría de los expertos recomienda comenzar con una evaluación de las vulnerabilidades para comprender el estado real de seguridad de su sistema y cómo podría mejorarse. Usted tiene a su disposición a profesionales de seguridad con experiencia en IBM i y también soluciones de software fáciles de usar, para hacer que este proyecto sea más rápido y sencillo. HelpSystems ofrece una amplia gama de opciones, desde una Evaluación de Riesgos muy minuciosa hasta un Security Scan rápido y gratuito.

Una vez que cuente con toda la información, puede comenzar a formular un plan que aborde las vulnerabilidades de seguridad de su organización. A partir de ahí, la seguridad se volverá algo habitual y no un momento de pánico después de una auditoría fallida o una filtración de datos.

HELPSYSTEMS ESTÁ AQUÍ PARA AYUDARLO CON IBM I

Verifique qué tan seguro es su IBM i con un Security Scan de HelpSystems. Security Scan es una herramienta gratuita y rápida, que revela las fallas de seguridad de su sistema. Después de ejecutarlo, nuestros especialistas en Seguridad lo pueden ayudar a formular un plan para remediar sus vulnerabilidades de seguridad.

ANEXO: SOLUCIONES DE SEGURIDAD DE HELPSYSTEMS

Como experto líder en seguridad de IBM i, HelpSystems ha desarrollado una extensa línea de soluciones potentes diseñadas para abordar vulnerabilidades en el sistema operativo, proporcionar funciones avanzadas de control y auditoría de accesos, y alivianar el costo y la carga de mantener el cumplimiento normativo.

La Tabla 2 describe los módulos de seguridad disponibles y sus fines.

Tabla 2: Conjunto de soluciones de seguridad integrales

SOFTWARE DE SEGURIDAD

Compliance Monitor	Auditoría y generación de informes personalizada
Network Security	Control de accesos mediante programas de salida
Authority Broker	Gestión de usuarios privilegiados
Interact	Reportes de seguridad en tiempo real
DataThread	Monitoreo de base de datos en tiempo real
Command Security	Monitoreo y control de comandos
PowerAdmin	Gestión centralizada de perfiles de usuario
StandGuard Anti-Virus	Detección nativa avanzada de virus
Password Self Help	Autoservicio de restablecimiento de contraseña
Agent for RSA SecurID	Autenticación de dos factores para IBM i
Policy Minder	Aplicación de políticas de seguridad automatizada
Risk Assessor	Evaluación integral de seguridad
Security Scan	Escaneo gratuito de IBM i
Crypto Complete	Encriptación y gestión clave
GoAnywhere	Gestión de transferencia de archivos

SERVICIOS DE SEGURIDAD

Risk Assessment	Evaluación detallada de vulnerabilidades
Penetration Testing	Prueba de vulnerabilidades
Architecture	Plan de acción de seguridad
Remediation	Implementación de la arquitectura
Managed Security Services	Monitoreo e informes mensuales de seguridad

ACERCA DEL AUTOR

Robin Tatam es un referente en la industria, con más de 25 años de experiencia en IBM i. Es copresidente del grupo QUSER en Minneapolis, un galardonado orador, experto en materia de seguridad para COMMON, y miembro de su Speaker Excellence Hall of Fame. Robin cuenta con la certificación de Administrador Certificado de Seguridad de la Información (CISM) de ISACA y es el coautor de la publicación Redbook de IBM sobre la codificación de datos de IBM i.

ROBIN TATAM

Director de Tecnologías de Seguridad

Acerca de HelpSystems

HelpSystems es el experto líder en soluciones automatizadas de seguridad para servidores IBM Power Systems, que ayuda a los usuarios a administrar el cumplimiento de las regulaciones actuales y las amenazas sobre la privacidad de datos. Nuestras soluciones y servicios de seguridad protegen los valiosos recursos de IT, garantizando su protección y tranquilidad.

Debido a que los servidores Power Systems a menudo albergan datos corporativos confidenciales, las organizaciones necesitan ejercer un cumplimiento proactivo en materia de seguridad. Como Partner Avanzado de IBM, con una base de clientes que sigue creciendo en todo el mundo, HelpSystems entiende la vulnerabilidad corporativa y los riesgos asociados con la privacidad de los datos y el control de acceso. Las soluciones y los servicios de seguridad de HelpSystems son el estándar corporativo para la seguridad de IBM i en muchas de las principales instituciones financieras internacionales.

HelpSystems ha demostrado un compromiso con el mercado de seguridad y el cumplimiento normativo. Líder de la industria en lo que respecta a la concientización sobre los problemas de seguridad de IBM i y las soluciones, aprovecha la experiencia de los expertos más reconocidos en materia de seguridad de IBM i del mundo, como Robin Tatam y Carol Woodbury.

- HelpSystems es miembro del PCI Security Standards Council, un organismo internacional que proporciona orientación para el Estándar de Seguridad de Datos para la Industria de Tarjeta de Pago (PCI DSS). HelpSystems trabaja con el consejo para hacer evolucionar el estándar PCI DSS y otras normas de pago y protección de datos.

- HelpSystems es miembro del consejo Independent Software Vendor (ISV) de IBM i.

- HelpSystems publica el estándar IBM i Security Standard como parte de su misión para promover la concientización sobre los desafíos de seguridad más comunes y asegurar la integridad y confidencialidad de los datos de IBM i.

helpsystems

www.helpsystems.com

Acerca de HelpSystems

Organizaciones de todo el mundo confían en HelpSystems para simplificar la vida de los departamentos de IT y mantener sus negocios funcionando sin problemas. Nuestros productos y servicios monitorizan y automatizan procesos, cifran y protegen datos, y proporcionan un fácil acceso a la información que las personas necesitan.