Wayne O Evans Consulting, Inc.

400 Security Training and Consulting

Políticas de Seguridad para el AS400

En las revisiones de seguridad que he dirigido en instalaciones con AS400 , el problema que más comúnmente aparece es que no existe una política de seguridad en casi el 70 % de las instalaciones. Pocas organizaciones con AS/400 tienen una política de seguridad y si la tienen, a menudo disponen de ella sólo porque así lo requiere algúna entidad reguladora. La política de seguridad se crea entonces para encajar con esos requisitos y sólo sirve para almacenar el polvo encima de ella. La efectividad de una política de seguridad se mide fácilmente preguntando al responsable de la seguridad del AS/400 por una copia de la politica de seguridad. Si tiene que preguntarle a alguien dónde está el documento, entonces la política de seguridad no es una herramienta útil. No existen datos actualizados para medir la efectividad de la política de seguridad pero sospecho que menos del 10% de las organizaciones con AS/400 disponen de una política de seguridad que sea un documento utilizado como parte de las decisiones diarias acerca de la seguridad

El documento siguiente contiene algunos ejemplos de políticas de seguridad. Cada política contendrá a su vez lo siguiente :

- Una descripción breve de una línea.
- Una descripción extensa y las razones para la política
- Detalles técnicos del AS/400 .

1. Valores de Sistema

1.1. El nivel de seguridad del sistema debe adecuarse para prevenir el acceso a los datos.

La configuración recomendada para el valor de sistema es QSECURITY = 40.

El valor de sistema QSECURITY determina el nivel de seguridad a comprobar forzado por el sistema operativo.

- El nivel de seguridad 20 permite a los usuarios acceso no restringido a los objetos de datos y confía en los controles de la aplicación. Los usuarios de PC y de Internet fácilmente saltarían los controles de la aplicación. Este nivel de seguridad no es adecuado.

- El nivel de seguridad 30 puede usarse para restringir el acceso a objetos individuales. No obstante, programas escritos en MI (machine interface) pueden saltarse algunos controles. Si un usuario tiene acceso al trabajo (*JOBD) que nombra los perfiles de usuario, el usuario podría someter trabajos como el usuario que aparece en la descripción del trabajo.

- El nivel de seguridad 40 elimina el riesgo asociado con el nivel 30 sin impactos en el uso. Como el nivel 40 bloquea algunos interfaces , algunos programas de terceros podría no ejecutarse en este nivel de seguridad.

- El nivel de seguridad 50 está diseñado para sistemas que necesitan tener el nivel de seguridad certidicado C2. C2 no se requiere para la mayoría de aplicaciones comerciales así que el nivel de seguridad 50 no está recomendado porque puede causar impactos en el uso.

AS/400 Detalles Técnicos
Comprobar el valor de sistema QSECURITY

2. Contraseñas

2.1. Las contraseñas deberían cambiarse periódicamente

La configuración recomendada para el valor de sistema QPWDEXPITV es 30-90 días según el entorno de seguridad del sistema.
Si las contraseñas se utilizan durante períodos largos de tiempo, la posibilidad de que sean descubiertas aumenta. Para prevenir el acceso al sistema de extraños, se debe requerir a los usuarios el cambio de sus contraseñas según unas reglas. El valor de sistema QPWDEXPITV se puede usar para pedir un cambio periódico de las contraseñas.

AS/400 Detalles Técnicos
Comprueba el valor de sistema QPWDEXPITV según el entorno de seguridad del sistema.La recomendación es que se sitúe entre 30 y 90 .

2.2. Las contraseñas deben contener dígitos.

La configuración recomendada para el valor de sistema QPWDRQDDGT es ‘1’.

Los ”hackers” intentan adivinar las contraseñas utilizando un diccionario de palabras comunes. Pedir que las contraseñas de los usuarios contengan al menos un dígito elimina el riesgo de un “ataque de diccionario”.

AS/400 Detalles Técnicos
Comprueba el valor de sistema QPWDRTDDGT = ‘1’

2.3. Las contraseñas no deben contener digítos adyacentes.

La configuración recomendada para el valor de sistema QPWLMTAJC es ‘1’ lo cual previene de digítos adyacentes en la contraseña.

Los usuarios a menudo usan contraseñas triviales como su número de teléfono, su dirección, su número de empleado o número de la seguridad social. Un "hacker" familiarizado con el usuario puede conocer esta información personal y usarla , así que la utilización de esta información relativa a los usuarios debe prevenirse. Requerir que las contraseñas de usuario no contengan digitos adyacentes reduce el riesgo de que las contraseñas se puedan adivinar.

AS/400 Detalles Técnicos
Comprueba el valor de sistema QPWDLMTAJC = '1'

3. Perfiles de usuario

3.1. No debe haber acceso *PUBLIC para los perfiles de usuario.

El permiso PUBLIC para perfiles de usuario debe ser *EXCLUDE.

Cuando un usuario tiene acceso *USE a otros perfiles de usuario,los trabajos batch pueden ser sometidos como otro usuario. Existen algunos perfiles de usuario que requeriran *PUBLIC acceso , pero la mayoría de perfiles deben tener acceso *EXCLUDE .

AS/400 Detalles Técnicos
Comprueba el permiso *PUBLIC para los perfiles de usuario. Hay algunos perfiles de sistema (QDBSHR, QSPLJOB, QTMPLPD) que deben tener autorización pública , los otros perfiles deberían estar *EXCLUDE

4. Perfiles de grupo

4.1. Los perfiles de grupo no deberían tener contraseña.

La contraseña para los perfiles de grupo debe ser *NONE.

Una contraseña *NONE previene que los usuarios se identifiquen como el perfil de grupo. Los usuarios deben acceder usando su perfil individual de usuario y no el perfil de grupo.

AS/400 Detalles Técnicos
Todos los perfiles de grupo deberían tener contraseña *NONE excepto el perfil de usuario QSECOFR que sí debe tener una.

4.2. Los perfiles de usuario que provee IBM no deberían usarse como perfil del grupo.

No es recomendable la utilización de los perfiles que da IBM como perfiles de grupo.

Mejor que usar los perfiles de IBM (QSECOFR, QSYSOPR, QPGMR, QUSER, QSRV y QSRVBAS) como perfiles de grupo, es crear perfiles definidos para cada instalación con los atributos y permisos que se desee. IBM cambia con cierta periodicidad el acceso de los perfiles IBM de usuario en las distintas releases. El cambio puede ser un problema para los usuarios si los perfiles IBM se usan como perfiles de grupo.

AS/400 Detalles Técnicos

Determinar si cualquiera de los perfiles IBM (QSECOFR, QSYSOPR, QPGMR, QUSER, QSRV, y QSRVBAS) son perfiles de grupo.

4.3. Perfiles con permisos especialmente potentes no deben usarse como perfiles de grupo.

Los perfiles de grupo no deberían tener permisos especiales de *ALLOBJ, *SERVICE o *SPLCTL.

El permiso especial para el perfil de grupo está disponible para todos los miembros del grupo. Dar una autorización especial al perfil de grupo es como dar esa autorización a cada miembro . Los permisos especiales de especial inquietud son aquéllos que permiten a los usuarios acceso sin restricciones al sistema:

- *ALLOBJ Acceso a todos los objetos del sistema.Usuarios con este nivel de acceso no pueden ser sometidos a restricciones.
- *SERVICE El uso de herramientas de servicio del sistema puede usarse para sortear la seguridad.
- *SPLCTL Acceso a todos los ficheros de spool del sistema. Outputs especialmente delicados como la nómina o información del Dpto.de Recursos Humanos pueden ser leídas por los usuarios con autorización especial *SPLCTL .

Existen otros permisos especiales que generan un riesgo aunque menor en la seguridad y que pueden usarse en los perfiles de grupo.

La práctica recomendada es limitar con cuidado estos permisos y mejor concederlos a usuarios individuales que a los perfiles de grupo.

AS/400 Detalles Técnicos

Comprobar los permisos especiales de los perfiles de grupo.

*ALLOBJ
*SERVICE
*SPLCTL
*IOSYSCFG
*SECADM
*AUDIT
*JOBCTL

5. Acceso a BIBLIOTECAS

5.1. Las bibliotecas de la parte de sistema de la lista de bibliotecas deberían tener acceso *USE público.

La lista de bibliotecas del AS/400 consiste en una parte de sistema y una parte de usuario. La parte de sistema es la misma para todos los trabajos del sistema mientras que la parte de usuario puede ser modificada para trabajos individuales. La biblioteca de sistema llamada QSYS contiene los programas y comandos que soporta el OS/400 . Las bibliotecas de usuario pueden añadirse a la lista de bibliotecas.

Los comandos y programas de la lista de bibliotecas son direccionables para todos los trabajos del sistema. El acceso *PUBLIC a las bibliotecas de la parte de sistema de la lista de bibliotecas debe ser *USE para permitir el uso de los objetos de la biblioteca , pero no permite la incorporación de nuevos objetos.Si los usuarios tuvieran el permiso *ADD es posible que insertaran nuevos objetos a la biblioteca que podrían comprometer la seguridad ,un Caballo de Troya que habilitara funciones extra si las usara un usuario con capacidad. Las bibliotecas de la lista de bibliotecas anteriores a QSYS deberían estar estrechamente controladas pues añadir un objeto a esas librerías podría reemplazar funciones del sistema operativo.

AS/400 Detalles Técnicos

Recuperar la parte de sistema de la lista de bibliotecas desde el valor de sistema QSYSLIBL. Comprobar el permiso *PUBLIC para cada biblioteca de la lista de bibliotecas.

5.2. El equipo de programadores no debe estar autorizado a insertar objetos en las bibliotecas de producción.

El equipo de programadores puede necesitar acceso *USE a las bibliotecas de producción para así ejecutar programas y leer los ficheros de producción. El

equipo de programadores no debe estar autorizado a modificar los contenidos de las bibliotecas de producción ni los objetos de programas o datos. Todos los cambios en los programas de producción debe realizarse en bibliotecas de test. Cuando un cambio se haya testeado y esté listo para su inclusión en producción, se utiliza un procedimiento de control para crear archivos con las copias de los objetos antes de realizar los cambios en las bibliotecas de producción. Estas copias de archivo pueden usarse si los cambios necesitan retrocederse.

AS/400 Detalles Técnicos
Recuperar la lista de bibliotecas (usuario y sistema) desde los valores de sistema QSYSLIBL y QUSRLIBL. Comprobar QPGMR y la autorización *PUBLIC para cada biblioteca de la lista de bibliotecas.

5.3. Las bibliotecas de producción no deberían tener acceso *PUBLIC de *ALL

Las bibliotecas de producción deberían tener una acceso *PUBLIC de *USE o menor. Si un usuario tiene acceso *ALL a todas las bibliotecas de producción podría borrar la librería.

AS/400 Detalles Técnicos
Recuperar la lista de bibliotecas del sistema .
Comprobar el permiso *PUBLIC para cada biblioteca equivalente a *ALL

6. Acceso a programas de producción

6.1. Los programas de producción no deben tener acceso *PUBLIC de *CHANGE

Los programas de producción deben tener acceso *PUBLIC de *USE o menor. Si un usuario tiene acceso *CHANGE a los programas , las facilidades para debug del AS/400 podrían usarse para parar la ejecución del programa y cambiar los datos del mismo. Si los usuarios tienen acceso *USE a los programas pueden ejecutar los programas pero no usar las herramientas de depuración del sistema.

AS/400 Detalles Técnicos
Recuperar la lista de bibliotecas (usuario y sistema) desde los valores de sistema QSYSLIBL y QUSRLIBL. Comprobar cada programa en la/s biblioteca/s si dispone de autorización *PUBLIC mayor que *USE.

7. Auditoría

7.1. Auditar las acciones de los usuarios.

Los usuarios con permisos especiales muy amplios (*ALLOBJ, *SERVICE o *SPLCTL) deben tener activada la auditoría de comandos. Las acciones de estos usuarios con acceso potente deben ser registradas en el journal de auditoría.

AS/400 Detalles Técnicos

En un entorno de alta y media seguridad, verificar que la auditoría está activada comprobando los valores de sistema.

QAUDCTL debe contener *AUDLVL
QAUDLVL.debe incluir ambos, *AUTFAIL y *SERVICE

7.2. Los usuarios con permisos especiales deben ser auditados.

Los usuarios con permisos con amplio poder (*ALLOBJ, *SERVICE or *SPLCTL) deben tener activada la auditoría de comandos. Las acciones de estos usuarios con acceso potente deben ser registradas en el journal de auditoría.

AS/400 Detalles Técnicos

En un entorno de alta seguridad, al usar perfiles de permisos especiales (SPCAUT) de *ALLOBJ, *SERVICE o *SPLCTL, verificar que la auditoría de comandos AUDLVL está activada.

7.3. El Journal de auditoría debe cambiarse cada 31 días

El journal de auditoría debería cambiarse cada mes. El journal de auditoría consume espacio en el sistema y puede escribirse en un backup y liberar espacio. Esto se realiza mejor con una tarea programada. Cambios con más frecuencia son innecesarios.

AS/400 Detalles Técnicos

Cuando el journaling está activo, recuperar la fecha de la última journal que se añadió al sistema y comprobar la fecha que se añadió del receptor del journal.