LABORATORIO 17 RBAC

*Este laboratorio se trabajó en equipo por lo que se verá implementado en el proyecto.

Preguntas:

¿En qué consiste el acceso basado en roles?

Se utiliza como una función de seguridad para controlar el acceso de usuarios a cierto tipo de tareas que por lo general están restringidas al superusuario. Gracias a la aplicación de estos atributos de seguridad se pueden dividir las capacidades de superusuario entre varios administradores.

Esta gestión de derechos a ciertas acciones se implementa a través de privilegios, que se definen a través de RBAC. De tal forma que los empleados solamente pueden interactuar con la información necesaria y solamente la necesaria para cumplir con sus deberes. [1]

Investiga y describe 6 sistemas, 3 conocidos que empleen RBAC y 3 desconocidos que no, junto con su funcionamiento general.

Emplean RBAC:

Microsoft Azure:

> Es un sistema de autorización más nuevo que proporciona una administración de acceso detallada a los recursos de Azure. RBAC incluye muchos roles integrados, puede asignarse a diferentes ámbitos y le permite crear sus propios roles personalizados. Para administrar recursos en Azure AD, como usuarios, grupos y dominios, existen varias funciones de administrador de Azure AD. [2]

Solaris:

> Role Based Acces Control, es una evolución introducida en Solaris 8 -hace ya tiempo- para poder gestionar las acciones mediante privilegios. De esta forma, podemos tener un grupo de privilegios para nuestros operadores nivel 1, para que puedan iniciar/detener/checkear el Sistema de monitorización de Nagios, pero que no puedan hacer un reboot de la máquina. Para solucionar este problema, se introdujeron los privilegios y los roles.

Oracle DBMS:

> RBAC ofrece la capacidad de empaquetar privilegios de superusuario para asignarlos a cuentas de usuario. Con RBAC, puede brindar a los usuarios la capacidad de resolver sus propios problemas al asignarles paquetes de los privilegios apropiados. Las capacidades del superusuario se pueden disminuir dividiendo esas capacidades en varios paquetes y asignándolas por separado a las personas que comparten responsabilidades administrativas.
>
> RBAC permite la separación de poderes, la delegación controlada de operaciones privilegiadas a otros usuarios y un grado variable de control de acceso. [4]

No utilizan RBAC:

- Sistemas en algunas tiendas de Misceláneo.
- Sistemas de facturación y puntos de venta locales.
- Sistemas de registro de inventario en escuelas públicas.

Beneficios:

1. Reducción del trabajo administrativo y cambios técnicos.
2. Maximización de la eficiencia operacional. [5]

Desventajas:

1. No se puede configurar un permiso utilizando parámetros que son desconocidos para el sistema antes de que un usuario comience a trabajar.
2. Los permisos solo se pueden asignar a roles de usuario, no a objetos y operaciones.
3. Puede restringir el acceso a ciertas acciones en su sistema, pero no a ciertos datos. [6]

Referencias:

[1] https://docs.oracle.com/cd/E24842_01/html/E23286/rbac-1.html

[2] https://docs.microsoft.com/en-us/azure/role-based-access-control/rbac-and-directory-admin-roles

[3] http://unix-linux-server.blogspot.com/2015/05/modelo-de-seguridad-de-solaris-rbac.html

[4] https://docs.oracle.com/cd/E19455-01/805-7229/6j6q8svdh/index.html

https://digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more

[5] https://www.ekransystem.com/en/blog/rbac-vs-abac

[6]https://www.cio.com/article/3250296/establishing-role-based-access-control-in-the-workplace.html