

Consideraciones sobre seguridad en la implantación de soluciones de búsqueda

Una solución de búsqueda puede ayudar a potenciar la productividad de la empresa haciendo que la información útil esté siempre a disposición de quienes la necesitan.

INTRODUCCIÓN: REQUISITOS DE SEGURIDAD PARA LAS SOLUCIONES DE BÚSQUEDA

Una solución de búsqueda para la empresa implantada de forma correcta puede implicar poner información fundamental al alcance de la mano de los trabajadores del conocimiento y otros empleados de una organización, cumpliendo así con las expectativas de estos respecto a la capacidad de los sistemas de la empresa de proporcionar el mismo nivel de funcionalidad, transportabilidad y facilidad de uso que los servicios de Internet. El secreto reside en lograr que los trabajadores del conocimiento obtengan la información que necesitan, protegida adecuadamente, para acceder únicamente a la información que les corresponde.

Una de las directrices fundamentales de la seguridad aplicada a la búsqueda general en las organizaciones reside en el cumplimiento con las políticas de seguridad empresarial subyacentes y los requisitos normativos. Asimismo, también resulta fundamental que la seguridad de la búsqueda sea compatible con los esquemas de seguridad de las diversas fuentes de contenido de la empresa. Para acometer la creación de un marco de seguridad, BearingPoint considera que es fundamental centrarse en la autenticación, autorización, auditoría y administración del acceso y la identidad.

AUTENTICACIÓN

La autenticación puede adoptar diversas formas y métodos. Tanto si está basada en directorios como en aplicaciones, los estándares más habituales de autenticación son el nombre de usuario y la contraseña. La inseguridad inherente a este método puede o no resultar un motivo de preocupación, dependiendo del entorno de la empresa. El reto que supone la búsqueda empresarial es lograr asociar un método de autenticación a los resultados de búsqueda solicitados. No toda la información se crea de la misma forma, así como tampoco todas las compañías aplican los mismos requisitos de seguridad a los controles de acceso a la información.

Una tecnología de autenticación estricta puede desempeñar un papel importante si se pone información confidencial a disposición de los usuarios. Un simple nombre de usuario y contraseña dejan de resultar aceptables como método de autenticación. Al mismo tiempo, la investigación de los usuarios, o la verificación de su identidad se ve limitada por los costes o porque no forma parte de la filosofía empresarial. Los certificados de infraestructura de clave pública (PKI, Public key infrastructure), la autenticación biométrica y de múltiples factores son herramientas que pueden resultar necesarias para superar esta resistencia corporativa.

Existen tres conceptos de nivel de autenticación básicos que se pueden ampliar para satisfacer las necesidades de una empresa determinada.

- **Nivel de autenticación 1:** se acepta y se considera suficiente que el usuario pueda acceder a su estación de trabajo con un nombre de usuario y una contraseña correctos.

EN ESTE PUNTO DE VISTA:

INTRODUCCIÓN: REQUISITOS DE SEGURIDAD PARA LAS SOLUCIONES DE BÚSQUEDA	1
AUTENTICACIÓN	1
La autenticación y el motor de búsqueda	2
AUTORIZACIÓN	2
La autorización y el motor de búsqueda	2
AUDITORÍA	3
La auditoría y el motor de búsqueda	3
ADMINISTRACIÓN DEL ACCESO Y LA IDENTIDAD	3
Administración del acceso y la identidad y el motor de búsqueda	4
CREACIÓN DE UN ENTORNO DE BÚSQUEDAS SEGURAS	4

- **Nivel de autenticación 2:** requiere acceso, bien manual o a través de inicio de sesión único (SSO), para cada uno de los vínculos que precise información confidencial adicional.
- **Nivel de autenticación 3:** uso de autenticación de dos o varios factores que emplea un certificado x509 multipropósito o datos biométricos para mostrar la información del certificado, convertir certificados a varios formularios, firmar solicitudes de certificado como una autoridad de certificación a pequeña escala o editar la configuración de fiabilidad del certificado.

La autenticación y el motor de búsqueda

De manera inmediata, una solución de búsqueda puede ser compatible con dos métodos de autenticación para el rastreo de contenido: autenticación básica/NTLM (NT LAN Manager) y autenticación basada en formularios. La autenticación básica/NTLM funciona en prácticamente todas las implementaciones de servidor web que son compatibles al menos con HTTP/1.0. Asimismo, también la admiten servidores basados en el sistema operativo (SO) Microsoft®. Por norma general, si las credenciales de un usuario residen en un SO Microsoft y utilizan NTLM, el motor de búsqueda podrá aprovecharlas.

La autenticación basada en formularios se implanta, habitualmente, en entornos web protegidos por el inicio de sesión único. Una de las actuales limitaciones de los motores de búsqueda es la posibilidad de utilizar a la vez únicamente un sistema SSO basado en formulario.

Una vez que el motor de búsqueda ha rastreado el contenido y un usuario desea realizar una búsqueda entre los resultados, el motor de búsqueda deberá publicar el contenido de un modo seguro. Los motores de búsqueda hacen uso de la autenticación básica/NTLM y basada en formularios mediante solicitudes HEAD de contenido basado en web a un servidor web.

Generalmente, el motor de búsqueda puede configurarse para que albergue contenido tanto público como protegido. Cuando el usuario trata de acceder a contenido que ha sido definido como protegido, aparece un cuadro de diálogo en la sesión del navegador para solicitar al usuario las credenciales necesarias. Este evento tiene lugar una vez por sesión.

En el caso de la autenticación basada en formularios, el motor de búsqueda puede utilizar tanto el reenvío de cookies como la suplantación absoluta del usuario. En ambos casos, el motor captura la información de acceso en una cookie y la reenvía a los sistemas que se están rastreando.

En el caso de implementaciones más complejas que utilicen contenido externo, serán necesarios adaptadores personalizados y API (interfaces de programación de aplicaciones). Los proveedores ofrecen interfaces de proveedor de servicios de autorización (SPI) que hacen posible que los servicios web comuniquen la SPI de autorización del motor de búsqueda con el servidor que proporciona los servicios de control de acceso.

AUTORIZACIÓN

El objetivo que se le plantea a la autorización es lograr un equilibrio de los derechos de los usuarios para que estos puedan realizar su trabajo. La búsqueda empresarial no es ajena a este reto.

Lograr la orientación de los datos o los resultados de búsqueda correctos dentro del ámbito de los derechos del usuario y la presentación exclusiva de esos datos continúa siendo un objetivo que hay que alcanzar. Directorios federados y certificados SSO y PKI son ejemplos de los servicios de autorización que se pueden utilizar para ayudar a la identificación de los usuarios y la validación de sus identidades.

A continuación, se ofrecen algunos ejemplos de los conceptos de nivel de autorización. No representan una lista exhaustiva de todas las opciones.

- **Nivel de autorización 1:** información pública interna accesible para todos y cuyo único requisito es disponer de acceso a la red para poder verla.
- **Nivel de autorización 2:** información confidencial que requiere un segundo registro a fin de poder consultarla.
- **Nivel de autorización 3:** información confidencial, como derechos de propiedad corporativos o información sobre nóminas, a la que únicamente pueden tener acceso grupos específicos.

La autorización y el motor de búsqueda

Las SPI de autorización permiten que los motores de búsqueda utilicen credenciales de usuario almacenadas fuera de los esquemas de autenticación NTLM típicos o autenticación basada en formularios de una fuente exclusiva. La implementación de una autorización SPI se basa en el estándar del lenguaje de marcas para condiciones de seguridad (SAML, security assertion markup language) 2.0 y está codificada con dicho estándar.

Cuando un usuario realiza una búsqueda y el motor de búsqueda debe determinar si puede publicar el resultado, éste pondrá en contacto el host de destino, o "conector de acceso", con la URL o destino en cuestión y la identidad del usuario.

En cada ocasión, cumpliendo con los estándares SAML 2.0, el host de destino permitirá, denegará u ofrecerá una respuesta indeterminada. El protocolo de acceso a objetos simples (SOAP, Simple object access protocol) sobre el protocolo de transferencia de hipertexto seguro (HTTPS) es lo que permite esta función. Sin embargo, se pueden producir retrasos en este proceso si el motor de búsqueda almacena en la memoria caché estos resultados durante la sesión. Es posible configurar los tiempos de la caché.

AUDITORÍA

Una implementación eficaz de cualquier solución de seguridad requiere la capacidad de efectuar auditorías.

Con una solución de búsqueda en toda la empresa, la auditoría se centra en los cambios. Si bien la mayoría de las organizaciones se centran en amenazas externas, las principales amenazas pueden proceder de la propia empresa. Una solución de búsqueda debe garantizar la seguridad de las búsquedas a la vez que, si resulta necesario, limitar por grupos la capacidad de búsqueda del usuario. La auditoría de acceso a la información, que sigue siendo importante, pasa ahora a un segundo plano tras los derechos del usuario.

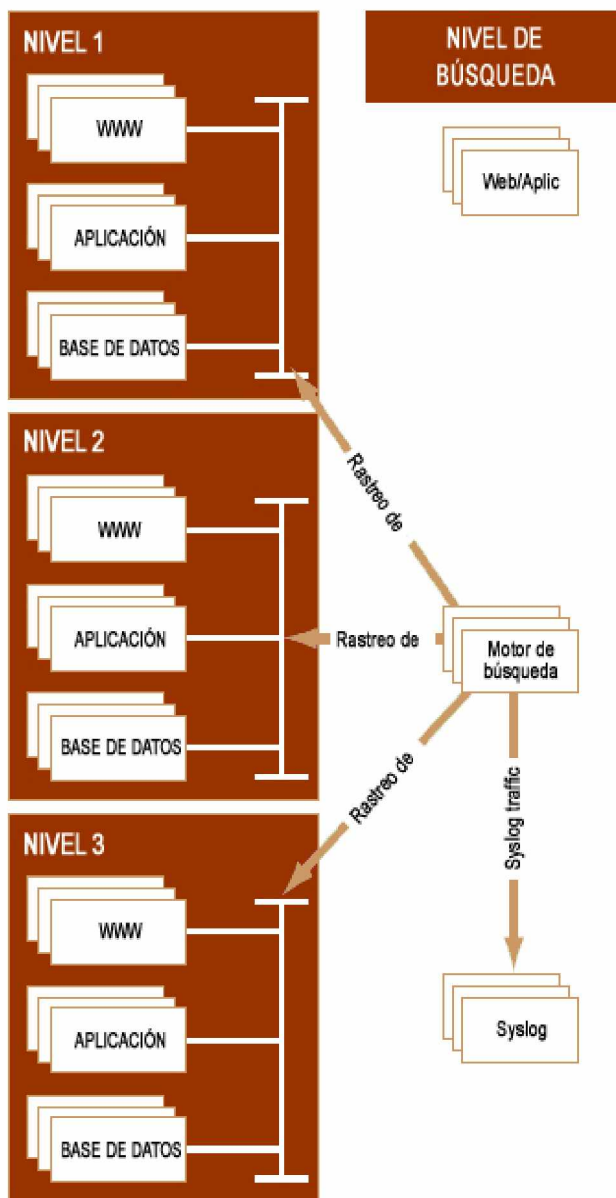
Al centrarse en los derechos del usuario, existe una mayor garantía respecto al hecho de que quienes necesitan la información realizan búsquedas seguras. Algunos puntos clave que hay que considerar son la presentación de derechos no autorizados; los movimientos, adiciones y cambios de usuario; los usuarios que acceden a información confidencial utilizando credenciales falsas y los que están en posesión de los derechos de que disfrutaban en situaciones anteriores, que les permiten acceder a información confidencial.

La auditoría y el motor de búsqueda

A fin de implementar funciones de auditoría en toda la empresa, es preciso implantar unos servicios de auditoría apropiados en la infraestructura existente. Se revisarán los sistemas a los que se puede acceder en la implantación de la búsqueda a fin de que la implementación de la auditoría resulte adecuada.

Los motores de búsqueda disponibles cuentan con una funcionalidad incorporada, que ofrece funciones de acceso a auditorías a través de un servidor syslog externo que es el que proporciona datos a un archivo de texto que se envía a un servidor syslog independiente. Es aconsejable la implantación de un servidor syslog dedicado para habilitar una funcionalidad de auditoría adecuada dentro del motor de búsqueda. De manera adicional, si los servidores de acceso a las auditorías y los mensajes no se capturan en los sistemas accesibles, será necesario implantar esta función. La Imagen 1 representa una implantación típica en la que el motor de búsqueda utiliza un servidor syslog independiente para recopilar los archivos de registro independientes creados por la actividad de búsqueda del usuario final.

Ilustración 1. Función de auditoría del motor de búsqueda



ADMINISTRACIÓN DEL ACCESO Y LA IDENTIDAD

Una solución de búsqueda puede plantear problemas de seguridad si no se han aplicado los controles pertinentes con anterioridad a la implementación. No obstante, se puede extraer algo positivo de ello. Dado que la información se rastrea y se presenta, resulta más fácil detectar los agujeros en la seguridad que existen desde hace tiempo o los almacenes de datos no protegidos y, por lo tanto, solucionarlos.

La autenticación, la autorización y la auditoría son las piezas fundamentales de la administración del acceso y la identidad. Otros aspectos importantes de una implementación bien estructurada son:

- **Configuración de contraseñas y políticas de caducidad.** Al utilizar un nombre de usuario y contraseña para acceder a información segura, resulta fundamental disponer de políticas de contraseña estrictas. Las contraseñas serán alfanuméricas, y se les asignará un período de operatividad en función de la información a la que otorguen acceso: cuanto mayor sea la confidencialidad de la información, mayor será la frecuencia de cambio de la contraseña.
- **Inicio de sesión único.** El inicio de sesión único (SSO) se puede emplear para combatir los costes de restablecer contraseñas para aquellas aplicaciones protegidas a las que se accede con poca asiduidad, ya que puede generar de manera automática contraseñas temporales. Esta función logra eliminar las contraseñas demasiado sencillas o vulnerables y evita que se compartan. Elimina también la necesidad de que el usuario se registre varias veces cuando acceda a datos seguros, proporcionando un entorno más seguro, lo que fomentará que la comunidad de usuarios haga uso de la búsqueda.
- **Separación de obligaciones (SoD).** La separación de roles sin generar gastos adicionales mediante un aumento de la plantilla puede suponer un equilibrio delicado. La SoD se ha diseñado para evitar que los usuarios lleven a cabo acciones potencialmente peligrosas. Salvo en las pequeñas empresas, una persona generalmente no disfruta de acceso a las cuentas a pagar y a las cuentas a cobrar. En un entorno de búsqueda empresarial, la persona que concede derechos de usuario no debe ser la misma que decide a qué colecciones tendrán acceso los usuarios.
- **Control de acceso basado en las funciones desempeñadas.** La ingeniería de funciones constituye una tarea de gran envergadura, pero que puede crear un entorno más seguro. La concesión de derechos se realiza de tres formas: explícita, implícita y heredada. Se pueden establecer normas para evitar la asignación de funciones conflictivas al mismo usuario y, por lo tanto, poner en práctica las políticas SoD que se han creado. La posibilidad de que los usuarios puedan filtrar una búsqueda con una función específica, incluso si disponen de varias, puede proporcionar datos más precisos y al mismo tiempo más seguros. El acceso basado en funciones está directamente vinculado a la SoD. Al atribuir funciones definidas a los usuarios, con normas que eviten la aparición de un conflicto de tareas, los resultados de búsqueda que se ofrezcan estarán directamente relacionados con las necesidades de cada usuario y con aquella información a la que tengan acceso.
- **Aprovisionamiento y desaprovisionamiento del usuario.** Se puede crear un entorno más seguro a través de modelos centralizados y delegados de administración de usuarios, flujos de trabajo, administración de contraseñas y control de acceso basado en funciones centralizadas y delegadas. El doble objetivo es asegurar que los nuevos usuarios disponen de acceso inmediato a la información que necesitan y cancelar lo antes posible el acceso a aquellos otros

que ya no gozan de autoridad para ello. Aunque no en relación directa con la búsqueda, un aprovisionamiento adecuado tiene un impacto directo en las funciones y la SoD. Se trata del punto de acceso a muchas iniciativas de seguridad.

Administración del acceso y la identidad y el motor de búsqueda Los motores de búsqueda están disponibles con soluciones líderes del mercado para la administración de la identidad, que utilizan autorización basada en formularios y que emplean un SPI de autorización.

Aún está por determinar el modo en que muchos motores de búsqueda se integrarán con sistemas heredados SSO no basados en la web y sistemas similares a SSO. Muchas organizaciones disponen de diversos sistemas de seguridad implantados de variadas formas: SSO basado en web, SSO interno, protocolo ligero de acceso a directorios (LDAP, lightweight directory access protocol) y otros depósitos de nombre de usuario/contraseña.

Dado que los requisitos de la solución de búsqueda son exclusivos de cada empresa, es fundamental establecer el alcance de la implantación. Se puede utilizar una combinación de tecnologías, incluido un SPI de autorización, API, adaptadores personalizados y mecanismos de autenticación basados en formularios del motor de búsqueda.

CREACIÓN DE UN ENTORNO DE BÚSQUEDA SEGURO

La implantación de soluciones de búsqueda para empresas sugiere nuevas consideraciones respecto a la seguridad. Si las organizaciones tratan de solucionarlas desde su aparición mediante un enfoque de seguridad exhaustivo, podrán obtener beneficios de las ventajas que ofrecen las soluciones de búsqueda a la vez que protegerán la información confidencial.

Si desea obtener más información sobre la forma en que nuestras soluciones pueden aportar valor añadido a su empresa, [hablemos](#).

ADMINISTRACIÓN GLOBAL Y CONSULTORÍA DE TECNOLOGÍA PARA EL CONTEXTO EMPRESARIAL ACTUAL

BearingPoint es un proveedor líder en servicios de consultoría tecnológica y gestión global para las compañías Global 2000 y muchas de las compañías de servicios públicos más importantes del mundo. Nuestros expertos ayudan a las empresas de todo el mundo a prepararse para conseguir sus objetivos y crear valor empresarial. Al adaptar sus procesos empresariales a los sistemas de información, les ayudamos a adquirir una ventaja competitiva y a obtener resultados rápidamente. Para obtener más información, póngase en contacto con nosotros en el número 1.866.661.FIND (+1.603.589.4089 si llama desde fuera de Estados Unidos y Canadá) o visite nuestro sitio web en www.bearingpoint.com.

BearingPoint proporciona servicios de consultoría estratégica, servicios de aplicaciones, soluciones tecnológicas y servicios de gestión a las empresas Global 2000 y a entidades gubernamentales.



Bearing Point
1676 International Drive
McLean, VA 22102
www.bearingpoint.com