Solutions de recherche pour les entreprises

Sécurité et déploiement de solutions de recherche

BearingPoint
Management & Technology Consultants

Une solution de recherche pour les entreprises permet d'améliorer la productivité organisationnelle en facilitant l'accès aux données.

INTRODUCTION : L'IMPÉRATIF DE SÉCURITÉ POUR LES SOLUTIONS DE RECHERCHE

Une solution de recherche pour l'entreprise bien déployée peut mettre de grandes quantités d'informations à la portée des responsables de l'information et des autres employés d'une entreprise, permettant ainsi de répondre à l'aspiration croissante des professionnels de voir les systèmes d'entreprise offrir le même niveau de fonctionnalité, de transportabilité et de facilité d'utilisation que les services Internet. Le défi consiste à permettre aux responsables de l'information d'accéder aux données dont ils ont besoin, tout en s'assurant qu'ils ne peuvent consulter que celles auxquelles ils sont autorisées à accéder.

Le principe directeur de la sécurité dans le domaine de la recherche en entreprise est la conformité avec les règles de sécurité fondamentales de l'entreprise. Il est également important que la sécurité liée à la recherche soit compatible avec les schémas de sécurité associés aux diverses sources de contenu au sein de l'entreprise. Pour créer un cadre de sécurité, BearingPoint pense qu'une attention particulière doit être portée aux aspects d'authentification, d'autorisation, d'audit et de gestion de l'identité et des accès.

AUTHENTIFICATION

L'authentification peut être réalisée sous différentes formes et selon diverses méthodes. Le principe le plus courant de l'authentification, que celle-ci soit basée sur un annuaire ou sur une application, est l'utilisation d'un nom d'utilisateur et d'un mot de passe. Les risques d'insécurité inhérents à ces méthodes peuvent éventuellement constituer un problème selon l'environnement de l'entreprise. Le défi à relever pour la recherche en entreprise est d'associer la méthode ou la forme appropriée d'authentification aux résultats de recherche requis. De même que toutes les informations ne sont pas de nature équivalentes, toutes les sociétés n'ont pas les mêmes exigences de sécurité en matière de contrôle de l'accès aux données.

Lorsque le volume de données sensibles accessibles aux utilisateurs augmente, une procédure d'authentification plus exigeante peut jouer un rôle important.
L'authentification par simple nom d'utilisateur et mot de passe peut être insuffisante dans certains cas. Parallèlement, la validation des utilisateurs, ou le contrôle effectif de leur identité, peut être impossible pour des raisons de coût ou de philosophie de l'entreprise. Ce problème peut être résolu par l'utilisation de certificats PKI (public key infrastructure), de la biométrie ou de l'authentification multifacteur.

On peut distinguer trois niveaux d'authentification principaux permettant de répondre aux besoins de sécurité d'une société :

- **Niveau d'authentification 1** : la possibilité pour l'utilisateur de se connecter à son poste de travail avec un nom d'utilisateur et un mot de passe corrects est considérée comme une sécurité suffisante.

DANS CE POINT DE VUE :

- **Niveau d'authentification 2** : un nom d'utilisateur et un mot de passe de connexion doivent être entrés, manuellement ou via la fonction d'authentification unique (SSO), pour chaque lien vers des données plus sensibles.
- **Niveau d'authentification 3** : recours à l'authentification multifacteur ou bifacteur qui utilise un certificat multifonction x509 ou la biométrie pour afficher les informations de certificat, convertir les certificats sous différentes formes, signer des demandes de certificat comme une mini-autorité de certification ou modifier des paramètres de certificats de confiance.

Authentification et moteur de recherche

Dans sa version standard, une solution de recherche peut prendre en charge deux méthodes d'authentification pour l'exploration de contenu : l'authentification de base/NTLM (NT LAN Manager) et l'authentification par formulaire. L'authentification de base/NTLM fonctionne sur la quasi-totalité des implémentations de serveur Web qui prennent en charge au minimum HTTP/1.0. Elle est également prise en charge par les serveurs utilisant le système d'exploitation Microsoft®. En termes généraux, cela signifie que si un ensemble d'informations d'authentification d'utilisateur réside sur un système d'exploitation Microsoft et utilise NTLM, le moteur de recherche peut exploiter ces informations.

L'authentification par formulaire est généralement déployée dans les environnements SSO Web. L'une des limites actuelles des moteurs de recherche est qu'ils ne peuvent exploiter qu'un seul système SSO par formulaire à la fois.

Lorsque le moteur de recherche a exploré le contenu et qu'un utilisateur souhaite rechercher les résultats, le moteur de recherche doit proposer le contenu de manière sécurisée. Les moteurs de recherche exploitent l'authentification de base/NTLM et l'authentification par formulaire par le biais de requêtes HEAD envoyées à un serveur Web pour le contenu Web.

Le moteur de recherche peut généralement être configuré pour héberger à la fois du contenu public et du contenu sécurisé. Lorsque l'utilisateur tente d'accéder à du contenu qui a été défini comme sécurisé, une boîte de dialogue apparaît dans la session du navigateur en invitant l'utilisateur à fournir les informations d'authentification requises. Cela se produit une seule fois par session.

Dans le cas de l'authentification par formulaire, le moteur de recherche peut utiliser soit la transmission de cookies, soit l'emprunt d'identité utilisateur complète. Dans les deux cas, le moteur enregistre les informations de connexion dans un cookie et les transmet aux systèmes explorés.

Pour des implémentations plus complexes utilisant du contenu externe, des adaptateurs personnalisés et des interfaces de programmation d'application (API) sont requis. Les fournisseurs offrent des interfaces SPI (service provider interfaces) d'autorisation qui permettent aux services Web d'effectuer le transfert entre la SPI d'autorisation du moteur de recherche et le serveur qui fournit les services de contrôle d'accès.

AUTORISATION

Le défi à relever dans le domaine de l'autorisation consiste à équilibrer les droits des utilisateurs de manière qu'ils puissent accomplir leurs tâches. La recherche en entreprise n'échappe pas à cette règle.

La mise en correspondance des données ou des résultats de recherche appropriés tout en tenant compte des droits des utilisateurs, puis la présentation de ces seules données restent un défi. Les annuaires fédérés et les certificats SSO et PKI sont des exemples de services d'autorisation qui peuvent être utilisés pour identifier les utilisateurs et valider leur identité.

Des exemples de niveaux d'autorisation sont fournis ci-dessous. Ces exemples ne représentent pas la liste complète des options.

- **Niveau d'autorisation 1** : informations publiques internes accessibles à tous et pouvant être consultées par toute personne possédant un accès réseau.
- **Niveau d'autorisation 2** : informations confidentielles consultables uniquement avec une connexion secondaire.
- **Niveau d'autorisation 3** : données sensibles, telles que des informations sur la propriété intellectuelle de l'entreprise ou sur la paie, auxquelles seuls des groupes spécifiques ont accès.

Autorisation et moteur de recherche

Les SPI d'autorisation permettent aux moteurs de recherche d'exploiter les données d'authentification d'utilisateur stockées en dehors des schémas d'authentification NTLM type ou de l'authentification par formulaire pour une source unique. L'implémentation d'une SPI d'autorisation repose sur la norme SAML (security assertion markup language) 2.0 et elle est codée selon cette norme.

Lorsqu'un utilisateur effectue une recherche et que le moteur de recherche doit déterminer s'il peut fournir ce résultat, ce dernier contacte l'hôte cible ou le "connecteur d'accès", avec l'URL ou la cible en question et l'identité de l'utilisateur.

À chaque fois, en conformité avec les normes SAML 2.0, l'hôte cible donne une réponse d'autorisation, de refus ou d'absence de détermination. Le protocole SOAP (simple object access protocol) sur le protocole HTTPS (hypertext transfer protocol secure) autorise cette fonctionnalité. Toutefois, des délais peuvent en résulter, car le moteur de recherche place ces résultats en mémoire cache durant la session. Le délai de mise en mémoire cache est configurable.

AUDIT

La mise en place effective d'une solution de sécurité requiert la possibilité de réaliser un audit.

Dans le cadre de la recherche en entreprise, la cible de l'audit change. Alors que la plupart des organisations s'intéressent essentiellement aux menaces externes, il apparaît que les menaces internes peuvent être plus préoccupantes. Une solution de recherche doit garantir des recherches sécurisées tout en limitant les recherches utilisateur à des collections si nécessaire. L'audit de l'accès aux données, bien qu'il soit important, devient secondaire par rapport à l'audit des droits d'utilisateur.

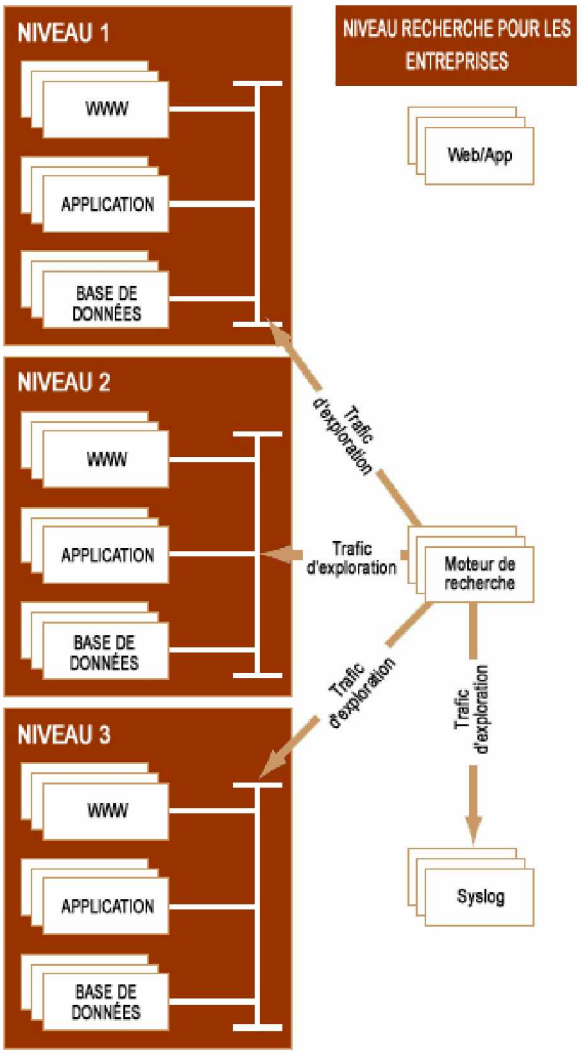
En effet, celui-ci permet d'assurer que les personnes qui ont besoin d'informations peuvent effectuer des recherches dans un environnement sécurisé. Les points clés à surveiller comprennent l'élévation non autorisée des droits, les déplacements, ajouts et modification d'utilisateurs, l'accès d'utilisateurs aux données avec de fausses informations d'authentification, les utilisateurs conservant des droits associés à des fonctions précédentes et pouvant accéder ainsi à des données sensibles.

Audit et moteur de recherche

Pour mettre en œuvre des fonctions d'audit dans une entreprise, il est nécessaire de déployer les services d'audit appropriés sur l'infrastructure existante. En particulier, les systèmes concernés par le déploiement de la recherche doivent être vérifiés pour garantir une mise en œuvre correcte de l'audit.

Les moteurs de recherche disponibles intègrent des fonctions de journalisation de l'audit via un serveur syslog externe, qui fournit une sortie dans un fichier texte qui est ensuite envoyé à un serveur syslog distinct. Il est recommandé de déployer un serveur syslog dédié pour assurer une fonction d'audit appropriée au sein du moteur de recherche. De plus, si les serveurs et les messages de journalisation d'audit ne sont pas enregistrés sur les systèmes accessibles, cette fonctionnalité doit être mise en place. La figure 1 représente un déploiement type dans lequel le moteur de recherche utilise un serveur syslog séparé pour collecter les fichiers journaux créés par l'activité de recherche de l'utilisateur.

Figure 1. Fonctionnalité d'audit du moteur de recherche



GESTION DE L'IDENTITÉ ET DES ACCÈS

Une solution de recherche peut réellement créer des problèmes de sécurité si les contrôles appropriés n'ont pas été mis en place avant son implémentation. Mais cela peut également avoir des retombées positives. À mesure de l'exploration et de la présentation des données, des failles durables dans les systèmes de sécurité ou des zones de stocakge de données non protégées peuvent être mises à jour, puis résolues.

L'authentification, l'autorisation et l'audit sont des éléments clés de la gestion de l'identité et des accès. Voici d'autres aspects importants permettant une approche maîtrisée :

- **Règles de configuration et d'expiration des mots de passe :** Le nom d'utilisateur et le mot de passe étant la clé permettant d'accéder aux données sécurisée, il est essentiel de définir des règles strictes concernant le mot de passe. Les mots de passe doivent être alphanumériques et leur date d'expiration doit être définie en fonction des données consultées ; plus les données sont sensibles, plus le mot de passe doit être fréquemment changé.
- **Connexion unique :** La connexion unique (SSO, single sign-on) peut être utilisée pour limiter les coûts liés à la redéfinition de mots de passe utilisateur pour des applications utilisées de manière irrégulière mais sécurisée, car elle peut générer automatiquement des mots de passe avec date d'expiration. Cette fonctionnalité peut éliminer les mots de passe souples ou simples et éviter l'échange des mots de passe. Elle évite de devoir se connecter plusieurs fois pour accéder à des données sécurisées, encourageant ainsi les utilisateurs à utiliser la fonction de recherche, tout en maintenant un environnement plus sécurisé.
- **Séparation des tâches et des fonctions (SoD) :** Séparer les différentes des fonctions sans avoir à engager de dépenses supplémentaires du fait des besoins plus importants en personnel peut être difficile à réaliser. Le système SoD est conçu pour empêcher les utilisateurs d'effectuer des actions potentiellement dangereuses. Excepté dans les petites entreprises, une même personne ne peut généralement pas accéder à la fois aux comptes fournisseurs et aux comptes clients. Dans un environnement de recherche en entreprise, la personne octroyant les droits d'utilisateur ne doit pas être la même que celle qui détermine les collections auxquelles les utilisateurs ont accès.
- **Contrôle des accès basé sur les rôles :** Ce type d'ingénierie est assez complexe à réaliser mais contribue à créer un environnement plus sûr. Les droits sont accordés de trois manières : explicite, implicite et héritée. Des règles peuvent être définies pour éviter d'affecter plusieurs rôles incompatibles au même utilisateur, mettant ainsi en œuvre les règles SoD créées. La possibilité pour les utilisateurs de filtrer une recherche en fonction d'un rôle spécifique, même s'ils ont plusieurs rôles, leur permet d'obtenir des résultats plus adaptés mais également sécurisés. Le contrôle d'accès basé sur les rôles est directement lié au système SoD. Si les utilisateurs ont des rôles définis, avec des règles évitant les conflits, les résultats de recherche seront directement adaptés aux besoins de l'utilisateur et aux types d'informations auxquels il a accès.
- **Administration du cycle de vie des utilisateurs :** Un environnement plus sûr peut être créé grâce à une gestion centralisée et déléguée des utilisateurs, des flux de travail, des modèles de contrôle de l'accès basé sur les rôles et de gestion des mots de passe. Le double objectif à atteindre est d'assurer que les nouveaux utilisateurs peuvent immédiatement accéder aux informations dont ils ont besoin et de retirer les droits d'accès dans les meilleurs délais aux utilisateurs qui ne sont plus autorisés à consulter certaines informations. Bien qu'elle ne soit pas directement liée à la recherche, la mise à disposition des services a un impact direct sur les rôles et le système SoD. C'est le point de départ pour un grand nombre d'initiatives de sécurité.

Gestion de l'identité et des accès et moteur de recherche

Certains moteurs de recherche intègrent des solutions de gestion de l'identité avancées en utilisant l'authentification par formulaire et en exploitant une SPI d'autorisation.

Il reste à déterminer le nombre de moteurs de recherche qui s'intègreront à d'anciens systèmes SSO pour applications non Web et de type SSO. Un grand nombre de sociétés utilisent plusieurs systèmes de sécurité déployés sous différentes formes : SSO pour le Web, SSO interne, protocole LDAP (lightweight directory access protocol) et autres référentiels de noms d'utilisateur/mots de passe. Les exigences liées aux solutions de recherche étant propres à chaque entreprise, il est impératif de définir correctement l'étendue du déploiement. Il est possible d'utiliser une combinaison de diverses technologies, incluant une SPI d'autorisation, des API et des adaptateurs personnalisés ainsi que le mécanisme d'authentification par formulaire du moteur de recherche.

CRÉATION D'UN ENVIRONNEMENT DE RECHERCHE SÉCURISÉ

Le déploiement de solutions de recherche pour l'entreprise soulève de nouveaux problèmes de sécurité. En relevant ce défi dès le départ grâce à une approche complète de la sécurité, les entreprises peuvent bénéficier des avantages offerts par les solutions de recherche tout en assurant la protection des informations sensibles.

Pour en savoir plus sur la manière dont votre entreprise peut tirer parti de nos solutions, contactez-nous.

CONSEIL EN GESTION GLOBALE ET EN TECHNOLOGIE POUR LES ENTREPRISES D'AUJOURD'HUI

BearingPoint est une société internationale de conseil, leader en matière de technologie et de gestion, qui travaille avec les sociétés Global 2000 et plusieurs grandes sociétés de services publics dans le monde. Nos experts aident les entreprises du monde entier à définir une direction dans le but d'atteindre leurs objectifs et de créer de la valeur. En alignant leurs processus métier et leurs systèmes d'information, nous aidons nos clients à se positionner en leader face à la concurrence, grâce à des résultats rapides. Pour en savoir plus, contactez-nous au 1.866.661.FIND (+1.603.589.4089 en dehors des États-Unis et du Canada) ou visitez notre site Web à l'adresse www.bearingpoint.com.

BearingPoint propose des conseils stratégiques, des services d'application, des solutions technologiques et des services gérés aux sociétés Global 2000 et aux organisations gouvernementales.

BearingPoint
1676 International Drive
McLean, VA 22102
www.bearingpoint.com