Zoekoplossingen voor de onderneming

Beveiligingsoverwegingen bij de implementatie van zoekoplossingen

BearingPoint
Management & Technology Consultants

Zoekoplossingen voor het bedrijf kunnen een stimulans zijn voor de bedrijfsproductiviteit doordat nuttige informatie direct en gemakkelijk beschikbaar wordt gemaakt voor mensen op het moment dat ze die nodig hebben.

INLEIDING: DE BEVEILIGINGSVEREISTEN VOOR ZOEKOPLOSSINGEN

Door een goed geïmplementeerde zoekoplossing voor de onderneming hebben kenniswerkers en andere medewerkers binnen een bedrijf een schat aan informatie voor het grijpen — waardoor tegemoet wordt gekomen aan de toenemende behoefte van werknemers dat bedrijfssystemen hetzelfde niveau van functionaliteit, overdraagbaarheid en gebruiksgemak bieden als Internetservices. De truc is ervoor te zorgen dat kenniswerkers met de juiste beveiliging de informatie krijgen die ze nodig hebben, waarbij ze uitsluitend die informatie kunnen ophalen waarvoor zij de toegangsrechten hebben.

Een leidraad voor de beveiliging van bedrijfszoekoplossingen is dat die voldoen aan het onderliggende beveiligingsbeleid en de reglementen van de onderneming. Daarnaast is het van belang dat de zoekbeveiliging compatibel is met de beveiligingsschema's van de diverse inhoudsbronnen binnen de onderneming. BearingPoint is van mening dat bij het creëren van een beveiligingsstructuur veel aandacht moet worden besteed aan verificatie, autorisatie, controle en identiteits- en toegangsbeheer.

VERIFICATIE

Er bestaan allerlei vormen en methoden van verificatie. De algemene verificatiestandaard is een gebruikersnaam en een wachtwoord, zowel bij directory-gerichte als bij toepassingsgerichte verificatie. Het inherente beveiligingsrisico bij deze methode kan, afhankelijk van de bedrijfsomgeving, mogelijk problemen opleveren. De uitdaging van een zoekoplossing voor de onderneming is het koppelen van de juiste methode of vorm van verificatie aan de opgevraagde zoekresultaten. Niet alle informatie wordt op dezelfde wijze gemaakt en evenmin hebben alle ondernemingen dezelfde beveiligingsvereisten voor gegevenstoegangscontrole.

Naarmate er meer gevoelige gegevens beschikbaar komen voor gebruikers, wordt een krachtige verificatiemethode steeds belangrijker. De eenvoudige methode van gebruikersnaam en wachtwoord is mogelijk niet langer afdoende als verificatiemethode. Anderzijds is het compleet doorlichten van gebruikers om hun identiteit te achterhalen wellicht te duur of niet passend in de bedrijfsfilosofie. PKI (public key infrastructure) certificaten, biometrische verificatie en meervoudige (multifactor) verificatie kunnen dan eventueel uitkomst bieden.

Er bestaan drie eenvoudige verificatieniveau-concepten die kunnen worden aangepast aan de bedrijfsbehoeften.

- **Verificatieniveau 1**—Het opgeven van de juiste gebruikersnaam en het correcte wachtwoord is voldoende voor een werknemer om zich aan te melden bij zijn werkstation.

IN DIT PERSPECTIEF:

INLEIDING: DE BEVEILIGINGSVEREISTEN VOOR ZOEKOPLOSSINGEN 1
VERIFICATIE 1
Verificatie en de zoekmachine 2
AUTORISATIE 2
Autorisatie en de zoekmachine 2
CONTROLE 3
Controle en de zoekmachine 3
IDENTITEIT- EN TOEGANGSBEHEER 3
Identiteit- en toegangsbeheer en de zoekmachine 4
EEN BEVEILIGDE ZOEKOMGEVING MAKEN 4

- **Verificatieniveau 2** — Aanmelding vereist, ofwel handmatig of via single sign-on (SSO), bij iedere link die gevoelige gegevens vereist.
- **Verificatieniveau 3** — Gebruik van multi- of two-factor-verificatie, waarbij gebruik wordt gemaakt van een x509-certificaat of biometrische kenmerken voor het weergeven van certificaatgegevens, het converteren van certificaten naar verschillende formulieren, het ondertekenen van certificaatverzoeken, zoals een mini-certificaatautoriteit, of het bewerken van de betrouwbaarheidsinstellingen van het certificaat.

Verificatie en de zoekmachine

Een zoekoplossing ondersteunt standaard mogelijk twee verificatiemethoden voor het doorzoeken van inhoud: NTLM (NT LAN Manager)-basisverificatie en formulierverificatie. NTLM-basisverificatie werkt in vrijwel alle webserverimplementaties die minimaal HTTP/1.0 ondersteunen. Deze vorm van verificatie wordt ook ondersteund door servers die zijn gebaseerd op het Microsoft® besturingssysteem (OS). Doorgaans kan de zoekmachine de gebruikersgegevensset gebruiken als deze zich in een Microsoft-besturingssysteem bevindt en NTLM gebruikt.

Formulierverificatie wordt meestal gebruikt in online SSO-omgevingen. Een beperking van de huidige zoekmachines is dat zij slechts één SSO-formuliersysteem per keer kunnen gebruiken.

Als een gebruiker de zoekresultaten wil doorzoeken nadat de zoekmachine inhoud heeft doorzocht, moet de inhoud wel beveiligd worden gepresenteerd. Zoekmachines maken voor webinhoud gebruik van NTLM-basisverificatie en formulierverificatie via HEAD-verzoeken aan een webserver.

De zoekmachine kan worden geconfigureerd voor hosting van zowel openbare als beveiligde inhoud. Waneer een gebruiker probeert toegang te verkrijgen tot beveiligde inhoud, wordt tijdens de browsersessie een dialoogvenster weergegeven, waarin de gebruiker wordt gevraagd zijn gebruikersgegevens op te geven. Dit vindt eenmaal per sessie plaats.

In het geval van formulierverificatie, kan de zoekmachine gebruik maken van het doorsturen van cookies of van volledige gebruikernabootsing. In beide gevallen legt de zoekmachine de aanmeldingsgegevens vast in een cookie en stuurt deze door naar de systemen die worden doorzocht.

Voor ingewikkelde implementaties, waarbij gebruik wordt gemaakt van externe inhoud, zijn aangepaste adapters en API's (application programming interfaces) vereist. Er zijn autorisatie SPI's (service provider interfaces) op de markt, waarmee webservices de communicatie kunnen regelen tussen de autorisatie-SPI van de zoekmachine en de server die de toegangscontroleservices levert.

AUTORISATIE

Bijautorisatie gaat het e rom dat er juist wordt ingespeeld op de toegangsrechten van de gebruikers, zodat zij hun werk kunnen doen. Een bedrijfszoekoplossing vormt hierop geen uitzondering.

Op basis van de gebruikersrechten de juiste gegevens of zoekresultaten toewijzen en vervolgens uitsluitend die gegevens presenteren, blijft een hele uitdaging. Federatieve directory's en SSO- en PKI-certificaten zijn voorbeelden van autorisatieservices die kunnen helpen bij het identificeren van gebruikers en het valideren van hun identiteit.

Hieronder vindt u voorbeelden van autorisatieniveau-concepten. De lijst is overigens niet volledig:

- **Autorisatieniveau 1** — Interne, openbare informatie die voor iedereen toegankelijk is en die ter inzage niets meer vereist dan netwerktoegang.
- **Autorisatienivau 2** — Vertrouwelijke informatie die een tweede aanmelding vereist om te kunnen worden bekeken.
- **Autorisatieniveau 3** — Gevoelige gegevens, zoals het intellectuele eigendom van een onderneming of salarisgegevens, waartoe slechts bepaalde groepen toegang hebben.

Autorisatie en de zoekmachine

Autorisatie-SPI's stellen zoekmachines in staat gebruikersgegevens te gebruiken die buiten de gebruikelijke NTLM-verificatieschema's zijn opgeslagen, of one-source-only formulierverificatie. Implementatie van een autorisatie-SPI steunt op de SAML 2.0-standaard als basis en wordt met deze standaard gecodeerd.

Wanneer een gebruiker een zoekopdracht uitvoert en de zoekmachine moet bepalen of het resultaat kan worden gepresenteerd, neemt de zoekmachine met behulp van de URL van de betreffende bestemming en de identiteit van de gebruiker eerst contact op met de bestemmingshost, of 'toegangsconnector'.

De bestemmingshost zal vervolgens op grond van SAML 2.0-standaards toestemming verlenen, toestemming weigeren of antwoorden dat de toestemming onbepaalbaar is. SOAP (Simple object access protocol) via HTTPS (hypertext transfer protocol secure) maakt deze functie mogelijk. Er kan echter vertraging optreden, omdat de zoekmachine deze resultaten tijdens de sessie in een cache-geheugen opslaat. Cache-tijd kan worden geconfigureerd.

CONTROLE

Effectieve implementatie van een beveiligingsoplossing vereist de mogelijkheid van controle.

Bij zoekoplossingen voor de onderneming verschuift de focus van de controle. Ofschoon de meeste bedrijven zich concentreren op externe bedreigingen, is de bedreiging van binnen het bedrijf mogelijk veel groter. Een zoekoplossing moet garant staan voor beveiligd zoeken, waarbij zoekopdrachten van gebruikers in collecties eventueel beperkt moet kunnen worden. Gegevenstoegangscontrole is nog altijd belangrijk, maar wordt ondergeschikt aan gebruikersrechten.

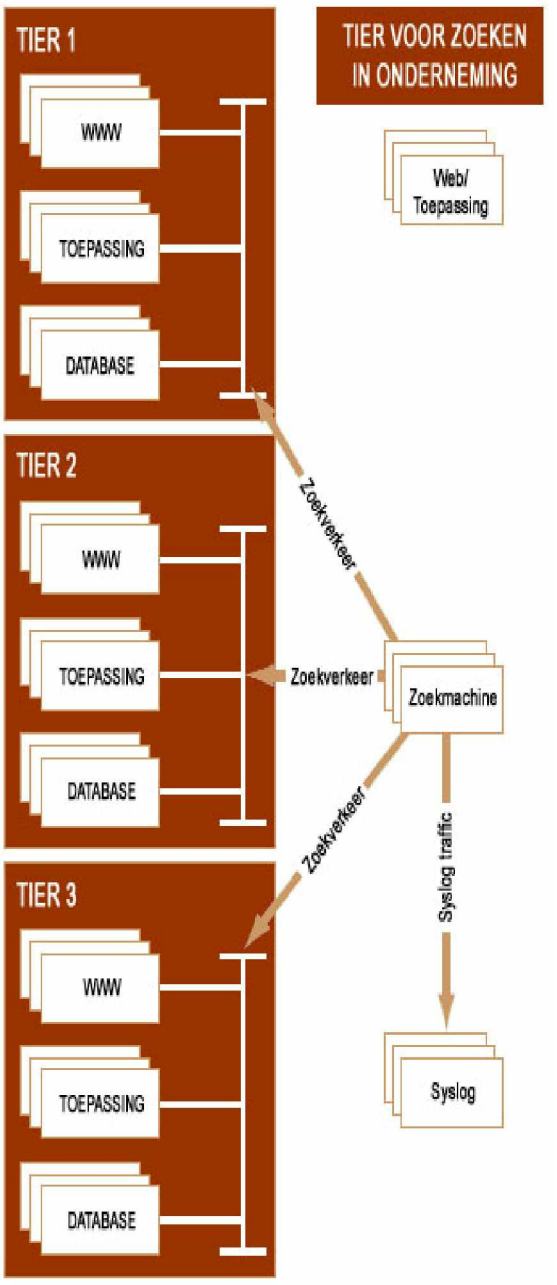
Door de nadruk te leggen op gebruikersrechten, wordt meer garantie geboden dat de mensen die op zoek zijn naar informatie beveiligde zoekopdrachten zullen uitvoeren. Belangrijke aandachtspunten zijn niet-geautoriseerde uitbreiding van toegangsrechten; verplaatsingen, toevoegingen en wijzigingen van gebruikers; gebruikers die met valse gebruikersgegevens zich toegang verschaffen tot gevoelige gegevens en gebruikers die gebruik maken van toegangsrechten op grond van eerdere functies om zich toegang te verschaffen tot gevoelige gegevens.

Controle en de zoekmachine

Om controlefuncties binnen de onderneming te implementeren, moeten passende controleservices binnen de bestaande infrastructuur worden geïmplementeerd. De systemen die doorzocht gaan worden, moeten vooraf worden beoordeeld op de mogelijkheid van een goede controle-implementatie.

De beschikbare zoekmachines hebben ingebouwde functionaliteit voor audit-logging via een externe syslogserver, waarbij een tekstbestand naar een afzonderlijke syslogserver wordt verstuurd. Implementatie van een speciale syslogserver, die een goede controlefunctionaliteit binnen de zoekmachine mogelijk maakt, wordt aanbevolen. Als audit-logging-servers en berichten niet worden vastgelegd op de toegankelijke systemen, moet deze functionaliteit worden geïmplementeerd. In afbeelding 1 wordt een gebruikelijke implementatie weergegeven, waarin de zoekmachine gebruik maakt van een aparte syslogserver voor het verzamelen van logboekbestanden die zijn aangemaakt als gevolg van zoekactiviteiten van eindgebruikers.

Afbeelding 1. Controlefunctie van zoekmachine



IDENTITEIT- EN TOEGANGSBEHEER

Een zoekoplossing kan beveiligingsproblemen veroorzaken wanneer de juiste controlefuncties niet vóór de implementatie werden geïntegreerd. Maar daar zit mogelijk ook een positieve kant aan. Bij het doorzoeken en presenteren van gegevens kunnen oude beveiligingsgaten en onbeveiligde gegevensopslagplaatsen aan het licht komen, die vervolgens kunnen worden gerepareerd.

Verificatie, autorisatie en controle vervullen een cruciale rol bij identiteit- en toegangsbeheer. Andere belangrijke aspecten van een afgewogen benadering zijn:

- **Wachtwoordconfiguratie en geldigheidsbeleid.** Wanneer een gebruikersnaam en een wachtwoord worden gebruikt voor toegang tot beveiligde gegevens, is een krachtig wachtwoordbeleid van cruciaal belang. Wachtwoorden moeten alfanumeriek zijn en geldend blijven op basis van de gegevens waartoe toegang wordt verleend —hoe gevoeliger de gegevens, des te vaker wordt het wachtwoord gewijzigd.
- **Eenmalige aanmelding (single sign-on).** SSO kan worden gebruikt ter bestrijding van de kosten van het resetten van gebruikerswachtwoorden voor weinig gebruikte, maar beveiligde toepassingen, omdat hiermee verlopen wachtwoorden automatisch kunnen worden gegenereerd. Met deze functie kunnen gemakkelijke of te eenvoudige wachtwoorden worden geëlimineerd en worden voorkomen dat wachtwoorden worden doorgegeven aan anderen. Ze kan de noodzaak voor de gebruiker wegnemen zich meerdere keren te moeten aanmelden om toegang te krijgen tot beveiligde gegevens, waardoor een veiliger omgeving wordt gecreëerd en de gebruikers worden aangemoedigd de zoekfunctie te gebruiken.
- **Scheiding van taken (SoD).** Scheiding van taken zonder dat daardoor extra overheadkosten ontstaan door meer personeel, is niet altijd even gemakkelijk. SoD is ontworpen om te voorkomen dat gebruikers potentieel gevaarlijke acties uitvoeren. Behalve in kleine ondernemingen, heeft niet een en dezelfde persoon gewoonlijk toegang tot zowel de debiteurenadministratie als de crediteurenadministratie. In een bedrijfszoekomgeving moet de persoon die de gebruikersrechten verleent niet dezelfde zijn als de persoon die beslist tot welke collecties gebruikers toegang hebben.
- **Functiegerichte toegangscontrole.** Functie-engineering is geen simpele taak , maar er kan een veiliger omgeving door worden gecreëerd. Rechten worden op drie manieren verleend — expliciet, impliciet en overgenomen. Er kunnen regels worden opgesteld die, door het gemaakte SoD-beleid in werking te stellen, voorkomen dat conflicterende functies aan dezelfde gebruiker worden toegekend. De mogelijkheid van gebruikers om een zoekopdracht middels een specifieke functie te filteren, zelfs al beschikken zij over meerdere functies, kan leiden tot schonere en nog altijd beveiligde resultaten. Functiegerichte toegang is direct gekoppeld aan SoD. Door gebruikers een specifieke functie te geven, met regels om te voorkomen dat taken conflicteren, zullen de gepresenteerde resultaten relevant zijn voor hun zoekopdracht en in overeenstemming met hun toegangsrechten.
- **Gebruiker-provisioning/de-provisioning.** Door gecentraliseerd en gedelegeerd gebruikersbeheer, workflows, wachtwoordbeheer en functiegerichte toegangscontrolemodellen kan een veiliger omgeving worden gecreëerd. Een tweeledig doel is ervoor te zorgen dat nieuwe gebruikers directe toegang hebben tot de benodigde informatie en dat andere gebruikers die niet langer bevoegdheid hebben zo snel mogelijk de toegang wordt ontzegd. Hoewel niet direct verbonden met zoeken, heeft het juiste provisioning een direct effect op functies en SoD. Dit is het startpunt van veel beveiligingsinitiatieven.

Identiteits- en toegangsbeheer en de zoekmachine

Er zijn zoekmachines beschikbaar met toonaangevende beheeroplossingen, waarbij gebruik gemaakt wordt formulierverificatie en een autorisatie-SPI.

Wat nog moet worden vastgesteld, is hoeveel zoekmachines integreren met niet-online SSO- en SSO-achtige legacy-systemen. Veel bedrijven hebben meerdere beveiligingssystemen geïmplementeerd in verschillende vormen — online SSO, interne SSO, LDAP (lightweight directory access protocol) en andere gebruikersnaam/wachtwoord-opslagplaatsen. Aangezien voor ieder bedrijf de beveiligingsvereisten weer anders zijn, is de juiste omvang van de implementatie essentieel. Mogelijk wordt een mengeling van technologieën gebruikt, waaronder een autorisatie-SPI, aangepaste API's en adapters en het zoekmachine-mechanisme formulierverificatie.

EEN BEVEILIGDE ZOEKOMGEVING MAKEN

De implementatie van zoekoplossingen voor de onderneming werpt nieuwe beveiligingsvragen. Door die beveiligingsproblemen van het begin af op te lossen door een allesomvattende beveiligingsmethode, kunnen bedrijven optimaal profiteren van de zoekoplossingen terwijl hun gevoelige informatie wordt beschermd.

Neem contact met ons op voor meer informatie over de wijze waarop onze oplossingen uw bedrijf kunnen helpen.

WERELDWIJD BEHEER EN TECHNOLOGIEADVIES VOOR DE MODERNE BEDRIJFSOMGEVING

BearingPoint is een toonaangevend consultancybureau dat wereldwijd beheer- en technologieadvies levert aan bedrijven uit de Global 2000 en veel van 's werelds grootste publieke bedrijven. Onze ervaren professionals helpen bedrijven rond de wereld hun doelstellingen te behalen en waarde voor de onderneming te genereren. Door hun bedrijfsprocessen en informatiesystemen af te stemmen, helpen we onze klanten aan een concurrentievoordeel omdat ze informatie sneller kunnen leveren. Neem voor meer informatie contact met ons op via 1.866.661.FIND (+1.603.589.4089 buiten de Verenigde Staten en Canada) of ga naar onze website op www.bearingpoint.com.

BearingPoint biedt strategisch advies, toepassingsservices, technologieoplossingen en beheerde services aan Global 2000-bedrijven en overheidsinstellingen.

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

© 2006 BearingPoint, Inc. Alle rechten voorbehouden. Gedrukt in de Verenigde Staten.
Alle handelsmerken en logo's in dit document zijn het eigendom van de respectieve eigenaren. 0206-01 -USRD709