

Söklösningar för företag

Säkerhetsfrågor vid implementering av sökning

En söklösning för företaget kan hjälpa till att **stimulera produktiviteten** genom att göra användbar information lättillgänglig för dem som behöver den.

INTRODUKTION: SÄKERHETSKRAV FÖR SÖKLÖSNINGAR

En välimplementerad söklösning för företaget kan göra en stor mängd information tillgänglig för kunskapsarbetare och andra inom en organisation – vilket uppfyller den växande förväntan hos arbetarna att företagssystem ska tillhandahålla samma nivå av funktionalitet, rörlighet och användarvänlighet som på Internet. Problemet är att se till att kunskapsarbetare kan nå den information de behöver, med korrekt säkerhetsnivå så att de bara når den information som de har behörighet till.

En vägledande princip för säkerhet vid organisationsomfattande sökning är att den ska bygga på företagets underliggande säkerhetssystem och gällande regler. Det är även viktigt att sökningssäkerheten är kompatibel med de säkerhetssystem som används för olika innehållskällor inom företaget. Vid skapandet av en säkerhetsstruktur anser BearingPoint att betydande uppmärksamhet ska läggas på verifiering, auktorisering, revision samt identitets- och åtkomsthantering.

VERIFIERING

Verifiering kan göras på många sätt. Oavsett om den är katalogbaserad eller programbaserad är den vanligaste standarden för verifiering att använda användarnamn och lösenord. Den säkerhetsrisk som denna metod innebär kanske eller kanske inte är ett problem, beroende på företagets verksamhetsmiljö. Utmaningen med organisationsomfattande sökning är associeringen av korrekt säkerhetsmetod eller identitetsverifiering med de begärda sökresultaten. Inte all information har likvärdig betydelse och alla företag har heller inte samma säkerhetskrav för dataåtkomstkontroller.

Noggrann identitetsverifiering kan vara viktigt när mer känsliga data blir tillgängliga för användarna. Ett enkelt användarnamn och lösenord kanske inte längre är en acceptabel verifieringsmetod. Samtidigt begränsas en gallring av användarna (eller att verkligen säkert identifiera användarna) av den kostnad som det innebär eller på grund av att det inte ingår i företagets policy. Certifikat för offentliga nycklar (PKI), biometri och dubbel verifiering är verktyg som kan behövas för att övervinna detta.

Det finns tre grundläggande begrepp för verifieringsnivå som kan anpassas till ett visst företags behov.

- **Verifieringsnivå 1** – Utgår ifrån att det är tillräckligt att användaren kunde logga in till sin arbetsstation med korrekt användarnamn och lösenord.

I DETTA PERSPEKTIV:

INTRODUKTION: SÄKERHETSKRAV FÖR SÖKLÖSNINGAR	1
VERIFIERING	1
Verifiering och sökmotorn	2
AUKTORISERING	2
Auktorisering och sökmotorn	2
REVISION	3
Revision och sökmotorn	3
IDENTITETS- OCH ÅTKOMSTHANTERING	3
Identitets- och åtkomsthantering och sökmotorn	4
SKAPAR EN SÄKER SÖKMILJÖ	4

- **Verifieringsnivå 2** – Kräver inloggning, antingen manuellt eller via ett enkelt inloggningssystem (SSO), för varje länk som innehåller mer känsliga data.
- **Verifieringsnivå 3** – Använda avancerad eller dubbel verifiering med hjälp av ett x509-certifikat eller biometri för att visa certifikatinformation, omvandla certifikatet till olika formulär, signera certifikatbegäran, som till exempel en minicertifiering, eller för att redigera nivåer för certifikatinställningar.

Verifiering och sökmotorn

Vid leverans kan en söklösning stödja två metoder för verifiering av sökning i innehållet: grundläggande/NTLM (NT LAN Manager) verifiering och formulärbaserad verifiering. Grundläggande/NTLM-verifiering fungerar i nästan alla webbserverimplementeringar som stöder minst HTTP/1.0. Det stöds även av servrar baserade på Microsoft®-operativsystem (OS). Allmänt gäller att om en användaridentitet finns inom ett Microsoft OS och NTLM används så kan sökmotorn söka i användarens delmängd.

Formulärbaserad verifiering används oftast i webbaserad SSO-miljöer. En begränsning hos befintliga sökmotorer är att endast ett formulärbaserat SSO-system kan användas åt gången.

Efter att sökmotorn har genomsökt innehållet och en användare vill söka i resultatet måste sökmotorn visa innehållet på ett säkert sätt. Sökmotorer använder grundläggande verifiering/NTLM-verifiering och formulärbaserad verifiering med hjälp av HEAD-begäran till en webbserver för webbaserat innehåll.

Sökmotorn kan oftast konfigureras för både offentligt och säkert innehåll. När användaren försöker att få åtkomst till innehåll som har definierats som säkert visas en dialogruta inom webbläsarens session så att användaren måste ange användaridentitet. Det görs en gång per session.

Med formulärbaserad verifiering kan sökmotorn antingen använda cookieverifiering eller fullständig användaridentifiering. I båda fallen sparar sökmotorn inloggningsinformationen i en cookie och skickar den till de system som genomsöks.

Mer komplexa system använder externt innehåll kommer anpassade adaptorer och API-gränssnitt att krävas. Leverantörer erbjuder verifieringsleverantörsgrenssnitt (SPI) som låter webbtjänster översätta mellan sökmotorverifierad SPI och den server som tillhandahåller åtkomstkontrolltjänster.

AUKTORISERING

Utmaningen med auktorisering är att balansera användarnas behörighet så att de kan utföra sina arbetsuppgifter. Organisationsomfattande sökning är inget undantag.

Länkning av rätt data eller sökresultat inom domänen till användarens behörighet och att sedan endast visa dessa data är fortfarande en utmaning. Särskilda kataloger och SSO- och PKI-certifikat är exempel på auktoriseringstjänster som kan användas för att hjälpa till att identifiera användare och verifiera deras identiteter.

Nedan ges exempel på begrepp för auktoriseringsnivå. De utgör inte någon fullständig lista över alla tillgängliga alternativ:

- **Auktoriseringsnivå 1** – Intern offentlig information som är tillgänglig för alla och inte kräver mer än nätverksåtkomst för att kunna visas.
- **Auktoriseringsnivå 2** – Konfidentiell information som kräver ytterligare en inloggning för att kunna visas.
- **Auktoriseringsnivå 3** – Känsliga data, som till exempel företagets immateriella egendomar eller löneinformation, som endast specifika grupper har åtkomst till.

Auktorisering och sökmotorn

Auktoriserings-SPI:er tillåter att sökmotorer kan använda externt sparad användaridentitetsinformation i vanliga NTLM-verifieringsscheman eller i ett formulärbaserat SSO-system. Implementering av ett auktoriserings-SPI använder standarden SAML 2.0 som grund.

När en användare utför en sökning och sökmotorn måste fastställa om den kan visa resultatet kommer sökmotorn att kontakta målets värd, eller "åtkomstanslutning" med webbadressen eller angivet mål och användarens identitet.

Varje gång, enligt standarden för SAML 2.0, kommer målets värd att antingen tillåta, neka eller svara att identiteten är okänd. Denna möjlighet försäkras genom användning av SOAP (Simple Object Access Protocol) via säker HTTP (HTTPS, Hypertext Transfer Protocol Secure). Det kan däremot uppstå förseningar med denna metod eftersom sökmotorn endast sparar dessa resultat under sessionen. Cachetiden kan konfigureras.

REVISION

För varje effektiv implementering av någon säkerhetslösning krävs möjligheten att revidera.

Med företagstäckande sökning skiftar fokuseringen. Medan de flesta organisationer inriktar sig på externa hot kan större hot komma inifrån. En säker söklösning måste tillhandahålla säkra sökningar medan den begränsar användarnas sökningar till samlingar om så krävs. Revision av dataåtkomst är fortfarande viktigt men det är mindre viktigt än användarbehörigheter.

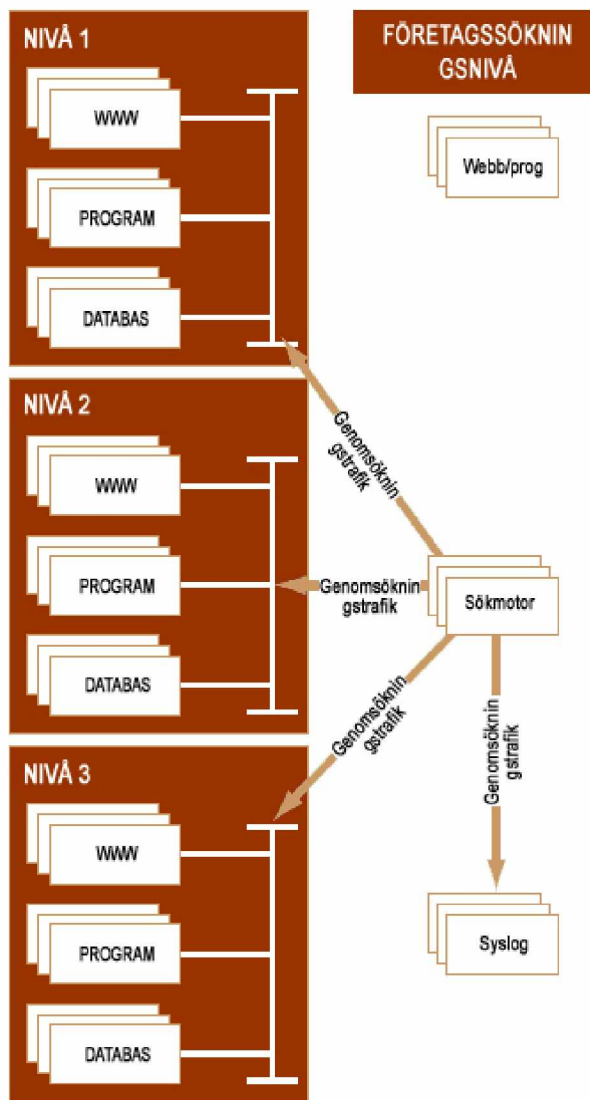
Inriktning på användarbehörigheter ger bättre försäkring om att de personer som behöver informationen utför säkra sökningar. Nyckelområden att tänka på inkluderar obehörig åtkomst; flyttningar, tillägg och ändringar för användare; användare som visar känsliga data med falsk identitet samt användare som bibehåller behörighet från föregående roller och därmed får tillgång till känsliga data.

Revision och sökmotorn

För att kunna implementera revisionsfunktioner över hela organisationen måste korrekta revisionstjänster distribueras i den befintliga infrastrukturen. System som kommer att ingå i sökningen måste kontrolleras för korrekt revisionsimplementering.

Tillgängliga sökmotorer har funktioner inbyggda för revisionsloggning via en extern syslogserver som skapar en textfil som måste skickas till en separat syslogserver. Användning av en särskild syslogserver för korrekt revisionsfunktion inom sökmotorn rekommenderas. Om revisionsloggningsservrar och meddelanden dessutom inte sparas på åtkomliga system behöver denna funktion implementeras. Bild 1 visar en typisk distribution där sökmotorn använder en separat syslogserver för att samla loggfiler som skapas av slutanvändarens sökningar.

Bild 1. Funktion för sökmotorns analys



IDENTITETS- OCH ÅTKOMSTHANTERING

En söklösning kan faktiskt utgöra en säkerhetsrisk om korrekta kontroller inte har inkluderats före implementeringen. Men det kan finnas en positiv effekt av det. Efterhand som data genomsöks och visas kan gamla säkerhetshål eller oskyddade databaser upptäckas och därmed åtgärdas.

Verifiering, auktorisering och revision är viktiga delar för identitets- och åtkomsthantering. Andra viktiga aspekter för en väl fungerande metod är:

- **Lösenordskonfiguration och äldre riktlinjer.** När användarnamn och lösenord används för åtkomst till säkra data ska säkra lösenord användas. Lösenorden ska vara alfanumeriska och ska ändras regelbundet beroende på vilka data som de ger åtkomst till – ju mer känsliga data, desto oftare ska lösenordsändringar göras.
- **Enkelt inloggningssystem.** Enkelt inloggningssystem kan användas för att minska kostnaden för återställning av användarnas lösenord för sällan använda men säkra program eftersom de själva kan skapa tidsbegränsade lösenord. Denna funktion kan ersätta enkla lösenord och förhindra att lösenord delas av många. Det kan göra att en användare inte behöver logga in flera gånger för att få åtkomst till säkra data, vilket ger en säkrare miljö och uppmuntrar användaren till att utnyttja sökfunktionen.
- **Separation av uppgifter (SoD).** Separation av roller utan att skapa ytterligare kostnader genom tillagd personal kan vara en svår balans. SoD har utformats så att användaren förhindras från att utföra potentiellt skadliga åtgärder. Förutom i småföretag har en person vanligtvis inte åtkomst till både leverantörsreskontra och kundreskontra. I en organisationsomfattande sökningsmiljö ska inte den person som ger användarbehörigheter vara samma som den som bestämmer vilka samlingar som användaren har åtkomst till.
- **Rollbaserad åtkomstkontroll.** Skapandet av roller är ingen enkel uppgift, men det kan skapa en säkrare miljö. Behörighet ges på tre sätt — uttrycklig, underförstådd och ärvd. Regler kan uppställas för att förhindra att motsägande roller ges till samma användare, vilket därmed stärker de SoD-riktlinjer som har skapats. Möjligheten för användare att filtrera en sökning med en specifik roll, även om de har flera roller, kan ge både renare och säkrare resultat. Rollbaserad åtkomst är direkt länkad till SoD. Genom att användarna har definierade roller, med regler som förhindrar motstridiga roller, kommer de sökresultat som visas att vara direkt relaterade till vad de behöver och ska ha åtkomst till.
- **Användarprovisionering/avprovisionering.** En säkrare miljö kan skapas genom centraliserad och delegerad användarhantering, arbetsflöden, lösenordshantering och rollbaserade åtkomstkontrollmodeller. Ett dubbelt mål är att kontrollera att nya användare får omedelbar åtkomst till den information som de behöver och att åtkomst nekas

för användare som inte längre har en viss behörighet. Även om det inte är direkt relaterat till sökning har korrekt provisionering en direkt inverkan på roller och SoD. Det är utgångspunkten för många säkerhetsinitiativ.

Identitets- och åtkomsthantering och sökmotorn

Sökmotorer finns tillgängliga med ledande identitetshanteringslösningar med hjälp av formulärbaserad verifiering och utnyttjande av en auktoriserande SPI.

Vad som fortfarande behöver fastställas är hur många sökmotorer som kommer att integreras med icke-webb-baserad SSO och SSO-liknande bakåtkompatibla system. Många organisationer använder flera säkerhetssystem som distribuerats i olika former – webbaserat SSO, internt SSO, LDAP och andra källor för användarnamn/lösenord.

Eftersom kraven för söklösningar är unika för varje organisation är en korrekt omfattning av distributionen mycket viktigt. En blandning av olika tekniker kan användas, inklusive en auktoriserings-SPI, egna API:er och adapterer och sökmotorns formulärbaserade verifieringsmekanism.

SKAPAR EN SÄKER SÖKMILJÖ

Distribution av söklösningar för företag uppställer nya säkerhetsfrågor. Genom att hantera dessa krav från början med en omfattande säkerhetslösning kan organisationer utnyttja fördelarna med söklösningar, samtidigt som känslig information skyddas.

Om du vill lära dig mer om hur våra lösningar kan stärka ditt företag kan du [höra av dig](#).

GLOBAL LEDNING OCH TEKNISK KONSULTERING FÖR DAGENS AFFÄRSMILJÖ

BearingPoint är ett ledande globalt hanterings- och teknikonsulteringsföretag som arbetar för många av världens största offentliga organisationer. Vår erfarna personal hjälper organisationer runtom i världen att fokusera sina ansträngningar att nå deras mål och skapa värde för företaget. Genom att samstämna deras affärsprocesser med deras informationssystem hjälper vi våra kunder att få en konkurrenskraftig fördel — tillhandahåller snabba resultat. Om du vill lära dig mer kan du kontakta oss på 1.866.661.FIND (+1.603.589.4089 från andra länder än USA och Kanada) eller gå till vår webbplats på adressen www.bearingpoint.com.

BearingPoint tillhandahåller strategisk konsultering, programtjänster, tekniska lösningar och övervakningstjänster till stora företag och myndighetsorganisationer.

BearingPoint

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

