

Søkeløsninger for bedriften

Sikkerhets- hensyn ved innføring av søk

En søkeløsning for bedriften kan øke organisasjonens produktivitet ved å gjøre nyttig informasjon lett tilgjengelig for personer som trenger det.

INTRODUKSJON: SIKKERHETSKRAVENE FOR SØKELØSNINGER

En godt innført søkeløsning for bedriften, kan være et skattekammer av informasjon for kunnskapsarbeidere og andre i en organisasjon – som oppfyller den voksende forventningen hos de ansatte om at bedriftssystemer skal gi samme grad av funksjonalitet, mobilitet og brukervennlighet som Internett-tjenester. Trikset er å sørge for at kunnskapsarbeidere kan få tak i den informasjonen de trenger og under god sikkerhet få tilgang til bare den informasjonen de skal ha.

Et veiledende prinsipp for organisasjonsomfattende søkesikkerhet, er samsvar med underliggende retningslinjer for bedriftssikkerhet og forskriftsmessige krav. Det er også viktig at søkesikkerheten er kompatibel med sikkerhetssystemene for forskjellige innholdskilder i bedriften. BearingPoint mener at det ved opprettelse av et rammeverk for sikkerhet, må legges betydelig vekt på autentisering, godkjenning, overvåking og identitets- og tilgangsadministrasjon.

AUTENTISERING

Autentisering kan anta mange former og bestå av flere metoder. Enten den er katalog- eller programbasert, er brukernavn og passord den vanligste metoden for autentisering. Den iboende usikkerheten ved denne metoden er eller er ikke til bekymring, avhengig av bedriftsmiljøet. Utfordringen ved organisasjonsomfattende søk er å forene den riktige metoden eller formen for autentisering med søkeresultatene. Ikke all informasjon er lik, og ikke alle bedrifter har samme sikkerhetskrav til datatilgangskontroller.

God autentisering kan spille en viktig rolle etter hvert som mer sensitive data blir tilgjengelig for brukere. Det er ikke sikkert at et enkelt brukernavn og et passord lenger er en akseptabel metode for autentisering. Samtidig er brukerkontroll, eller virkelig kjennskap til hvem brukerne er, begrenset av kostnader eller fordi det ikke er en del av bedriftsfilosofien. PKI (Public Key Infrastructure)-sertifikater, biometri og autentifisering bygd på flere faktorer, er verktøy som kan bli nødvendige for å overvinne dette.

Det er tre grunnleggende konsepter for autentiseringsnivå, som kan skaleres til å tilfredsstille en gitt bedrifts behov.

- **Autentiseringsnivå 1** – Anse det som godt nok at brukeren kan logge på sin arbeidsstasjon med riktig brukernavn og passord.

I DETTE SYNSPUNKT:

INTRODUKSJON: SIKKERHETSKRAVENE FOR SØKELØSNINGER	1
AUTENTISERING	1
Autentisering og søkemotoren	2
GODKJENNING	2
Godkjenning og søkemotoren	2
OVERVÅKING	3
Overvåking og søkemotoren	3
IDENTITETS- OG TILGANGSADMINISTRASJON	3
Identitets- og tilgangsadministrasjon og søkemotoren	4
HVORDAN SKAPE ET SIKKERT SØKEMILJØ	4

- **Autentiseringsnivå 2** – Krever pålogging, enten manuelt eller via SSO (Single Sign-On), til hver kobling som krever mer sensitive data.
- **Autentiseringsnivå 3** – Bruker to- eller flerfaktors autentisering som benytter et x509 universalsertifikat eller biometri til å vise sertifikatinformasjon, konvertere sertifikater til forskjellige former, signere sertifikatforespørsler, for eksempel minisertifiseringsinstans eller redigere klareringsinnstillinger for sertifikater.

Autentisering og søkemotoren

Når den først tas i bruk, kan søkeløsningen kanskje støtte to metoder for autentisering for gjennomgang av innhold: Grunnleggende autentisering eller NTLM-autentisering (NT LAN Manager) og skjemabasert autentisering. Grunnleggende autentisering eller NTLM-autentisering fungerer i nesten alle webserverimplementeringer som støtter minst HTTP/1.0. Den støttes også av servere som er basert på Microsoft® operativsystemer. Hvis et legitimasjonssett ligger i et Microsoft operativsystem og bruker NTLM, kan søkemotoren stort sett styrke dette brukersettet.

Skjemabasert autentisering er vanligvis innført i webbaserte SSO-miljøer. Det er for tiden en begrensning for søkemotorer at de ikke kan utnytte mer enn ett skjemabasert SSO-system om gangen.

Når søkemotoren har gjennomgått et innhold og en bruker ønsker å søke i resultatene, må søkemotoren vise innholdet på en sikker måte. Søkemotorer benytter grunnleggende autentisering eller NTLM-autentisering ved å bruke HEAD-forespørsler mot en webserver for webbasert innhold.

Søkemotoren kan vanligvis konfigureres til å ta både allment tilgjengelig innhold og sikkert innhold. Når brukeren forsøker å få tilgang til innhold som er definert som sikkert, vises en dialogboks i webleserøkten, som forlanger å få det nødvendige legitimasjonssettet fra brukeren. Dette skjer én gang per økt.

Når det gjelder skjemabasert autentisering, kan søkemotoren enten bruke videresending av informasjonskapsler eller full brukerrepresentasjon. I begge tilfeller legger søkemotoren påloggingsinformasjonen i en informasjonskapsel og videresender den til systemet som blir gjennomgått.

For mer komplekse implementasjoner med bruk av innhold utenfra, kreves tilpasninger og API (Application Programming Interfaces). Leverandører tilbyr godkjenning-SPI-er (Service Provider Interfaces), som webtjenester kan bruke til å overføre mellom søkemotorens autorisasjons-SPI og serveren som leverer tilgangskontrolltjenesten.

GODKJENNING

Utfordringen ved godkjenning er å balansere brukerrettighetene slik at de kan utføre jobben sin. Organisasjonsomspennende søk er ikke noe unntak fra dette.

Tilordning av riktige data eller søkeresultater innenfor grensene for brukerens rettigheter og presentasjonen av bare disse dataene, er fortsatt en utfordring. Forente kataloger og SSO- og PKI-sertifikater er eksempler på autorisasjonstjenester som kan brukes til å identifisere brukere og kontrollere deres identitet.

Nedenfor finner du eksempler på konsepter på godkjenningnivå. Dette er ikke en komplett oversikt over alternativene:

- **Godkjenningnivå 1** – Intern, offentlig informasjon som er tilgjengelig for alle, og som ikke krever annet enn nettverkstilgang.
- **Godkjenningnivå 2** – Konfidensiell informasjon som krever en andre pålogging.
- **Godkjenningnivå 3** – Sensitive data, som for eksempel åndsverk eller lønningslister, som bare bestemte grupper har tilgang til.

Godkjenning og søkemotoren

Med godkjenning-SPI-er kan søkemotorer bruke brukerlegitimasjoner som er lagret utenfor typiske NTLM-godkjenningsskjemaer eller skjemabasert godkjenning fra bare én kilde. Implementering av en godkjenning-SPI er avhengig av standarden SAML 2.0 (Security Assertion Markup Language) som grunnlag og at den er kodet med den standarden.

Når en bruker utfører et søk og søkemotoren må avgjøre om den kan vise resultatet, kontakter søkemotoren målverten eller tilgangskontakten med webadressen eller målet det gjelder og brukerens identitet.

Hver gang vil målverten, underlagt SAML 2.0-standarder, enten tillate, avslå eller svare med ubestemt. SOAP (Simple Object Access Protocol) over HTTPS (Hypertext Transfer Protocol Secure) muliggjør dette. Men dette kan gi forsinkelser fordi søkemotoren hurtigbuffer disse resultatene under økten. Hurtigbufferingstiden kan justeres.

OVERVÅKING

Effektiv implementering av en hver sikkerhetsløsning, krever mulighet til å overvåke.

Ved bedriftsomspennende søk, skifter overvåkingen fokus. Mens de fleste organisasjoner fokuserer på trusler utenfra, kan større trusler komme innenfra. En søkeløsning må foreta sikre søk samtidig som den begrenser brukersøk til en samling om nødvendig. Selv om overvåking av datatilgang fortsatt er viktig, kommer det etter brukerrettigheter.

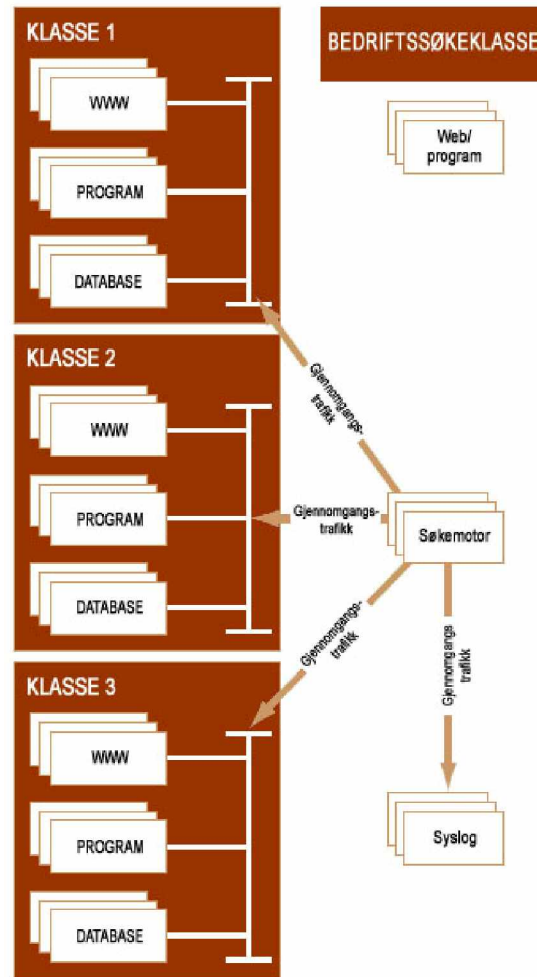
Fokusering på brukerrettigheter gir større sikkerhet for at personer som trenger informasjon gjennomfører sikre søk. Viktige forhold som må vurderes, er ikke-godkjent rettighetsforfremmelse, brukerflytting, tilføyelser og endringer, brukere som får tilgang til sensitive data ved bruk av falske legitimasjoner og brukere som sitter på rettigheter fra tidligere roller og som får tilgang til sensitive data.

Overvåking og søkemotoren

For å implementere organisasjonsomspennende overvåkingsfunksjoner må riktige overvåkingstjenester innføres i den eksisterende infrastrukturen. Systemer det skal gis tilgang til under innføringen av søkeløsning, må gjennomgå for å se om tilfredsstillende overvåking er implementert.

Tilgjengelige søkemotorer har innebygd funksjonalitet som gir muligheter for overvåkingslogging via en ekstern syslog-server som leverer utdata til en tekstfil som må sendes til en separat syslog-server. Det bør settes opp en egen syslog-server for å få tilfredsstillende overvåkingsfunksjonalitet i søkemotoren. Og hvis servere for overvåkingslogging og meldinger ikke avbildes på det tilgjengelige systemet, må denne funksjonaliteten implementeres. Figur 1 beskriver en typisk innføring der søkemotoren bruker en separat syslog-server til å samle loggfiler som opprettes av sluttbrukernes søkeaktivitet.

Figur 1. Søkemotorens overvåkingsfunksjon



IDENTITETS- OG TILGANGSADMINISTRASJON

En søkeløsning kan faktisk skape sikkerhetsproblemer hvis ikke de riktige kontrollene er på plass før implementeringen. Men dette kan gi et positivt resultat. Etter hvert som data gjennomgås og vises, kan gamle sikkerhetshull oppdages og ubeskyttede data oppdages, og feilene kan rettes opp.

Autentisering, godkjenning og overvåking er viktige deler av identitets- og tilgangsadministrasjonen. Andre viktige sider ved en velbalansert tilnæringsmåte er:

- **Passordkonfigurasjon og retningslinjer for foreldelse.** Med brukernavn og passord som brukes for å få tilgang til sikre data, er det avgjørende å ha strenge retningslinjer for passord. Passord bør være alfanumeriske og bør foreldes basert på hvilke data de gir tilgang til – jo flere sensitive data, desto oftere må passordet endres.
- **Enkel pålogging (SSO).** Enkel pålogging kan brukes til å redusere kostnadene ved å tilbakestille passord for sjeldent brukte, men sikre programmer fordi de kan generere nye passord automatisk. Denne funksjonen eliminerer enkle passord og hindrer at passord sendes rundt. Den kan eliminere brukerens behov for å logge på gjentatte ganger for å få tilgang til sikre data og gi et sikrere miljø og oppfordre brukerne til å bruke søkefunksjonen.
- **SoD (Separation of Duties).** Å skille roller uten å skape ekstra kostnader ved å øke staben, kan bli en vanskelig balansegang. SoD er utviklet for å hindre brukere fra å utføre potensielt risikable handlinger. Bortsett fra i mindre bedrifter, har vanligvis ikke en person tilgang til både leverandørreskontro og kundereskontro. I et organisasjonsomspennende søkemiljø, bør ikke den personen som tildeler brukerrettigheter være den samme som den som bestemmer hvilke samlinger brukerne skal få tilgang til.
- **Rollebasert tilgangskontroll.** Rolleutforming er ingen liten oppgave, men den skaper et sikrere miljø. Rettigheter tildeles på tre måter – eksplisitt, implisitt og overført. Regler kan innføres for å hindre bruk av motstridende roller for samme bruker og slik forsterke SoD-retningslinjene som er opprettet. Brukernes mulighet til å filtrere et søk med en bestemt rolle, selv om de har flere roller, kan gi et tydeligere, men allikevel sikkert resultat. Rollebasert tilgang er koblet direkte til SoD. Ved å gi brukerne definerte roller, med roller som hindrer oppgavekonflikter, kan søkeresultatet som vises, relateres direkte til hva de trenger og bør få tilgang til.
- **Brukerklarering/deklarering.** Det kan opprettes et sikrere miljø ved bruk av sentralisert og delegert brukeradministrasjon, arbeidsflyt, passordadministrasjon og rollebaserte modeller for tilgangskontroll. Det er et todelt mål å sørge for at nye brukere får øyeblikkelig tilgang til den informasjonen de trenger og at tilgang så raskt som mulig fratas

brukere som ikke lenger har godkjenning. Selv om det ikke har noen direkte forbindelse med søking, har riktig klarering en direkte påvirkning på roller og SoD. Dette er startpunktet for mange sikkerhetstiltak.

Identitets- og tilgangsadministrasjon og

søkemotoren Søkemotorer er tilgjengelig med ledende løsninger for identitetsadministrasjon som benytter skjemabasert autentiserings- og godkjenning-SPI.

Det gjenstår å bestemme hvor mange søkemotorer som skal integreres med ikke-webbasert SSO og eldre SSO-lignende systemer. Mange organisasjoner har innført flere sikkerhetssystemer av forskjellige typer – webbasert SSO, intern SSO, LDAP (Lightweight Directory Access Protocol) og andre oppbevaringssteder for brukernavn og passord. Fordi søkeløsningskravene er spesielle for hver enkelt organisasjon, er det påkrevd med riktig omfang på innføringen. En blanding av teknologier kan være i bruk, inkludert en godkjenning-SPI, tilpassede API-er og andre tilpasninger, og søkemotorens skjemabaserte autentiseringsmekanisme.

HVORDAN SKAPE ET SIKKERT SØKELØSNINGSMILJØ

Innføring av søkeløsninger for bedriften, skaper nye sikkerhetshensyn. Ved å ta tak i disse betingelsene i starten, med en omfattende sikkerhetstilnærming, kan organisasjonene dra nytte av fordelene av søkeløsninger samtidig som de beskytter sensitiv informasjon.

Hvis du vil lære mer om hvilke fordeler våre løsninger kan innebære for din bedrift, kan du [kontakte oss](#).

GLOBAL ADMINISTRASJONS- OG TEKNOLOGIRÅDGIVNING FOR DAGENS FORRETNINGSMILJØER

BearingPoint er et ledende selskap innen global administrasjons- og teknologirådgivning, som betjener Global 2000 og mange av verdens største offentlige organisasjoner. Våre erfarne eksperter hjelper organisasjoner over hele verden med å nå oppsatte mål og skape verdier for bedriften. Ved å samkjøre kundenes forretningsprosesser og informasjonssystemer kan vi hjelpe våre klienter med å skaffe seg konkurransefordeler – resultatene kommer raskere enn før. Hvis du ønsker mer informasjon, kan du kontakte oss på +1 603 589 4089 (1.866.661.FIND fra USA) eller besøke vårt webområde på www.bearingpoint.com.

BearingPoint tilbyr strategisk rådgivning, programvaretjenester, teknologiløsninger og administrasjonstjenester til Global 2000-selskaper og offentlige organisasjoner.

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

