

Yrityskäyttöön suunnitellut hakuratkaisut

Tietosuojan huomiointi haun käyttöön- otossa

Yrityshakuratkaisu voi lisätä organisaation tuottavuutta tuomalla hyödyllisen tiedon työntekijöiden saataville.

JOHDANTO: HAKURATKAISUJEN TURVALLISUUSVAATIMUS

Hyvin käyttöön otettu yrityshakuratkaisu voi tuoda arvokkaita tietoja tietotyöläisten ja muiden organisaatioon kuuluvien henkilöiden ulottuville vastaten näin työntekijöiden kasvaviin odotuksiin siitä, että yritysjärjestelmät tarjoavat samantasoista toimivuutta, siirrettävyyttä ja helppokäyttöisyyttä kuin Internet-palvelut. On tärkeää varmistaa tietotyöläisten pääsevän käsiksi tarvitsemiinsa tietoihin huomioimalla samalla riittävä tietosuoja ja käyttöoikeuksien tarkistus.

Organisaationlaajuisen hakuratkaisuuden tärkein periaate on, että se vastaa yrityksen tietosuojakäytäntöjä ja sääntelyvaatimuksia. Hakuratkaisuuden on myös vastattava yrityksen eri sisältölähteiden tietosuojajärjestelmiä. BearingPoint uskoo, että tietosuojajärjestelmää laadittaessa on kiinnitettävä erityistä huomiota käyttöoikeuksien tarkistukseen, valtuutukseen, valvontaan sekä henkilöllisyyden ja käyttöoikeuksien hallintaan.

KÄYTTÖOIKEUKSIEN TARKISTUS

Käyttöoikeuksien tarkistus voidaan toteuttaa monella eri tavalla. Riippumatta siitä, onko kyseessä hakemisto- vai sovelluspohjainen tarkistus, yleisin tapa tarkistaa käyttöoikeudet on tehdä se käyttäjänimen ja salasanan avulla. Käytännöstä aiheutuva turvallisuuden vaarantuminen voi olla ongelma yritykselle tai sitten ei, yritysympäristöstä riippuen. Organisaationlaajuisen haun haasteena on liittää oikea käyttöoikeuksien tarkistustapa tai -muoto pyydettyihin hakutuloksiin. Kaikkia tietoja ei ole luotu samanarvoisiksi, eikä kaikilla yrityksillä ole samoja turvallisuusvaatimuksia tietojen käyttöoikeuksien hallinnan suhteen.

Hyvä käyttöoikeuksien tarkistus voi olla tärkeää, kun arkaluontoiset tiedot tulevat käyttäjien saataville. Pelkkä käyttäjänimi ja salasana eivät välttämättä enää ole riittävä käyttöoikeuksien tarkistustapa. Käyttäjien todellisen henkilöllisyyden selvittämistä rajoittavat kuitenkin sen kustannukset tai se ei kuulu yrityksen yritysfilosofiaan. Asian ratkaiseminen voi edellyttää PKI (Public Key Infrastructure) -varmenteiden tai biometristen tai moniosaisten käyttöoikeuksien tarkistustapojen käyttöä.

Käyttöoikeuksien kolme eri tarkistustasoa vastaavat yritysten erilaisiin tarpeisiin.

- **Tarkistustaso 1**—Edellyttää käyttäjän pystyvän kirjautumaan työasemalleen oikealla käyttäjänimellä ja salasanalla .

TÄSSÄ NÄKÖKULMASSA:

JOHDANTO: HAKURATKAISUJEN TURVALLISUUSVAATIMUS	1
KÄYTTÖOIKEUKSIEN TARKISTUS	1
Käyttöoikeuksien tarkistus ja hakukone	2
VALTUUTUS	2
Valtuutus ja hakukone	2
VALVONTA	3
Valvonta ja hakukone	3
HENKILÖLLISYYDEN JA KÄYTTÖOIKEUKSIEN HALLINTA	3
Henkilöllisyyden ja käyttöoikeuksien hallinta ja hakukone	4
TURVALLISEN HAKUYMPÄRISTÖN LUOMINEN	4

- **Tarkistustaso 2**— Edellyttää kaikkiin luottamuksellista tietoa sisältäviin linkkeihin kirjautumista joko manuaalisesti tai SSO (Single sign-on) -järjestelmän kautta.
- **Tarkistustaso 3** — Käytetään kahden tai useamman tekijän avulla tehtävää käyttöoikeuksien tarkistusta, jossa käytetään x509-monikäyttövarmennetta tai biometriikkaa varmennetietojen näyttämiseksi, varmenteiden muuntamiseksi eri muotoihin, varmennepyyntöjen (kuten Mini Certification Authority) allekirjoittamiseksi tai varmenteen asetusten muokkaamiseksi.

Käyttöoikeuksien tarkistus ja hakukone

Mikäli hakuratkaisu otetaan käyttöön sellaisenaan, se tukee kahta käyttöoikeuksien tarkistustapaa sisällön indeksoinnissa: perus/NTLM (NT LAN Manager) - tarkistusta ja lomakkeeseen perustuvaa tarkistusta. Perus/NTLM-tarkistus toimii lähes kaikissa Web-palvelinkokoonpanoissa, jotka tukevat vähintään HTTP/1.0-protokollaa. Lisäksi sitä tukevat Microsoft®-käyttäjärjestelmään perustuvat palvelimet. Hakukone voi yleensä käyttää Microsoft-käyttäjärjestelmässä olevia ja NTLM-varmennusta käyttäviä käyttäjätietoja.

Lomakkeisiin perustuvaa käyttöoikeuksien tarkistusta käytetään yleensä Web-pohjaisissa SSO-ympäristöissä. Hakukoneiden yleisenä rajoituksena on se, että ne pystyvät käyttämään vain yhtä lomakkeisiin perustuvaa SSO-järjestelmää kerrallaan.

Hakukoneen indeksoitua sisällön ja käyttäjän tehdessä niistä hakuja hakukoneen on näytettävä sisältö turvallisella tavalla. Hakukoneet käyttävät perus/NTLM- ja lomakkeisiin perustuvaa käyttöoikeuksien tarkistusta pyytämällä HEAD-pyyntöillä Web-palvelimelta Web-pohjaista tietoa.

Hakukone voidaan yleensä määrittää isännöimään sekä julkista että suojattua sisältöä. Käyttäjän yrittäessä käyttää suojatusti määriteltyä sisältöä näyttöön ilmestyy selainistunnon aikana valintaikkuna, jonka avulla tarkistetaan käyttäjän turvatiedot. Tämä tapahtuu kerran kunkin istunnon aikana.

Lomakkeisiin perustuvassa käyttöoikeuksien tarkistuksessa hakukone käyttää joko evästeiden välittämistä tai käyttäjäksi tekeytymistä. Molemmissa tapauksissa kone kaappaa kirjautumistiedot evästeestä ja välittää ne indeksoitaville järjestelmille.

Monipolvisemmissä kokoonpanoissa, jotka käyttävät ulkopuolista sisältöä, edellytetään mukautettujen sovitimien ja ohjelmointirajapintojen (API) käyttöä. Toimittajat tarjoavat tarkistukseen SPI (Service Provider Interface) -rajapintoja, joiden avulla Web-palvelut voivat toimia hakukoneen SPI-tarkistusrajapinnan ja käyttöoikeuksien hallintapalveluja tarjoavan palvelimen välillä.

VALTUUTUS

Valtuutuksen haasteena on käyttäjien oikeuksien tasapainottaminen niin, että he voivat suorittaa työtehtävänsä. Tämä pitää paikkansa myös organisaationlaajuisen haun kohdalla.

On haasteellista kartoittaa, mitkä ovat käyttäjän oikeuksien mukaiset tiedot ja hakutulokset, ja sitten esittää vain nämä tiedot. Yhdistetyt hakemistot sekä SSO- ja PKI-varmenteet ovat esimerkkejä käyttöoikeuksien tarkistuspalveluista, joiden avulla voidaan tunnistaa käyttäjiä ja varmentaa heidän henkilöllisyytensä.

Seuraavassa annetaan esimerkkejä käyttöoikeuksien valtuutustason käsitteistä. Niiden lisäksi on kuitenkin muitakin vaihtoehtoja.

- **Valtuutustaso 1** — Sisäinen julkinen tieto, joka on kaikkien käytettävissä ja edellyttää vain pääsyä verkkoon.
- **Valtuutustaso 2** — Luottamuksellista tietoa, jonka katselu edellyttää toista kirjautumista.
- **Valtuutustaso 3** — Arkaluontoiset tiedot, kuten yrityksen immateriaaliomaisuus tai palkkatiedot, joiden käyttöoikeus on vain tietyillä ryhmillä.

Valtuutus ja hakukone

SPI-varmennuksen avulla hakukone voi käyttää käyttäjän käyttöoikeustietoja, jotka on tallennettu tyypillisten NTLM-varmennusjärjestelmien ulkopuolelle, tai yhteen lähteeseen ja lomakkeisiin perustuvaa käyttöoikeuksien tarkistusta. SPI-varmennuksen käyttöönotto perustuu SAML (Security Assertion Markup Language) -kielen 2.0-standardiin, ja se on koodattu standardin mukaisesti.

Kun käyttäjä tekee haun ja hakukoneen on määriteltävä, näyttääkö se tuloksen, se ottaa yhteyttä kohdeisäntään tai käyttöoikeuspalvelimeen ja ilmoittaa URL-osoitteen tai kohteen sekä käyttäjän henkilöllisyyden.

Joka kerta kohdeisäntä SAML 2.0 -standardien mukaisesti joko sallii tai evää pääsyn tai vastaa ennalta määrittelemättömästi. Toiminnon mahdollistaa SOAP (Simple Object Access Protocol) -protokolla suojatun HTTPS-yhteyden kautta. Tästä voi kuitenkin olla seurauksena viiveitä, sillä hakukone tallentaa tulokset välimuistiin istunnon aikana. Välimuistin aikamääriytyksiä voidaan muuttaa.

VALVONTA

Minkä tahansa turvallisuusratkaisun käyttöönotto edellyttää mahdollisuutta valvontaan.

Yrityksenlaajuisessa haussa valvonnan painopiste muuttuu. Suurin osa organisaatioista keskittyy ulkoisiin uhkiin, vaikka suurimmat uhkat tulevat organisaation sisältä. Hakuratkaisun on tehtävä turvallisia hakuja samalla, kun se tarvittaessa rajoittaa käyttäjien hakuja kokoelmiin. Tietojen käyttöoikeuksien valvonta on edelleen tärkeää, mutta sitä tärkeämpiä ovat kuitenkin käyttöoikeudet.

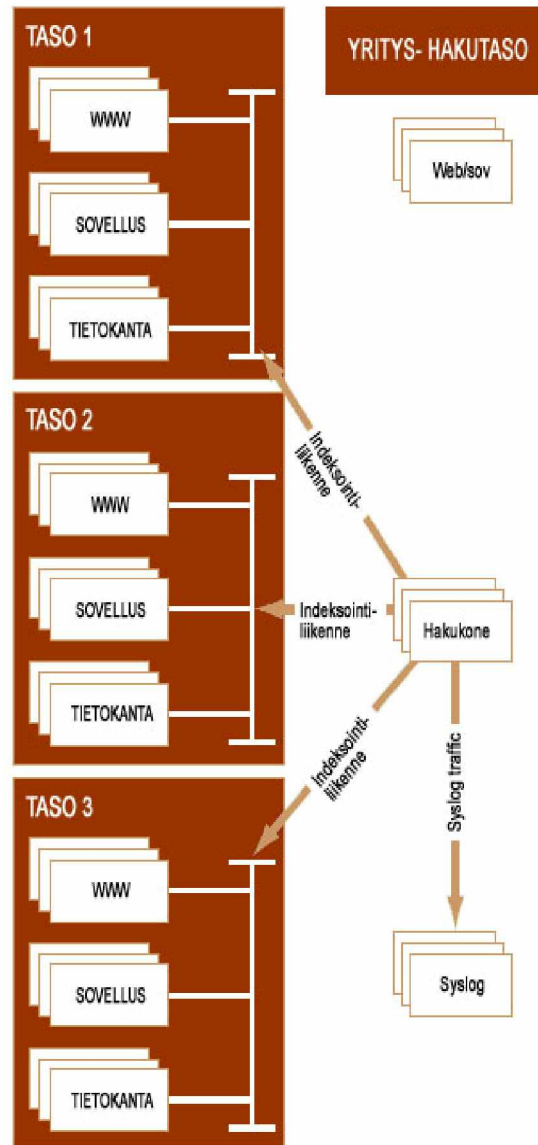
Käyttöoikeuksiin keskittymällä voidaan varmistaa paremmin, että tietoja tarvitsevat henkilöt tekevät turvallisia hakuja. Tärkeitä tähän liittyviä asioita ovat käyttöoikeuksien luvaton lisääminen, käyttäjien liikkuminen ja vaihtuminen, käyttäjämäärän lisääntyminen sekä väärillä käyttöoikeustiedoilla tai edellisten roolien oikeuksilla arkaluontoisia tietoja käyttävät käyttäjät.

Valvonta ja hakukone

Organisaationlaajuisen valvontatoimintojen käyttöönoton edellytyksenä on asianmukaisten valvontapalvelujen ottaminen käyttöön olemassa olevassa infrastruktuurissa. Haussa käytettävät järjestelmät on tarkistettava, jotta valvonta voidaan ottaa asianmukaisesti käyttöön.

Saatavilla olevissa hakukoneissa on sisäänrakennettu toiminto, jonka avulla voidaan kerätä valvontatietoja ulkoisen lokipalvelimen kautta. Palvelin esittää tiedot tekstitiedostossa, joka on lähetettävä erilliselle lokipalvelimelle. On suositeltavaa ottaa käyttöön oma lokipalvelin, jotta hakukoneen valvontatoiminto toimii kunnolla. Ellei käytettävissä olevissa järjestelmissä ole käytössä valvontatietojen keräämiseen käytetyn palvelimen ja viestien kaappaaminen, tämä toiminto on otettava käyttöön. Kuvassa 1 esitetään tyypillinen käyttöönotto, jossa hakukone käyttää erillistä lokipalvelinta kerätäkseen loppukäyttäjän toiminnan perusteella luotuja lokitiedostoja.

Kuva 1. Hakukoneen valtuutustoiminto



HENKILÖLLISYYDEN JA KÄYTTÖOIKEUKSIEN HALLINTA

Hakuratkaisu voi aiheuttaa turvallisuusongelmia, ellei ennen käyttöönottoa ole huolehdittu asianmukaisesta tietosuojasta. Ongelma voidaan kuitenkin ratkaista. Tietojen indeksoinnin ja esittämisen aikana pitkäaikaiset tietoturva-aukot tai suojaamattomat tietovarastot voidaan saada selville ja asia voidaan korjata.

Henkilöllisyyden ja käyttöoikeuksien hallinnan keskeisimmät osatekijät ovat käyttöoikeuksien tarkistus, valtuutus ja valvonta. Muita tärkeitä huomioon otettavia seikkoja ovat:

- **Salasanamääritykset ja vanhentumiskäytännöt.** Mikäli suojattuihin tietoihin pääsee käsiksi käyttäjänimen ja salasanan avulla, on tärkeää käyttää vahvoja salasanakäytäntöjä. Salasanojen on oltava aakkosnumeerisia ja niiden on vanhentuttava käytetyn tiedon laadun mukaan. Mitä arkaluontoisemmasta tiedosta on kyse, sitä useammin salasanan on vaihdettava.
- **Kertakirjautuminen (Single sign-on, SSO).** Kertakirjautumisella eli SSO:lla voidaan säästää kustannuksissa, jotka aiheutuvat käyttäjien salasanojen palauttamisesta harvoin käytetyissä mutta suojatuissa sovelluksissa, sillä ne voivat luoda vanhentuvat salasanat automaattisesti uudelleen. Ominaisuudella voidaan välttyä heikoilta tai yksinkertaisilta salasanoilta ja estää salasanojen levittämistä. Ominaisuuden ansiosta käyttäjän ei tarvitse kirjautua useita kertoja käyttäessään suojattua tietoa, jolloin käyttöympäristöstä tulee turvallisempi ja käyttäjät käyttävät hakuja mielellään.
- **Tehtävien erottelu (Separation of duties, SoD).** Voi olla vaikeaa antaa käyttäjille eri rooleja hankkimatta lisää henkilökuntaa ja kasvattamatta kuluja. Tehtävien erottelu eli SoD on kehitetty estämään käyttäjiä suorittamasta mahdollisesti vaarallisia toimenpiteitä. Pieniä yrityksiä lukuun ottamatta samalla henkilöllä ei esimerkiksi ole yleensä käyttöoikeutta sekä tilivelkoihin että tilisaamisiin. Organisaationlaajuisessa hakuympäristössä käyttöoikeuksia myöntävän henkilön ei pitäisi olla sama henkilö, joka päättää, mitä kokoelmia käyttäjät saavat käyttää.
- **Roolipohjainen käyttöoikeuden hallinta.** Roolisuunnittelu voi olla työläs prosessi, mutta se voi saada aikaan turvallisemman käyttöympäristön. Oikeuksia annetaan kolmella eri tavalla — eksplisiittisesti, implisiittisesti ja perimällä. Voidaan määrittää sääntöjä, joilla estetään päällekkäisten roolien antaminen samalle käyttäjälle ja vahvistetaan luotuja SoD-käytäntöjä. Käyttäjien mahdollisuus suodattaa haku tiettyä roolia käyttämällä (vaikka heillä olisikin useita rooleja) mahdollistaa selkeämmät, mutta samalla turvalliset tulokset. Roolipohjainen käyttö liittyy suoraan SoD-ominaisuuteen. Kun käyttäjillä on tehtävien päällekkäisyyksiä ehkäisevät määritetyt roolit, näytetyt hakutulokset liittyvät suoraan siihen, mitä tietoja he tarvitsevat ja mitä tietoja he saavat käyttää.
- **Käyttöoikeuksien jakaminen/poistaminen.** Käyttöympäristön turvallisuutta voidaan lisätä keskitetyllä ja delegoidulla käyttäjähallinnalla, asiankäsitteilyllä, salasanahallinnalla ja roolipohjaisilla käyttöoikeuksien hallintamalleilla. Kaksinkertaisella tavoitteella varmistetaan, että uudet käyttäjät pääsevät heti käyttämään tarvitsemiaan tietoja

ja että käyttöoikeudet poistetaan mahdollisimman nopeasti käyttäjiltä, joilla ei enää ole niihin valtuuksia. Käyttöoikeuksien oikeanlainen jakaminen vaikuttaa suoraan rooleihin ja tehtävien erotteluun, vaikka se ei suoraan liitykään tietojen hakemiseen. Se on lähtökohta monille turvallisuusaloitteille.

Henkilöllisyyden ja käyttöoikeuksien hallinta ja hakukone

On saatavilla hakukoneita, joissa on johtavia henkilöllisyyden hallintaratkaisuja, jotka käyttävät lomakkeisiin perustuvaa käyttöoikeuksien tarkistusta ja SPI-varmennusta.

Ei ole vielä määritetty, miten useat hakukoneet integroituvat ei-Web-pohjaisiin SSO-järjestelmiin ja vanhastaan käytössä oleviin SSO-tyypisiin järjestelmiin. Monissa organisaatioissa käytetään monia turvajärjestelmiä eri muodoissa. Näitä ovat Web-pohjainen SSO, sisäinen SSO, LDAP (Lightweight Directory Access Protocol) sekä muut käyttäjänimi- ja salasanatietovarastot.

Hakuratkaisuihin kohdistuvat vaatimukset ovat eri organisaatioissa erilaisia, joten on tärkeää mitoittaa käyttöönnotto oikein. On mahdollista käyttää useita eri tekniikoita, kuten SPI-valtuutusta, mukautettuja ohjelmointirajapintoja ja sovittimia sekä hakukoneen lomakkeisiin perustuvia käyttöoikeuksien tarkistusmenetelmiä.

TURVALLISEN HAKUYMPÄRISTÖN LUOMINEN

Yrityshakuratkaisujen käyttöönoton yhteydessä on huomioitava uusia turvallisuuteen liittyviä vaatimuksia. Vaatimuksiin vastaaminen alusta alkaen kattavalla tietosuojamenetelmällä organisaatiot voivat hyödyntää hakuratkaisujen tarjoamat edut ja samaan aikaan suojata arkaluontoiset tietonsa.

Saat lisätietoja siitä, kuinka ratkaisumme voivat auttaa sinun yritystäsi [ottamalla meihin yhteyttä](#).

MAAILMANLAAJUISTA JOHTAMIS- JA TEKNOLOGIAKONSULTAATIOTA TÄMÄN PÄIVÄN LIIKETOIMINTAYMPÄRISTÖSSÄ

BearingPoint on maailman johtava maailmanlaajuinen johtamis- ja teknologiakonsultaatioyritys, joka tarjoaa palveluja Global 2000 -yrityksille ja useille maailman suurimmista julkispalveluorganisaatioista. Kokeneet ammattilaisemme auttavat yrityksiä ympäri maailman saavuttamaan tavoitteitaan ja luomaan yritysarvoa. Kohdentamalla asiakkaidemme liiketoimintaprosessit ja tietojärjestelmät autamme heitä saavuttamaan kilpailuetuja — tuottamalla tuloksia nopeasti. Jos haluat lisätietoja, soita numeroon +1 603 589 4089 tai vieraile Web-sivustossamme osoitteessa www.bearingpoint.com.

BearingPoint tarjoaa strategisia konsultaatio- ja sovelluspalveluja sekä teknologiaratkaisuja ja hallintapalveluita Global 2000 -yrityksille ja julkishallinnon organisaatioille.

BearingPoint

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

