Google-sovellusten tietoturva- ja suojausmenetelmät

Google-asiakirja, helmikuu 2007

Google-sovellusten tietoturva

LISÄTIETOJA

Verkossa www.google.com/a
Sähköposti apps-enterprise@google.com

Verkkopohjaisten sovellusten suojaaminen hyökkäysyrityksiltä on ensisijaisen tärkeää järjestelmän toimivuudelle. Suojaaminen on vielä tärkeämpää, kun kyseessä on sähköposti- tai yhteistyötoiminto. Google käyttää miljardeja dollareita tekniikkaan, henkilöstöön ja prosesseihin varmistaakseen sen, että Google-sovelluksiin tallennetut tiedot ovat turvassa. Googlen tietoturva-asiantuntijatiimi vastaa siitä, että turvallisuus otetaan huomioon suunnitteluvaiheesta lähtien. Suunnitelmat, ohjelmakoodi ja valmis tuote tarkastetaan sen varmistamiseksi, että tuote vastaa Googlen tiukkoja suojaus- ja tietosuojastandardeja. Samalla infrastruktuurilla, jolla ylläpidetään Google-sovelluksia ja suojataan satojentuhansien käyttäjien tiedot, hallitaan myös miljoonien kuluttajien tietoja ja miljardien mainoskuluja. Google-sovelluksissa tiedot ovat turvassa.

Johdanto

Osana pyrkimystään järjestää maailman tiedot ja saattaa ne avoimesti kaikkien saataville Google on vastuussa kymmenien miljoonien käyttäjien tietojen suojaamisesta. Tähän vastuuseen suhtaudutaan vakavasti, ja Google on tehnyt parhaansa ollakseen käyttäjien luottamuksen arvoinen. Google näkee turvalliset tuotteet keskeisinä käyttäjien luottamuksen ylläpitämisessä ja pyrkii kehittämään innovatiivisia tuotteita, jotka palvelevat käyttäjien tarpeita ja toimivat heidän parhaakseen.

Laaja-alainen kokemus auttaa turvallisten ja luotettavien Google-sovellusten toteuttamisessa. Googlen tuotteet ja palvelut yhdistävät pitkälle kehitettyjä teknisiä ratkaisuja alan johtaviin suojauskäytäntöihin, jotta asiakkaiden ja käyttäjien tiedot ovat turvassa. Mahdollisimman turvallisen ja luotettavan ympäristön luomiseen tiedoille ja sovelluksille investoidaan miljardeja dollareita. Google keskittyy erityisesti niihin turvallisuusnäkökohtiin, jotka ovat tärkeitä yritysasiakkaille:

- Organisaation ja toiminnan turvallisuus: Käytännöt ja menettelytavat, jotka varmistavat turvallisuuden jokaisessa suunnitteluun, käyttöönottoon ja toimintaan liittyvässä vaiheessa.
- Tietoturva: Sen varmistaminen, että asiakkaiden tiedot tallennetaan suojattuihin tiloihin, suojattuihin palvelimiin ja suojattuihin sovelluksiin.
- Uhkien välttäminen: Käyttäjien ja heidän tietojensa suojaaminen hyökkäyksiltä ja hakkereilta.
- Turvallinen käyttö: Sen varmistaminen, että vain valtuutetut henkilöt pääsevät käsiksi tietoihin ja että käyttökanava on turvallinen.
- Tietosuoja: Luottamuksellisen tiedon turvaaminen ja salassapito.

Tämä asiakirja kuvaa Googlen turvallisuusstrategiaa, johon kuuluu useita fyysisiä, loogisia ja toiminnallisia suojaustapoja mahdollisimman tehokkaan tietoturvan ja yksityisyyden suojan takaamiseen.

Organisaation ja toiminnan turvallisuus

Googlen turvallisuusstrategia lähtee ihmisistä ja prosesseista. Turvallisuus on ihmisten, prosessien ja tekniikan yhdistelmä, joka oikein koottuna tekee tietokoneen käytöstä suojattua ja vastuullista. Turvallisuus ei ole asia, joka voidaan arvioida jälkikäteen. Se täytyy suunnitella osaksi tuotetta, arkkitehtuuria, infrastruktuuria ja järjestelmiä alusta alkaen. Googlella on suojaustiimi, joka kehittää, dokumentoi ja toteuttaa kattavia tietoturvakäytäntöjä. Tiimissä on maailman parhaita tietojärjestelmien, sovellusten ja verkkojen turvallisuuden asiantuntijoita.

Suojaustiimi on jaettu ulkoisen suojauksen, infrastruktuurin suojauksen, sovellusten suojauksen ja haavoittuvuuksien havaitsemisen toiminta-alueisiin. Ennen Googlea monet asiantuntijoistamme ovat työskennelleet vaativissa tietoturvatehtävissä Fortune 500 -yrityksissä. Tiimi keskittyy ennaltaehkäisyyn sen varmistamiseksi, että ohjelmakoodi ja järjestelmät ovat turvallisia alusta alkaen, ja ryhmällä on valmius reagoida turvallisuusongelmiin nopeasti.

.

Kehitysmetodologia
Google huomioi turvallisuuden tuotteen suunnitteluvaiheesta lähtien. Yrityksen suunnittelu- ja tuotetiimeillä on perusteellinen tietoturvakoulutus. Googlen kehitysmetodologia koostuu useista vaiheista, joissa suoritetaan tarkistuksia ja valvontaa.

Googlen suojaustiimi on mukana kaikissa tuotekehityksen vaiheissa suunnittelusta, koodin tarkistuksesta, järjestelmä- ja toimintatestauksesta tuotteen lopulliseen hyväksyntään. Google käyttää useita kaupallisia ja itse kehittämiään tekniikoita takaamaan sovellusten turvallisuuden kaikilla tasoilla. Tiimin vastuulla on myös sen varmistaminen, että tietoturva huomioidaan kehitysprosesseissa asiakkaan tietojen suojaamiseksi.

Toiminnan turvallisuus
Googlen tietoturvatiimin tehtävä on toimintajärjestelmien, kuten tietojenkäsittelyn ja järjestelmänhallinnan, turvallisuuden ylläpitäminen. Tiimin jäsenet tarkistavat säännöllisesti tietokeskusten toiminnan ja arvioivat Googlen fyysisiin ja loogisiin resursseihin kohdistuvien uhkien mahdollisuutta.

Ryhmä vastaa myös siitä, että kaikki työntekijät arvioidaan ja koulutetaan tekemään työnsä asiantuntevasti ja turvallisuutta noudattaen. Google tarkistaa jokaisen työntekijän taustan ennen palkkaamista. Tietoturvaprosesseista ja -menettelyistä vastaavalla henkilöstöllä on perusteellinen koulutus, jota päivitetään jatkuvasti.

Tietoturvayhteisö ja neuvonantajat
Yllä mainittujen prosessien lisäksi Google työskentelee aktiivisesti tietoturvayhteisön osana, ja voi siten hyödyntää parhaiden asiantuntijoiden kokoamaa tietoa. Tämä auttaa Googlea ennakoimaan turvallisuuteen liittyviä suuntauksia, reagoimaan nopeasti uhkiin ja hyödyntämään sekä yrityksen sisäistä että ulkopuolisten tahojen asiantuntemusta. Google toimii aktiivisesti ja vastuullisesti tietoturvayhteisön jäsenenä. Osoitteessa **http://www.google.com/corporate/security.html** on lisätietoja ohjelmasta ja asiantuntijoista, joiden kanssa Google tekee yhteistyötä.

Uusia suojausongelmia saattaa ilmetä kaikista turvatoimenpiteistä huolimatta, ja Googlella on valmiudet reagoida nopeasti hälytyksiin ja haavoittuvuuksiin. Googlen suojaustiimi tarkistaa infrastruktuurin mahdollisten suojausongelmien varalta, ja korjaa tunnetut ongelmat suunnittelutiimin kanssa välittömästi. Google-sovellusten premium-versiota käyttäville asiakkaille ilmoitetaan käyttäjiin vaikuttavista tietoturvaongelmista sähköpostitse mahdollisimman pian.

Tietoturva
Googlen suojaus- ja tietoturvatiimien pyrkimyksenä on yritysten ja käyttäjien tietojen suojaaminen. Googlen liiketoiminta perustuu käyttäjien luottamukseen, ja siksi luottamus on avainasemassa koko yrityksen menestyksessä. Kaikki Googlen työntekijät ymmärtävät olevansa vastuussa käyttäjille. Tietojen turvaaminen on Googlelle ensisijaisen tärkeää. Yrityksen vastuulla on turvata miljardien dollarien arvosta kuluttajien ja mainostajien toimintaa. Suojaamme viestintä- ja yhteistyötekniikat yhtä tehokkaasti.

Tämä on yrityksellemme ensisijaisen tärkeää, se näkyy myös toimintaohjeissamme, jotka ovat osoitteessa **http://investor.google.com/conduct.html.**

Fyysinen turvallisuus
Googlella on käytössään yksi maailman laajimmista hajautetuista tietokeskusverkoista, ja yritys tekee parhaansa turvatakseen keskusten sisältämät tiedot ja aineettoman omaisuuden. Tietokeskukset toimivat eri puolilla maailmaa. Monet niistä ovat yksinomaan Googlen omistuksessa ja hallinnassa, mikä varmistaa sen, etteivät ulkopuoliset tahot pääse keskuksiin. Tietokeskusten maantieteelliset sijainnit on valittu niin, että keskukset ovat suojassa katastrofeilta. Vain harvoilla Googlen työntekijöillä on pääsy tietokeskuksiin ja oikeus käyttää niiden palvelimia, ja tätä rajoitusta valvotaan tarkasti. Turvallisuutta valvotaan ja hallitaan paikallisesti tietokeskuksessa ja keskitetysti Googlen maailmanlaajuisista valvontakeskuksista.

Toimipaikat on suunniteltu mahdollisimman tehokkaiksi, turvallisiksi ja luotettaviksi. Monitasoinen vikasietoisuus varmistaa käytön jatkumisen ja palveluiden saatavuuden myös hankalimmissa tilanteissa. Se koostuu keskuksen monitasoisesta vikasietoisuudesta, generaattorilla ylläpidettävästä toimintojen varmuuskopioinnista ja täydellisestä vikasietoisuudesta useiden keskusten välillä. Keskusten paikallisessa ja etähallinnassa käytetään huipputason valvontaa. Käytössä on myös automaattinen varmistusjärjestelmä.

Looginen turvallisuus
Verkkopohjaisessa tietojenkäsittelyssä tietojen ja sovellusten looginen turvallisuus on yhtä tärkeää kuin fyysinen turvallisuus. Google tekee parhaansa varmistaakseen, että sovellukset ovat suojattuja, tietoja käsitellään turvallisuutta noudattaen ja vastuullisesti, ja että asiakkaiden tai käyttäjien tietoja ei voida käyttää luvatta. Tämän saavuttamiseksi Google käyttää alan standardeihin perustuvia tekniikoita ja innovatiivisia ratkaisuja. Yksi näistä ratkaisuista on hyödyntää tiettyä käyttötarkoitusta varten suunniteltua tekniikkaa, jota käytetään yleiskäyttöön tarkoitettujen ohjelmistojen sijaan.

Suuri osa Googlen tekniikasta on suunniteltu juuri tiettyä käyttötarkoitusta varten. Esimerkiksi verkkopalvelintaso on suunniteltu ja toteutettu niin, että vain tiettyjen sovellusten tarvitsemat toiminnot ovat käytettävissä. Siksi siinä on vähemmän suojausongelmia kuin monessa vastaavassa kaupallisessa ohjelmistossa.

Google on tehnyt turvallisuussyistä muutoksia myös moniin ydinkirjastoihin. Koska Googlen infrastruktuuri koostuu erillisistä sovelluksista eikä ole yleiskäyttöön suunniteltu laitealusta, monia tavallisen Linux-käyttöjärjestelmän tarjoamista palveluista voidaan rajoittaa tai poistaa käytöstä. Nämä muutokset tähtäävät järjestelmän tehon parantamiseen haluttuja toimintoja varten ja tarpeettomien heikkouksien poistamiseen järjestelmästä.

Googlen palvelimet on suojattu hyökkäyksiltä myös useilla palomuuritasoilla. Liikennettä tarkkaillaan mahdollisten hyökkäysyritysten varalta, ja hyökkäyksiin reagoidaan käyttäjien tietojen suojaamiseksi.

Tietojen saatavuus
Tiedot, kuten esimerkiksi sähköpostiviestit, tallennetaan suorituskykyä varten optimoidussa koodimuodossa sen sijaan, että ne tallennettaisiin perinteiseen kansiojärjestelmään tai tietokantaan. Tiedot jaetaan useisiin fyysisiin ja loogisiin tallennuspaikkoihin vikasietoisuuden ja nopean käytön varmistamiseksi. Siksi tietoja ei voi peukaloida. Googlen palvelimien fyysinen suojaus varmistaa, ettei niihin voi päästä käsiksi. Henkilöstö käyttää tuotantojärjestelmiä salatulla SSH-yhteydellä (secure shell). Käyttäjätietoihin pääseminen edellyttäisi tietorakenteiden ja Googlen kehittämän infrastruktuurin tarkkaa tuntemusta. Tämä on yksi suojauksen taso, joka turvaa Google-sovelluksiin tallennetut henkilökohtaiset tiedot.

Googlen hajautettu arkkitehtuuri on suunniteltu turvallisemmaksi ja luotettavammaksi kuin perinteinen arkkitehtuuri. Yksittäisten käyttäjien tiedot on hajautettu useisiin anonyymeihin palvelimiin, ryppäisiin ja tietokeskuksiin. Tämä varmistaa, etteivät tiedot katoa, ja turvaa ne luvattomalta käytöltä.

Käyttäjätiedot ovat saatavilla vain asianmukaisilla kirjautumisoikeuksilla. Näin asiakas ei voi nähdä toisen asiakkaan tietoja ilman tarkkoja kirjautumistietoja. Tämä testattu järjestelmä tarjoaa miljoonille käyttäjille päivittäiset sähköposti-, kalenteri- ja asiakirjapalvelut. Sen lisäksi se toimii yli 10 000 Googlen työntekijän ensisijaisena laiteympäristönä.

Vikasietoisuus
Googlen käyttämä sovellus- ja verkkoarkkitehtuuri on suunniteltu mahdollisimman luotettavaksi ja toimivaksi. Googlen ritilärakenteinen tietojenkäsittelyalusta on valmiudessa laiterikon varalta, ja vahva ohjelmistopohjainen varmistusjärjestelmä kestää häiriöt. Kaikkien Googlen järjestelmien rakenne on vikasietoinen, eikä mikään alijärjestelmä ole riippuvainen tietystä fyysisestä tai loogisesta palvelimesta toiminnon suorittamiseksi.

Tiedot kopioidaan useisiin Googlen aktiivisiin palvelinryppäisiin, jotta laiterikon sattuessa tiedot ovat edelleen saatavilla toisen järjestelmän kautta. Myös käyttäjätiedot kopioidaan useisiin tietokeskuksiin. Jos kokonaisen tietokeskuksen toiminta pysähtyy tai sen läheisyydessä tapahtuu onnettomuus, toinen tietokeskus pystyy välittömästi ottamaan toiminnan hallintaansa ja tarjoamaan palvelut käyttäjille.

Uhkien välttäminen
Sähköpostivirukset, verkkourkinta ja roskaposti ovat suurimpia turvallisuusuhkia tämän päivän yrityksissä. Raporttien mukaan yli kaksi kolmasosaa saapuvasta sähköpostista on roskapostia, ja uusia sähköpostiviruksia syntyy ja leviää Internetissä päivittäin. Tilanteen tasalla pysyminen voi vaikuttaa mahdottomalta tehtävältä. Niilläkin yrityksillä, joilla on roskaposti- ja virustorjunta käytössä, on vaikeuksia pitää torjunta uusimpien uhkien tasalla. Verkkopohjaiset sovellukset ovat usein hyökkäysten kohteena, joissa niiden tietoja yritetään muuttaa tai palvelun toiminta pyritään estämään. Googlen huippuluokan välineet uhkien estoon suojaavat käyttäjiä tietoihin sekä viestien ja tiedostojen sisältöön kohdistuvilta hyökkäyksiltä

Roskaposti- ja virussuojaus
Google-sovellusten käyttäjät saavat käyttöönsä alan parhaat roskaposti- ja verkkourkintasuodattimet. Google on suunnitellut pitkälle kehitetyt suodattimet, jotka oppivat roskapostiksi tunnistettujen viestien lähetystavat. Nämä suodattimet oppivat jatkuvasti lisää miljardeista uusista sähköpostiviesteistä. Tästä syystä Google tunnistaa roskapostin, verkkourkintahyökkäykset ja virukset erittäin tarkasti ja pystyy varmistamaan sen, että käyttäjien postilaatikot, kalenterit ja asiakirjat ovat turvassa.

Googlen verkkopohjaisen käyttöliittymän virustorjunta estää käyttäjien tietämättään levittämien virusten leviämisen yrityksessä tai sisäisessä verkossa. Perinteisistä asiakaspohjaisista sähköpostiohjelmista poiketen viestejä ei ladata työpöydälle. Sen sijaan ne tarkistetaan palvelimella virusten varalta, eikä Gmail anna käyttäjän avata liitetiedostoa, ennen kuin se on tarkistettu ja mahdolliset uhat on poistettu. Tämän ansiosta sähköpostivirukset eivät voi käyttää asiakasohjelman suojausongelmia hyväkseen, eivätkä käyttäjät pysty vahingossa avaamaan viruksen sisältäviä asiakirjoja.

Sovellus- ja verkkohyökkäykset
Sen lisäksi, että Google suodattaa sisällön roskapostin ja virusten varalta, Google suojaa sekä itsensä että asiakkaansa vihamielisiltä hyökkäyksiltä. Hakkerit yrittävät jatkuvasti etsiä tapoja, joilla he voisivat tunkeutua verkkopohjaisiin sovelluksiin tai kaataa niitä. Palvelunestohyökkäykset, huijausosoitteet, haitalliset HTML-syötteet ja syöttötietojen peukalointi ovat eräitä hyökkäystyyppejä, joita verkoissa ilmenee päivittäin. Google. joka on yksi maailman suurimmista

verkkopohjaisten palveluiden tuottajista, on pyrkinyt suojautumaan tällaisilta uhkilta monin tavoin. Kaikki ohjelmistot tutkitaan erilaisilla kaupallisilla ja yrityksen omilla verkkojen ja sovellusten tarkistusohjelmilla. Googlen suojaustiimi työskentelee myös ulkopuolisten tahojen kanssa Googlen infrastruktuurin ja sovellusten turvatason testaamiseksi ja parantamiseksi.

Turvallinen käyttö
Vaikka tiedot olisivat turvassa tietokeskuksessa, käyttäjän tietokoneelle ladattuna niistä tulee haavoittuvia. Tutkimuksissa on todettu, että kannettavassa tietokoneessa on keskimäärin yli 10 000 tiedostoa ja tuhansia ladattuja sähköpostiviestejä. Kuvittele, mitä tapahtuisi, jos yksi yrityksen kannettavista tietokoneista päätyisi vääriin käsiin. Lisäämällä verkkolevyn luvaton käyttäjä pääsisi käsiksi yrityksesi aineettomaan omaisuuteen ja yrityssalaisuuksiin. Google-sovelluksia käyttävät yritykset voivat pienentää tätä riskiä vähentämällä tarvetta tallentaa tietoja käyttäjien kannettaviin koneisiin.

Käyttäjien suojaaminen
Google-sovellusten verkkopohjainen arkkitehtuuri auttaa varmistamaan sen, että käyttäjät saavat aina käyttöönsä tarvitsemansa tiedot, jotka myös pysyvät turvassa Googlen palvelimissa. Sen sijaan, että sähköposteja tallennettaisiin kannettavaan tietokoneeseen tai pöytäkoneeseen, käyttäjillä on työpöytäsovelluksen tasoinen selainpohjainen käyttöliittymä sähköpostin, kalenterin ja pikaviestien käyttöön.

Google-dokumentit-sovellus antaa käyttäjille laajat valtuudet hallita tietoja. Asiakirjat pysyvät palvelimella, mutta käyttäjät voivat muokata niitä selaimen kautta. Sen lisäksi käyttäjät voivat hallita asiakirjojen käyttöoikeuksia ja luoda luettelon käyttäjistä, jotka saavat muokata tai tarkastella niitä. Oikeudet tarkistetaan aina, kun asiakirjaa käytetään. Näin estetään sisäisen asiakirjan lähettäminen sähköpostitse yrityksen ulkopuolelle. Tuotteilla voi seurata tarkasti asiakirjojen muutoksia ja sitä, kuka teki viimeisimmät muutokset ja minä ajankohtana.

Google-sovellukset suojaavat tietojen lähettämistä myös kiinteässä verkossa sen varmistamiseksi, että käyttäjät voivat käyttää tietoja turvallisesti ilman uhkaa luottamuksellisten tietojen sieppaamisesta. Google-sovellusten verkkopohjaista hallintakonsolia ja useimpia käyttäjäsovelluksia voidaan käyttää SSL-yhteyden kautta. Useimpia Google-sovelluksia on mahdollista käyttää HTTPS-yhteydellä, ja tuote voidaan määrittää hyväksymään vain HTTPS-yhteydet tärkeimpiin sovelluksiin, kuten sähköpostiin ja kalenteriin. Tätä toiminnallisuutta käytettäessä kaikki tietojen käyttö ja liikenne salataan.

Google ei koskaan käytä evästeitä salasanojen tai asiakastietojen tallentamisessa asiakkaan järjestelmään. Evästeitä käytetään istuntojen tietoihin ja käytön helpottamiseen, mutta niiden tallentamat tiedot eivät koskaan ole luottamuksellisia, eikä evästeillä voi murtautua käyttäjätileihin.

Oma hallinta
Yllä mainittujen suojausten lisäksi yritykset voivat integroida Google-sovelluksiin yritysturvallisuus-, käyttö-, tarkistus- ja varmennusmenetelmiä. Google-sovelluksissa on SAML 2.0-versioon perustuva kertakirjautumisen sovellusliittymä, jonka avulla yritykset voivat käyttää olemassa olevia varmennusmekanismejaan Google-sovelluksissa. Yritykset voivat käyttää esimerkiksi Active Directory -varmennusta, jolloin käyttäjien kirjautumistietoja ei lähetetä Googlen palvelimien kautta verkkopohjaisia työkaluja käytettäessä. Näin yritykset voivat pitää olemassa olevat käytäntönsä salasanan vahvuuteen ja vaihtoväliin liittyen.

Tuotteessa on myös hallintakonsoli ja sovellusliittymä käyttäjien hallintaa varten. Järjestelmänvalvojat voivat lopettaa tietyn tilin käytön välittömästi tai poistaa tilin tarvittaessa. Nämä toiminnot voidaan myös sitoa sisäisiin prosesseihin, joilla määritetään käyttäjien lisääminen ja poistaminen sovellusliittymän avulla.

Sähköpostia ja pikaviestintää varten on mahdollista sijoittaa sähköpostiyhdyskäytävä sähköpostijärjestelmän eteen. Näin kaikki saapuvat ja lähtevät sähköpostiviestit kulkevat asiakkaan järjestelmän kautta, jotta viestit voidaan tarkistaa ja arkistoida sekä lisätä valvontaa.

Tietosuoja

Google suhtautuu vakavasti yritysten ja käyttäjien tietosuojaan, ja ymmärtää, että sovelluksiin tallennettu tieto on luottamuksellista ja henkilökohtaista. Google-sovelluksissa tiedot ovat turvassa. Googlen juridisesti sitova tietosuojakäytäntö, joka koskee kaikkia palveluita, on osoitteessa **http://www.google.com/privacypolicy.html**. Tämän käytännön ja muiden Google-sovelluksiin kuuluvien palveluiden käytäntöjen mukaisesti Googlen työntekijät eivät koskaan käsittele luottamuksellisia käyttäjätietoja. Google takaa myös sen, ettei tätä käytäntöä muuteta mahdollisesti vahingolliseen suuntaan ilman asiakkaan ja/tai käyttäjän erillistä kirjallista suostumusta.

Yhteenveto

Google-sovellukset ovat turvallinen ja luotettava ympäristö tiedoillesi. Ne käyttävät viimeisintä tekniikkaa ja parhaita käytäntöjä tietokeskusten hallinnassa, verkkosovellusten turvallisuudessa ja tietojen koskemattomuuden takaamisessa. Kun tallennat yrityksesi tiedot Googlen sovelluksiin, voit luottaa siihen, että Googlen investoinnit tekniikkaan ja infrastruktuuriin takaavat tietojesi turvallisuuden, yksityisyyden suojan ja koskemattomuuden.

Lisätietoja Google-sovelluksista saat osoitteesta **http://www.google.com/a** tai lähettämällä sähköpostia osoitteeseen **apps-enterprise@google.com.**