Omfattande granskning av säkerhet och skydd mot säkerhetsbrister för Google Apps

Ett Google-policydokument, februari 2007

Säkerhet för Google Apps

OM DU BEHÖVER MER INFORMATION:

Online www.google.com/a
E-post apps-enterprise@google.com

Säkring av nätverksbaserade program mot hackare är oumbärligt för att systemets ska fungera väl. När det gäller e-post och samarbete är det ytterst viktigt. Google investerar miljarder dollar i teknik, personal och processer för att försäkra sig om att data i Google Apps är säkra och privata. Googles hängivna team av säkerhetsproffs ansvarar för planering med säkerhet i åtanke från första början, granska all design, kod och den färdiga produkten för att garantera att den uppfyller Googles strikta standard för säkerhet och datasekretess. Samma infrastruktur som används för Google Apps och som skyddar hundratusentals användares data används även för att hantera miljoner konsumenters data och miljarder dollar i annonseringstransaktioner. Med Google Apps är informationen säker.

Inledning

I enlighet med vår målsättning att organisera världens information ansvarar Google för att skydda information för miljontals enskilda användare. Vi ser mycket allvarligt på detta ansvar och vi har arbetat hårt för att förtjäna och behålla våra användares och kunders förtroende. På Google vet vi att säkra produkter är ytterst viktigt när det gäller att behålla användarnas förtroende och vi strävar efter att skapa innovativa produkter som tjänar användarnas syften och fungerar som de önskar.

Google Apps drar nytta av denna omfattande driftserfarenhet genom att producera säkra och tillförlitliga produkter. Googles produkter och tjänster kombinerar avancerade tekniklösningar med branschledande säkerhetsrutiner för att försäkra att kunder och användardata är säkra. Miljarder dollar i kapital har investerats för att garantera den mest säkra, tillförlitliga miljön för data och program. Google fokuserar speciellt på flera säkerhetsaspekter som är mycket viktiga för affärskunder:

- Organisations- och driftsäkerhet – policy och procedurer för att garantera säkerhet i varje fas under design, införande och pågående verksamhet.
- Datasäkerhet – garanterar att kundens data sparas i säkra lokaler, på säkra servrar och i säkra program.
- Hotavvärjning – skyddar våra användare och deras information från fientliga attacker och hackare.
- Säker åtkomst – garanterar att endast behöriga användare kan komma åt data och att åtkomstkanalen är säker.
- Datasekretess – garanterar att konfidentiell information hålls privat och konfidentiell

Det här dokumentet beskriver Googles säkerhetsstrategi, som består av flera fysiska, logiska och driftsmässiga säkerhetsåtgärder i avsikt att garantera bästa möjliga datasäkerhet och sekretess.

Organisations- och driftsäkerhet

Grunden för Googles säkerhetsstrategi börjar med företagets personal och processer. Säkerhet är en kombination av personal, processer och teknik, som när det kombineras korrekt ger en säker och ansvarig datoranvändning. Säkerhet är inte något som helt enkelt kan läggas till i efterhand. Det är snarare något som ingår i designen av produkterna, arkitekturen, infrastrukturen och systemen, ända från början. Google har ett heltidsarbetande säkerhetsteam som arbetar med att utveckla, dokumentera och genomföra omfattande säkerhetspolicyn. Googles säkerhetsteam består av några av världens främsta experter inom säkerhet för information, program och nätverk.

Säkerhetsteamet är indelat i funktionsområden som inriktar sig på perimeterskydd, infrastrukturskydd, programskydd och på att upptäcka och åtgärda säkerhetsbrister. Många kommer till Google med erfarenhet från ledande befattningar inom informationssäkerhet hos Fortune 500-företag. Detta team satsar en stor del av sitt arbete på förebyggande åtgärder för att garantera att programkoden och systemen är säkra från början och de är beredda på att omedelbart ta itu med eventuella säkerhetsfrågor som kan uppstå.

.

Utvecklingsmetoder
Från första början när en produkt börjar planeras prioriteras säkerheten hos Google. Googles utvecklingspersonal och produktteam får omfattande utbildning i säkerhetsfrågor. Googles utvecklingsmetoder bygger på en plan i flera steg, med bestämda kontrollpunkter och kompletta granskningar.

Googles programsäkerhetsteam är inblandat i alla stadier i produktutvecklingens livscykel, inklusive designgenomgång, kodgranskning, systemtestning och funktionstestning samt det slutliga lanseringsgodkännandet. Google använder ett antal kommersiella och patentskyddade Google-metoder för att garantera att programmen är säkra på varje nivå. Googles programsäkerhetsteam ansvarar även för att säkra utvecklingsprocesser följs för att garantera kundernas säkerhet.

Driftsäkerhet
Googles säkerhetsgrupp inriktar sig på att upprätthålla säkerheten för systemen, inklusive databehandling och systemhantering. Dessa personer granskar rutinmässigt funktionen i datacentren och genomför fortgående hotanalyser mot Googles fysiska och logiska tillgångar.

Denna grupp ansvarar även för att garantera att alla anställdas bakgrund har undersökts ordentligt och att de utbildats så att de kommer att utföra sitt jobb på ett professionellt och säkert sätt. Google utför vid behov noggranna bakgrundsundersökningar för att verifiera en persons bakgrund innan han/hon tillåts att arbeta inom organisationen. All personal som ansvarar för underhåll av säkerhetsprocesser och säkerhetsprocedurer ges en grundlig utbildning när det gäller säkerhetsprinciper och deras utbildning påbyggs kontinuerligt.

Säkerhetsföretag och rådgivare
Utöver de processer som beskrivs ovan arbetar Google aktivt tillsammans med säkerhetsföretag för att kunna dra nytta av den sammantagna kunskapen hos världens bästa och smartaste. Det hjälper Google att ligga före på säkerhetsfronten och snabbt reagera på nya hot, samt att få ut det mesta av den expertis som finns både inom och utanför företaget. Google deltar aktivt i denna större säkerhetsgrupp genom ansvarskännande säkerhetsavslöjanden. Besök **http://www.google.com/corporate/security.html** om du vill få mer information om detta program och några av de viktiga säkerhetsexperter som Google för en fortgående dialog med.

Även med alla dessa skyddsnivåer kan okända säkerhetsluckor uppstå och Google har den kapacitet som krävs för att snabbt åtgärda de säkerhetsvarningar och säkerhetsluckor som rapporteras. Googles säkerhetsteam granskar all infrastruktur för potentiella säkerhetsluckor och arbetar direkt med teknikerna för att omedelbart korrigera alla kända problem. Kunderna för Google Apps Premierutgåva meddelas per e-post så snart som praktiskt möjligt vid säkerhetsproblem som påverkar användarna.

Datasäkerhet
Säkerheten för företagets och användarnas data är A och O för Googles säkerhetsgrupp. Googles affärer bygger på användarens förtroende och det är därför en av de viktigaste punkterna för Googles fortsatta framgång som företag. Alla anställda inom Google ingjuts med en känsla av ansvar gentemot slutanvändaren. Att skydda data är kärnan av vad Google sysslar med. Google är mycket noga med att skydda de transaktioner där kunder och annonsörer betalar miljarder dollar, och vi är lika noga med vår egen teknik för kommunikation och samarbete.

Du kan se att detta är mycket viktigt för oss som företag om du läser vår uppförandekodex på adressen **http://investor.google.com/conduct.html**.

Fysisk säkerhet
Google driver ett av världens största nätverk över utspridda datacenter och lägger ned mycket arbete på att skydda alla data och immateriella tillgångar i dessa center. Google driver datacenter över hela världen och många av Googles datacenter är helägda och drivs enbart av Google, vilket garanterar att inga utomstående kan få tillgång till någon information. Läget för dessa datacenter har valts utifrån principen bästa skydd mot katastrofer. Endast vissa utvalda anställda inom Google har tillgång till lokalerna för dessa datacenter och de servrar som finns där, och denna åtkomst är noggrant kontrollerad och övervakad. Säkerheten övervakas och kontrolleras både lokalt på platsen och centralt i Googles internationella säkerhetscenter.

Själva anläggningen har planerats inte bara för maximal effektivitet utan även med säkerhet och pålitlighet i åtanke. Flera nivåer av redundans garanterar fortgående drift och tillgänglighet även under de mest krävande och extrema förhållandena. Detta inkluderar flera nivåer av redundans inom ett center, generatordriven strömförsörjning för fortsatt drift och full redundans över flera utspridda center. Ytterst avancerade kontroller används för att sköta dessa center både lokalt och genom fjärranslutning, och det finns automatiserade reservsystem för att garantera systemens funktion.

Logisk säkerhet
Inom webbaserad datoranvändning är den logiska säkerheten för data och program lika viktig som den fysiska säkerheten. Google arbetar ytterst noggrant med att garantera att programmen är säkra, att data hanteras på ett säkert och ansvarsfullt sätt samt att det inte finns någon möjlighet till obehörig dataåtkomst. För att uppnå detta mål använder Google ett antal standardtekniker såväl som några egna, innovativa metoder. En sådan metod är utnyttjandet av specialutvecklad teknik i stället för allmän programvara.

Mycket av Googles teknik har utvecklats för funktioner med ett visst syfte i motsats till en mer allmän datoranvändning. Webbserverlagret har t.ex. specialutvecklats av Google för att endast använda de funktioner som krävs för användningen av specifika program. Därför är det inte så känsligt för den stora mängd attacker som de flesta kommersiella programlösningar kan utsättas för.

Google har även av säkerhetsskäl utfört ändringar i kärnbiblioteket. Eftersom Googles infrastruktur är ett särskilt programsystem snarare än en allmän datoranvändningsplattform kan ett antal tjänster som återfinns i ett normalt Linux-operativsystem vara begränsade eller inaktiverade. Dessa ändringar inriktar sig på att förbättra den funktion i systemet som krävs för den uppgift som ska utföras och inaktivering eller avlägsnande av de aspekter av systemet som inte krävs och som skulle kunna utgöra en säkerhetsrisk.

Googles servrar skyddas även på flera nivåer av brandväggar som skyddar mot attacker. Trafiken inspekteras för att upptäcka försök till attacker och åtgärda alla försök för att skydda användarnas data.

Informationstillgänglighet
Data, som t.ex. e-post, sparas i ett kodat format är optimerat för prestandan, snarare än att de sparas i ett vanligt filsystem eller i en vanlig databas. Data fördelas över ett antal fysiska och logiska volymer för redundans och snabb åtkomst, vilket gör det svårare för obehöriga att ändra dessa data. Googles fysiska skydd som beskrivs ovan garanterar att det inte finns någon möjlighet till fysisk åtkomst till servrarna. All åtkomst till produktionssystem utförs av personal via kryptering med SSH (secure shell). Specialiserad kunskap om datastrukturen och Googles egna infrastruktur krävs för att kunna få meningsfull åtkomst till slutanvändarens data. Detta är ett av många säkerhetslager som garanterar säkerheten för känsliga data inom Google Apps.

Googles distribuerade arkitektur har skapats för att ge en högre säkerhetsnivå och större tillförlitlighet än en traditionell enkel arkitektur. Enskilda användares data fördelas över ett antal anonyma servrar, klustrar och datacenter. Det garanterar att data inte bara skyddas mot potentiell förlust utan det är även ett mycket säkert system.

Användarnas data kan endast nås med korrekta inloggningsuppgifter, vilket garanterar att det inte finns någon möjlighet till att en kund får tillgång till någon annan kunds data utan uttrycklig kännedom om den kundens inloggningsinformation. Detta beprövade system utnyttjas inte bara av de miljoner konsumenter som dagligen använder e-post, kalendertjänster och dokument utan det används även av Google som den huvudsakliga plattformen för företagets mer än 10 000 anställda.

Redundans
Program- och nätverksarkitekturen som Google använder sig av är utformad för maximal pålitlighet och drifttid. Googles nätbaserade datoranvändningsplattform räknar med maskinvarufel och därför används reservsystem för att förhindra avbrott. Alla Google-system är helt redundanta i sin utformning, och varje undersystem är oberoende av särskilda fysiska eller logiska servrar för att kunna fungera.

Data kopieras flera gånger över Googles grupperade aktiva servrar, vilket innebär att data fortfarande kommer att vara tillgängliga via något annat system om det skulle inträffa något maskinvarufel någonstans. Dessutom kopieras användardata mellan olika datacenter. Det innebär att om ett helt datacenter skulle sluta att fungera av något skäl skulle ett annat datacenter omedelbart kunna ta över och förmedla tjänsterna till användarna.

Hotavvärjning
E-postvirus, nätfiskeattacker och skräppost är några av dagens största säkerhetsrisker inom företag. Rapporter visar att mer än två tredjedelar av den inkommande e-posten är skräppost och nya e-postvirus skapas och distribueras över Internet varje dag. Det kan vara en överväldigande uppgift att värja sig mot detta och även företag med filter mot skräppost och virus har svårt att ständigt hålla dessa uppdaterade för att hantera de senaste säkerhetsriskerna. Dessutom är nätverksbaserade program mål för fientliga attacker som försöker att ändra data eller stoppa tjänsten helt. Googles förstklassiga hotavvärjning skyddar användarna från attacker på informationen och på innehållet i meddelanden och filer.

Skydd mot skräppost och virus
Kunderna för Google Apps kan dra fördel av ett av de bästa filtren för skräppost och nätfiske som finns idag. Google har utvecklat avancerade teknikfilter som lär sig mönster i meddelanden som identifierats som skräppost, och dessa filter används kontinuerligt för miljarder e-postmeddelanden. Detta innebär att Google korrekt kan identifiera skräppost, lösenordsfiske och virus, samt säkerställa att användarnas inkorgar, kalendrar och dokument är skyddade.

Genom Googles webbaserade gränssnitt blockerar virusskyddet möjligheten att användarna ovetande kan sprida ett virus genom företaget eller ett internt nätverk. Till skillnad från klientbaserade e-postprogram hämtas inte alla meddelanden till själva datorn. I stället skannas de på servern efter virus och Gmail kommer inte tillåta att användaren öppnar en bilaga innan den har skannats och alla eventuella hot har undanröjts. Detta innebär att e-postvirus inte kan dra nytta av säkerhetsluckor hos klienten och användarna kan inte ovetande öppna dokument som innehåller virus.

Attacker på program och nätverk
Förutom att filtrera datainnehåll från skräppost och virus arbetar Google ständigt för att skydda sig och kunderna mot fientliga attacker. Hackare letar alltid efter olika sätt att ta sig in i webbaserade program eller att stoppa dem. Blockeringsangrepp, IP-kapning, felhänvisande skriptlänkning och paketmanipulation är bara några typer av attacker som sker på nätverk varje dag. Google, som är en av världens största leverantörer

av webbaserade tjänster, har vidtagit långtgående åtgärder för att skydda sig mot sådana hot och andra hot. All programvara genomsöks med ett flertal olika kommersiella lösningar och egna lösningar för genomsökning av nätverk och program. Googles säkerhetsteam arbetar även med externa parter för att ständigt testa och förbättra säkerheten för Googles infrastruktur och program.

Säker åtkomst

Oavsett hur säkra data är inom ett datacenter blir dessa data utsatta så snart som de har hämtats till en användares lokala dator. Studier har visat att den genomsnittliga bärbara datorn har mer än 10 000 filer och tusentals hämtade e-postmeddelanden. Tänk dig vad som skulle hända om någon av dessa företagsdatorer skulle hamna i händerna på en fientlig användare. Genom att helt enkelt montera en disk kan en obehörig användare få åtkomst till ditt företags immateriella tillgångar och hemligheter. Med Google Apps kan företagen minska denna risk genom att undvika lokal lagring av data på användarnas bärbara datorer.

Skydd för slutanvändarna

Genom den webbaserade designen för Google Apps ges användarna direkt åtkomst till sin information var de än befinner sig, samtidigt som informationen är säker på Googles servrar. Snarare än att e-postmeddelanden sparas på en skrivbordsdator eller bärbar dator får användarna mycket interaktiva gränssnitt för e-post, kalender och snabbmeddelanden direkt från en webbläsare.

På liknande sätt ger program som t.ex. Google Dokument användarna en god kontroll över informationen. Dessa dokument stannar på servern, men användarna ges goda redigeringsmöjligheter via webbläsaren. Dessutom har användarna noggrann kontroll över vem som har åtkomst till dessa dokument och de kan skapa en lista över personer som kan redigera eller läsa dem. Dessa behörigheter gäller all åtkomst till dokumentet, vilket gör att du undviker problem med att ett internt dokument skulle kunna vidarebefordras per e-post till någon utanför företaget. Dessutom spåras alla ändringar noggrant, vilket gör det möjligt att se vem som

gjorde vilka ändringar och när ändringarna gjordes.

Google Apps skyddar även den elektroniska överföringen av data för att garantera att användarna kan visa data säkert utan risk för att konfidentiella data ska kunna snappas upp av andra. Åtkomsten till den webbaserade administrativa konsolen till Google Apps såväl som de flesta slutanvändarprogram erbjuds via en SSL-anslutning (Secure Socket Layer). Google erbjuder HTTPS-åtkomst för de flesta tjänster inom Google Apps och produkten kan konfigureras att endast tillåta HTTPS-åtkomst till viktiga tjänster, som t.ex. e-post och kalender. Med denna funktion är all användaråtkomst till data och all samverkan krypterad.

Google använder aldrig cookies för att spara lösenord eller kundinformation på användarens system. Cookies används för sessionsinformation och för att göra det enkelt för användare, men denna information är aldrig känslig och kan heller inte användas för att bryta sig in i en användares konto.

Kontroll

Förutom att tillhandahålla dessa skydd för företagets och användarens data ger Google företagen möjlighet att integrera företagets egna rutiner för säkerhet, åtkomst, granskning och verifiering i Google Apps. Google Apps har ett API med enkel inloggning baserat på SAML 2.0, vilket låter företagen använda befintliga verifieringsmetoder för att ge användarna åtkomst till Google Apps. Företagen kan t.ex. använda Active Directory-verifiering för att logga in en användare och inloggningsuppgifterna skickas inte till Googles servrar för åtkomst till de webbaserade verktygen. Därmed kan företag fortsätta att använda samma lösenordssystem och samma frekvens för lösenordsbyten.

Dessutom tillhandahåller Google en administrationskonsol och ett API för användaradministration. Administratörer har möjlighet att vid behov ögonblickligen stänga all åtkomst till ett konto eller ta bort ett konto. Detta kan även länkas till företagets interna processer för användaradministration via systemets API.

När det gäller e-post och snabbmeddelanden erbjuder Google även möjligheten att placera en e-post-gateway framför e-postsystemet. Med denna konfiguration passerar all inkommande och utgående e-post genom kundens system, vilket ger möjlighet att granska och arkivera e-post, såväl som att det tillåter övervakningskontroller.

Datasekretess

Google är mycket måna om säkerheten för företagets och användarens sekretess och vi vet att de data som finns i programmen är konfidentiell och känslig information. Google garanterar genom Google Apps att informationen inte äventyras. Googles juridiskt bindande sekretesspolicy som skyddar alla tjänster hittar du på följande adress **http://www.google.com/privacypolicy.html**. Enligt denna policy och relaterade policyn för enskilda tjänster inom Google Apps har Googles anställda inte under någon omständighet tillgång till användarnas konfidentiella data. Google försäkrar också att denna policy inte kommer att ändras på något potentiellt skadligt sätt utan uttryckligt skriftligt samtycke från kunden och/eller användaren.

Slutsats

Google Apps tillhandahåller en säker och tillförlitlig plattform för era data och tillför er den senaste tekniken och de bästa arbetsmetoderna för datacenterhantering, nätverkssäkerhet och dataintegritet. När du anförtror ditt företags information till Google kan du göra det med tillförsikt om att Googles omfattande teknik och infrastruktur kommer att utnyttjas till fullo för att garantera säkerheten, sekretessen och integriteten för alla data.

Om du vill ha mer information om Google Apps kan du besöka **http://www.google.com/a** eller skicka ett meddelande till **apps-enterprise@google.com.**