Celkový přehled zabezpečení a ochran proti zranitelnosti služby Google Apps

Podrobná zpráva Google, leden 2007

Zabezpečení Google Apps

VÍCE INFORMACÍ

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

Zabezpečení síťových aplikací proti případným hackerům je klíčem k úspěchu jakéhokoli systému. Význam zabezpečení je zcela zásadní v případě emailů a spolupráce. Google investuje miliardy dolarů do technologií, odborníků a procesů, aby zajistil, že data ve službě Google Apps budou chráněná a důvěrná. Vyhrazený tým bezpečnostních odborníků Google nese zodpovědnost za vývoj bezpečnostních opatření od samotného počátku a kontroluje všechny návrhy, kódy a konečný produkt, aby zajistil, že je vše v souladu s přísnými normami společnosti Google, které se týkají bezpečnosti a utajení dat. Pro hoštění služby Google Apps a zajištění bezpečnosti údajů statisíců uživatelů se používá stejná infrastruktura jako pro spravování miliónů údajů o zákaznících a miliard dolarů při inzertních transakcích. Se službou Google Apps jsou informace v bezpečí a chráněné.

Úvod

V rámci svého poslání uspořádávat informace z celého světa nese Google odpovědnost za bezpečné uchovávání dat desítek milionů uživatelů. Tuto odpovědnost bereme velmi vážně a Google udělal opravdu mnoho, aby si získal a udržel důvěru svých uživatelů. Google si je vědom, že bezpečné produkty jsou prostředkem k udržení důvěry uživatelů a snaží se tvořit nové produkty, které odpovídají požadavkům uživatelů a pracují v jejich prospěch.

Google Apps těží z této rozsáhlé provozní zkušenosti s vývojem bezpečných a spolehlivých produktů. Produkty a služby Google v sobě kloubí pokročilá technická řešení a nejvyspělejší zabezpečovací postupy, aby byla zaručena bezpečnost dat zákazníků a uživatelů. Investujeme miliardy dolarů, abychom zajistili co nejbezpečnější a nejspolehlivější prostředí pro data a aplikace. Google se obzvláště zaměřuje na několik bezpečnostních hledisek, která jsou zásadní pro firemní zákazníky:

- Organizační a provozní zabezpečení – postupy a procedury pro zajištění bezpečnosti během každé fáze vývoje zavádění a provozu.
- Zabezpečení dat – zajištění, že jsou data zákazníků uložena v bezpečných zařízeních, na bezpečných serverech a v rámci bezpečných aplikací.
- Prevence před ohrožením - ochrana uživatelů a jejich informací před zákeřnými útoky a případnými hackery.
- Bezpečný přístup – zajištění, že k datům mají přístup pouze oprávnění uživatelé a že přístupový kanál je bezpečný.
- Utajení dat – zajištění, že důvěrné informace zůstanou soukromé a utajené

Tento dokument pojednává o bezpečnostní strategii společnosti Google, která využívá mnoha fyzických, logických a provozních bezpečnostních norem, které zajišťují nejvyšší míru bezpečnosti a utajení dat.

Organizační a provozní zabezpečení

Základem bezpečnostní strategie společnosti Google jsou její lidé a postupy. Bezpečnost je kombinací lidského faktoru, postupů a technologií, které, při správné kombinaci, vedou k bezpečnému a zodpovědnému vývoji programů. Bezpečnost nelze prostě ověřit až na základě výsledků. Spíše se do všech produktů, uspořádání, infrastruktury a systémů promítá už od jejich počátku. Google zaměstnává tým plně se věnující bezpečnosti, který vyvíjí, dokumentuje a zavádí komplexní bezpečnostní postupy. Bezpečnostní tým společnosti Google se skládá ze špičkových světových odborníků na zabezpečení informací, aplikací a sítí.

Bezpečnostní tým je rozdělen podle oblastí činnosti na ochranu zvenčí, ochranu infrastruktury, ochranu aplikací a odhadování zranitelnosti. Mnoho zaměstnanců do společnosti Google přichází se zkušenostmi z vysokých postů v informačním zabezpečení z prestižních společností na seznamu Fortune 500. Tento tým věnuje velkou část svého úsilí preventivním opatřením, aby zajistil, že kódování a systémy jsou bezpečné od prvopočátku, a je připraven dynamicky zareagovat.
.

Metodologie vývoje
Bezpečnost patří pro Google mezi jeho hlavní zájmy od chvíle, co je nový produkt navržen. Vývojářské a tvůrčí týmy společnosti Google prochází obsáhlým školením v základech bezpečnosti. Vývojová metodologie Googlu přestavuje mnohostupňový plán s průběžnými kontrolami a celkovými prověrkami.

Tým zabezpečení aplikací Google je zapojený do všech částí vývoje nového produktu, včetně revize návrhu, prověrky kódování, testování systému a funkcí a konečného schválení uvedení do provozu. Google využívá celé řady komerčních a patentovaných technologií pro zajištění, že jsou aplikace bezpečné na všech úrovních. Tým zabezpečení aplikací společnosti Google rovněž nese odpovědnost za to, že budou dodržovány bezpečné vývojové postupy za účelem zajištění bezpečnosti pro zákazníky.

Provozní zabezpečení
Tým zabezpečení provozu Google se zaměřuje na zabezpečení operačních systémů včetně zpracovávání dat a správy systému. Jeho členové provádí běžné prověrky provozu datových center a neustále vyhodnocují hrozby pro fyzický a logický majetek společnosti Google.

Tato skupina je rovněž odpovědná za to, že jsou všichni zaměstnanci řádné prověřeni a vyškoleni, aby mohli vykonávat svou práci profesionálním a bezpečným způsobem. Google rovněž v patřičné míře zkoumá a prověřuje minulost každého jedince, než vstoupí do organizace. Všichni zaměstnanci odpovědní za dodržování bezpečnostních postupů a procedur projdou důkladnou vzdělávací průpravou a jsou soustavně doškolováni.

Bezpečnostní odborníci a poradenství
Vedle výše uvedených postupů Google aktivně spolupracuje s odbornou veřejností zabývající se otázkami bezpečnosti a spoluvytváří a využívá společných znalostí těch nejlepších odborníků na světě. To společnosti Google pomáhá držet si náskok v rámci bezpečnostních trendů a rychle reagovat na objevující se hrozby a využít odborných znalostí jedinců uvnitř i mimo společnost. Google se aktivně angažuje v tomto širším okruhu bezpečnostních odborníků zodpovědným sdílením poznatků. Na stránce **http://www.google.com/corporate/security.html** naleznete více informací o tomto programu a o některých klíčových odbornících na bezpečnost, se kterými Google trvale spolupracuje.

I přes všechny tyto úrovně ochrany se můžou objevit neznámá zranitelná místa a Google je připraven pohotově reagovat na bezpečnostní výstrahy a zranitelnosti. Bezpečnostní tým společnosti Google prověřuje celou infrastrukturu a hledá potenciální zranitelná místa a přímo spolupracuje s techniky na okamžité nápravě všech známých problémů. Zákazníci služby Google Apps Premier jsou na bezpečnostní problémy upozorněni e-mailem v nejkratší možné době.

Zabezpečení dat
Zabezpečení dat společností a uživatelů je hlavním úkolem bezpečnostních a provozních týmů společnosti Google. Činnost společnosti Google je založeno na důvěře uživatelů, a proto jde o jeden z klíčů k pokračujícímu úspěchu Googlu jako společnosti. Všem zaměstnancům společnosti Google je vštěpována hodnota zodpovědnosti vůči koncovému zákazníkovi. Ochrana dat je základem všeho, co Google znamená. Google se pečlivě stará o ochranu miliard dolarů během zákaznických a inzertních transakcí a stejnou péči věnujeme technologiím Google pro komunikaci a spolupráci.

Jak zásadní je to pro to, kdo jsme jako společnost, můžete zjistit z našich zásad jednání na **http://investor.google.com/conduct.html**.

Fyzické zabezpečení
Google provozuje jednu z největších sítí datových center na světě a vyvíjí obrovské úsilí na ochranu dat a duševního vlastnictví v těchto centrech. Společnost Google provozuje datová střediska po celém světě a mnohé z nich jsou v jejím plném vlastnictví a pod její správou, což zajišťuje, že nikdo jiný k nim nemůže získat přístup. Geografická umístění datových center byla vybrána tak, aby byla chráněna před katastrofickými událostmi. Pouze vybraní zaměstnanci společnosti Google mají přístup do zařízení datových center a k serverům, které se nacházejí uvnitř, a tento přístup je striktně kontrolován a prověřován. Zabezpečení je monitorováno a řízeno jak lokálně přímo na místě, tak centrálně přes bezpečnostní centra Google po celém světě.

Tato zařízení jsou zkonstruována nejen tak, aby byla vysoce efektivní, ale rovněž bezpečná a spolehlivá. Vícenásobné úrovně zálohování zajišťují trvalý provoz a dostupnost služeb i v těch nejtěžších a nejextrémnějších podmínkách. To zahrnuje mnohonásobné úrovně zálohování uvnitř center, zálohování probíhajících operací se samostatnými generátorovými zdroji a plné zálohování v četných odděleně rozmístěných centrech. Pro lokální i vzdálené sledování těchto center se využívají nejmodernější prostředky a k dispozici jsou automatizované systémy pro zabezpečení v případě selhání.

Logické zabezpečení
Při vývoji webových systémů je logické zabezpečení dat a aplikací stejně důležité jako fyzické zabezpečení. Google si dává extrémně záležet, aby měl jistotu, že jsou aplikace bezpečné a data jsou zpracovávána bezpečným a odpovědným způsobem a že je plně zamezeno externímu neoprávněnému přístupu k zákaznickým či uživatelským datům. K dosažení tohoto cíle využívá Google řadu standardních postupů i některé jedinečné inovativní přístupy. Jedním z těchto přístupů je uplatnění jednoúčelových technologií místo univerzálního softwaru.

Mnoho z technologií Google je vyvinuto pro konkrétní jeden účel, na rozdíl od univerzálních programů. Například úroveň webového serveru Google speciálně vyvinul a zavedl tak, aby byly odhaleny pouze funkce požadované pro provoz určitých aplikací. Proto není zranitelný vůči široké škále útoků, kterým snadno podléhá většina komerčního softwaru.

Google rovněž z bezpečnostních důvodů učinil změny v hlavních knihovnách. Protože je infrastruktura Google založena na systému vyhrazených aplikací spíše než univerzálním výpočetním prostorem, lze řadu služeb, které poskytuje standardní operační systém Linux, omezit nebo vypnout. Tyto úpravy se zaměřují na podporu systémových funkcí, kterých je potřeba pro dané úkoly, a na vypnutí či odstranění všech zneužitelných částí systému, kterých není potřeba.

Servery Google jsou rovněž chráněny mnoho úrovněmi firewallů, které chrání před útoky. Provoz je kontrolován z hlediska pokusů o útoky a případné pokusy jsou řešeny tak, aby byla ochráněna data uživatelů.

Dostupnost informací
Data, jako jsou například e-maily, jsou uložena v kódovaném formátu s optimalizovaným výkonem, místo aby byla uložena tradičním souborovým systémem či formou databáze. Data jsou rozložena mezi řadu fyzických a logických disků z důvodu zálohování a vhodného přístupu, čímž je ztížena neoprávněná manipulace s nimi. Výše popsaná fyzická ochrana Google zaručuje, že fyzický přístup k serverům není možný. Veškerý přístup k produkčním systémům je prováděn personálem, který používá zašifrovaný SSH (secure shell). K získání smysluplného přístupu k datům cílových uživatelů by bylo třeba odborných znalostí v oblasti datových struktur a patentované infrastruktury Google. Toto je jedna z mnoha úrovní ochrany, která zajišťuje bezpečnost citlivých dat v rámci služby Google Apps.

Rozložená struktura Google je sestavena tak, aby poskytovala vyšší stupeň zabezpečení a spolehlivosti než tradiční struktura s jedním umístěním. Data jednotlivých uživatelů jsou rozptýlena mezi řadu anonymních serverů, klastrů a datových center. To zaručuje, že jsou data nejen chráněná proti potenciální ztrátě, ale také vysoce zabezpečená.

Uživatelská data jsou dostupná pouze s příslušnými osobními údaji, což zajišťuje, že neexistuje možnost, aby měl jeden uživatel přístup k datům jiného uživatele, pokud přímo nezná jeho přihlašovací údaje. Tento osvědčený systém denně slouží nejen desítkám milionů uživatelů e-mailových služeb, kalendářů a dokumentů, ale je rovněž používán společností Google jako základní platforma pro obsluhu její zaměstnanecké základny čítající více než 10.000 pracovníků.

Záložní zdroje
Aplikační a síťová struktura provozovaná společností Google je navržena pro maximální spolehlivost a provozuschopnost. Výpočetní platforma společnosti Google ve formě mřížky předem počítá se selháním hardwaru a masivní softwarové zabezpečení případné poruše odolá. Všechny systémy Google jsou již navrženy jako ze své podstaty záložní a provoz žádného subsystému není závislý na konkrétním fyzickém nebo logickém serveru.

Data jsou mnohonásobně zálohována mezi skupinovými aktivními servery, takže v případě poruchy hardwaru jsou data dostupná z jiného systému. Vedle toho jsou uživatelská data zálohována i mezi datovými centry. Kdyby tedy došlo k selhání celého datového centra nebo jeho zasažení živelnou pohromou, jeho funkci přebere jiné datové centrum.

Prevence před ohrožením
E-mailové viry, phishingové útoky a spamy dnes patří mezi největší bezpečnostní hrozby v rámci společností. Podle různých zpráv více než dvě třetiny příchozích e-mailů jsou spamy a každý den vznikají a přes internet se šíří nové e-mailové viry. Vyrovnat se s tím může být velmi obtížné a i společnosti se spamovými a virovými filtry zápasí s neustálou potřebou aktualizací, aby se vyrovnaly s nejnovějšími hrozbami. Navíc jsou síťové aplikace terčem zákeřných útoků, které se snaží neoprávněně nakládat s daty či zničit službu. Prevence před ohrožením společnosti Google je na světové úrovni a chrání uživatele před útoky na data a v rámci obsahu jejich zpráv a souborů.

Ochrana proti virům a spamu
Zákazníci služby Google Apps těží z jednoho v současnosti z nejsilnějších spamových a phishingových filtrů. Společnost Google vyvinula filtry založené na moderních technologiích, které se dokáží učit ze vzorů zpráv, které byly označeny jako spam, a tyto filtry jsou soustavně vylepšovány pomocí miliard e-mailových zpráv. Díky tomu Google dokáže velmi přesně identifikovat spam, pokusy o phishing a viry, a ochránit tak doručenou poštu, kalendáře a dokumenty uživatelů.

Pomocí webového rozhraní od Google blokuje virová ochrana hrozbu od nic netušících uživatelů, kteří šíří virus v rámci firemní či interní sítě. Na rozdíl od tradičních klientských e-mailových aplikací nejsou zprávy stahovány do počítače. Místo toho procházejí antivirovou kontrolou již na serveru a Gmail nedovolí uživateli otevřít žádnou přílohu, dokud nebude zkontrolována, čímž je riziko minimalizováno. Díky tomu e-mailové viry nemohou využít zranitelnosti v zabezpečení na straně klientských aplikací a uživatelé nemohou nevědomky otevřít dokument s virem.

Útoky na síť a aplikace
Vedle filtrování nevyžádané pošty a virů z datového obsahu Google nepřetržitě chrání sebe i uživatele před zákeřnými útoky. Hackeři se vždy snaží nalézt způsoby, jak proniknout do webových aplikací, nebo jak je vyřadit z provozu. Vyřazení služby z provozu, falšování adres IP, skriptování napříč stránkami a neoprávněné nakládání s pakety je jen pár druhů útoků, které jsou dnes používány proti sítím. Google jako jeden z největších poskytovatelů webových služeb na světě

vynakládá velké úsilí s cílem zabránit těmto a podobným hrozbám. Veškerý software je kontrolován pomocí různých komerčních i vlastních patentovaných balíčků pro kontrolu sítí a aplikací. Bezpečnostní tým Google rovněž spolupracuje s externími subjekty při testování a zlepšování infrastruktury Google a zabezpečení aplikací.

Bezpečný přístup
Ať jsou v datovém centru data jakkoli bezpečná, když je stáhnete na místní počítač uživatele, jsou tato data napadnutelná. Výzkumy ukázaly, že průměrný přenosný počítač obsahuje více než 10.000 souborů a tisíce stažených e-mailových zpráv. Představte si, že se jeden z firemních přenosných počítačů dostane do rukou uživatele s nekalými úmysly. Pouhým přístupem na disk se neoprávněný uživatel může dostat k duševnímu vlastnictví a tajným dokumentům vaší společnosti. Google Apps umožňuje společnostem toto riziko minimalizovat, protože data nejsou uložena na počítačích uživatelů.

Ochrana koncového uživatele
Webový charakter služby Google Apps umožňuje uživatelům stálý přístup k jejich datům odkudkoli, zatímco data zůstávají v bezpečí na serverech Google. Místo toho, aby byly e-maily uloženy na stolních či přenosných počítačích, mají uživatelé k dispozici vysoce interaktivní rozhraní v kvalitě stolního počítače pro e-maily, kalendáře a chaty, zatímco stále používají internetový prohlížeč.

Obdobně aplikace jako Dokumenty Google poskytují uživatelům vysoký stupeň kontroly nad informacemi. Tyto dokumenty zůstávají na serveru, ale uživatelé mají široké možnosti je upravovat přes internetový prohlížeč. Navíc mají uživatelé přesnou kontrolu nad tím, kdo má k těmto dokumentům přístup, a mohou nastavit seznam osob, které jsou oprávněny dokumenty upravovat či prohlížet. Tato oprávnění jsou uplatňována při jakémkoli přístupu k dokumentu, což vám umožňuje vyhnout se problému, kdy jsou interní dokumenty odeslány e-mailem mimo vaši společnost. A nakonec, tyto produkty velmi podrobně sledují změny, takže vidíte, kdo, kdy a jaké změny provedl.

Google Apps rovněž chrání data během kabelového přenosu, čímž uživatelům zajišťuje bezpečný přístup k datům, aniž by hrozilo zachycení důvěrných dat na síti. Přístup k internetovému administrativnímu ovládacímu panelu Google Apps a většině aplikací určených koncovým uživatelům je poskytován pomocí připojení Secure Socket Layer (SSL). Google nabízí přístup HTTPS pro většinu služeb v rámci Google Apps a tento produkt můžete nastavit tak, aby ke klíčovým službám jako e-mail a kalendář umožňoval pouze přístup HTTPS. S touto funkcí jsou veškerý přístup uživatelů k datům a všechny interakce šifrovány.

Google nikdy nepoužívá cookies pro uložení hesel či zákaznických dat v uživatelském systému. Cookies se používají pro informace o práci na počítači a pro pohodlí uživatelů, ale nikdy se nepoužívají pro citlivé informace, ani nemůžou být použity pro neoprávněný přístup na účet uživatele.

Kontrola ve vašich rukou
Kromě těchto způsobů ochrany firemních a uživatelských dat dává Google podnikům možnost začlenit do Google Apps firemní metody zabezpečení, přístupů, prověrek a ověřování. Google Apps poskytuje API jednotného přihlášení založené na SAML 2.0, které umožňuje firmám používat stávající ověřovací mechanizmy k přihlášení uživatelů do služby Google Apps. Firmy mohou například pro přihlášení uživatele používat ověřování Active Directory, ale ověřovací údaje nejsou přenášeny přes servery Google pro přístup k nástrojům umístěným na internetu. Toto rovněž firmám umožňuje, aby nadále uplatňovaly svá pravidla pro bezpečnost a frekvenci změn hesel.

Navíc Google poskytuje administrátorský ovládací panel a API pro správu uživatelů. Správci mohou s okamžitou platností uzavřít přístup k účtu či na požádání účet vymazat. Je rovněž možné vytvořit napojení na interní postupy pro přidělování a odebírání přístupu uživatelům prostřednictvím API.

Co se týče e-mailů a chatů, poskytuje Google rovněž možnost umístit před poštovní systém poštovní bránu. Při tomto nastavení prochází všechny příchozí a odchozí zprávy zákaznickým systémem, což vám dává možnost kontrolovat a archivovat zprávy a také zavést regulační dohled.

Utajení dat

Google klade velký důraz na utajení firemních a uživatelských dat a uvědomuje si, že údaje umístěné v aplikacích jsou důvěrné a choulostivé. Google zaručuje, že se službou Google Apps nebudou informace prozrazeny. Právně závazná pravidla společnosti Google, která se vztahují na všechny služby, můžete najít na **http://www.google.com/privacypolicy.html**. Podle těchto pravidel a souvisejících pravidel, která se týkají jednotlivých služeb v rámci Google Apps, nemají zaměstnanci společnosti Google nikdy přístup k důvěrným datům uživatelů. Google rovněž zaručuje, že se tato pravidla nijak nepříznivě nezmění bez výslovného písemného souhlasu zákazníka a/nebo uživatele.

Závěr

Služba Google Apps poskytuje bezpečný a spolehlivý prostor pro vaše data, přináší vám ty nejnovější technologie a nejlepší postupy pro správu datových center, bezpečnost síťových aplikací a integritu dat. Svěříte-li své firemní informace společnosti Google, můžete tak učinit s důvěrou a vědomím, že obrovské investice společnosti Google do technologií a infrastruktury zajišťují bezpečnost, utajení a integritu vašich dat.

Chcete-li získat více informací o službě Google Apps navštivte **http://www.google.com/a** nebo pošlete e-mail na adresu **apps-enterprise@google.com.**