Někteří uživatelé služby Google Dokumenty byli nemile překvapeni, když byly jejich soubory zablokovány kvůli porušení podmínek služby. Měli totiž falešný pocit, že internetový gigant do obsahu jejich dokumentů nevidí. Google se ale netají tím, že obsah souborů kontroluje.
Uživatelé Google Docs začali mít v posledních problém s přístupem k soukromým dokumentům. Místo toho, jak někteří napsali do diskuzí na Google poradnách, se jim zobrazila zpráva o porušení podmínek služby.

Přestože Google přístup k dokumentům rychle obnovil, upozornil tím na fakt, že ví, co je obsahem soukromých uživatelských dokumentů. Nejedná se však o odhalení žádné konspirace. V právních podmínkách služby (se kterými musel každý uživatel souhlasit) americká společnost tuto informaci dávno zmiňuje. Problém je, že je četl jen nepatrný zlomek uživatelů.

Co Google ví a jak s informacemi nakládá?

Dalo by se říci, že Google ví o všem, co mu povíte. Proč by ale prohlížel zrovna soukromé dokumenty uživatelů? Internetový gigant se snaží kontrolovat obsah dokumentů kvůli **hrozbám, pornografii či spamu** a snaží se tak zabránit jejich dalšímu šíření. Při poslední aktualizaci byl však algoritmus přeci citlivější a kvůli špatné konfiguraci blokoval i bezproblémový obsah.

Uživatele může uklidnit, že **kontrola probíhá automatizovaně** a bez lidského zásahu. Vaše dokumenty tedy prochází jakýsi robot, který porovnává klíčová slova a vizuální podobu obsahu a následně vyhodnocuje jejich závadnost. Google potvrdil, že již problém napravil a zablokované soubory mají uživatelé zase přístupné.
Je dobře, že se po incidentu znovu rozproudila diskuze ohledně bezpečnosti informací uložených u třetích stran. Pokud ukládáte v cloudu třetí strany citlivé informace ke kterým by se neměl nikdo dostat, měli byste se dobře zamyslet nad výběrem poskytovatele, nebo zvážit další ochranu souborů např. za pomoci šifrování.

V roce 2009 byl novinkou na trhu model s technickým označením Huawei U7510, do kterého bylo možné uložit až 1000 telefonních kontaktů a disponoval na svoji dobu úctyhodnou interní pamětí 100 MB. V nabídce telefonu byla také možnost dohledat až 30 příchozích, odchozích, nebo ztracených hovorů. O deset let později vyvinul Huawei technologický skvost Mate 20 Pro, pro mnohé uživatele nejlepší smartphone na světě, který již nepotřebuje místo na ukládání kontaktů a ani se nechlubí možností dohledat ztracené hovory, zato disponuje dostatečnou kapacitou vnitřní paměti o kapacitě 128 GB.

V dnešní zrychlené době jednoduše zapomínáme na fakt, že technologický pokrok se zrychluje opravdu neskutečně a pomalu se začínáme dostávat do fáze, kde ještě nedávno sci-fi koncepty se pomalu začínají stávat realitou. Hlasové ovládání včetně povídání s umělou inteligencí, ohebné displeje, výkon telefonů překonávající nedávné počítače a spousta dalšího.

Bezpečnost dat v praxi

Bezpečnost dat bez ochrany/zabezpečení ve formě řízení přístupu je srovnatelná s šancí nevidomého přejít bez úhony za pomoci svého vodícího psa za plného provozu dálnici. Přesto je v laické praxi význam ochrany dat podceňován a lidé se uchylují ke slepé víře v schopnosti jim dostupných technologií. Reálná hodnota dat bývá jejich vlastníkem doceněna až při jejich neautorizovaném využití, zničení nebo momentální, či trvalé nedostupnosti.

Pro zabezpečení dat je nutné znát jejich cenu, dokázat ohodnotit rizika a mít ochotu investovat do protiopatření. Bezpečnost lze definovat jako zajištěnost proti hrozbám, minimalizaci rizik a komplex administrativních, technických, logických a fyzických opatření pro prevenci a detekci neautorizovaného využití dat. I z tohoto důvodu je nutné si vymezit rámec, který má na bezpečnost dat zásadní vliv, kde bezpečnost v informačním prostředí lze zjednodušeně rozdělit na následující domény:
· komunikační bezpečnost - ochranu přenášených dat a zamezování nežádoucího datového provozu,
· fyzickou bezpečnost - ochranu před přírodními hrozbami, jako je například požár, a fyzickými útočníky, například zábranou, detektory pohybu atp.,
· personální bezpečnost - ochranu před vnitřními útočníky již při náboru, během jejich práce i po skončení pracovního poměru,
· bezpečnost informačních systémů a technologií - ochranu infratsruktury informačních systémů uchovávající data v elektronické podobě proti relevantním hrozbám typu neuatorizovaný přístup, malidní software (viry, trojské koně), výpadky systému apod.

Základní bezpečnostní atributy v těchto doménách jsou:
· důvěrnost - prevence neautorizovaného vyzrazení dat,
· integrita - prevence neautorizované úpravy dat,
· dostupnost - prevence ztráty přístupu k datům.

Výše uvedené základní bezpečnostní atributy se následně mohou jemněji dělit i na další, jako je například autentičnost, odpovědnost, nepopiratelnost nebo spolehlivost. V článku se však jimi nebudeme zabývat a dále se pro účely diskuse soustředíme na výše uvedené atributy ochrany dat.

Důvěrnost
Důvěrnost je zajištěna schopností ujistit se, že je vynucena nezbytná úroveň míry utajení v každém okamžiku, kdy dochází ke zpracování dat a je zajištěna prevence jejich neautorizovaného vyzrazení. Taková úroveň důvěrnosti by měla přetrvat jak během uchovávání dat v systémech, tak při jejich přenosu nebo po předání adresátovi. Různé situace vedoucí k porušení důvěrnosti mohou nastat například v průběhu útoku, kdy budou překonány mechanismy zajišťující důvěrnost sledováním síťového provozu, odpozorováním stisků kláves přes rameno či z dat na obrazovce, krádeží nebo třeba sociálním inženýrstvím. Důvěrnost může být dále porušena v situaci, kdy uživatelé například záměrně, nebo svojí chybou vyzradí citlivou informaci tím, že ji nezašifrují před odesláním jiné osobě, podlehnou sociálnímu inženýrství a svěří obchodní tajemství nebo opomenou zvláštní opatření při zpracování citlivých dat.

Integrita
Integrita je udržena, když je zajištěno, že data jsou přesná, se zaručeným obsahem a jsou provedena opatření proti jejich neautorizované změně. Hardwarové, softwarové a komunikační prostředky musí pracovat tak, aby data uchovávaly a zpracovávaly správně a přesně, přenášely je do požadovaného cíle bez nežádoucích změn. Systémy a síť musí být

chráněny před vnějším rušením či kontaminací původní informace. Integrita může být útočníkem narušena například počítačovým virem, pomocí trojského koně, tj. podvrženého programu či aplikace, jež se chová korektně pouze navenek, zadními vrátky do systému, tzv. back door metoda, což může vést k následné kontaminaci původních dat. Rovněž uživatelé mohou narušit integritu vlastní chybou, či zlomyslností, a to například smazáním důležitých konfiguračních souborů při uvolňování použitého místa na disku nebo mylným, či úmyslným zadáním cifer v účetnictví atp.

Dostupnost
Zapříčinění nedostupnosti dat je populární metodou útočníků, kteří se tak snaží ovlivnit produktivitu, či daný systém zcela vyřadit z provozu. Proto musí být dostupnost zajištěna spolehlivou a včasnou dispozicí dat a zdrojů autorizovaným jednotlivcům. Informační systémy a sítě musí mít datovou kapacitu dimenzovanou tak, aby v definovaném čase poskytovaly dostatečný výkon, musí být schopny zotavit se z výpadků transparentním a rychlým způsobem, aby nebyla negativně narušena produktivita. Dále musí být omezena úzká místa, zavedeny redundantní mechanismy. Dostupnost může být například narušena chybou v zařízení či chybou v software, proto se využívají jak záložní zařízení pro možnost rychlé náhrady kritických systémů, tak i proškolení zaměstnanců k provedení náležitého zásahu pro uvedení systému do funkčního stavu.

Běžná denní praxe
S problematikou bezpečnosti dat se často nevědomky setkáváme při každodenních činnostech. V praxi nechráníme pouze soubory, ale i jiné formy dat. Například když jdeme na koncert do tlačenice, bereme s sebou minimum potřebných dokladů, v dopravních špičkách v MHD dáváme pozor na kapsáře, při výběru z bankomatu se snažíme zadat PIN, aniž by jej někdo mohl odpozorovat atp. Přesto může nastat situace, kdy dojde ke ztrátě, respektive cizímu zneužití chráněných údajů, což bývá způsobeno tím, že hrozby a rizika se mění s technologickým pokrokem a novými postupy. Pokrok bývá využíván v pozitivním směru, ale nové technologie a postupy jsou často zneužity i k negativním záměrům. Absolutní eliminace rizik tak není možná. Ochrana dat pouze snižuje pravděpodobnost úspěchu útoku, tj. útočník například musí vynakládat nesrovnatelně více prostředků k dosažení cíle.

Co s tím - možná protiopatření
Je třeba nastavit žádoucí míru ochrany datových aktiv tak, aby veškerá rizika byla pokud možno minimalizována. Slabiny v ochraně dat se označují jako zranitelná místa. Hrozbou se označuje možnost využít zranitelné místo k narušení integrity, důvěrnosti nebo dostupnosti datových aktiv. Hrozby lze kategorizovat jako úmyslné, náhodné nebo přírodního charakteru (tab. 1). Protiopatření mohou být administrativní, fyzická či logická. Podle okamžiku uplatnění je lze kategorizovat jako: · preventivní - odstraňující zranitelná místa, · heuristická - potenciálně snižující riziko dané nějakou hrozbou, · detekční a opravná - detekují pokus o datový podvod a minimalizují účinky zjištěného útoku.

Rizikem rozumíme pravděpodobnost zneužití zranitelného místa a následného dopadu tohoto zneužití. Existence hrozby představuje riziko. Aby bylo možno data náležitě chránit, je třeba provést tzv. analýzu rizik, ve které je nutné zodpovědět otázky typu: Co se má chránit a proti čemu? Jaké jsou priority ochrany? Jakákoliv změna hrozeb, aktiv, zranitelností a ochranných opatření může rizika významně ovlivnit. Z toho mimo jiné plyne, že v praxi je zajišťování bezpečnosti dat neustálým procesem. Následující odstavce ukazují, jaká protiopatření se používají k zajištění základních atributů ochrany dat.

Ochrana důvěrnosti
Důvěrnost se zajišťuje převážně prostřednictvím šifrování: · symetrickou kryptografií, · asymetrickou kryptografií.

Šifrování se může provádět při ukládání dat nebo jejich přenosu. V praxi se například používá software typu Pretty Good Privacy (PGP) nebo komplexní řešení v podobě vybudování tzv. infrastruktury veřejných klíčů PKI, například prostřednictvím produktu Entrust PKI. Za jistých podmínek lze důvěrnosti docílit i pouhým řízením přístupu k datům - fyzickým, či logickým, kde přístupové seznamy definují autorizaci přístupu daného subjektu. V praxi se používají tyto modely řízení přístupu nebo jejich kombinace: · mandatory access control (MAC) -

subjekty nemají velké šance ovlivnit přístup k jejich datům, definuje je management/správce a vynucuje operační systém či daná technologie, · discretionary access control DAC - vlastník zdroje může specifikovat, co nebo kdo má k němu přístup, · role based access control RBAC - funkční role má definována potřebná práva a subjektu je pouze přidělena daná role.

Při ochraně důvěrnosti je rovněž důležitým prvkem spolehlivé ověřování subjektů přistupujících k datům, v praxi tuto roli po technické stránce velmi dobře zajišťuje například autentizační systém Kerberos nebo parametry PKI.

Ochrana integrity
Zabezpečuje se většinou prostřednictvím mechanismů digitálního podpisu, tj. opět další základní funkcionalitou obsaženou v řešení na bázi PGP, OpenSSL nebo Entrust PKI. Za určitých podmínek ji zajišťuje i výše zmíněné řízení přístupu nebo také prostředky umožňující vrácení se k předchozímu stavu dat před chybou uživatele, havárii či útoku. Dále lze jako podpůrné prostředky pro zachování integrity využít antivirový software, desktop firewally atp. Překvapivě i šifrování dat může kromě zajištění důvěrnosti zamezit rovněž jejich nežádoucí modifikaci při přenosu, kdy narušení obsahu šifrované informace vede po dešifrování ke kolizním výsledkům.

Ochrana dostupnosti
Data jsou nejčastěji zpracovávána v elektronické podobě a přístup k nim umožňují aplikace, které běží na daném operačním systému a příslušném hardware. Dostupnost se pak zajišťuje nejen zřizováním on-line kopií či off-line záloh, rezervními zdroji, ale i robustností software a operačního systému a hardware hostitelského systému, který umožňuje provoz aplikací.

Prostředky ochrany dat v často užívaných operačních systémem

Z pohledu důvěrnosti:
· Windows - v základní funkcionalitě poskytují důvěrnost lokálních dat prostřednictvím tzv. Encrypted File System (EFS), dále zahrnují sofistikovaný systém řízení přístupu typu DAC - přidělování práv nejen k souborům a adresářům. Ověřování uživatelů zde lze provádět prostřednictvím systému Kerberos i rozšíření Public Key Cryptography for Initial Authentication (PKINIT). Síťová vrstva podporuje IP Security Protocol (IPSec). Dodatečně lze rozšířit mechanismy řízení přístupu i stávající kryptografické funkce například prostřednictvím sady produktů HP ProtectTools. Šifrování na širší úrovni použití lze dosáhnout například PKI řešením firmy Entrust nebo na jisté úrovni prostřednictvím PGP.
· Unix - komerční unixové systémy disponují rovněž vhodnými modely řízení přístupu typu DAC i MAC, umožňují použití různých autentizačních modulů, které poskytují například Kerberos, PKINIT, přístup k HW tokenům atp. Systémová jádra mohou poskytovat dokonce volitelné stupně ochrany aplikací a procesů. Dodatečně lze opět používat software typu Entrust PKI, PGP. Existuje také řada bezpečnostních doplňků, jako například Bastille pro HP-UX či Linux. V Linuxu dále Linux Intrusion Detection System (LIDS). Rule Set Access Control (RSBAC) nebo Security Enhanced Linux (SELinux), které kromě jiného rozšiřují standardní modely řízení přístupu.

Z pohledu integrity:
· Windows - chrání integritu procesů mechanismem "security contextů", systém částečně umožňuje filtrovat síťový provoz a v jistých případech integritu brání systémem řízení přístupu. Dodatečně se integrita dat zajišťuje převážně prostředky PKI či softwarem typu PGP, dále se pro filtrování nežádoucího datového provozu do systému přidává Kerio Personal Firewall, různé antivirové programy a virové štíty
· Unix - unixové systémy umožňují filtrovat síťový provoz, poskytují dobré prostředky pro monitorování prováděných operací a potenciálních pokusů o útok. Umožňují omezení počtu nutných služeb pro provoz systému na minimum a spouštění procesů s velmi omezenými právy. Software typu PGP, Entrust či OpenSSL zde opět poskytuje integritu i na vyšší úrovni. V Linuxu opět pomáhá zajistit integritu SELinux, LIDS či RSBAC.

Z pohledu dostupnosti:
· Windows - dostupnost zajišťují spíše širokou škálou podporovaného hardware, například prostřednictvím podpory řadičů diskových polí, ale také schopností jednoduše připojit nový hardware, kterým může být třeba záložní linka. Systém také umožňuje automatický restart vybraných služeb v případě jejich selhání. Zálohování dat se řeší většinou systémem Legato Networker či třeba systémem Bacula a dostupnost služeb je kontrolovaná například systémem Nagios nebo HP OpenView.
· Unix - unixové systémy umožňují použití žurnálových souborových systémů. Podporují pole disková i softwarově emulovaná. Služby mohou být jednoduše replikovány. Základní doplňkový software pro zálohování a dostupnost služeb je typově stejný jako pro Windows.

Autentizace
ověření identity uživatele a jeho oprávnění k přístupu

Autorizace
pověření k určité činnosti dané přístuovými právy a příslušným oprávněním (pracovat s daty, provádět různé úkony, funkce apd.)

Accounting

Bezpečnost
vlastnost daného prvku v rámci informačního systému , který je chráněn proti známému trojímu "z": ztrátě, zneužití nebo zničení

Bezpečnostní politiky
souhrn požadavků, potřeb, pravidel, směrnic, předpisů a zásad, které jsou definovány pro zabezpečení všech prvků na všech úrovních přístupu odpovídajícím potřebám a možnostem instituce

Hacker

označení uživatele, který využívá své odborné znalosti ku prospěchu celku
objevuje a vyhledává bezpečnostní díry
chybu nahlásí a většinou zveřejní na hackerském fóru

1) Hacker je člověk, který se vyžívá v bádání po detailech programových systémů a překračování jejich schopností, což je odlišné od jednání vetšiny uživatelů, kteří se raději naučí jen nutné minimum. V dokumentu RFC 1392 (Internet Users' Glossary) hackera popisují jako člověka, který má potešení z detailních znalostí vnitřních pochodů systému, počítačů a počítačových sítí.
2) Ten kdo programuje se zanícením (někdy s posedlostí), nebo ten kdo má požitek spíše z programování samotného, než z pouhého teoretizování o programování.
3) Osoba schopná pochopit/ocenit hodnotu hacku.
4) Člověk zdatný v rychlém programování.
5) Expert na určitý program, nebo někdo, kdo tento program často užívá. (Definice 1 a 5 si jsou podobné a lidé je spojují dohromady)
6) Expert nebo nadšenec v čemkoliv. Například astronomický hacker,

elektrotechnický hacker, síťový hacker atd.
7) Někdo kdo si užívá intelektuální výzvu v překonávání, nebo obcházení limitů.
8) [-nesprávně-] Škodlivý slídil, který se šťouráním snaží odhalit citlivé informace. Použito např. v názvech programů jako "Hence password hacker", "network hacker" - správně se ale člověk zabývající takovou činností nazývá cracker.

Hacking

Činnosti, které pravý hacker provádí a kterými získává uznání a respekt, jsou:

* získání a zpřístupnění zdrojového kódu programů
* odhalení slabin informačního systému a zpřístupnění příslušných informací
* publikování užitečných informací na Internetu
* pomoc při administraci a provozu diskuzních skupin, seznamů mailů, archivů atd.
* pomoc při testování nových programů (tzv. beta verzí)
* propagace hackerské kultury

Cracker

využívá nalezené chyby hackerem, které používá ke svému obohacení
po průniku zpravidla destrukce systému

Pharming

Nejnovější forma internetových podvodů založenou na DNS spoofingu (změna překladu DNS adres seriozního serveru). Po zadání adresy serveru je uživatel přesměrován na nepravou kopii skutečných stránek.

Spyware

aplikace, která je bez vědomí uživatele nainstalována na počítači a monitoruje jeho činnost
nasbíraná data odesílána ke tvůrci spyware a často používána při servírování reklamy
nepoškozuje počítač ani software přímo, ale škodí přímo uživateli ->parazituje na jeho soukromí

co o Vás může spyware zjišťovat a posílat:

* Spyware může vyčíst všechny Vaše systémová jména zapsaná v registrech

Windows.
* Vaši IP adresu (adresa Vašeho počítače po připojení k internetu)
* Seznam reklam na které jste se koukli.
* Veškeré informace o tom, kde všude jste na internetu byli a případně i jména a hesla které jste použili.
* Seznam všech programů, filmů, písniček, prostě všeho co prošlo přes Váš počítač a nezáleží na tom, jestli jste je stáhli z internetu, nebo je máte na cd/dvd.
* Pokud se připojujete na internet pomocí obyčejné telefonní linky (dial up), tak telefonní čísla, přihlašovací jména a hesla všech Vašich spojení.
* Každé otevření multimediálniho souboru (např.: *.avi, *.jpg, *.mp3, *.gif a spousta dalších formátů).
* Používáte k platbám na internetu platební kartu? Máte její číslo uložené v počítači? Tak pravděpodobně nejste sami kdo ho zná.

Spyware rozdělujeme do skupin:

Adware - Spyware, které vás většinou obtěžuje při práci na PC reklamou.
Browser helper object - Jde o DLL knihovnu, která umožňuje programátorům změnit a sledovat Internet Explorer.
Hijacker - Spyware, které vám mění domácí stránku.
Dialery - Spyware, které přesměrovává telefoní linku na drahé telefoní tarify.
Keystroke Logger - Spyware, které sledují každý pohyb na vaší klávesnici. Některé druhy odesílají vaše hesla, na email autora spyware.
Malware - Spyware, které je obsaženo v programech, které tvrdí, že spyware odstraní.
Miscellaneous - Spyware, které je mixem skupin spyware. Obsahuje od každého něco.
Remote Administration - Spyware, které umožní vzdálenému uživateli, ovládat vaše PC.