Uživatel a počítačová bezpečnost

Andrea Kropáčová, CESNET CERTS[1]

Nejslabším článkem počítačové bezpečnosti obecně je vždy uživatel. Proto by měl být průběžně vzděláván a je nutné mu neustále připomínat základní pravidla pro bezpečné používání počítačů a služeb. Tento článek není návodem jak zajistit bezpečnost celé sítě nebo počítače, ani návodem na jejich bezpečnou konfiguraci. Je zaměřen na základní rizika a pravidla, která by měl každý uživatel znát a dodržovat tak, aby jeho prostřednictvím nedošlo k narušení bezpečnosti ať už konkrétně jeho dat nebo celého systému.

Základní pravidlo

Každý uživatel by měl vědět, že je nedílnou součástí širší počítačové bezpečnosti. Že bezpečnost jeho stanice není záležitostí pouze správce, nýbrž že on sám se na bezpečnosti své pracovní stanice i celé sítě aktivně podílí. Každá koncová stanice s narušenou bezpečností se může stát přestupním prvkem pro útok na ostatní zdroje v síti. Proto se počítačová bezpečnost týká všech prvků, i té nejobyčejnější pracovní stanice. *Každý systém je nejsnáze napadnutelný zevnitř.*

Vhodná volba hesla a jeho pravidelná změna

Pro automatické nástroje není problém vyzkoušet během několika minut stovky tisíc hesel; jako heslo nejsou tedy vhodná běžná slova (vyskytující se ve slovníku). Optimální nejsou ani jména oblíbených filmových či knižních hrdinů, záměna znaků s diakritikou za numerické symboly ležící na stejné klávese nebo použití dat identifikujících uživatele (adresa, čísla dokladů, data narození apod.). Hesla by měla pokud možno obsahovat i jiné než jen alfanumerické znaky (např. znaky `,.:;-=+_`). Měla by být také adekvátně dlouhá – řekněme alespoň 8 znaků – a je třeba je občas změnit.

[1] CERTS – Computer Security Incident Response Team

Ochrana hesel a klíčů

Není vhodné si heslo v otevřené textové podobě kamkoliv poznamenávat – do diáře, na papírky, na doklady, na nástěnku, na stůl, na displej počítače. Pokud uživatel nevěří své paměti, je vhodné chránit heslo například další šifrou a pro uložení použít externí médium (disketu, CD-ROM, DVD, CF, Palm), které je pak třeba adekvátně ochránit před zcizením. Heslo samozřejmě není žádoucí komukoliv sdělovat a také obráceně – nedovolte, aby někdo sděloval své heslo vám!

V případě přístupu k více službám nebo strojům, které nejsou autentizovány centrálně, není dobré používat všude stejné heslo. Pamatovat si pro různé služby různá hesla je sice trochu nepohodlné, ale nižší uživatelský komfort vynahradí vyšší bezpečnost vašich dat a programů.

Je třeba také dbát na správné používání hesla. Jestliže máte například heslo pro přístup k poště, není dobré zkoušet toto heslo ad-hoc pro jiné služby – obzvláště ne ty, o kterých nic nevíte nebo které jsou z principu nešifrované (FTP). Obecně platí, že je dobré zeptat se správce, který vám heslo vydal, ke kterým službám je možné je používat.

Mnoho uživatelů používá pro zjednodušení přístupu na vzdálené servery ssh klíče – typicky v případě, kdy potřebují pracovat s více vzdálenými servery, na kterých jsou hesla spravována individuálně. V těchto případech je nutné pečlivě zvážit, kde je možné uložit privátní klíč. Optimální je mít privátní ssh klíč uložen pouze na své pracovní stanici, byť to může komplikovat přenos dat mezi vzdálenými servery navzájem.

Ochrana obsahu zprávy a identity

Uživatelé si často neuvědomují, jak jednotlivé služby fungují. To je vede k mylné představě třeba o tom, kdo se může k jejich datům dostat a jak. Asi nejtypičtějším příkladem je elektronická pošta. Většinu běžných uživatelů šokují především dvě zjištění:

– že k obsahu jejich zpráv se může dostat každý, kdo má potřebné znalosti a možnosti (například odposlechem síťové komunikace

nebo přímým přístupem k souborům na poštovním serveru). Jedinou skutečně spolehlivou cestou jak ochránit data posílaná elektronickou poštou, je jejich *šifrování*. Optimální ochranu poskytují metody založené na *asymetrické kryptografii*, například *PGP klíče a X.509 certifikáty*.

– že kdokoliv na světě může poslat e-mail, který bude mít jako odesilatelskou adresu uvedenu adresu jejich. To, že do položky *Odesilatel* může každý vložit cokoliv, se uživatel většinou dozví až v okamžiku, kdy jim od nich samých přijde nesmyslný e-mail, o kterém ví, že si jej určitě neposlali. Stejně jako v případě ochrany obsahu zprávy, i tento problém má řešení – tím je *elektronický podpis*. Elektronický podpis je navíc řešením i při ochraně integrity zprávy. Umožňuje totiž zjistit, jestli zpráva nebyla cestou změněna.

O problematice šifrování zpráv a elektronického podpisu se podrobněji zmíníme v některém z dalších článků.

Ochrana certifikátů a revokační klíče

K používání elektronického podpisu a šifrování obsahu zpráv nás motivuje snaha ochránit svá data, jejich integritu a svoji identitu. Neméně nutné je ovšem chránit privátní části klíčů (PGP, X.509 certifikátů) a být připraven na možnost zcizení nebo zničení privátního klíče. V takovémto případě je důležité klíč co nejrychleji revokovat. Revokací (zneplatněním) vlastník klíče nebo certifikátu říká, že jeho elektronickému podpisu již není možné dále věřit. Pro případ zničení privátního klíče je rozumné, aby se uživatel na tuto možnost včas připravil; např. tím, že již při generování klíčů si vygeneruje zároveň i příslušný revokační klíč.

V souvislosti s elektronickým podepisováním zpráv a jejich šifrováním je nutné dbát na pravidelnou kontrolu toho, jestli nedošlo ke zneplatnění některého z klíčů nebo certifikátů, které máme uloženy ve svém klientovi (veřejné klíče lidí, se kterými jsme v e-mailovém kontaktu). Certifikační Autority, které certifikáty vydávají, obvykle nějakou vhodnou formou zveřejňují seznam revokovaných certifikátů (například prostřednictvím svých webových stránek nebo el. poštou). Tyto seznamy by měly být v systémech uživatelů pravidelně aktualizovány.

Pečlivost a pozornost

Uživatelé by měli neustále dbát i na záležitosti typu *zamykání počítače* při opuštění pracoviště (a to i krátkodobém) a na *uzavření aplikací* typu poštovní klient před odchodem z práce. Rovněž například v internetových kavárnách, obecně u jakéhokoliv počítače, u kterého jste hostem, je vhodné po skončení práce *vypnout spuštěné aplikace*. Je třeba být opatrný i při sdílení přenosových médií, například u médií vyměňovaných s kolegou. Obecně by měla být vždy aplikována zásada „důvěřuj, ale prověřuj“.

Přenosová média

Uživatelé by měli mít na paměti, že pravidelná antivirová ochrana jejich stanice je potřebná, není však univerzálním samospasitelným řešením. Používáme-li externí média, například při transporu dat mezi domácím a firemním počítačem, je nezbytné věnovat pravidelnou (antivirovou) péči i těmto médiím.

Archivace a šifrování citlivých dat

Pokud jsou výsledkem naší práce data, která nejsou určena pro každého a jejichž prozrazení by mohlo způsobit problémy, je vhodné data před uložením zašifrovat a mít je archivované pouze v šifrované podobě. K šifrování je možné použít např. již zmíněné PGP klíče nebo certifikáty. Dobrou volbou jak zvýšit bezpečnost dat je samozřejmě i *šifrovaný souborový systém*.

Znalost funkcionality používaných nástrojů a OS

Velkou bolestí současných technologií je skutečnost, že spolu se zvyšováním jejich uživatelské přítulnosti se zmenšuje povědomí uživatelů o tom, jak dané aplikace vlastně fungují a co jejich chování může způsobit. Pozdě se potom diví, jak je možné, že jejich „soukromý“ e-mail si může přečíst i někdo jiný než adresát, že data, která sami osobně smazali, jsou na pevném disku jejich stroje k nalezení ještě dlouho poté, co tak učinili, že se dopustili porušení autorských práv,

že na jejich e-mailovou adresu chodí velké množství spamů, že mají zavirovaný počítač a podobně. Je proto vhodné znát následující pravidla a řídit se jimi:

- Nepoužívat zdánlivě užitečnou funkci zapamatovat heslo pro příští použití, kterou nabízí např. www-prohlížeč nebo poštovní klient. Uživateli tak sice přibude trocha práce navíc, ale ta za bezpečnost určitě stojí.
- Pro mazání souborů používat sofistikované metody, které zajistí skutečné fyzické smazání dat samotných, nikoliv pouze informací o nich. Zde je dobré zmínit, že je potřeba dát pozor na citlivá data například při reklamování vadného paměťového média. To, že médium nefunguje, neznamená, že data na něm jsou nečitelná. Vhodným řešením může být používání šifrovaného souborového systému nebo šifrování citlivých souborů.
- Pro bezpečnou elektronickou komunikaci používat šifrování zpráv, např. pomocí osobního X.509 certifikátu nebo pomocí PGP klíčů. Pro ochranu identity elektronické zprávy podepisovat.
- Neotevírat podezřelé e-maily a zvláště ne jejich přílohy. Na zjevný spam zásadně neodpovídat a nežádat o vyřazení z evidence, i když se to v dopise nabízí. V případě, že tak učiníte, jen potvrdíte funkčnost své adresy a podnítíte její zařazení do spamové databáze adres.
- Při používání klientů pro sdílení dat může dojít při špatné konfiguraci k tomu, že již v okamžiku stahování se data automaticky nabízí ke stažení jiným uživatelům; uživatel to často netuší a spoléhá se na to, že když stahuje autorským zákonem chráněná data výlučně pro osobní použití a nehodlá je distribuovat dál, tak se ničeho špatného nedopouští. Netuší, že jeho klient automaticky tato data zpřístupní již v okamžiku stahovací fáze.
- K většině důležitých služeb a nástrojů existují jejich zabezpečené verze. Například pro práci s elektronickou poštou jsou to protokoly IMAPS, POPS a SMTPS, pro přístup na vzdálené servery a přenos dat jsou protokoly SSH a SCP, což jsou zabezpečené obdoby nechráněných programů telnet a FTP.
- Instalovat programy pocházející jen ze spolehlivých zdrojů! Není-li si uživatel jist, měl by instalaci nových věcí nechat na správci.

Psychologický nátlak

Každý uživatel by měl vědět o možnostech psychologického nátlaku, kterého se může stát obětí i on samotný. Měl by vědět, že nikdo – kolega, správce, ani nadřízený – nemá právo po něm pod jakoukoliv záminkou žádat sdělení hesla, a že taková žádost je nelegální, podezřelá a neměla by zůstat bez odezvy. Správce daného stroje heslo uživatele k ničemu nepotřebuje, protože má jiné prostředky, jak se v systému dostat tam, kam v souvislosti se svou rolí správce potřebuje. Nadřízený pracovník má zase k dispozici formální postupy, které může uplatnit v souladu s pravidly firmy. Nikdo nemá nárok, aby mu kolega prozradil heslo ke svému účtu, ke klíči a podobně. Vždy je vhodné si uvědomit paralelu z běžného života – souseda, nebo šéfa také neučíte svůj podpis podle bankovního podpisového vzoru. O možnostech a rizicích psychologického nátlaku by měli být informováni především začínající studenti a noví zaměstnanci.

Do této kategorie rovněž patří poplašné e-maily typu „honem si změň heslo na 'zbcdef', jinak dojde ke zneužití tvého účtu“. Ke zneužití skutečně dojde, pokud takovéto výzvy uposlechnete.

Základní znalost práv, povinností a rizik

Uživatel se může dostat do vážných problémů i zdánlivě nevinnou činností jen proto, že nezná základní práva a povinnosti. Typickým příkladem je *porušení autorských práv* vystavením autorsky chráněných dat (filmů, hudby, software) na www-stránce nebo prostřednictvím klienta poskytujícího data veřejně ke stažení. Tímto činem se dopustí nelegálního šíření dat chráněných autorským zákonem a to může vést až k žalobě postiženou osobou a žádosti o finanční kompenzaci. Občas si uživatelé myslí, že se jim na poli autorkého práva nemůže nic stát, protože „Co mi může udělat firma z USA? Do České republiky na mě přece nedosáhne“. Je to představa mylná; většina zemí včetně ČR má zákony, které postihují nelegální šíření dat chráněných autorským právem a každý (i osoby ze zahraničí) se

jejich prostřednictvím mohou zneužití svých dat bránit.

Dalším poměrně častým prohřeškem, kterého se uživatelé dopouštějí, je spamování (spamming). Rozesláním například reklamních informací velkému množství příjemců se uživatel dopouští nejen prohřešku proti slušnosti a síťové etiketě, ale v některých případech také porušuje platné zákony.

Velkou bolestí je lehkomyslné zacházení s privátními údaji a daty. V posledních letech je velmi populární tzv. *phishing*, který svádí uživatele, aby sami prozradili svůj přístupový kód k bankovnímu účtu či jiným službám. Princip je velmi jednoduchý: uživateli přijde poplašná zpráva, že jeho bankovnímu účtu hrozí zneužití, ktere může vést ke ztrátě financí. Že tomu ale může zabránit tím, když okamžitě změní svůj přístupový kód – a to prostřednictvím uvedeného odkazu. Problém je však v tom, že příslušný odkaz nevede na stránky zmíněné banky (i když se tak tváří), nýbrž na stránky útočníka, kde je uživatel vyzván k vyplnění důležitých údajů. Pokud tak skutečně učiní, jeho osud je zpečetěn.

Na tomto poli je opravdu asi nejlepším doporučením chladná hlava, zdravý selský rozum a používání analogií z neinternetového života. Neznámému příchozímu, který by tvrdil, že vaše konto bude za 5 minut zneužito, ale on vás může zachránit když mu dáte své doklady a naučíte jej svůj podpis, také asi nebudete věřit, ale půjdete se informovat do své banky.

Spolupráce správce a uživatele

Velice důležitým bodem na poli bezpečnosti je komunikace mezi uživatelem a správcem. Uživatel by měl vědět, že správce je zde od toho, aby mu maximálním způsobem pomohl, obzvláště v případě problémů na poli bezpečnosti. Uživatelé se často stydí přiznat, že pravděpodobně udělali něco, co může vést k narušení bezpečnosti (např. kompromitace hesla) a tuto skutečnost tutlají – ať již ze strachu před správcem, před nadřízenými nebo z obavy o svou osobní prestiž. To je však zásadní chyba. Včasným a vhodným zásahem může správce ještě mnohé zachránit. Čím déle uživatel s upozorněním na svou chybu váhá, tím horší situace nakonec může být. Proto platí: správce se nebojte, zhřešivšího uživatele správce nezastřelí, ale pomůže mu.

Také je dobré si uvědomit, že i správce je jen člověk a není vševědoucí. Proto pojme-li uživatel podezření, že něco není s jeho počítačem nebo s konkrétní službou v pořádku, měl by vždy správci své podezření sdělit, byť by se nakonec ukázalo jako mylné.

Následky narušení bezpečnosti počítače/sítě

Uživatelé si často myslí, že bezpečnost jejich dat, počítače a sítě obecně se jich samotných netýká. Zvláště pak v případě, kdy jsou pouze „pasivními“ uživateli a o počítač, který při své práci používají, se stará „správce“. Mají pocit, že za vše zodpovídá správce a v případě narušení bezpečnosti se jim nemůže stát žádná újma a za nic neponesou odpovědnost. Jedná se samozřejmě o představu mylnou – i pasivní uživatel se může na porušení bezpečnosti svého počítače aktivně podílet. Například tím, že kolegovi „půjčí“ k použití svůj počítač nebo své heslo, použije zavirované přenosové médium nebo prostě jen svou naivitou a nevědomostí (porušení autorkých práv, spamming). Další mylnou představou, se kterou někteří uživatelé předem kalkulují, je, že v případě narušení bezpečnosti nelze zjistit, jak přesně k němu došlo a kdo je za problém zodpovědný. Většina zkušených správců ale je schopna tyto věci odhalit. Významnou pomoc v pátrání po slabém místě napadeného systému představují například systémy pro obnovu smazaných dat nebo centrální log-servery, které zaznamenávají důležité operace (jako například přihlášení do systému, změna dat a podobně). Uživatelé by o těchto technologiích měli vědět (stejně jako o faktu, že správce je člověk zvídavý a případy narušení bezpečnosti, když už nastanou, bere jako příležitost se něco nového naučit), zvyšuje to totiž jejich pocit odpovědnosti. Jakmile se dozvědí, že ve světě počítačů nic nemizí nenávratně, jejich přístup se změní ve prospěch bezpečnosti. Dále je vhodné informovat

uživatele o možných důsledcích narušení bezpečnosti. Ty mohou být velice vážné – často jde o zneužití identity uživatele a jeho osobních dat například pro získání přístupu k privátním datům nebo k oklamání ostatních.

To všechno může vést k narušení soukromí, ke ztrátě osobní prestiže, dobrého jména, financí, k problémům v rodině a partnerském životě, k problémům v zaměstnání a následně jeho ztrátě, k vyloučení ze školy.

Obecný recept jak dosáhnout 100% zabezpečení asi neexistuje, co proto říct závěrem? Asi nejvýstižnější je pionýrské „buď připraven“ a v případě, že k narušení bezpečnosti dojde, reagovat rychle a efektivně se snahou odstranit vzniklý problém s co možná nejmenšími následky. Dále platí, že klíčem k bezpečnosti počítačů a aplikací je koncový uživatel. Čas vynaložený na jeho vzdělávání se určitě vyplatí – čili „se učit, se učit, se učit …“. □