Zabezpečení operačních systémů

Úvod

Zabezpečení operačních systému je v dnešní době čím dál více řešeným tématem. Schopnost uchovávat data v počítači, serverech, telefonech či televizích je skvělá vlastnost se kterou však přichází i řada rizik. Často se totiž stává, že informace uložené v zařízení mají větší hodnotu než samotné zařízení. Proto musíme umět pochopit proč a jak funguje zabezpečení jednotlivých operačních systémů, abychom mohli naše data zabezpečit před odcizením či zneužitím.

Klíčové pojmy

Bezpečnost – obtížnost dostat se neoprávněně k informacím, ochrana systému před riziky a hrozbami

Spolehlivost – očekávání, že objekt bude fungovat vždy určitým předpokládaným způsobem

Linux/Unix

Systémová oprávnění

Linux je víceuživatelský operační systém, který umožňuje, aby více uživatelů mohlo přistupovat k souborům najednou s různými oprávněními. Každý soubor má přiděleného/né uživatele s nastavenými oprávněními, která vznikají s vytvořením daného souboru.

Linuxové systémové oprávnění se dělí podle vlastníka na tři základní typy:

- Owner (u) – Většinou ten, kdo vytváří soubor. Je definován jako jeho vlastník (owner ≠ root) a má většinou má nejvyšší oprávnění.
- Group (g) – Skupina uživatelů jíž se definují oprávnění pro práci se soubory.
- Others (o) {ergo. „The World"} – Ostatní užitelné. Všichni ti, co nejsou definováni v systému. Toto se definuje na serverech a jiných zařízeních, kde je vysoká možnost připojení z jiného zařízení a pro zobecnění se tito uživatelé označují touto formou.

Tito vlastníci označují, pod koho spadá jakýkoliv soubor v systému a definují jednotlivé pravomoci k práci s každým souborem. V Linuxu oproti Windows máme jen 3 druhy oprávnění:

- Read – Opravňuje uživatele číst daný soubor
- Write – Opravňuje uživatele modifikovat daný soubor
- Execute – Opravňuje uživatele spouštět daný soubor

Number	Permission Type	Symbol	Binary
0	No Permission	---	000
1	Execute	--x	001
2	Write	-w-	010
3	Execute + Write	-wx	011
4	Read	r--	100
5	Read + Execute	r-x	101
6	Read + Write	rw-	110
7	Read + Write + Execute	rwx	111

Příkazy

`ls -l` – zobrazí soubory ve složce včetně parametrů a dalších vlastností

`useradd` – vytvoří nového uživatele nebo upraví stávajícího

`chown` = spravuje vlastnictví souborů, složek v Linuxovém souborovém systému
Parametry:

- **`--help`** – vypíše nápovědu
- **`--version`** – vypíše aktuální verzi skriptu
- **`-c, --changes`** – zobrazí změny, které byly provedeny
- **`-R, --recursive`** – u složek změní oprávnění i pro jejich podsložky a podsoubory

Příklad:
`sudo chown -Rc myuser:mygroup otherfiles`
sudo – spouštění příkazu jako root
chown – spuštění příkazu pro úpravu vlastnictví
-Rc – atribut pro rekurzi, změní všechny vlastnictví pro podložky a podsoubory a zároveň parametr pro zobrazení změn (v Linuxu to lze psát takto dohromady; je to samé jako „-R -c“)
myuser:mygroup – změna vlastníka na uživatele: „myuser“ a na skupinu: „mygroup“
otherfiles – soubor nebo soubory, které jsou modifikované

Windows

Systémová oprávnění

Windows je stejně jako Linux víceuživatelský operační systém, který umožňuje stejně jako Linux, aby více uživatelů mohlo přistupovat k souborům najednou s různými oprávněními. Každý soubor má přiděleného/né uživatele s nastavenými oprávněními, která vznikají s vytvořením daného souboru.
(ergo. To samé jako u Linuxu)

Windows zobrazuje uživatele jako skupiny:

- Administrators – uživatelé, kteří mají veškerou kontrolu nad systémem a vše v něm včetně uživatelských profilů
- Backup Operators – účty, které jsou používány k záloze a obnově dat
- Users – nejčastější profil; uloží se do počítače a uživatel se pomocí něj přihlašuje do domény
- Guests – uživatel, kteří mají dočasné profily; po odhlášení se smažou
- Power Users – mají stejná práva jako administrátoři, ale nemohou modifikovat Administrátorskou skupinu.

Dále má Windows ještě 7 identit, jak popsat uživatele:

- Everyone – představuje všechny uživatele, kromě uživatelů pod identitou *Anonymous Logon*
- Creator Owner – uživatel, který vytvořil (nebo v budoucnu vytvoří) vybraný soubor/složku anebo převzal její vlastnictví
- Authenticated User – všichni uživatelé, kteří se přihlásili svým jménem a heslem (Výjimka je uživatel guest, který i s heslem není *Authenticated User*)
- Interactive – Uživatelé připojení místně anebo pomocí programu "Připojení ke vzdálené ploše"
- Anonymous Logon – Připojení z internetu/sítě, které nemá prověření (může být zároveň *Interactive*)
- Dial – Uživatelé, kteří se k počítači připojí pomocí telefonického připojení
- Network – Všichni uživatelé, kteří k počítači přistupují z internetu/sítě, s výjimkou těch, kteří jsou připojeni pomocí "Připojení ke vzdálené ploše"

K těmto identitám můžeme přiřadit jednotlivá oprávnění, která jsou u Windows poměrně rozsáhle (neprakticky) zpracovaná. Zde jsou pouze ty nejdůležitější:

- Úplné řízení – umožňuje uživateli/skupině úplné řízení vybraného souboru/složky
- Měnit – umožňuje uživatelům/skupinám číst, měnit, vytvářet a odstraňovat soubory, nikoliv ale měnit oprávnění nebo převzít vlastnictví souborů
- Číst a spouštět – umožňuje uživatelům/skupinám zobrazovat soubory a spouštět programy
- Zobrazovat obsah složky (pouze u složek) - poskytuje stejná oprávnění jako možnost "Číst a spouštět" a je k dispozici pouze u složek
- Číst – umožňuje uživatelům/skupinám zobrazit obsah složky, atributy souborů, číst oprávnění a synchronizovat soubory
- Zapisovat – umožňuje uživatelům/skupinám vytvářet soubory, zapisovat data, číst atributy a oprávnění a synchronizovat soubory
- Speciální oprávnění – pokud jsou tato oprávnění vybrána, znamená to, že nastavená oprávnění neodpovídají žádné přednastavené šabloně; toto je možné dopodrobna nastavit

Příkazy

`gpresult` = zobrazí informace o uživatelích

Aktualizace systému

Jedním z klíčových prvků ochrany a zabezpečení systému jsou aktualizace. Jak na Linuxu, kde si uživatel aktualizuje sám (na některých distribucích zautomatizované) tak i na Windows, kde jsou uživatelé povinni aktualizovat svůj systém po vydání aktualizace ihned při dalším restartu počítače (Windows 10).
Důvodem těchto aktualizací je záplatování chyb a děr v kódu systému, přes kterou by mohl útočník napadnou počítač a získat data či citlivé údaje. Pro tento typ případu vzniká i nový typ útoku, který se jmenuje day-zero attack. Tento útok je používán před vydáním aktualizace a spoléhá, že uživatel si nenaistaluje aktualizaci včas (více viz. Útoky).

Social engineering

Jedná se o jeden ze způsobů, jak lze proniknout do systému a získat informace. Při tomto typu útoku se zneužívá lidského faktoru (zpravidla neproškolených zaměstnanců), kteří nevědomě zpřístupní nebo jen ulehčí útočníkovi průnik do systému. Je to pro ně jednoduší cesta než dešifrovat hesla, popřípadě hledat chyby v systému, které by mohli napadnout.
Při tomto typu útoku útočník může použít řadu nástrojů – email, telefon atd. Útočník si potřebuje zajistit pouze základní informace o firmě/uživateli a zapracovat na psychologii, aby při lhaní měl jasný a rázný hlas a působil věrohodně.

Fyzické zabezpečení

Další velmi důležitá věc, které je často opomíjena je fyzické zabezpečení serveru. Musí být jasné, že pokud se útočník, ať už přes social engineering nebo kvůli nízké bezpečnosti se dostane ke zdroji (serveru), tak mu zcela usnadníme přístup k naším datům. K přístupu k datům mu už může zabránit jen šifrovaný souborový systém, který pokud nemá kvalitní heslo je k ničemu.
Server, switche či jakékoliv rozvody by měli být i hardwarově zabezpečené (většinou na klíč, kód, přístupovou kartu) kvůli omezení přístupu více osob.

Zdroj (server) samozřejmě nemusí zničit pouze člověk, ale i přírodní jevy:

- Elektřina – výpadky, přepětí, bouřky, zkraty
- Oheň – protipožární pravidla, automatizovaný protipožární systém, ideální hasící přístroje
- Teplota a vlhkost vzduchu – klimatizace a udržení teploty
- Voda – záplavy, prasklé vodovodní rozvody, vodní chlazení

Hesla

Heslo je v dnešní době nejběžnější způsob ověřování identity. Často je to i jediný způsob, jak uživatele autentizovat. Většina lidí tomuto nevěnuje skoro žádnou pozornost, avšak je to Váš osobní klíč k Vaším datům a osobním údajům.

Aby heslo bylo co nejbezpečnější a nejefektivnější musíme použít následují pravidla:

- Heslo nesmí být stejné jako uživatelské jméno
- Nesmí být triviální a používané jako: „12345“, „qwertz“, „asdfgh“, „aaa“, „098765“)
- Nesmí být pouze jedno slovo, ať už je v jakémkoliv jazyce
- Jednoduše zjistitelné informace – jméno, přímení, telefon, datum narození
- Mělo by být složeno z kombinace malých a velkých písmen + nějaké speciální znaky
- Jakékoliv heslo, které splňuje tyto podmínky, ale nikomu jste ho neřekli

Samozřejmě pokud budeme mít heslo dlouhé 40 znaků s významem nějaké věty tak pravděpodobnost, že ho někdo rozšifruje je mizivá.
Heslo by také mělo být jednoduše zapamatovatelné pro danou osobu, aby se předešlo jeho ztrátě.

Linux

Hesla v Linuxu jsou šifrována jednosměrně tj. porovná se heslo zadané uživatelem s originálem. Pokud identifikace souhlasí je uživatel vpuštěn do systému.

Hesla jsou uložena v souboru *etc/shadow* a jsou zahešována. K tomuto souboru má přístup pouze root.

Prolomení hesla

Je řada způsobů, jak prolomit hesla. Dnešní počítače používají nejčastěji 3 metody:

- Brute-force – vyzkouší všechny možné kombinace znaků, dokud netrefí správnou kombinaci
- Dictionary attack – vyzkouší slova a fráze ze všech slovníků + častá hesla
- Kombinace – kombinace Brute-force a dictionary attack

Dnešní počítače mají s prolomením hesel problém, avšak s nástupem kvantových počítačů tento problém rychle mizí.

Antivirus

Antivirový program je software, který slouží k identifikaci a lokalizaci škodlivého softwaru(=malware) a jeho následné odstranění. Tuto kontrolu provádí antivirus dvěma způsoby:

1. Heuristická analýza – prohlížení dat na lokálním disku a hledáním sekvencí kódu, který odpovídá viru
2. Sledováním činnosti počítače a zjišťování podezřelých aktivit; Analýza dat na portech a síti.

Úspešnost závisí na účinnosti antiviru, na jeho aktuálnosti a schopnosti analyzovat nástroje, které uživatel používá. Některé antiviry dokonce upozorňují na bezpečnost uživatelských hesel uchová je ve své vnitřní databázi. Samozřejmě antivirus nesmí být pro počítač zátěž a musí pracovat tak, aby využíval minima zdrojů.

Nejznámější antivirové programy jsou – ESET, AVAST, BitDefender, Microsoft Defender, Kaspersky Antivirus, AVG, McAfee a mnoho dalších.

Linux

Antivirus na Linuxu je poněkud kontroverzní téma. Většina uživatelů věří v to, že antivirus není potřeba, protože většina virů není vytvořená pro Linux a tím pádem na Linuxu jednoduše nefungují. Je sice pravda že 99 % virů je vytvořeno pro Windows, avšak to 1 % je pořád velké riziko v dlouhodobém měřítku. Antivirový program by měl být na každém zařízení jako povinná výbava (jak to nedávno udělal Windows s Windows Defenderem). Většina antivirových programů na Linux je kompatibilní s Linuxem.

Škodlivý software (malware) – tytyty soft

Škodlivý software (malware) je nežádoucí software, který má za úkol vniknout a poškodit počítač, systém či data v něm, popřípadě je odeslat útočníkovi. Hlavní motivací malwaru je však šířit se po síti dál. Cílem těchto malwarů je způsobit škodu uživatelům nebo přinést nějaký peněžní obnos tvůrcům malwaru (ad-ware, randsom-ware atd.).

Druhy škodlivého softwaru

- Worms – virus, který se automaticky replikuje a přeposílá se do dalších počítačů; většinou přebírá kontrolu nad síťovou komunikací
- Trojan horses – je ukryt v programu, který si uživatel nainstaluje; tato část programu, typicky skrytě, koná nějakou funkci, se kterou uživatel nesouhlasí
- Ransomware – vyděračský software, který požaduje peněžní obnos za rozšifrování dat či odblokování počítače
- Crimeware – je určen k páchání trestné činnosti např. krádeže identit, platebních karet pomocí sociálního inženýrství
- Spyware - využívá stránky k odeslání dat z počítače bez vědomí uživatele (můžou odesílat hesla, čísla kreditních karet, data pro cílenou reklamu apod.)
- Adware – je virus, který znepříjemňuje práci a zaplavuje systém/aplikace reklamami
- Scareware – je malware, který pomocí sociálního inženýrství manipuluje a donucuje si uživatele si koupit nechtěný software

Rootkit – je technika která napomáhá utajení škodlivého software v počítači modifikování operačního systému a skrývání ho v něm
Backdoors – je metoda, která útočníkovi umožní obejít autentizační systémy a tím v budoucnu zajistit opakovaný přístup k počítači

Útoky

- Denial of service (DDOS) – je útok na internetové služby/stránky, s cílem je odstavit nebo znepřístupnit ostatním uživatelům. Často se vytváří přehlcením serveru požadavky.
- Day-zero – je útok, který se snaží zneužít zranitelnosti počítačového software, která není známá nebo zatím není vytvořená obrana (např. aktualizace vyjde za pár dní). Počítač je ohrožen až do doby aktualizace.

Firewall

Firewall je software nebo hardware, který pomocí filtrů analyzuje provoz ze sítě/internetu do soukromé sítě nebo přímo do počítače a naopak. Můžeme nastavit určitá pravidla pro provoz na síti (blokovat porty nebo určité formáty apod.) anebo pouze filtrovat potenciálně nežádoucí data.
Firewall používá 3 metody ke správě provozu na síti:

1. Packet filtering – přednastavené filtry, kterými packety musí projít; pokud se tak nestane paket bude zahozen
2. Proxy service – data jsou nejdříve poslána do firewallu a poté co jsou prohlédnuta a schválena mohou být odeslána do systému a naopak
3. Stateful inspections – Novější metoda, která neprozkoumává kompletně všechna data, ale pouze se dívá po klíčových částí dat a porovnává je se svou databází ověřených dat; pokud je tam charakterová shoda tak packet pustí dál

Firewalls chrání před již dříve zmíněnými útoky (viz. Útoky) a dokáže analyzovat většinu nežádoucího softwaru, než se dostane do PC. Samozřejmě opět záleží, jaký firewall si pořídíme a jaké má vlastnosti (stejně jak u antivirů).
Mnohem účinnější je hardwarový firewall, který je ale náročnější na správu, a ne každý si ho může dovolit.

Windows firewall

Jeden z nejzákladnějších firewallů vůbec. Je defaultně předinstalovaný na operačním systému Windows. Není jeden z nejúčinnějších, avšak dokáže většinu uživatelů ochránit před většinou hrozeb na internetu. Do Windows jde doinstalovat jiný lepší, který ho nahradí.

Uncomplicated firewall

Jeden z nejjednodušších firewallů na Linux (má to i v názvu). Je designován tak, aby byl jednoduše pochopitelný, nastavitelný a funkční. Má poměrně malou sadu příkazů, ale i přes to plní svoji práci překvapivě dobře.

LDAP

Je protokol, který umožňuje spravovat a uchovávat informace o složkách a zprostředkovávat s nimi práci přes internet, jako např. sdílení informací o: „uživatelích, systému, aplikacích, ale i jména, emaily, telefonní čísla. Jde o centrální správní jednotku obsahující informace o všech objektech sítě.
V Linuxu se používá OpenLDAP což je ekvivalent k LDAP, který se používá na Windows.

Active directory

Je název pro vytvoření adresářových služeb, které fungují na Windows pomocí LDAP. V počítačové síti zajišťuje autentizaci a autorizaci uživatelů, počítačů a dalších služeb.

Diskové kvóty

Je omezení paměti/počtu souborů na disku pro daného uživatele v síti. Operační systém při překročení nedovolí uložení více dat, než je nastaveno. Je potřeba speciálního souborového systému např. NTFS, ext2, ext3 nebo ReiserFS pro nastavení diskových kvót.

Parametry diskových kvót:

- Hard limit – maximální možné obsazení diskového prostoru, nad tuto hranici si uživatel už nic neuloží
- Soft limit – hranice lze ji překročit, nicméně uživatel bude varován a poběží mu grace period

- Grace period – uživatel může dočasně uložit na disk více, než je uvedeno v parametru "Soft limit" na dobu zadanou parametrem "Grace period“; po uplynutí této doby se uživateli nepodaří na disk uložit více, i když ještě nepřekročil mez zadanou parametrem "Hard limit"
- Inodes, Blocks – kvóty lze nastavit jak na celkový objem dat na disku, tak na počet souborů

Pro každého uživatele lze zvlášť nastavit různé parametry.

Zdroje

1. https://cs.wikipedia.org/wiki/Diskov%C3%A1_kv%C3%B3ta
2. https://cs.wikipedia.org/wiki/Heuristick%C3%A1_anal%C3%BDza
3. https://cs.wikipedia.org/wiki/Prolomen%C3%AD_hesla
4. https://cs.wikipedia.org/wiki/Slovn%C3%ADkov%C3%BD_%C3%BAtok
5. https://cs.wikipedia.org/wiki/Po%C4%8D%C3%ADta%C4%8Dov%C3%BD_%C4%8Derv
6. https://en.wikipedia.org/wiki/Dictionary_attack
7. https://en.wikipedia.org/wiki/Antivirus_software
8. https://en.wikipedia.org/wiki/Malware
9. https://cs.wikipedia.org/wiki/Crimeware
10. https://cs.wikipedia.org/wiki/Denial_of_service
11. https://cs.wikipedia.org/wiki/Trojsk%C3%BD_k%C5%AF%C5%88_(program)
12. https://cs.wikipedia.org/wiki/Spyware
13. https://cs.wikipedia.org/wiki/Adware
14. https://cs.wikipedia.org/wiki/Ransomware
15. https://en.wikipedia.org/wiki/Scareware
16. https://cs.wikipedia.org/wiki/Zero_day_%C3%BAtok
17. https://cs.wikipedia.org/wiki/Exploit
18. https://searchsecurity.techtarget.com/definition/firewall
19. https://computer.howstuffworks.com/firewall4.htm
20. https://en.wikipedia.org/wiki/Windows_Firewall
21. https://en.wikipedia.org/wiki/Uncomplicated_Firewall
22. https://cs.wikipedia.org/wiki/Active_Directory
23. https://cs.wikipedia.org/wiki/LDAP
24. https://en.wikipedia.org/wiki/Lightweight_Directory_Access_Protocol
25. https://www.root.cz/clanky/lehky-uvod-do-ldap/
26. https://searchwindowsserver.techtarget.com/definition/Active-Directory
27. https://support.zcu.cz/index.php/LPS:Active_Directory
28. https://digilib.k.utb.cz/bitstream/handle/10563/24983/havl%c3%ad%c4%8dek_2013_bp.pdf?sequence=1&isAllowed=y
29. https://cs.wikipedia.org/wiki/Heslo
30. https://avonet.cz/24880-zabezpeceni-windows-pc
31. https://dspace.vutbr.cz/bitstream/handle/11012/6054/BcMilanPolach.pdf?sequence=-1
32. http://digilib.k.utb.cz/handle/10563/12490
33. http://help.elsatnet.cz/?q=zabezpeceni
34. https://en.wikipedia.org/wiki/Zero-day_(computing)
35. https://blog.thesysadmins.co.uk/group-policy-gpresult-examples.html
36. https://docs.microsoft.com/en-us/windows-server/administration/windows-commands/gpresult
37. https://ksi.fjfi.cvut.cz/prava-souboru-ve-windows
38. https://wintip.cz/505-jak-ve-windows-10-pridat-mistni-uzivatelsky-ucet-bez-uctu-microsoft
39. https://slideplayer.cz/slide/3207595/
40. https://cs.wikipedia.org/wiki/Microsoft_Windows#Opr%C3%A1vn%C4%9Bn%C3%AD
41. https://cs.wikipedia.org/wiki/Windows_10
42. https://terminal-server.cz/napoveda/nastaveni-uzivatelu-a-pristupovych-prav/
43. https://jnp.zive.cz/jak-spravne-upravit-ucty-ve-windows
44. https://www.internetembezpecne.cz/internetem-bezpecne/navody/windows-uzivatelske-ucty/
45. https://docs.microsoft.com/cs-cz/dotnet/framework/security/wif-overview
46. https://www.samuraj-cz.com/clanek/opravneni-u-souboru-a-slozek-ve-windows/
47. https://linux.die.net/man/8/adduser
48. https://cs.wikibooks.org/wiki/Linux:P%C5%99ehled_z%C3%A1kladn%C3%ADch_p%C5%99%C3%ADkaz%C5%AF#Utility_pro_pr%C3%A1ci_se_soubory
49. https://www.guru99.com/file-permissions.html
50. https://www.linuxquestions.org/questions/linux-general-1/what-is-the-user-1000-a-4175510196/
51. https://www.computerhope.com/unix/uchown.htm
52. https://www.centos.org/docs//2/rhl-gsg-en-7.2/s1-navigating-ownership.html
53. https://www.interval.cz/clanky/uvod-do-zabezpeceni-vps-linuxu/
54. https://www.linuxexpres.cz/praxe/pruvodce-linuxem-8-zabezpeceni-linuxu
55. https://digilib.k.utb.cz/handle/10563/24983
56. https://access.redhat.com/documentation/en-US/Red_Hat_Enterprise_Linux/4/html/Step_by_Step_Guide/s1-navigating-ownership.html
57. http://www.abclinuxu.cz/ucebnice/zaklady/principy-prace-se-systemem/pristupova-prava
58. https://cs.wikipedia.org/wiki/Spolehlivost_(po%C4%8D%C3%ADta%C4%8Dov%C3%A9_s%C3%ADt%C4%9B)