

Správa pracovních stanic

Radomír Orkáč
VŠB-TUO, CIT 872
20. 5. 2009, Praha

radomir.orkac@vsb.cz



Správa pracovních stanic

- Správa systému (zodpovědnost, pravidelnost)
- Vhodné umístění v síti
- Firewall [Daniel Studený]
- Aktualizace
- Anti-malware nástroje
- Nástroje na vyhledávání rootkitů
- Antispamová ochrana
- Auditovací nástroje

Správa pracovních stanic

- **Skenery založené na signaturách nenajdou 58% malware (Global Threat Report)**
 - Kontrola běžících procesů
 - Nežádoucí komunikace v síti
 - Kontrola logu (událostí)
 - Kontrola integrity souborů
- **Osvěta uživatelů a správců**
- Směrnice, nařízení, pravidla

Umístění pracovních stanic

- Umístění do lokální sítě za firewall instituce
- Pro zvýšení bezpečnosti zajistit :
 - Reverse path filter
 - Port security
 - DHCP snooping + ARP inspection
 - Oddělovat skupiny koncových stanic VLANy
- Koncovým stanicím je vhodné přidělovat doménová jména pod dohledatelným identifikátorem (pcs1a – místnost S1)
- Registrace MAC adres (dohledatelnost)

Základní ochrana - firewall

- Firewall – pracovní stanice
 - Umožňuje filtraci a případně i monitorování síťového provozu
 - Chrání před únikem dat či napadením služeb

- Základní konfigurace
 - Počítač smí komunikovat sám se sebou. Povolení veškeré komunikace z adresy 127.0.0.1
 - Povolit odchozí komunikaci – na vyžádání aplikace
 - Povolit příchozí komunikaci již navázanou ze stanice a zakázat ostatní příchozí spojení na pracovní stanici ze sítě

Základní ochrana - firewall

- Konfigurace pravidel pro protokol IPv6
- Vzdálené ověření funkčnosti a správné konfigurace (nmap, telnet)
- V bezpečnosti nespoléhat na NAT (překlad adres) či „hlavní“ firewall
- Počítat s útoky z vnitřní sítě
- Evidence pravidel (kdy a koho kontaktovat)
- Ostatní doplňky
 - Port knocking
 - Kontrola obsahu (content filter)

Základní ochrana - aktualizace

- Aktualizace OS a aplikací
 - Každý program (systém) obsahuje chyby!
 - Aktualizace Windows – každé druhé úterý v měsíci
 - CVE - Common Vulnerabilities and Exposures
- CTUpdate
 - Nástroj pro stahování a offline instalaci potřebných aktualizací ze stránek Microsoftu
 - Win 2000 – Windows Server 2008, Office

Správa systému

- Zastavení nepotřebných, nebezpečných služeb
 - NetMeeting, Indexing service, ...
 - FTP, telnet, vzdálená správa (VNC, ...)
 - Nemusí zvýšit pouze bezpečnost (stabilita, výkon)
- Odinstalování nepotřebných aplikací
- Kontrola integrity
 - `C:\> sfc /verifyonly`
 - Tripwire, Integrit
- Audit zabezpečení, konfigurací, licencí
 - MS Baseline Security Analyzer, WinAudit

Kontrola běžících procesů

- Malware může být odhalen i pokud není známa jeho signatura či projev
- Analýza (Hijackthis, ComboFix, UPM)
 - Podezřelé názvy - např. „anivirus”, reader_s
 - Online knihovna procesů
<http://www.processlibrary.com>
 - Fórum, kde Vám poradí
<http://www.viry.cz/forum/>
- Automatická (online) analýza logu
<http://www.hijackthis.cz/>

Nežádoucí komunikace v síti

- Pravidelnou kontrolou otevřených portů a navázaných spojení můžeme odhalit:
 - Síťovou aktivitu malware
 - Nežádoucí skenování ostatních počítačů
 - Navázané připojení na útočnickem řízený server
 - ...
- Pomocné programy
 - Netstat, Active ports, TCPView
 - Nmap
 - Ngrep, IDS Snort

Malware

- Malware
 - „Malicious“ (zákeřný) software, škodlivé programy
- Souhrnné označení malware zahrnuje:
 - viry, trojské koně, červy, špionážní software (spyware), „reklamní“ software (adware), únosce (hijackers), dialers,
- Motivace tvůrců:
 - vtip, experiment, pomsta, zviditelnění, finanční prospěch, získávání informací, šíření nezákonného obsahu, získání technických prostředků.

Viry

- Vlastní mechanismy šíření
 - Schopnost replikace → kód připojen k souborům
- Nutná asistence uživatele
 - Aktivace (otevření/spuštění souboru)
 - Přenos na další systémy (paměťová média, e-mail)
- Rozdělení podle oblasti napadení
 - Makroviry, boot viry, souborové viry
- Rozdělení podle chování
 - Polymorfní, stealth

Červi

- Vlastní mechanismy šíření
 - Bez asistence uživatele
- Skenovací modul
 - Hledání vhodného cíle pro další šíření
- Penetrační modul
 - Průnik do cílového systému
 - Vybrané zranitelnosti
- Propagační modul
 - Vytvoření kopie celého červa
 - Přesun na cílový systém

Trojský kůň, sběrači informací

- Trojský kůň
 - Vlastními prostředky není schopen replikace a šíření → spoléhá na uživatele
 - Návštěva webových stránek, stažení aplikace, otevření dokumentu, warez, p2p
 - Šetřič obrazovky, hra, podvodný antivir
- Sběrači informací (data collectors)
 - Spyware (špionský software)
 - Keylogger (zaznamenává stisknuté klávesy)
 - Sniffer (zaznamenává síťový provoz)

Botnet

- Bot
 - Program, který je řízen počítačem útočníka
 - Využívá IRC, P2P pro spojení s centrálou
 - Firewall často filtruje jen příchozí spojení
- Botnet (bot networks)
 - Počítače (tisíce, milióny) infikovány stejným botem
 - Rozesílání spamu, hromadné útoky, pay-per-click

Anti-malware

- Anti-malware nástroje
 - Slouží k hledání, odstranění či izolaci počítačových virů, spyware a jiného škodlivého software
- Metody detekce
 - Kontrola dat na základě porovnání s databází signatur (průběžně aktualizovanou!)
 - Kontrola podezřelých aktivit
 - Heuristická analýza
- Možnost spouštění
 - Ruční, rezidentní štít, online skener, live CD

Analýza - podezřelý soubor

- **Podezřelý soubor na běžném PC nespouštět!**
- Zobrazení tisknutelných znaků

```
$ strings dhaywcq.exe  
USER %s %s %s :%s  
PASS %s  
NOTICE %s :  
NICK
```

- Získání MD5 hashe

```
$ md5sum dhaywcq.exe 61081640b1f491ef216d79cf73557687
```

- Google → ... Backdoor.IRCBot! ...

Online skener

Online skener, např. <http://www.virustotal.com/>

Soubor před spuštěním:

Antivirus	Version	Last Update	Result
a-squared	-	-	Backdoor.Win32.PoeBot.C!IK
AhnLab-V3	-	-	Win32/IRCBot.worm.Gen
AntiVir	-	-	BDS/Backdoor.Gen
Antiy-AVL	-	-	Backdoor/Win32.VanBot
Authentium	-	-	W32/Heuristic-257!Eldorado
Avast	-	-	Win32:EggDrop-AE
AVG	-	-	Worm/Agobot.FWF
BitDefender	-	-	Backdoor.Agent.YRG
CAT-QuickHeal	-	-	Backdoor.VanBot.ej
ClamAV	-	-	Exploit.DCOM.Gen
Comodo	-	-	TrojWare.Win32.Trojan.Agent.~
DrWeb	-	-	BackDoor.IRC.Sdbot.2665
eSafe	-	-	-
eTrust-Vet	-	-	Win32/Linkbot!generic
F-Prot	-	-	W32/Heuristic-257!Eldorado
Fortinet	-	-	MS06040.A!exploit
GData	-	-	Backdoor.Agent.YRG
Ikarus	-	-	Backdoor.Win32.PoeBot.C

Soubor po spuštění (zaktualizoval se):

Antivirus	Version	Last Update	Result
a-squared	4.0.0.101	2009.05.13	Trojan-Dropper.Kobcka!IK
AhnLab-V3	5.0.0.2	2009.05.13	-
AntiVir	7.9.0.166	2009.05.12	-
Antiy-AVL	2.0.3.1	2009.05.13	-
Authentium	5.1.2.4	2009.05.13	-
Avast	4.8.1335.0	2009.05.12	-
AVG	8.5.0.327	2009.05.12	Win32/Heur
BitDefender	7.2	2009.05.13	-
CAT-QuickHeal	10.00	2009.05.13	-
ClamAV	0.94.1	2009.05.13	-
Comodo	1157	2009.05.08	-
DrWeb	5.0.0.12182	2009.05.13	-
eSafe	7.0.17.0	2009.05.12	-
eTrust-Vet	31.6.6502	2009.05.12	-
F-Prot	4.4.4.56	2009.05.13	-
F-Secure	8.0.14470.0	2009.05.13	-
Fortinet	3.117.0.0	2009.05.13	-
GData	19	2009.05.13	-
Ikarus	T3.1.1.49.0	2009.05.13	Trojan-Dropper.Kobcka

Hijackthis – po napadení

Trend Micro HijackThis - v2.0.2

Below are the results of the HijackThis scan. Be careful what you delete with the 'Fix checked' button. Scan results do not determine whether an item is bad or not. The best thing to do is to 'AnalyzeThis' and show the log file to knowledgeable folks.

- R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName = Odkazy
- O4 - HKLM\..\Run: [VBoxTray] C:\WINDOWS\system32\VBoxTray.exe
- O4 - HKLM\..\Run: [Microsoft Anivirus Monitor Process] antiv.exe ●
- O4 - HKLM\..\Run: [Microsft Security Monitor Process] mssmpp.exe
- O4 - HKLM\..\Run: [reader_s] C:\WINDOWS\System32\reader_s.exe ●
- O4 - HKLM\..\Run: [Windows Update] ssms.exe
- O4 - HKLM\..\Run: [Windows Logon Application] C:\WINDOWS\system32\winlogon.exe ●
- O4 - HKLM\..\Run: [Application Layer Gateway Service] C:\WINDOWS\system32\algs.exe
- O4 - HKLM\..\RunServices: [Microsoft Anivirus Monitor Process] antiv.exe
- O4 - HKLM\..\RunServices: [Microsft Security Monitor Process] mssmpp.exe
- O4 - HKLM\..\RunServices: [Windows Update] ssms.exe
- O4 - HKCU\..\Run: [CTFMON.EXE] C:\WINDOWS\system32\ctfmon.exe
- O4 - HKUS\S-1-5-19\..\Run: [CTFMON.EXE] C:\WINDOWS\system32\CTFMON.EXE (User 'LOCAL SERVICE')
- O4 - HKUS\S-1-5-20\..\Run: [CTFMON.EXE] C:\WINDOWS\system32\CTFMON.EXE (User 'NETWORK SERVICE')
- O4 - HKUS\S-1-5-18\..\Run: [CTFMON.EXE] C:\WINDOWS\system32\CTFMON.EXE (User 'SYSTEM')
- O4 - HKUS\DEFAULT\..\Run: [CTFMON.EXE] C:\WINDOWS\system32\CTFMON.EXE (User 'Default user')
- O9 - Extra button: Messenger - {FB5F1910-F110-11d2-BB9E-00C04F795683} - C:\Program Files\Messenger\msmsgs.exe
- O9 - Extra 'Tools' menuitem: Windows Messenger - {FB5F1910-F110-11d2-BB9E-00C04F795683} - C:\Program Files\Messenger\msmsgs.exe
- O23 - Service: VirtualBox Guest Additions Service (VBoxService) - Unknown owner - C:\WINDOWS\system32\VBoxService.exe (file missing)

Scan & fix stuff

Scan **Fix checked**

Info on selected item...

AnalyzeThis
Upload to TrendSecure

Main Menu

















Other stuff

Info... Config...

Add checked to ignorelist

Hijackthis – analýza

Online skener, např. <http://www.hijackthis.cz>

R0 - HKCU\Software\Microsoft\Internet Explorer\Toolbar,LinksFolderName = Odkazy	 Bezpečný.	 Very safe	This entry was classified from our visitors as good.
O4 - HKLM\..\Run: [VBoxTray] C:\WINDOWS\system32\VBoxTray.exe	 Bezpečný.	 Safe	Safe (3.83 / 5.00)
O4 - HKLM\..\Run: [Microsoft Anivirus Monitor Process] antiv.exe	 Neznámý	 Extremely nasty	Neznámá aplikace.
O4 - HKLM\..\Run: [Microsoft Security Monitor Process] mssmpp.exe	 Neznámý	 Nasty	Neznámá aplikace.
O4 - HKLM\..\Run: [reader_s] C:\WINDOWS\System32\reader_s.exe	 Špatný	 Extremely nasty	Nasty (1.13 / 5.00)
O4 - HKLM\..\Run: [Windows Update] ssms.exe	 Špatný	 Extremely nasty	Neznámá aplikace. This entry was classified from our visitors as bad.
O4 - HKLM\..\Run: [Windows Logon Application] C:\WINDOWS\system32\winlogon.exe	 Špatný	 Extremely nasty	Musí být opraven! Added by the LINKBOT.M WORM!
O4 - HKLM\..\Run: [Application Layer Gateway Service] C:\WINDOWS\system32\algs.exe	 Špatný	 Extremely nasty	Musí být opraven! Added by the LINKBOT.M WORM!

Active ports – po napadení

Process	P...	Local IP	Local Port	Remote IP	Remote Port	State	Protocol	Path
TCP winlogon.exe	592	10.0.2.15	1059	218.93.205.24	65520	ESTABLISHED	TCP	C:\WINDOWS\system32\winlogon.exe
UDP lsass.exe	664	0.0.0.0	4500			LISTEN	UDP	C:\WINDOWS\system32\lsass.exe
UDP lsass.exe	664	0.0.0.0	500			LISTEN	UDP	C:\WINDOWS\system32\lsass.exe
UDP firewall.exe	876	10.0.2.15	69			LISTEN	UDP	C:\WINDOWS\system32\firewall.exe
TCP firewall.exe	876	10.0.2.15	1105	89.185.227.240	135	SYN_SENT	TCP	C:\WINDOWS\system32\firewall.exe
TCP firewall.exe	876	10.0.2.15	1103	89.185.227.239	135	SYN_SENT	TCP	C:\WINDOWS\system32\firewall.exe
TCP firewall.exe	876	10.0.2.15	1102	89.185.227.238	135	SYN_SENT	TCP	C:\WINDOWS\system32\firewall.exe
TCP firewall.exe	876	10.0.2.15	1099	89.185.227.237	135	SYN_SENT	TCP	C:\WINDOWS\system32\firewall.exe
TCP firewall.exe	876	10.0.2.15	1097	89.185.227.236	135	SYN_SENT	TCP	C:\WINDOWS\system32\firewall.exe
TCP firewall.exe	876	10.0.2.15	1096	89.185.227.235	135	SYN_SENT	TCP	C:\WINDOWS\system32\firewall.exe
TCP firewall.exe	876	10.0.2.15	1070	72.10.172.218	2293	ESTABLISHED	TCP	C:\WINDOWS\system32\firewall.exe
TCP firewall.exe	876	0.0.0.0	54548			LISTEN	TCP	C:\WINDOWS\system32\firewall.exe
TCP service.exe	896	0.0.0.0	113			LISTEN	TCP	C:\WINDOWS\system32\service.exe
TCP ssms.exe	932	10.0.2.15	1277	10.21.158.9	135	SYN_SENT	TCP	C:\WINDOWS\system32\ssms.exe
TCP ssms.exe	932	10.0.2.15	1276	10.212.229.29	135	SYN_SENT	TCP	C:\WINDOWS\system32\ssms.exe
TCP ssms.exe	932	10.0.2.15	1273	10.146.45.179	445	SYN_SENT	TCP	C:\WINDOWS\system32\ssms.exe
TCP ssms.exe	932	10.0.2.15	1272	10.146.45.179	135	SYN_SENT	TCP	C:\WINDOWS\system32\ssms.exe
TCP ssms.exe	932	10.0.2.15	1271	10.146.45.179	135	SYN_SENT	TCP	C:\WINDOWS\system32\ssms.exe
TCP ssms.exe	932	10.0.2.15	1267	10.16.188.92	135	SYN_SENT	TCP	C:\WINDOWS\system32\ssms.exe
TCP ssms.exe	932	10.0.2.15	1266	10.16.188.92	445	SYN_SENT	TCP	C:\WINDOWS\system32\ssms.exe
TCP ssms.exe	932	10.0.2.15	1265	10.16.188.92	135	SYN_SENT	TCP	C:\WINDOWS\system32\ssms.exe
TCP ssms.exe	932	10.0.2.15	1263	10.141.75.6	135	SYN_SENT	TCP	C:\WINDOWS\system32\ssms.exe
TCP ssms.exe	932	10.0.2.15	1262	10.141.75.6	135	SYN_SENT	TCP	C:\WINDOWS\system32\ssms.exe
TCP ssms.exe	932	10.0.2.15	1071	68.118.151.61	65146	ESTABLISHED	TCP	C:\WINDOWS\system32\ssms.exe
TCP ssms.exe	932	0.0.0.0	43764			LISTEN	TCP	C:\WINDOWS\system32\ssms.exe
TCP svchost.exe	980	0.0.0.0	135			LISTEN	TCP	C:\WINDOWS\system32\svchost.exe
UDP svchost.exe	1024	10.0.2.15	27065			LISTEN	UDP	C:\WINDOWS\System32\svchost.exe
UDP svchost.exe	1024	127.0.0.1	123			LISTEN	UDP	C:\WINDOWS\System32\svchost.exe
UDP svchost.exe	1024	10.0.2.15	52436			LISTEN	UDP	C:\WINDOWS\System32\svchost.exe
UDP svchost.exe	1024	10.0.2.15	1057			LISTEN	UDP	C:\WINDOWS\System32\svchost.exe
UDP svchost.exe	1024	0.0.0.0	3544			LISTEN	UDP	C:\WINDOWS\System32\svchost.exe
UDP svchost.exe	1024	0.0.0.0	1060			LISTEN	UDP	C:\WINDOWS\System32\svchost.exe
UDP svchost.exe	1108	0.0.0.0	1111			LISTEN	UDP	C:\WINDOWS\system32\svchost.exe

Netstat – po napadení

```

C:\WINDOWS\system32\cmd.exe

Proto  Místní adresa          Cizí adresa            Stav
TCP    0.0.0.0:135             0.0.0.0:0              NASLOUCHÁNÍ
TCP    0.0.0.0:445             0.0.0.0:0              NASLOUCHÁNÍ
TCP    0.0.0.0:38277          0.0.0.0:0              NASLOUCHÁNÍ
TCP    10.0.2.15:139          0.0.0.0:0              NASLOUCHÁNÍ
TCP    10.0.2.15:1033        158.196.1.54:135      SYN_SENT
TCP    10.0.2.15:1034        72.10.172.218:7763    NAVÁZÁNO
TCP    10.0.2.15:1035        158.196.1.55:135      SYN_SENT
TCP    10.0.2.15:1036        158.196.1.56:135      SYN_SENT
TCP    10.0.2.15:1037        158.196.1.57:135      SYN_SENT
TCP    10.0.2.15:1038        158.196.1.58:135      SYN_SENT
TCP    10.0.2.15:1039        158.196.1.59:135      SYN_SENT
TCP    10.0.2.15:1040        158.196.1.60:135      SYN_SENT
TCP    10.0.2.15:1041        158.196.1.61:135      SYN_SENT
TCP    10.0.2.15:1042        158.196.1.62:135      SYN_SENT
TCP    10.0.2.15:1043        158.196.1.63:135      SYN_SENT
TCP    127.0.0.1:1027        0.0.0.0:0              NASLOUCHÁNÍ
UDP    0.0.0.0:445           ***
UDP    0.0.0.0:500           ***
UDP    0.0.0.0:1033          ***
UDP    0.0.0.0:4500          ***
UDP    10.0.2.15:69          ***
UDP    10.0.2.15:123         ***
UDP    10.0.2.15:137         ***
UDP    10.0.2.15:138         ***
UDP    10.0.2.15:1900        ***
UDP    127.0.0.1:123         ***
UDP    127.0.0.1:1900        ***

C:\Documents and Settings\Administrator>

```

C:\> netstat -na

- Malware skenuje síť
- Navázáno spojení s řídicím serverem přes IRC

Osvěta uživatelů a správců

- **Největší slabina systému - uživatel!**
- Neotevírat neočekávané (cizí) emailové přílohy
- Nepoužívat warez
- P2P programy (způsob sdílení dat)
- Neukládat hesla
- Odhlašovat sezení
- Přidělování odpovídajících přístupových práv
- Vždy vyžadovat jméno, (bezpečné) heslo a zakázat anonymní účty

Vzájemná spolupráce

- Uživatel musí hlásit veškerá podezření
 - Podezřelá chování počítače (vyskakují okna, ...)
 - Nenainstalované aktualizace
 - ...
- Správce by si měl vést evidenci provedených úkonů (kvůli vlastní ochraně nebo případné kontrole)
- Odpovědnost z pohledu legislativy [J. Kolouch]











Prostor pro případné dotazy

Děkuji za pozornost.





MS Baseline Security Analyzer

Windows Scan Results

Administrative Vulnerabilities

Score	Issue	Result
	Incomplete Updates	A previous software update installation was not completed. You must restart your computer to finish the installation. If the incomplete installation was a security update, the computer is restarted. What was scanned How to correct this
	Administrators	More than 2 Administrators were found on this computer. What was scanned Result details How to correct this
	Password Expiration	Some user accounts (26 of 31) have non-expiring passwords. What was scanned Result details How to correct this
	Windows Firewall	Windows Firewall is not installed or configured properly, or is not available on this version of Windows.
	Automatic Updates	Updates are automatically downloaded and installed on this computer. What was scanned
	File System	All hard drives (2) are using the NTFS file system. What was scanned Result details
	Autologon	Autologon is not configured on this computer. What was scanned
	Guest Account	The Guest account is disabled on this computer. What was scanned
	Restrict Anonymous	Computer is properly restricting anonymous access. What was scanned
	Local Account Password Test	Password checks are not performed on a domain controller. What was scanned

Additional System Information

Score	Issue	Result
	Auditing	Neither Logon Success nor Logon Failure auditing are enabled. Enable auditing and turn on auditing for specific events such as logon and logoff. Be sure to monitor your access. What was scanned How to correct this
	Services	Some potentially unnecessary services are installed. What was scanned Result details How to correct this
	Shares	14 share(s) are present on your computer. What was scanned Result details How to correct this
	Windows Version	Computer is running Microsoft Windows Server 2003. What was scanned

Nevyžádaná pošta (spam)

- Neodpovídat na nevyžádanou poštu
- Neodhlašovat nevyžádanou poštu
- Chránit emailové adresy
 - radomir.orkac(zavinac)vsb(tecka)cz
 - email zadávat do formulářů uváženě
- Nepodporovat přeposílané maily
- Dávat si pozor na nebezpečné odkazy
 - www.webkdc.zcu.cz/RT?e123e132312ec.china.cn
 - [www.tn.cz](http://10.1.10.3/abc.php)
- Osvěta uživatelů (HOAX = poplašná zpráva)