16. Bezpečnost v OS

Chráněné objekty

- Paměť
- Procesor
- Spustitelné programy
- Sdílená zařízení typu disky
- Znovupoužitelná zařízení (tiskárny, pásky)
- Sdílená dat

Metody ochrany objektů v operačních systémech

- *Fyzická separace* – Procesy pro vykonávání operací různého stupně utajení používají oddělená zařízení
- *Časová separace* – Procesy prováděny v různém čase
- *Logická separace* – Oddělení procesů, že pro každý vytváří iluzi, že má celý počítač pro sebe
- *Kryptografická separace* – Díky kryptografickým metodám ukrytí svých dat
    - Možnost kombinace několika metod separace
    - Ty jsou seřazeny dle rostoucí složitosti a klesající spolehlivosti

Autentizace

- Proces, při kterém je ověřována identita určitého subjektu (uživatele nebo i aplikací, procesů)
- Nejjednodušší autentizace pomocí přihlašovacího jména a hesla (lehce napadnutelná) – **jedno faktorová** (jeden tajný parametr)

Autorizace

- Proces ověřování oprávnění subjektu k provedení akce
- Navazuje obvykle na autentizaci
- Základní informace pro autorizaci v datových strukturách **přístupový záznam** a **deskriptor zabezpečení objektu**
- Oprávnění, která záznam definuje, dědí všechny procesy a aplikace v relaci přihlášení

Interaktivní přihlašování ne Windows

- Základní autentizační úroveň ve Windows
- Údaje pro přihlášení porovnávány s parametrem místního nebo doménového účtu
- Proces zajištěn systémovým procesem Winlogon (winlogon.exe)
- Realizován pomocí balíčků, které provedou analýzu autentizačních údajů a pomocí určitého protokolu provedou ověření
- Pokud autentizace úspěšná, vzniká nová relace

Neinteraktivní přihlašování ve Windows

- Nastává po úspěšné interaktivní autentizaci

Správa hesel ve Windows

- Hesla jsou uložena pomocí šifrovacích obrazů (použití kryptografických algoritmů)
- **Hash** je nejslabší formou zabezpečení hesel ve Windows
- Pro větší bezpečnost nutnost využívat co nejrozmanitější hesla
- Potlačení zpětné kompatibility při ukládání LM hesel, použití více bezpečného algoritmu šifrování než DES a neukládání hesel v otevření podobě

Zabezpečení OS

- Aktualizace operačního systému
  - Pravidelně stahovat aktualizace
- Ochrana proti napadení z internetu
  - Firewall
- Antivirus
  - Avast
  - AVG
  - CA Antivirus
  - McAfee
  - BitDefender
  - TrustPort Workstation
  - …
- Ochrana proti spyware, addware
  - Ad Aware, SpyBot…
- Aktualizace veškerého software
- Zálohovat
- Přechod na jiný os (Linux)
  - Samotný Linux je sám o sobě na rozdíl od Windows bezpečnější OS
  - Škodlivý vir pro Linux prakticky neexistuje (i z důvodu menšího rozšíření a především není možná šířitelnost)
  - Binární spustitelné soubory (kde viry jsou) nejsou přenášeny, ale je přenášen pouze jejich zdrojový kód, který je na stroji přeložen do cílového tvaru
  - Mnohdy stačí aktivovat pouze Firewall, který je navíc zabudován v jádře a nezobrazuje se proto v systémové oblasti

Virus

Škodlivý program, který se dokáže sám šířit bez vědomí uživatele. Pro množení se vkládá do jiných spustitelných souborů či dokumentů. Chová obdobně jako biologický virus, který se šíří vkládáním svého kódu do živých buněk. V souladu s touto analogií se někdy procesu šíření viru říká nakažení či infekce a napadenému souboru hostitel. Viry jsou jen jedním z druhů zákeřného softwaru. V obecném smyslu se jako viry (nesprávně) označují červi a jiné druhy malwaru.

Virus nemusí infikovat pouze spustitelné EXE soubory, ale může klidně nakazit i soubory s příponou .DAT, to je možné proto, že jejich vnitřní struktura je podobná .EXE souborům. Minimální pravděpodobností je, že se infikuje nějaký datový soubor (.JPEG, .MP3), protože jeho šíření by potom nebylo z hlediska viru optimální.

Rezidentní / Nerezidentní virus

Nerezidentní vir se ve chvíli spuštění hostitele (ve chvíli, kdy se při spouštění hostitele spustí kód viru) rozšíří do nalezených nenakažených souborů

Rezidentní vir se pouze uloží do operační paměti počítače, ve které zůstane až do doby vypnutí počítače, a mezitím infikuje soubory (nebo např. diskety), se kterými uživatel pracuje.

Stealth viry

- Chrání se před detekcí antivirovým programem použitím tzv. stealth technik
  - Pokud je takový virus v paměti, pokouší se přebrat kontrolu nad některými funkcemi operačního systému a při pokusu o čtení infikovaných objektů vrací hodnoty odpovídající původnímu stavu

Polymorfní viry

- Pokouší se znesnadnit svou detekci tím, že mění vlastní kód. V napadeném souboru není možné najít typické sekvence stejného kódu.

Worms (Červy)

Mnoho lidí zaměňuje viry za červy. Ale jsou zde drobné rozdíly. Dnes už viry skoro vymizely a nahradily je červy. Červ je vlastně nezávislý program, kdežto vir potřebuje nějaký kus kódu, kde by mohl přežívat. Rozdílný je i způsob šíření, kdy vir byl spíše na nějakém médiu, a červ se šíří pomocí internetu, dnes už to tak zcela není. Červy dokáží poměrně snadno přepisovat svůj kód, a tím se stávají velkým problémem pro antiviry.

Trojan horse (trojský kůň)

Tento druh malware se moc neliší od unikátní taktické strategie Římanů v řecké Tróji ve 12. století před naším letopočtem. Stejně jako tehdy se i dnes trojské koně vydávají za neškodný, ba i důležitý software. Stalo se, že se trojský kůň vydával i za antivirový program, Winrar, nebo jen obyčejnou hru. Po nainstalování tohoto „neškodného“ programu se začnou ztrácet data na počítači, nebo vytvářet díry pro napadení další havětí. Instalace nemá ale vždy takovýto průběh. Je možné, že jakmile se dostane do systému, nainstaluje se sám a nahradí nějaké potřebné soubor v používaném programu.

Backdoor

„Zadní vrátka“, ale nemusí být vždy nutně nelegální. Spousta komerčních programů na vzdálenou správu využívá tohoto systému.

Logic bomb (logická bomba)

Podle Erica Filiola: logická bomba je samostatně se nereprodukující malware, který se nainstaluje do systému a čeká na nějakou spouštěcí událost, než začne provádět ničivou nebo jinou ofenzivní funkci.

Bombou může být klidně i kód od třetích stan, ve kterém se vás autoři ptají na licenční číslo produktu. Pokud ho nezadáte do určitého limitu, program přestane pracovat.

Exploit

Druh malware, který dokáže využít slabiny v operačním systému a získat tak přístupová práva. Jak se ve své knize zmiňuje Jirovský: exploity nemají příliš dlouhou životnost. To je způsobeno zejména tím, že ve chvíli, kdy se začne exploit široce využívat, si ho velmi rychle všimnou autoři daného programu a využívanou slabinu opraví.

Keylogger

Zaznamenávání kláves v určitých situacích (hesla, čísla kreditních karet…). Keylogger se hodně špatně hledá, jelikož není vždy aktivní.

Rootkit

Jednoúčelový program pro zamaskování při vniknuti hackera do počítače. Velmi těžko se nalézá. Téměř většinou to znamená reinstall počítače.

Dialer

Tento malware se už moc nepoužívá. Měl totiž v oblibě (u vytáčeného připojení) připojovat počítač třeba přes ústřednu v Asii nebo Tichomoří (60Kč/min).

URL injection

Tento druh je poměrně neškodný, změní třeba přesměrování webových adres. Může z uživatelů tak dostat různé osobní údaje (kódy, hesla k bankovním účtům…).

Spyware

Jde o programy většinou třetích stran, vytvářející statiku pro cílenou reklamu. Spyware nelze úplně označit, jako malware-nejedná se totiž o bezprostřední ohrožení, ani zde není možnost sebeaplikace. Ale nikdo neví, kdo, jak, na co, použije vaše údaje (jména uložená v registrech, seznam otevíraných souborů, informace o softwarech), k jejichž sběru nikdo nedostal žádný souhlas.

Adware

ADvertisement a softWARE (reklamní software). I tento typ nelze přesně označit jako malware. Opět nemá možnost sebeaplikace, uživatel musí souhlasit s instalací a potvrdit licenci. Bývá velmi často součástí programů. Jeho vedlejším účinkem může být i změna domovské stránky v internetovém prohlížeči, nebo vyskakující Pop-up okna.

Hoax

Poplašné zprávy, které si uživatelé posílají mezi sebou. Ve zprávách je napsáno smyšlené nebezpečí (útěk myši ze stolu, roztočení HDD opačným směrem apod.). Na konci bývá připojeno IBM (Microsoft, Apple…) varuje atd.

Phishing

Jsou to e-maily, třeba z fiktivní banky, ve kterých jsou přiloženy formuláře k vyplnění, které pobízejí uživatele vložit citlivé údaje.

Detekce viru

- Antivirový test využívá databázi známých počítačových virů
- Zahájí se logická analýza podezřelého testovaného kódu a porovnává se s kódem virů
- Velmi častým cílem jsou různé generátory klíčů, patche, cracky…

Heuristická metoda

- Vykonává v podstatě dva kroky
  - Pomocí virové databáze hledá známé viry
    - Porovnání dekompilovaného kódu s databází
  - Pokud vir nenajde
    - Zahájí se analýza kódu, testování objektu a posuzuje se, co kód znamená v praxi a jestli dělá něco neobvyklého oproti normálnímu chování kódu
- Podle rozhodujících pravidel nebo vážících metod

Většina antivirových programů, které používají heuristickou analýzu, vykonávají tuto funkci spouštěním programovacích příkazů podezřelého programu nebo spouštěním skriptu v rámci specializovaného virtuálního stroje, a tím umožňují antivirovému programu vnitřně simulovat, co se stane v případě, když podezřelý soubor bude spuštěn při zachování podezřelého kódu, izolovaného od reálného stroje. Ten pak analyzuje příkazy, tak jak jsou prováděny, monitoruje typické virové chování, jako je replikování, přepisování souborů a snaha o utajení existence podezřelého souboru. Jestliže je detekováno jedno nebo více virového chování, je podezřelý soubor označen jako potencionální virus a uživatel je upozorněn.