Kybernetická bezpečnost

Typy KB útoků

Malware: Škodlivý software, nebo též malware se objevuje v mnoha formách. Mezi ty nejznámější patří trojské koně, viry, různí červi, ransomware nebo spyware.

Phishing : Pachatel se snaží získat neoprávněný přístup k peněžnímu účtu/platební kartě a následně z těchto zdrojů odčerpat dostupné finance.

Pharming : Cílem je přesměrovat oběť na škodlivou webovou stránku, která vypadá jako originál (legitimní obsah). Jedná se „vylepšený“ phishing, kdy se klientovi například místo internetového bankovnictví České spořitelny otevře stránka s obdobnou adresou a téměř totožným obsahem. Klient bez povšimnutí zadá údaje a útočník má, co potřeboval.

Spamming: Jedná se o zasílání nevyžádané elektronické pošty, zpravidla s reklamním obsahem.

SQL Injection a Cross-site scripting (XSS): Útočník podstrčí uživateli nebezpečný script.

DDoS: Cílem je udělat určité zdroje nedostupné oprávněným uživatelům.

Man-in-the-Middle (MIMT): Situace, kdy útočník zachytí komunikaci mezi dvěma stranami, aby ji tajně odposlouchával nebo i upravoval.

Hijacking: Útočník ukořistí tzv. Session ID (zkráceně SID). SID je náhodně vygenerovaný token, pomocí kterého se útočník může vydávat za uživatele (neboli nás).

Obecné dělení je možné také na:

Pasivní (jen odposlouchávající) - například skenování portů, keylogger či zadní vrátka

Aktivní (měnící svůj cíl) - například denial of service, man in the middle, využitím přetečení bufferu či přetečení zásobníku

Nebo také na:

Vnitřní útok - autorizovaná osoba systém nepoužívá správně (například když zaměstnanec i nevědomky spustí malware)

Vnější útok - útok zvenčí systému (sítě), který způsobují amatérští hackeři, teroristé (kyberterorismus), vlády (Vault 7)

Druhy virů

Boot viry:

napadají systémové oblasti disku. I přesto, že je jich méně než souborových virů, vyskytují se častěji. Šíří se následujícím způsobem: když restartujete počítač, který má povoleno zavádění systému z disketové mechaniky a v mechanice je disketa s boot virem, vir se spustí a napadne systémové oblasti pevného disku. Při dalším spuštění počítače se boot vir inicializuje z pevného disku a napadá diskety, které uživatel použije.

Souborové viry:

napadají pouze soubory, které obsahují prováděný kód - programy. V napadeném programu přepíší část kódu svým vlastním, nebo vlastní kód k programu připojí a tím změní jeho velikost a chování.

Multipartitní viry:

napadají soubory i systémové oblasti disku. S výhodou kombinují možnosti boot virů i souborových virů.

Makroviry:

napadají datové soubory- dokumenty vytvořené v některých kancelářských aplikacích. Využívají toho, že tyto soubory neobsahují pouze data, ale i makra, která viry využívají ke svému šíření. Jsou napadány především dokumenty aplikací MS Office, výjimečně byly zaznamenány i případy dokumentů jiných aplikací.

Makroviry jsou v současné době nejčastěji se vyskytující druh viru. Jsou také největší hrozbou do budoucna. Opatrný uživatel sice může omezit množství spustitelných souborů, které si kopíruje na počítač, ale výměně elektronických dokumentů se nevyhne.

V závislosti na některých dalších vlastnostech virů mluvíme o těchto typech virů:

Stealth viry

jsou viry, které se chrání 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.

Rezidentní viry:

zůstávají po svém spuštění přítomny v paměti.

Způsoby využití virů a možná ochrana

Viry jsou využívány ke spoustě činností a praktik. Mezi ty hlavní patří snaha poškodit uživatele klidně i úplným formátováním disku a zničením osobních dat. V odlišném případě dojde k odcizení vašich dat s následovným vydíráním, kdy pokud nezašlete peníze na uvedený účet, dojde ke smazání dat. Některé viry vám budou jen ukazovat reklamy a lákat vás ke koupi zboží. Jiné z vašeho počítače udělají „nefunkční krabici“.

Nejjednodušším řešením je zabránit úpravám souborů, tedy napadení / napíchnutí počítačového souboru. Pokud počítačové viry nebudou mít možnost infikovat / napadnout legální (korektní) soubory operačního systému nebo jiné aplikace (Office, prohlížeč, audio/ video přehrávač, atd.), tak naprostá většina počítačových virů nebude moci existovat.

Softwarová ochrana

Softwarová ochrana je realizována antivirovými programy .V základu se dají antiviry rozdělit do dvou kategorií, na základě toho, jakým způsobem škodlivý SW detekují.

1) antiviry skenují data uložená v paměti a hledají určité části dat (sekvence), které se shodují s částmi již známých virů, které má antivir ve své databázi. Jedná se o jednoduchý způsob ochrany, který chrání proti známým virům.

2) antiviry sledují chování programů a vyhodnocují její chování. Pokud program vykazuje zvláštní chování je označen jako škodlivý. Tento způsob detekce vyžaduje sledování portů, procesů programu a jejich dat. Tento způsob může detekovat i viry, které jsou nové a tedy neznáme.

Hardwarová ochrana

Kromě softwarové ochrany před viry existuje i možnost hardwarové ochrany. Ta je realizována pomocí rozšiřující karty, nebo čipu.

Příkladem takového zabezpečení je například řešení na zařízeních značky BlackBerry, které bylo nucené použít ve svých mobilních telefonech OS Android, který bohužel nesplňoval požadavky na zabezpečení, které by přijalo jako dostačující. Uvnitř telefonuje je několik čipů, které od výroby nesou jedinečný kryptovací klíč. Během spouštění telefonu, dochází ke kontroly integrity nejen HW komponent, ale i systémových aplikací, za pomocí těchto čipů. Tato kontrola probíhá i v případě použití některých aplikací, aby nedošlo k zneužití dat uživatele.

Social engineering

Cílem je vytvořit v člověku dojem, že situace je jiná, než ve skutečnosti opravdu je (člověk nepozná, že mu např. mailuje podvodník, a ne skutečná osoba).

Protože už existuje na počítačích řada zabezpečení, nastává úkol pro tvůrce virů přijít na to, jak přimět uživatele, aby přestal být opatrný, a to je úloha sociálního inženýrství.

Sociální inženýrství působí na uživatele nejrůznějšími metodami – např. poukazem na peněžní částku neexistující objednávky, přesvědčováním uživatele, že pro správný chod programu je nutno vypnout antivirové testování nebo zasíláním zdánlivě důvěryhodných automatických odpovědí na

e-maily apod.

Zákon a kybernetická bezpečnost

Zavedení pojmu kybernetické bezpečnosti velmi dobře demonstruje samotný charakter práva jako normativního systému. V právu si tedy mimo jiné můžeme dovolit i konstrukci zcela nového fenoménu, který v reálném světě nemá obdobu – a to byl právě případ kybernetické bezpečnosti.

Počítačová bezpečnost nebo síťová bezpečnost představují dnes již tradiční obory aplikované kybernetiky. Kryptografie, která s těmito víceméně moderními disciplínami sdílí základní ideu, tj. ochranu dat.

Byť to může znít paradoxně, nepředstavuje hlavní problém regulatorního fenoménu kybernetické bezpečnosti skutečnost, že nic takového jako kybernetická bezpečnost vlastně reálně neexistuje. Daleko větším problémem je, že nevíme, co chápat pod pojmem „bezpečnost“.

Problém metaforičnosti pojmu bezpečnosti se vcelku výrazně projevuje například v ústavním právu. Zabýváme se otázkou, zda je příkladně vhodné v zájmu bezpečnosti zasahovat do lidské svobody, soukromí nebo vlastnictví. Posouzení je nadmíru složité či dokonce nemožné za situace, kdy není jasné, jaké konkrétní bezpečnostní výhody nám z příslušného omezení jiného práva vyplynou.

Do Základní listiny práv a svobod (součást ústavního pořádku ČR) je právě IT zakomponovány. Hezkým příkladem je Listovní tajemství, která nám dává právo na soukromí našich odesílaných dat. Porušením Listovního tajemství je definováno takto:

§ 182 Porušení tajemství dopravovaných zpráv
(1) Kdo úmyslně poruší tajemství

a) uzavřeného listu nebo jiné písemnosti při poskytování poštovní služby nebo přepravované jinou dopravní službou nebo dopravním zařízením,

b) datové, textové, hlasové, zvukové či obrazové zprávy posílané prostřednictvím sítě elektronických komunikací a přiřaditelné k identifikovanému účastníku nebo uživateli, který zprávu přijímá, nebo

c) neveřejného přenosu počítačových dat do počítačového systému, z něj nebo v jeho rámci, včetně elektromagnetického vyzařování z počítačového systému, přenášejícího taková počítačová data,

bude potrestán odnětím svobody až na dvě léta nebo zákazem činnosti.

Pojmová neurčitost bezpečnosti se vedle ústavního práva projevuje třeba i v relativně nové oblasti mezinárodních vztahů označované jako kyberdiplomacie. Pokud totiž má být kybernetická bezpečnost předmětem mezinárodní spolupráce, je třeba příslušné nástroje stavět na stejné teleologii. Můžeme se tedy potýkat se skutečností, že různé národy si pod pojmem bezpečnosti mohou představovat něco úplně jiného.

Regulatorní fenomén kybernetické bezpečnosti lze řešit prakticky dvěma základními způsoby. První možností je taková kombinace technických a organizačních opatření, která ve výsledku zajistí identifikaci subjektu, který způsobil kybernetický bezpečnostní incident.

Základem právní úpravy české kybernetické bezpečnosti je zákon č. 181/2014 Sb.,(není potřeba si pamatovat toto číslo) který je proveden vyhláškami Národního bezpečnostního úřadu, resp. Národního úřadu pro kybernetickou a informační bezpečnost a Ministerstva vnitra. Do českého zákona č. 181/2014 Sb. je provedena i harmonizace prozatím jediného specializovaného sekundárního předpisu EU, kterým je směrnice (EU) č. 2016/1148

Revision #1
Created 2025-05-28 09:39:04 UTC by Magdalena Dobešová
Updated 2025-05-28 09:41:59 UTC by Magdalena Dobešová