# Kybernetická bezpečnost

Kybernetickou bezpečností rozumíme souhrn právních, organizačních a technických prostředků k zajištění **ochrany počítačových systémů** před útoky hackerů, napadením nejrůznějšími druhy malwaru a dalšími druhy bezpečnostních hrozeb z internetu.

Do budoucnosti se předpokládá nárůst množství kybernetických útoků na mobilní zařízení, internetová úložiště, internet věcí a kritickou infrastrukturu. Hackeři budou útočit i na virtuální měny a škodit firmám v rámci konkurenčního boje.

### Rizika spojená s využíváním internetu a sociálních sítí

* vše na internetu je dohledatelné, věčné, kopírovatelné, globální (pro kohokoli)
* ochrana osobních údajů a jejich zneužití
* důležitá ochrana vlastní on-line identity! a osobních údajů obecně – **problematika digitální stopy**(aktivní a pasivní), význam vyhledavačů, zpětný výmaz prakticky nemožný
* závislosti – netholismus, online gambling
* nevhodný a nelegální obsah online
* mobily – typické úložiště citlivých informací, funkce geolokace
* ochrana autorských práv
* společensky nebezpečné jevy - kyberšikana, kybergrooming, sexting, stalking

### Zásady bezpečného chování

* nestahovat a neotvírat žádné neznámé soubory
* nikomu na internetu nesdělovat své osobní údaje
* používat vícefaktorovou autentizaci
* pravidelně zálohovat data
* používat bezpečné heslo
* vyhodnocovat bezpečnost způsobu připojení (rizika veřejných wifi sítí), využít VPN
* nevěřit všemu, co je na internetu (faske news, phishing, sociální inženýrství)

### Internet a paragrafy, počítačová kriminalita

Počítačovou kriminalitu lze zjednodušeně rozdělit do dvou základních skupin:

1. Delikty, kde počítač, program, data, informační systém apod. jsou **nástrojem** trestné činnosti
2. delikty, kde počítač, program, data, informační systém atd. jsou **cílem** zločinného útoku,

Nový **trestní zákoník** vychází z Úmluvy Rady Evropy, která obsahuje nikoli definici počítačové kriminality, ale souhrn aktivit, které by měly být postihovány jako trestný čin. Jde o tyto aktivity:

- protiprávní přístup,

- protiprávní zachycení informací,

- zásah do dat,

- zásah do systému,

- zneužití zařízení,

- falšování údajů souvisejících s počítači,

- podvod související s počítači,

- trestné činy související s dětskou pornografií,

- trestné činy související s porušením autorského práva a práv příbuzných autorskému právu.

Náš trestní zákoník obsahuje následující paragrafy, které lze využít při stíhání počítačové kriminality:

* § 182 Porušení tajemství dopravovaných zpráv
* **§ 230** Neoprávněný přístup k počítačovému systému a nosiči informací
* § 231 Opatření a přechovávání přístupového zařízení a hesla k počítačovému systému a jiných takových dat
* § 232 Poškození záznamu v počítačovém systému a na nosiči informací a zásah do vybavení počítače z nedbalosti
* **§ 270** Porušení autorského práva, práv souvisejících s právem autorským a práv k databázi
* **Deep web** – označení pro tu část internetového obsahu, který je nepřístupný přes vyhledavače (neindexují ho), dle odhadů tvoří 96 % internetového obsahu.
* **Dark web** – část deep webu, kde jsou stránky přístupné přes prohlížeč/síť Tor (typicky nelegální, soukromý obsah), zaručena anonymita přístupu.

### Hacking

* je činnost **spočívající v hledání a využívání bezpečnostních děr v počítačových systémech**. Motivace hackerů nemusí být finanční, jde také o reputaci, zábavu a překonávání výzev. Často snaha o získání citlivých dat a jejich zneužití, přeprodej, snaha o manipulaci veřejného mínění. Může jít i o „etické“ hackry, kteří pomáhají s testováním aplikací a IT systémů.
* cracking = prolomení ochrany

### Dos a DDos útoky

DDoS je typ útoku na počítačové systémy, typicky na internetové služby. Jde o zkratku z anglického Distributed Denial of service, neboli odepření služby. Útočníci systém neovládnou, ale **přehltí jej požadavky** natolik, že havaruje a nedokáže odpovídat. Může jít o prosté přetížení serveru nebo využití nějaké chyby.

DoS = velké množství přístupů k jedné webové stránce z 1 IP adresy s cílem znepřístupnění webu – toto umí firewall blokovat.

DDoS (Distributed) – útoky přichází z různých IP adres (**botnet** - síť počítačů infikovaných speciálním softwarem, který je řízen z jednoho centra) – nelze předejít. Dané IP adresy napadeny pc virem.

*blíže* <http://tech.ihned.cz/c1-59451640-ddos-utoky-vysvetleni>

### Zneužití e-mailové komunikace

* Phishing, spam (další výrazy smishing, vishing, spoofing)
* Lze zfalšovat adresu odesilatele e-mailu
* Ochranou je např. **SPF záznam**. Jeho princip spočívá v ověření zdroje odeslané zprávy (tedy odesílajícího serveru) oproti definovaným serverům – IP adresy, které jsou oprávněny odesílat zprávy z dané domény. V případě, že zdrojem zprávy není žádný z oprávněných zdrojů, přijímací SMTP server zprávu odmítne přijmout, nebo ji bude filtrovat jako spam.

### Šifrování (kryptografie) dat

je proces, kterým se nezabezpečená elektronická data převádí na data šifrovaná, čitelná pouze pro majitele dešifrovacího klíče. Šifrování dat slouží k jejich ochraně proti nežádoucímu zjištění cizí osobou a uplatňuje se při ukládání dat, při jejich přenosu v síti, při ochraně elektronického bankovnictví.

<https://cs.khanacademy.org/computing/computer-science/computers-and-internet-code-org/internet-works-intro/v/the-internet-encryption-and-public-keys>

**Šifrování emailů**

Emailové zprávy lze elektronicky podepisovat a šifrovat pomocí emailového certifikátu. Tyto digitální certifikáty jsou založeny na principu **asymetrické kryptografie.** Asymetrická kryptografie (kryptografie s veřejným klíčem) je skupina kryptografických metod, ve kterých se pro šifrování a dešifrování používají odlišné klíče.

Oproti tomu symetrická kryptografie používá k šifrování i dešifrování jediný klíč. Šifrování emailů umožňuje zajistit, že nikdo kromě adresáta vlastnícího odpovídající soukromý klíč nebude moci email přečíst.

**Elektronický podpis** umožňuje emailovému klientovi příjemce ověřit, že přijatá zpráva je ve stejné podobě, v jaké byla odeslána. Zajišťuje tedy, že email skutečně odeslal majitel certifikátu a že na cestě k adresátovi případný útočník zprávu neodchytil a nepozměnil.

Protože je šifrování pro uživatele složité, je proces automatizován. E-maily jsou směřovány přes bránu, která je nakonfigurována v souladu s bezpečnostními a regulačními pravidly, a jsou automaticky zašifrovány a odeslány.

### Malware

Pc virus je program, který provádí nežádoucí, většinou destrukční operace a bez vědomí uživatele se šíří. Techniky virů a metody šíření se neustále vyvíjí.

**Malware** je počítačový program určený ke vniknutí nebo poškození počítačového systému

**Dělení virů**

* **klasické viry** – program je schopen sám sebe připojovat k jiným programům a dále se šířit
* **trojské koně** – program, který se vydává za něco nevinného, ale za uživatelovými zády provádí destrukční činnost (např. sleduje a odesílá z PC hesla, soubory). Neumí se množit a dále se šířit. Většinou stažen jako součást nějakého programu.
* **červi** (WORM) – nešíří se napadáním a rozesíláním souborů, ale přímo pomocí komunikace v síti jako pakety. K šíření využívají chyb v síťových programech nebo nezabezpečené služby operačního systému.

**Další typy infiltrace**

* **Backdoor** – slouží pro vzdálenou správu a ovládání PC (např. zneužití IP adresy pro rozesílání spamu, DDos útoky, těžba kryptoměny...)
* **Spyware** – program, který odesílá statistická i citlivá data z počítače bez vědomí jeho uživatele (např. navštívené stránky, přihlašovací údaje...)
* **Keylogger** – sleduje stisky kláves
* **Downloader** – škodlivý kód, který z internetu stahuje další havěť
* **Rootkit** – podobný trojskému koni, umí maskovat svoji činnost před AVP, slouží k utajení nekalé činnosti modifikací napadeného systému
* **Adware** – jde o produkt, který znepříjemňuje práci uživatele vnucující se reklamou. Typickým příznakem jsou „vyskakující“ pop-up reklamní okna během surfování.
* **Ransomware** – uzamyká/zašifruje data uživatele a za zpřístupnění požaduje výkupné v bitcoinech
* **Phishing** – podvodná technika používaná na Internetu k získávání citlivých údajů (přístupová jména a hesla k účtům, čísla kreditních karet apod.) od obětí útoku. Principem je rozesílání mailových zpráv, které se tváří jako oficiální žádost banky či jiné podobné instituce a vyzývají adresáta k zadání jeho údajů na odkazovanou stránku
* **SQL injekce** – napadení počítače/serveru s využitím jazyka SQL

**Šíření virů**

* přes internetové stránky

Nebezpečné jsou **odkazy**, a to např. odkazy na scripty, ve vyskakujících oknech a **stahování programů**

* elektronickou poštou

Nejnebezpečnější, nejrychlejší šíření, většinou jde o dosud neidentifikované novinky.

Vlastní zpráva virus obsahovat nemůže - pozor na **odkazy v těle** a **přílohy (**souborové viry, makroviry).Podezřelé formáty příloh: VBS, EXE, ZIP, BAT..., doc, xls – pouze pokud obsahuje makro

* nově i přes USB zařízení

Problémem je automatické spuštění dialogu po připojení zařízení, tj. defacto libovolného souboru.

**Systém ochrany počítače**

* **firewall** – ochranný prvek (program nebo zařízení), který sleduje síťovou komunikaci, odděluje vnitřní síť od zbytku světa, filtruje a blokuje síťový přenos.

Zachytí jak pokus viru, resp. červa o průnik do sítě, tak pokus hackera.

Jde o prvek tzv. aktivní ochrany.

* antispam, antiadware, antispyware
* nainstalovaný **antivirový program**

**Rezidentní** forma – neustále běží a kontroluje veškeré prováděné operace

př. AVG, AVAST, Eset Endpoint Antivirus, Norton AntiVirus, ...

### Deepfake

Jedná se o technologii umělé inteligence, která umožňuje vytvářet realistické obrazy, videa nebo audionahrávky s využitím falešných identit. Pomocí pokročilých algoritmů umí vytvářet realistické imitace obličeje, hlasu a pohybu. Generativní modely AI totiž umí generovat obsah, který je podobný existujícím datům. Počátky z roku 2017, rozmach v poslední době.

Příklady:

* Výroba pornografie (většina deepfake)
* Falešný hovor/videohovor „šéfa“, kolegy, důležitého úředníka (obecně důvěryhodné osoby), který např. dává pokyn k provedení platby či zjišťuje informace o firemních financích nebo jiných citlivých údajích
* Zneužití ve volebních kampaních, dehonestace či znevěrohodnění určitého politika, manipulace veřejným míněním
* Zneužití veřejně známých osob k propagaci výrobku/strany …
* Špionáž
* Ovlivnění ceny akcií, poškození brandu (značky)

Deepfake video může vytvořit v podstatě kdokoliv. Když do vyhledávače zadáte heslo „AI deepfake generator tools“, rychle zjistíte, jak snadno se člověk dostane k nástrojům, s jejichž pomocí může během několika minut vyrobit těžko rozpoznatelné deepfake video. Je nutný vysoký výpočetní výkon.

Je vůbec legální deepfake videa vytvářet? Legální status této technologie se liší v závislosti na jurisdikci jednotlivých států a kontextu použití. Obecně ale platí, že vytváření a šíření deepfake materiálů není samo o sobě nezákonné, pokud neporušují osobní nebo autorská práva. Také je zpravidla zakázané vytvářet obsah, který je jinak nelegální (jako například dětská pornografie). V některých zemích byly přijaty zákony zaměřené specificky na deepfake, které se snaží chránit oběti před zneužitím, zejména v kontextu pomluv a šíření nepravdivých informací.

Deepfake se stává klíčovým prvkem phishingových kampaní a dalších metod sociálního inženýrství. V důsledku podvodného obsahu můžou podniky utrpět výrazné škody – finanční nebo na reputaci. Většina společností si zatím významnost této hrozby neuvědomuje. Kromě organizačních/procesních opatření a proškolení zaměstnanců by měly firmy zvážit implementaci technologií pro detekci deepfakes a určení původu mediálního obsahu skrze ověřování zdroje informací. Důležité jsou také nástroje pro verifikaci v reálném čase nebo techniky pasivní detekce, mezi které patří třeba kontrola metadat spojených s podezřelým mediálním souborem.

Pokud chceme vizuálně deepfake rozlišit, všímáme si detailů – např. zda osoba mrká, synchronizace rtů se zvukem, blikání, detailů vlasů, šperků, zubů, tvaru rukou.

Vlády, univerzity a technologické firmy financují výzkum zaměřený na odhalování deepfake. Nedávno odstartovala první soutěž Deepfake Detection Challenge, kterou podpořily společnosti Microsoft, Facebook a Amazon.

S pokusem o deepfake se v nedávné době setkala např. firma Ferrari.

<https://www.novinky.cz/clanek/auto-ferrari-celilo-deepfake-utoku-podvodnik-temer-dokonale-napodobil-hlas-sefa-znacky-40482168#dop_ab_variant=0&dop_source_zone_name=novinky.sznhp.box&source=hp&seq_no=6&utm_campaign=&utm_medium=z-boxiku&utm_source=www.seznam.cz>