

Kyberbezpečnosť

1. Čo je kyberbezpečnosť

Kyberbezpečnosť je súbor opatrení, pravidiel a technológií, ktorých cieľom je chrániť počítače, siete, mobilné zariadenia a údaje pred zneužitím, útokmi alebo poškodením. V dnešnej dobe, keď využívame internet denne – na učenie, komunikáciu, zábavu či prácu – je kyberbezpečnosť mimoriadne dôležitá.

Kyberbezpečnosť sa netýka iba veľkých firiem alebo štátov, ale každého jednotlivca. Útok môže postihnúť obyčajného používateľa doma rovnako ako školu alebo banku. Cieľom útočníkov môžu byť osobné údaje, heslá, peniaze alebo len snaha poškodiť systém.

2. Základné pojmy v kyberbezpečnosti

Adware

Adware je typ softvéru, ktorý zobrazuje reklamy na zariadení používateľa. Často sa nainštaluje spolu s inými programami bez jasného upozornenia. Po nainštalovaní zobrazuje vyskakovacie okná, bannery alebo presmerováva na reklamné stránky. Môže tiež sledovať správanie používateľa, aby zobrazoval cielené reklamy. Aj keď býva menej nebezpečný ako vírusy, môže spomaľovať zariadenie a byť nepríjemný. Preto je dobré sťahovať programy len z overených zdrojov a používať ochranný softvér.

Červ

Počítačový červ (worm) je program so škodlivým kódom, ktorý napáda hostiteľský počítač, využíva jeho prepojenie cez sieť s ďalšími počítačmi a prostredníctvom nich sa automaticky šíri ďalej. Na rozdiel od niektorých iných typov malvéru nepotrebuje zásah používateľa – šíri sa sám, napríklad cez internet alebo lokálnu sieť.

Hlavnou vlastnosťou červa je, že:

- dokáže sa samostatne kopírovať
- využíva zraniteľnosti v systéme alebo sieti
- môže rýchlo infikovať veľké množstvo zariadení

DDoS

DDoS útok, je kybernetický útok, pri ktorom útočník zahlcuje webovú stránku alebo server veľkým množstvom požiadaviek z mnohých zariadení naraz. Cieľom je, aby služba prestala fungovať a bola nedostupná pre bežných používateľov.

Na ochranu sa používajú špeciálne programy a služby, ktoré dokážu odfiltrovať škodlivú prevádzku. Dôležité je aj sledovanie siete a využívanie služieb ako Cloudflare či antivírusové riešenia.

V roku 2016 spôsobil DDoS útok výpadok stránok ako Twitter, Netflix či Spotify. Podobné útoky môžu postihnúť aj banky, školy alebo e-shopy, najmä počas sviatkov alebo výpredajov.

Firewall

Firewall je ochranný systém, ktorý kontroluje komunikáciu medzi počítačom a internetom a blokuje nebezpečné pripojenia. Firewall je základným prvkom ochrany sietí a často sa používa v kombinácii s ďalšími bezpečnostnými technológiami, ako sú IDS Intrusion Detection System – detekuje a upozorní na útok alebo IPS (Intrusion Prevention System – aj zastaví útok) systémy.

Hacker

Hacker je osoba, ktorá sa snaží získať prístup k cudzím systémom. Nie každý hacker je zlý:

- white hat hacker – testuje bezpečnosť legálne
- black hat hacker – útočí nelegálne
- grey hat hacker – pohybuje sa na hranici zákona

Malvér

Malvér (z angl. malicious software) je všeobecné označenie pre všetok škodlivý softvér. Patria sem:

- vírusy
- červy
- trójske kone
- spyvér
- ransomvér

Počítačový vírus

Počítačový vírus je škodlivý program, ktorý sa šíri bez vedomia používateľa a môže poškodzovať počítač, dáta alebo systém.

Jednoducho povedané:

Je to program, ktorý sa pripojí k iným súborom alebo programom, šíri sa ďalej a robí neželané veci.

Čo môže počítačový vírus robiť:

- mazať alebo poškodzovať súbory
- spomaľovať počítač
- zobrazovať nechcené reklamy
- kraťnúť heslá alebo osobné údaje
- znefunkčniť celý systém

Ako sa vírusy šíria:

- cez internet (emailové prílohy, podvodné odkazy)
- stiahnutím nebezpečných programov
- cez USB kľúče
- návštevou infikovaných webstránok

Ako sa chrániť:

- používať antivírusový program
- neotvárať podozrivé emaily a odkazy
- sťahovať programy len z dôveryhodných stránok
- pravidelne aktualizovať systém

Phishing

Podvodná technika, pri ktorej sa útočník snaží vylákať:

- heslá
- čísla kariet
- osobné údaje

Najčastejšie cez:

- falošné emaily
- správy na sociálnych sieťach
- podvodné webstránky

Ransomvér

Ransomvér je veľmi nebezpečný typ malvéru, ktorý:

- zašifruje údaje
- požaduje výkupné za ich obnovenie

Rootkit:

- Rootkit sa snaží skryť v systéme tak, aby ho nebolo vidno.
- Umožňuje útočníkovi získať plnú kontrolu nad počítačom.

- Dokáže skrývať iné vírusy alebo škodlivé programy.
- Často sa nainštaluje hlboko do systému (napr. do operačného systému).
- Je ťažké ho odhaliť aj odstrániť.

Spam

Spam je nevyžiadaná správa, ktorú človek dostane bez toho, aby si ju vyžiadal. Najčastejšie ide o reklamné e-maily, SMS alebo správy na sociálnych sieťach. Spam môže obsahovať aj podvodné odkazy, ktoré sa snažia získať osobné údaje. Takéto správy bývajú posielané hromadne veľkému počtu ľudí. Preto je dôležité spam neotvárať a radšej ho označiť alebo vymazať.

Spayware

Je to druh softvéru, ktorý sa snaží získať informácie z počítača, bez povolenia používateľa a bez jeho vedomia. Nainštaluje sa a spustí sa bez akéhokoľvek upozornenia. Spyware monitoruje správanie používateľa na Internete zbiera o ňom informácie, spomaľuje počítač alebo mení nastavenia počítača. Po infikovaní do počítača sa nemusia prejavovať symptómy, ale môže to ovplyvniť fungovanie počítača.

Spayware sa najčastejšie inštaluje pomocou bezplatného softvéru (šetriče obrazovky, vyhľadávacie panely s nástrojmi alebo programy na zdieľanie súborov), cez webové stránky, prostredníctvom programov, ktoré sú nainštalované z diskov USB, externých pevných diskov, vymeniteľných médií a pod.

To, že máme spyware v počítači zistíme napríklad tým, že sa zmenila predvolená domovská stránka, v počítači používateľ zistí, že má nové panely s nástrojmi, automaticky sa zobrazujú otvárané okná aj keď používateľ nie je na internete, počítač funguje pomalšie a spúšťa sa sám.

Spyware môže byť v počítači aj vtedy, keď užívateľ nezbadá žiadne zmeny. Pri spustení programu *Windows Defender* pri každom použití počítača môže pomôcť vyhľadať a odstrániť tento softvér.

Trójsky kôň

Program, ktorý sa tvári ako neškodná aplikácia, ale po spustení umožní útočníkovi prístup k počítaču. *Trójskymi koňmi* bývajú označované programy, ktoré okrem užitočnej funkcie obsahujú skrytú časť, ktorá sa dá aktivizovať po splnení určitej podmienky (zvyčajne ide o viazanosť na určitý dátum, napr. 1. apríl, piatok trinásteho, dátum narodenia Michelangela 6. marca, Nový rok alebo Vianoce). Táto ukrytá časť spravidla vykonáva činnosť deštruktívneho charakteru (modifikácia údajov, vymazanie súborov, formátovanie disku a pod.) Ak je bežný program nakazený vírusom, stáva sa nielen ďalším jeho rozširovateľom, ale aj potenciálnym trójskym koňom, ktorého činnosť je priamo úmerná s nebezpečnosťou vírusu. Tieto typy vírusov sú v dnešnej dobe najmenej rozšírené keďže ich funkcia je relatívne rovnaká a tak pre anti-vírus nie je problém ju detegovať.

Troll

Troll je osoba na internete, ktorá zámerne provokuje ostatných používateľov. Snaží sa vyvolať hádky, konflikty alebo negatívne reakcie. Často píše urážlivé, nezmyselné alebo provokačné komentáre. Jeho cieľom nie je normálna diskusia, ale pobavenie na úkor iných. Najlepšie je trolla ignorovať a nereagovať na ich správy.

3. Druhy kybernetických hrozieb

3.1 Vírusy a červy

- poškodzujú súbory
- spomaľujú systém
- môžu sa rýchlo šíriť v sieti

4. Sociálne siete a kyberbezpečnosť

Sociálne siete sú častým cieľom útokov. Nebezpečenstvá zahŕňajú:

- krádež účtu
- zneužitie fotografií
- kyberšikanu
- falošné profily

Zásady bezpečného správania:

- nezverejňovať osobné údaje
- nastaviť súkromie profilu
- neprijímať neznáme kontakty
- používať silné heslá

5. Heslá a ich dôležitosť

Silné heslo je základom bezpečnosti.

Správne heslo by malo:

- mať aspoň 12 znakov
- obsahovať veľké a malé písmená
- obsahovať čísla a špeciálne znaky
- byť jedinečné pre každú službu

Zlé heslo: *123456, heslo, abc123*

Dobré heslo: *M0j\$k0mp!ut3r_2026*

Odporúča sa používať správcov hesiel a dvojfaktorové overenie (2FA).

6. Kyberšikana

Kyberšikana je forma šikanovania prostredníctvom internetu:

- urážlivé správy
- zosmiešňovanie
- zverejňovanie súkromných materiálov

Ako sa brániť:

- neodpovedať na útoky
- ukladať dôkazy
- blokovať útočníka
- obrátiť sa na dospelých alebo školu

7. Ochrana zariadení

7.1 Antivírusový program

- chráni pred malvérom
- musí byť aktuálny

7.2 Aktualizácie

- opravujú bezpečnostné chyby
- platí pre systém aj aplikácie

7.3 Zálohovanie dát

- ukladanie kópií súborov
- ochrana pred stratou dát

8. Kyberbezpečnosť v škole a v práci

V školách a firmách je dôležité:

- chrániť osobné údaje
- dodržiavať bezpečnostné smernice
- nešíriť podozrivý obsah

Zamestnanci aj študenti môžu neúmyselne spôsobiť bezpečnostný incident.

9. Prečo je kyberbezpečnosť dôležitá

Kyberútoky môžu viesť k:

- finančným stratám
- zneužitiu identity
- poškodeniu reputácie
- strate dát

Správne správanie na internete a základné znalosti kyberbezpečnosti pomáhajú týmto problémom predchádzať.

10. Záver

Kyberbezpečnosť patrí medzi najdôležitejšie témy súčasnosti. Každý používateľ internetu by mal vedieť:

- rozpoznať hrozby
- chrániť svoje údaje
- správať sa zodpovedne online

Vzdelávanie v oblasti kyberbezpečnosti je nevyhnutné pre bezpečnú digitálnu budúcnosť.

Ako môžeme zabrániť, aby sa počítač infikoval vírusom

Pravidelne by sme mali aktualizovať počítač, je dobré si zapnúť službu Windows Update a aktualizovať pravidelne programy na ochranu pred vírusom a antivírusovým programom. Veľa antivírusových programov obsahuje ochranu proti spyware, ale je potrebné ich udržiavať aktuálne, aby spĺňali svoju funkciu.

Pri preberaní bezplatného softvéru, ako napríklad šetriče obrazovky, si pozorne prečítajte licenčnú zmluvu, či neobsahuje klauzulu, pri ktorej musíte odsúhlasiť reklamu a automatické otváranie okien od danej firmy, treba dávať pozor aj na to, či softvér neodosiela informácie z počítača editirovi softvéru.

1. Čo je kyberbezpečnosť? (vysvetlené jednoducho)

<https://www.youtube.com/watch?v=inWWhr5tnEA>

2. Kybernetické hrozby – phishing, ransomware, hackeri

<https://edu.ceskatelevize.cz/video/15630-wifina-kyberneticke-hrozby>

3. Čo je penetračné testovanie? (etický hacking)

<https://www.youtube.com/watch?v=I7eCSxkApUI>