

# Kybernetické hrozby a prevence

**Kybernetická bezpečnost** (Cybersecurity) je disciplína zaměřená na ochranu systémů, sítí a dat před digitálními útoky. Tyto útoky se obvykle zaměřují na přístup k citlivým informacím, jejich změnu nebo zničení, vydírání uživatelů nebo narušení běžných obchodních procesů.

## 1. Klasifikace kybernetických hrozeb

Hrozby můžeme rozdělit do několika základních kategorií podle jejich povahy a cíle:

### A. Malware (Škodlivý software)

Souhrnné označení pro jakýkoli software navržený k poškození nebo zneužití počítače.

- **Ransomware:** Zašifruje soubory oběti a vyžaduje výkupné za dešifrovací klíč (např. WannaCry).
- **Trojské koně:** Škodlivý kód maskovaný jako legitimní software.
- **Spyware:** Software tajně shromažďující informace o uživateli (stisky kláves, historie prohlížení).

### B. Sociální inženýrství

Útoky, které místo technických slabín zneužívají lidskou psychologii a chyby.

- **Phishing:** Podvodné e-maily imitující důvěryhodné instituce za účelem krádeže přihlašovacích údajů.
- **Spear Phishing:** Cílený útok na konkrétní osobu nebo organizaci.
- **Pretexting:** Vytvoření falešného scénáře (pretextu), který má oběť přimět k vyzrazení informací.

### C. Síťové a infrastrukturní útoky

- **DDoS (Distributed Denial of Service):** Pokus o ochromení online služby jejím zahlcením provozem z mnoha zdrojů současně.
- **Man-in-the-Middle (MitM):** Útočník se vloží do komunikace mezi dvěma stranami, kterou může odposlouchávat nebo měnit.
- **SQL Injection:** Vložení škodlivého SQL kódu do databázového dotazu skrze vstupní pole aplikace.

## 2. Moderní metody prevence

Efektivní obrana vyžaduje kombinaci technických prostředků a správných uživatelských návyků.

## Technická opatření

- **Vícefaktorové ověřování (MFA):** Přidání další vrstvy zabezpečení (např. SMS kód, autentizační aplikace). To je dnes považováno za **nejúčinnější jednotlivé opatření**.
- **Šifrování:** Ochrana dat v klidu (na disku) i při přenosu (protokol HTTPS, TLS).
- **Segmentace sítě:** Rozdělení sítě na menší celky, aby se případný útok nemohl šířit napříč celou infrastrukturou.
- **Endpoint Protection:** Pokročilé systémy ochrany koncových zařízení (antiviry nové generace, EDR).

## Organizační opatření

- **Pravidlo zálohování 3-2-1:** 3 kopie dat, na 2 různých médiích, 1 kopie uložená mimo lokalitu (off-site).
- **Security Awareness Training:** Pravidelné vzdělávání zaměstnanců v rozpoznávání podvodných technik.
- **Incident Response Plan:** Předem definovaný postup, co dělat, když k útoku dojde.

—

## 3. Princip "Zero Trust"

Moderní bezpečnostní model **Zero Trust** (Nikdy nedůvěřuj, vždy prověřuj) vychází z předpokladu, že útočník se již v síti nachází. Každý požadavek na přístup k prostředkům musí být plně autentizován a autorizován bez ohledu na to, odkud přichází.

—

## 4. Legislativní rámec (NIS2 a GDPR)

V EU je bezpečnost regulována přísnými normami:

- **GDPR:** Zaměřuje se na ochranu osobních údajů.
- **NIS2:** Směrnice zvyšující úroveň kybernetické bezpečnosti v kritických odvětvích (energetika, bankovníctví, zdravotnictví).

---

*Související články:*

- [Síťové vrstvy a bezpečnost protokolu HTTP](#)
- [Penetrační testování a hledání zranitelností](#)
- [Základy kryptografie](#)

*Tagy: security cyberhrozby ransomware phishing mfa zero-trust backup*

From:

<http://serviceit.cz/> - **IT ENCYKLOPEDIE**

Permanent link:

[http://serviceit.cz/doku.php?id=it:sec:security\\_threats](http://serviceit.cz/doku.php?id=it:sec:security_threats)

Last update: **2026/01/02 13:46**

