NÚKIB

MINISTERSTVO ZDRAVOTNICTVÍ
ČESKÉ REPUBLIKY

Doporučení ke snížení kybernetických hrozeb spojených se současným ozbrojeným konfliktem mezi Ruskou federací a Ukrajinou

25.02.2022

Národní úřad pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“) ve spolupráci s Ministerstvem zdravotnictví ČR (dále jen „MZČR“) připravil následující doporučení ke snížení kybernetických hrozeb spojených s invazí ruských vojsk na Ukrajinu. Toto doporučení se vztahuje ke dvěma typům kybernetických útoků, které lze vzhledem k současné situaci důvodně očekávat.

NÚKIB a MZČR doporučují ovšem **vždy s ohledem na zachování plynulosti provozu** následující:

Distributed Denial of service (dále jen „DDoS): odepření služby jejím zahlcením požadavky:

Preventivní kroky:

- Prověřit **možnosti blokovat nežádoucí komunikaci** zahlcující nebo jinak omezující provozované systémy na hraničním prvku infrastruktury.
    - Např. prostřednictvím **kontaktování svého poskytovatele internetu**.
    - Ověřit a případně si zajistit schopnost kontaktovat svého poskytovatele internetu.
- Předpřipravit si **strategii a konfigurace prvků pro řízené omezování dostupnosti zbytných služeb** a maximální zachování dostupnosti nezbytných služeb.
- Připravit se na **možnost blokovat IP adresy**, IP rozsahy nebo ASN publikované na webových stránkách NÚKIB a případně následně blokovat.
- Připravit se na nutnost blokování překladu některých domén na DNS resolveru.
- Prověřit možnost přechodu do ostrovního provozu (odpojení od internetu).

Kroky při probíhajícím útoku:

- **Při útoku preventovat zahlcení linky i za cenu blokace legitimní komunikace** (GeoBlocking, blokace na základně ASN).
- V případě zahlcení linky **kontaktovat poskytovatele připojení** a koordinovat řešení zahlcení s poskytovatelem připojení.

Ransomwarový útok: znepřístupnění dat jejich zašifrováním:

Preventivní kroky:

- **Zamezit navazování komunikace svých informačních systémů do internetu**, vyjma takové komunikace, která je nezbytná pro poskytování služeb.
    - Zvážit možnost přechodu do ostrovního provozu (odpojení od internetu).

- **Vytvořit zálohy svých systémů a dat**, a tyto (popřípadě poslední pořízené zálohy) převést na off-line médium či do odděleného systému.
    - Zkontrolovat funkčnost záloh.
- Prověřit **platnost a použitelnost plánů kontinuity činností a plánů obnovy** s ohledem na možnou nedostupnost systémů.
    - Zajistit jejich uchování mimo informační systémy, pro které jsou zpracovány např. v listinné podobě.
    - **V případě jejich absence – vytvořit interní postup pro případ nedostupnosti informačních systémů, který by měl obsahovat náhradní postupy pro případ nedostupnosti systémů a případnou prioritizaci obnovy jednotlivých systémů pro období po útoku.**
    - Ověřit obeznámenost/obeznámit s nimi potřebné osoby v organizaci.
- **Varovat zaměstnance o riziku phishingových útoků**, a to následovně:
    - Co to phishing je a jak ho poznat.
    - Jak postupovat v pochybnostech o legitimitě identity protistrany (např. odesílatele e-mailů).
    - Rizikovost povolování maker v souborech MS Office – např. od neznámého odesílatele.
    - Na koho se v organizaci obrátit v případě podezření na phishing.
- **Zakázat použití nepodepsaných maker** v souborech typu MS Office, pokud nejsou nezbytně potřeba v rámci výkonu práce zaměstnanců.
- Zkontrolovat **aktualizaci nástroje pro ochranu před škodlivým kódem** na všech relevantních zařízeních případně jej, je-li to provozně možné, nasadit.

Detailnější informace o postupu proti ransomware lze dále nalézt ve varování, které NÚKIB vydal dne 16.04.2020 a ke kterému vydal i materiál obsahující doporučená bezpečnostní opatření, která zavést. Toto varování je dostupné na této adrese: https://www.nukib.cz/cs/uredni-deska/

Další doporučení či upozornění na hrozby či samotné rozsahy IP adres, které případně blokovat (viz výše), lze nalézt opět na webu NÚKIB, a to v rámci tohoto odkazu: https://www.nukib.cz/cs/infoservis/hrozby/

NÚKIB dále vydal **aktuální varování, které se týká širšího okruhu technik útoků**, které v současné době hrozí, toto lze nalézt na adrese: https://www.nukib.cz/cs/uredni-deska/

Dalším typem útoku, kterému je vhodné věnovat pozornost, je útok typu wiper, proti kterému NÚKIB zveřejnil na svém webu následující upozornění: https://www.nukib.cz/cs/infoservis/hrozby/1813-upozorneni-na-vyskyt-noveho-destruktivniho-malware-typu-wiper/