VAROVÁNÍ PŘED KYBERNETICKOU HROZBOU PODLE § 12 ZKB

Použití a dopady

Mgr. Vladěna Sasková
Odbor regulace
17. května 2019

Národní úřad
pro kybernetickou
a informační bezpečnost

Disclaimer

- Prezentace obsahuje informace platné ke dni 17. 5. 2019
- Informace, fakta a údaje obsažené v prezentaci mají informační a osvětový charakter
- Pro zajištění souladu se zákonem o kybernetické bezpečnosti je nutno vycházet z aktuálně účinné legislativy
- Aplikaci dále uvedených informací či opatření je nutné vždy vztahovat ke konkrétním systémům a institucím

Obsah prezentace

- Varování – charakter a použití
- Zohlednění varování při zadávání veřejných zakázek

První vydané varování NÚKIB

- Dne 17.12.2018 vydal NÚKIB varování před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation a jejich dceřiných společností.

Zdroje:

První vydané varování NÚKIB

- Dne 17.12.2018 vydal NÚKIB varování před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation a jejich dceřiných společností

Zdroje:
https://ct24.ceskatelevize.cz/ekonomika/2682797-cesky-urad-pro-kybernetickou-bezpecnost-varuje-pred-produkty-cinskych-firem-huawei

První vydané varování NÚKIB

- Dne 17.12.2018 vydal NÚKIB varování před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation a jejich dceřiných společností.

Zdroje:
https://ct24.ceskatelevize.cz/ekonomika/2682797-cesky-urad-pro-kybernetickou-bezpecnost-varuje-pred-produkty-cinskych-firem-huawei
https://www.idnes.cz/zpravy/domaci/huawei-zte-kyberneticka-hrozna-cinske-spolecnosti-nukib.A181217_152310_domaci_kuce

První vydané varování NÚKIB

- Dne 17.12.2018 vydal NÚKIB varování před používáním softwaru i hardwaru společností Huawei Technologies Co., Ltd., a ZTE Corporation a jejich dceřiných společností.

Zdroje:
https://ct24.ceskatelevize.cz/ekonomika/2682797-cesky-urad-pro-kybernetickou-bezpecnost-varuje-pred-produkty-cinskych-firem-huawei
https://www.idnes.cz/zpravy/domaci/huawei-zte-kyberneticka-hrozna-cinske-spolecnosti-nukib.A181217_152310_domaci_kuce
https://www.reuters.com/article/us-czech-huawei/czech-cyber-watchdog-calls-huawei-zte-products-a-security-threat-idUSKBN1OG1Z3

Obecná východiska

- **Zákon o kybernetické bezpečnosti (ZKB) a vyhláška o kybernetické bezpečnosti (VKB)**
  - Povinnosti jsou ukládány pouze povinným osobám, ty zavádí systém řízení bezpečnosti informací (ISMS)
  - ISMS se povinně nevztahuje na celou určenou organizaci, pouze na určené IS a KS
- **Risk based approach**
  - Přístup založený na riziku
  - **ZKB a VKB ukládají povinnosti – zavádění bezpečnostních opatření (ISMS)**
    - Jejich výběr a zavedení závisí na výsledku analýzy rizik
  - Hodnota rizika aktiva je vypočítána prostřednictvím funkce:
    - **Riziko = Dopad (hodnota aktiva) x Zranitelnost x Hrozba**
      - Výsledná míra rizika indikuje požadavky na ochranu, tedy na konkrétní bezpečnostní opatření, která jsou způsobilá snížit možnost naplnění nežádoucích jevů.
    - Konkrétní hodnoty prvků funkce volí subjekt obvykle na základě subjektivního hodnocení
- **Varování** = institut prostřednictvím kterého je upozorňováno na **hrozbu** (tj. potenciální příčinu kybernetické bezpečnostní události nebo kybernetického bezpečnostního incidentu, která může způsobit škodu)

Institut varování

- Jedno z opatření podle § 11 ZKB
  - = úkony, jichž je třeba k ochraně informačních systémů nebo služeb a sítí elektronických komunikací před hrozbou v oblasti kybernetické bezpečnosti nebo před kybernetickým bezpečnostním incidentem anebo k řešení již nastalého kybernetického bezpečnostního incidentu
  - = varování (nejméně drastické), reaktivní opatření, ochranné opatření
- Projev zákonné pravomoci NÚKIB analyzovat a monitorovat kybernetické hrozby a rizika
- **Nenahrazuje, pouze doplňuje** obecnou povinnost regulovaných subjektů identifikovat hrozby
- Specifický institut (srov. CHMÚ, SZPI, SÚKL), úkon podle části čtvrté zákona č. 500/2004 Sb.

§ 12 ZKB – Varování

(1) **Úřad vydá varování**, **dozví-li se** zejména z vlastní činnosti nebo z podnětu provozovatele národního CERT anebo od orgánů, které vykonávají působnost v oblasti kybernetické bezpečnosti v zahraničí, **o hrozbě v oblasti kybernetické bezpečnosti**.

(2) Varování **Úřad zveřejní na svých internetových stránkách a oznámí je orgánům a osobám uvedeným v § 3**, jejichž kontaktní údaje jsou vedeny v evidenci podle § 16 odst. 4.

Co varování znamená

- Prostřednictvím varování NÚKIB **upozorňuje na existenci hrozby** v oblasti kybernetické bezpečnosti, na kterou je nutné bezprostředně reagovat
- Varování je závazné pro regulované subjekty, neregulované subjekty mohou varování zohlednit dobrovolně
  - Regulované subjekty: poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací, orgán nebo osoba zajišťující významnou síť, správce a provozovatel informačního a komunikačního systému KII, správce a provozovatel VIS, správce a provozovatel informačního systému základní služby, provozovatel základní služby, poskytovatel digitální služby
- Varování nic nezakazuje ani nepřikazuje – ZKB však stanoví povinnost s informací obsaženou ve varování dále pracovat
  - Např. pokud jsou varováním za hrozbu označeny technické nebo programové prostředky určitých společností, **neznamená to bezpodmínečný zákaz používání** daných prostředků, ale nutnost zvážit případné bezpečnostní riziko související s jejich užíváním
  - Dovolí-li to výsledky analýzy rizik, uvedené technické nebo programové prostředky je možné i nadále používat

Význam varování pro regulované subjekty

- **Subjekty,** které spadají pod ZKB, **jsou povinny se touto hrozbou dále zabývat a zohlednit ji v analýze rizik**, kterou v souladu s požadavky ZKB a příslušné vyhlášky již pravidelně provádí
- Platí jak pro stávající, tak pro nově poptávané systémy (§ 4 odst. 4 ZKB)
- V rámci analýzy rizik je nutno aktualizovat katalog hrozeb o tuto hrozbu
  - Formulace hrozby – podle obsahu varování
  - Typová hrozba x konkrétní hrozba x definice z varování
- Hodnota hrozby – podle obsahu varování (dá se předpokládat, že nejčastěji půjde o hodnotu 4 ze 4, pokud je používána stupnice podle VKB)

Význam varování pro neregulované subjekty

- **Orgánům a osobám, kterým ZKB neukládá povinnost zavést a provádět bezpečnostní opatření, stejně tak jako široké veřejnosti, nezakládá varování NÚKIB žádnou povinnost**, a to ani zprostředkovaně
- Tyto subjekty tedy nejsou podle ZKB povinny varování NÚKIB zohlednit
- Další kroky s tím spojené jsou pouze na nich, jsou dobrovolné a nemohou být NÚKIB kontrolovány a sankcionovány
- Varování však může být zohledněno v analýze rizik (ISO 27001 a ISO 27005) – postup analogický s postupem regulovaných subjektů

Význam varování pro subjekty se vztahem na regulované

Dodavatelé, kteří dodávají technické nebo programové prostředky subjektům spadajícím pod ZKB, mohou být v pozici:

a) **provozovatele určeného informačního systému** podle § 2 písm. g) ZKB (pro povinný subjekt zajišťuje funkčnost technických a programových prostředků tvořících informační nebo komunikační systém), a tedy **budou subjektem spadajícím pod ZKB**

b) **běžného dodavatele,** kterého budou subjekty spadající pod ZKB řídit v rámci řízení dodavatelů

Implementace varování

- Správci a provozovatelé IS a KS KII, VIS a IS ZS jsou povinni podle § 5 VKB pro určené IS a KS provádět pravidelnou analýzu rizik, identifikovat rizika a identifikovaná rizika řídit
- Proces řízení rizik – povinnost **zohlednit mj. i opatření** podle § 11 ZKB, tedy i varování
- Na základě vyhodnocení rizik – **zavedení a provedení bezpečnostních opatření** v rozsahu nezbytném pro zajištění kybernetické bezpečnosti (§ 4 odst. 2 ZKB)
  - Akceptovatelná úroveň rizika x přiměřená bezpečnostní opatření x akceptace rizika
- Bezpečnostní opatření – blíže specifikována ve VKB
  - Organizační – bezpečnostní role, řízení dodavatelů, bezpečnost lidských zdrojů, řízení provozu a komunikací atd., technická – fyzická bezpečnost, správa a ověřování identit, řízení přístupových oprávnění, logování přístupů, kryptografické prostředky atd.
- **Na základě vydaného varování tedy musejí povinné osoby v rámci zavedeného řízení rizik provést analýzu rizik, ve které zohlední hrozbu, a následně na riziko reagovat přijetím bezpečnostních opatření, která musí být v souladu s nastavenými metrikami pro akceptovatelnost rizika a hodnotou daného rizika**

Zohlednění varování při zadávání veřejných zakázek

Konkrétní postup se odvíjí od fáze výběrového řízení (vždy založeno na výsledcích analýzy rizik):

1. Fáze přípravy zadávacího řízení
   - Zapracování výsledku analýzy rizik do **zadávací dokumentace**
2. Fáze probíhajícího zadávacího řízení
   a. Neuplynula lhůta pro podání žádosti o účast, předběžných nabídek nebo nabídek
      - **Změna / doplnění zadávacích podmínek** + prodloužení lhůty

   b. Lhůta uplynula
      - **Pokračování v zadávacím řízení** + **přijetí** takových **bezpečnostních opatření**, kterými nebude dotčen postup v ZŘ (např. organizační opatření uvnitř zadavatele)
      - **Zrušení zadávacího řízení**, pokud nelze pokračovat bez změny zadávacích podmínek (tj. přijetí jiných bezpečnostních opatření není možné)
3. Fáze po skončení zadávacího řízení a zadání zakázky uchazeči
   - Řízení rizik spojených s dodavateli
     - Nasazení **bezpečnostních opatření** ke snížení rizik
     - Postupné **nahrazení HW a SW** (podle možností)

Zohlednění varování při tvorbě zadávací dokumentace

- § 36 odst. 1 ZZVZ: Zadávací podmínky nesmí být stanoveny tak, aby určitým dodavatelům bezdůvodně **přímo nebo nepřímo zaručovaly konkurenční výhodu nebo vytvářely bezdůvodné překážky hospodářské soutěže**.
- § 4 odst. 4 ZKB: Orgány a osoby uvedené v § 3 písm. c) až f) jsou **povinny zohlednit požadavky** vyplývající z bezpečnostních opatření **při výběru dodavatele** pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. **Zohlednění požadavků** vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle tohoto zákona **nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži**.

= zákonná povinnost zohlednit požadavky založené na výsledcích analýzy rizik v zadávací dokumentaci

= řádné dodržení požadavků zákona nemůže představovat neodůvodněné nebo nezákonné omezení hospodářské soutěže

Zohlednění varování ze 17. 12. 2018 při tvorbě zadávací dokumentace

- Vydání varování **nelze automaticky považovat za důvod pro vyloučení uchazeče** ze zadávacího řízení
  - Nejde o kvalifikační požadavky, ale o požadavky na předmět plnění (technické podmínky)
  - Nejde o vyloučení konkrétního dodavatele – prakticky se zadávacího řízení může účastnit i společnost, jejíž technické a programové prostředky jsou varováním označeny za hrozbu, nicméně nemůže nabídnout vlastní výrobky
- Vyloučit technické a programové prostředky uvedené ve varování je možné cestou **technické specifikace**
  - Půjde o stanovení technických podmínek pomocí odkazu na konkrétního dodavatele nebo výrobky (§ 89 odst. 5 ZZVZ, nejpravděpodobněji písm. a/)
  - Případné vyřazení nabídky obsahující prostředky uvedené ve varování bude odůvodněno nesplněním zadávacích podmínek
- **Vyloučení technických a programových prostředků je nutné odůvodnit**
  - Odůvodnění poskytne analýza rizik

Metodická podpora NÚKIB

- Aktuální informace, podpůrné materiály – www.nukib.cz
- Vzorová analýza rizik (+ metodika) – polovina roku 2019
- Jakým způsobem zohlednit varování v zadávacím řízení (ve spolupráci s Ministerstvem pro místní rozvoj) – polovina roku 2019
- Dotazy, konzultace – regulace@nukib.cz

Děkuji Vám za pozornost!

regulace@nukib.cz
v.saskova@nukib.cz