Vznik zákona o kybernetické bezpečnosti (ZKB), jeho následné změny a doprovodná legislativa

Ing. Dušan Navrátil

Rizika

- **Závislost společnosti (jak soukromé, tak i státní sféry) na informačních a komunikačních technologiích (ICT)**
- **Zabezpečení provozu kritické infrastruktury**
- **Rostoucí podíl HDP závislý na ICT**

- **Zvýšené riziko vážných škod v případě zneužití / cíleného útoku na sítě ICT**

Situace v roce 2011

- **Kybernetická bezpečnost byla řešena prostřednictvím soukromých / akademických subjektů, bez právní regulace**
- **Nedostatek koordinace / nedostatečné sdílení informací**
- **Kybernetická ochrana byla roztříštěná a neefektivní**
- **Nebyly bezpečnostní standardy kybernetické bezpečnosti (s výjimkou utajovaných ICT)**

- **Nezbytnost regulace zákonem (stanovení povinností jak veřejným, tak i soukromým subjektům)**

Usnesení vlády č. 781 ze dne 19. října 2011

- **NBÚ ustaven gestorem problematiky kybernetické bezpečnosti a zároveň národní autoritou pro tuto oblast**
- **Zřízena Rada pro kybernetickou bezpečnost**
- **Ř/NBÚ má předložit návrh věcného záměru zákona o kybernetické bezpečnosti vládě do 31. března 2012**
- **Ř/NBÚ má vybudovat do 31. prosince 2015 plně funkční Národní centrum kybernetické bezpečnosti a jako jeho součást vládní koordinační místo pro okamžitou reakci na počítačové incidenty (vládní CERT - Computer Emergency Response Team)**

Základní principy navrhovaného řešení

- **Individuální zodpovědnost provozovatele za bezpečnost vlastní sítě (jak zajištění proti útokům zvenčí, tak i zabezpečení proti zneužití k útokům na jiné sítě)**

- **Rozdělení kyberprostoru na část spravovanou vládním CERT (kritická informační infrastruktura definovaná nařízením vlády) a národním CERT**

- **Nákladově efektivní řešení, bez přehnaného zasahování do práv soukromoprávních subjektů**

Cíle regulace

Stanovit / zřídit:

- **Definice pojmů v oblasti kybernetické bezpečnosti**
- **Jasný soubor pravidel kybernetické bezpečnosti včetně standardizace bezpečnostních opatření**
- **Kompetence ústředního orgánu státní správy odpovědného za kybernetickou bezpečnost**
- **Systém sdílení informací a včasného varování**
- **Koordinaci mezi státními a soukromými subjekty k prevenci útoků a opatření k nápravě škod**
- **Pravidla pro řešení mimořádných stavů (stav kybernetického nebezpečí)**

Role NBÚ/NÚKIB

- **Zřizuje a provozuje Národní centrum kybernetické bezpečnosti**
  - **Vládní CERT**
  - **Spolupráce s ostatními CERTs/CSIRTs;**
  - **Mezinárodní spolupráce**
  - **Výzkum, vývoj a vzdělávání**

- **Vydávání / navrhování prováděcí legislativ**

- **Vyhodnocování kybernetických bezpečnostních incidentů**

- **Ukládání sankcí za nedodržení povinností stanovených zákonem o kybernetické bezpečnosti**

- **Spolupráce s ostatními orgány státní správy**

- **Navrhuje vyhlášení stavu kybernetického nebezpečí (Vyhlašován předsedou vlády)**

Koho se ZKB týká?
Povinné osoby.

Povinné osoby podléhající regulaci

- **Správce a provozovatel informačního nebo komunikačního systému kritické informační infrastruktury (KII)**
- **Správce a provozovatel významného informačního systému (VIS)**
- **Poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací**
- **Orgán nebo osoba zajišťující významnou síť**
- **Provozovatel základní služby nebo správce a provozovatel informačního systému základní služby (PZS)**
- **Poskytovatel digitální služby (PDS)**
- **Orgán veřejné moci využívající služeb cloud computingu**

Původní ZKB 181/2014 platnost od 1.1.2015 Sb.

Novela ZKB 104/2017 Sb.

Novela ZKB 205/2017 Sb. (implementace evropské směrnice NIS I)

Novela ZKB 261/2021 Sb.

Kritická informační infrastruktura (KII)

- **Základem je „Krizový zákon“, Zákon č.240/2000 sb., krizovém řízení a o změně některých zákonů, který definuje kritickou infrastrukturu**
- **IS důležité pro chod státu a ekonomiky**
- **Určuje/navrhuje NÚKIB (před vznikem NBÚ)**
- **Určení IS je prováděno na základě Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury – dopadová a odvětvová kritéria**
- **IS státního i soukromého sektoru**

Provozovatel základní služby

. **Základní služba** = služba, jejíž poskytování je závislé na sítích nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení činností v některém z těchto odvětví:

1. energetika
2. doprava
3. bankovnictví
4. infrastruktura finančních trhů
5. zdravotnictví
6. vodní hospodářství
7. digitální infrastruktura
8. chemický průmysl

. **Informační systém základní služby** = systém, na jehož fungování je závislé poskytování základní služby

. **Provozovatel základní služby** = orgán nebo osoba, která je odpovědná za poskytování základní služby a která je určena NÚKIB

Určení na základě vyhlášky 437/2017 Sb. O kritériích pro určení provozovatele základní služby

Významný informační systém (VIS)

- **Významným informačním systémem se rozumí informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou ani informačním systémem základní služby a u kterého narušení bezpečnosti informací může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.**
-
- **Pouze veřejný sektor**

- **Postup určení původně:**
  - **orgán nebo osoba posoudí naplnění kritérií dle vyhlášky č. 317/2014 Sb. a nahlásí se jako povinná osoba NÚKIB**

    nebo
  - **informační systém je zahrnut do přílohy vyhlášky č. 317/2014 Sb**

- **Postup určení nyní dle vyhlášky č. 317/2014/Sb. ve znění změny 205/2016Sb. a 360/2020Sb. Je určeno striktně podle činností které IS vykonává pro veřejnou moc. Platnost je rozfázován do let 2021 až 2023.**

Poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací

Orgán nebo osoba zajišťující významnou síť

- **poskytnout kontaktní údaje**

- **další povinnosti pouze v případě vyhlášení stavu kybernetického nebezpečí, po vyhlášení jsou povinni vykonávat nařízené reaktivní opatření**

Regulace je především prováděna ČTU na základě zákona 127/2005 o elektronických komunikacích. Někteří poskytovatelé součástí KII.

Poskytovatel digitální služby (PDS)

Digitální služba je služba poskytovaná elektronickými prostředky na individuální žádost podanou elektronickými prostředky, poskytovaná zpravidla za úplatu.

- **on-line tržiště**
- **internetové vyhledávače**
- **cloud computing**

Komu povinné osoby podléhají?

V rámci ZKB kybernetický prostor rozdělen mezi Nukib/vládní CERT a národní CERT.

Povinné osoby podléhající regulaci

- **Správce a provozovatel informačního nebo komunikačního systému kritické informační infrastruktury (KII)**
- **Správce a provozovatel významného informačního systému (VIS)**
- **Poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací**
- **Orgán nebo osoba zajišťující významnou síť**
- **Provozovatel základní služby nebo správce a provozovatel informačního systému základní služby (PZS)**
- **Poskytovatel digitální služby (PDS)**
- **Orgán veřejné moci využívající služeb cloud computingu**

Povinné osoby podléhající NUKIBu/vládnímu CERTu

Povinné osoby podléhající ČTU a NUKIBu

Povinné osoby podléhající národnímu CERTu/CSIRTu (CZ.NIC)

CERT/CSIRT

- **CERT- Computer emergenci responce team**
- **CSIRT- Computer security incident responce team**

Jaké mají povinné osoby povinnosti?

Zavést a provádět bezpečnostní opatření

- **Správce a provozovatel informačního nebo komunikačního systému kritické informační infrastruktury (KII)**
- **Správce a provozovatel významného informačního systému (VIS)**
- **Poskytovatel služby elektronických komunikací a subjekt zajišťující síť elektronických komunikací**
- **Orgán nebo osoba zajišťující významnou síť**
- **Provozovatel základní služby nebo správce a provozovatel informačního systému základní služby (PZS)**
- **Poskytovatel digitální služby (PDS)**
- **Orgán veřejné moci využívající služeb cloud computingu**

Povinné osoby, které jsou povinny zavést a provádět bezpečnostní opatření stanovené ZKB a vyhláškou.

Povinné osoby, které jsou povinny zavést a provádět bezpečnostní opatření stanovené ZKB a vyhláškou v přiměřené míře.

Bezpečnostní opatření

Bezpečnostní opatření se rozumí souhrn úkonů, jejímž cílem je zajištění bezpečnosti informací v informačním systému a dostupnost a spolehlivost služeb a sítí elektronické komunikace v kybernetickém prostoru.

- **Organizační opatření**
- **Technická opatření**

Pozn. Byla zvolena cesta standardizace a ne certifikace. Bezpečnostní opatření jsou kontrolována kontrolním oddělením NUKIBU. NUKIB provádí certifikaci, tedy schvalování pouze u IS, které obsahují utajované informace. Certifikace probíhá na základě standardů NATO. Tyto systémy jsou pouze uzavřené, nejsou připojeny do internetu.

Bezpečnostní opatření

Organizační opatření:

- systém řízení bezpečnosti informací
- řízení rizik
- bezpečnostní politika
- organizační bezpečnost
- stanovení bezpečnostních požadavků pro dodavatele
- řízení aktiv
- bezpečnost lidských zdrojů
- řízení provozu a komunikací
- řízení přístupu osob
- akvizice, vývoj a údržba
- zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů
- řízení kontinuity činností
- kontrola a audit

Bezpečnostní opatření

Technická opatření:

- **fyzická bezpečnost**
- **nástroj pro ochranu integrity komunikačních sítí**
- **nástroj pro ověřování identity uživatelů**
- **nástroj pro řízení přístupových oprávnění**
- **nástroj pro ochranu před škodlivým kódem**
- **nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů**
- **nástroj pro detekci kybernetických bezpečnostních událostí**
- **nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí**
- **aplikační bezpečnost**
- **kryptografické prostředky**
- **nástroj pro zajišťování úrovně dostupnosti informací**
- **bezpečnost průmyslových a řídicích systémů**

Další povinnosti vůči NUKIB

- **Správci a provozovatelé systémů kritické informační infrastruktury (KII)**
- **Provozovatelé základních služeb, nebo správci a provozovatelé informačního systému základní služby (PZS)**
- **Správci a provozovatelé významných informačních systémů (VIS)**

jsou povinni:

- **oznámit NBÚ kontaktní údaje pro nepřetržité předávání informací o kybernetických bezpečnostních událostech;**
- **hlásit výskyt kybernetických bezpečnostních událostí vládnímu CERTu/NUKIBu**
- **provádět protiopatření, která jim vládní CERT/NUKIB stanoví.**

Národní CERT/CSIRT

- **Provozován soukromoprávním subjektem na základě veřejnoprávní smlouvy s NUKIBem, který není financován státem.**

- **Zprostředkovává sdílení informací, a to zejména pro soukromoprávní subjekty, akademickou sféru, oblast samosprávy, neziskový sektor, nespadající do kompetence vládního CERTu**

- **Po datu, kdy zákon začal platit byla uzavřena veřejnoprávní smlouva se sdružením CZ.NIC (správce domény CZ) o provozování národního CSIRTu (národní CSIRT byl tímto sdružením provozován na základě memoranda s MV o roku 2010)**

- **Poskytovatelé digitálních služeb (PDS) jsou povinni mu nahlásit kontaktní údaje**

NUKIB může ukládat sankce

pokud povinný subjekt…

- **neimplementuje bezpečnostní opatření**
- **neuchovává bezpečnostní dokumentaci**
- **nenahlásí kybernetické bezpečnostní incidenty**
- **nereaguje na protiopatření vydané NUKIB**
- **nenahlásí kontaktní údaje nebo změnu těchto informací**

může NUKIB ukládat finanční pokuty

Stav kybernetického nebezpečí (KN)

- **Stav mimořádný, speciální oproti mimořádným stavům vyhlašovaným podle ústavního zákona č. 110/1998 Sb. o bezpečnosti České republiky nebo podle krizového zákona č. 240/2000 Sb**

- **Možno vyhlásit pokud je ve velkém rozsahu ohrožena bezpečnost informací v IS, bezpečnost služeb nebo sítí elektronických komunikací a tím dojde k ohrožení nebo porušení zájmu České republiky.**

- **Stav KN vyhlašuje předseda vlády na návrh ředitele NUKIB.**

- **Vyhlašován na dobu nejdéle 7 dnů – prodloužení jen se souhlasem vlády.**

- **Za stavu kybernetického nebezpečí a za nouzového stavu v případech je NUKIB oprávněn vydat reaktivní opatření rovněž poskytovatelům služby elektronických komunikací a subjektům zajišťujícím síť elektronických komunikací a orgánům nebo osobam zajišťující významnou síť.**

Vyhlášky a nařízení vlády

- Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
- Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích, **Změna: 205/2016 Sb., 360/2020 Sb.**
- Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby , **ve znění vyhlášky č. 573/2020 Sb.**
- Nová vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti nahradila vyhlášku č. 316/2014 Sb., o kybernetické bezpečnosti
- **Vyhláška č. 316/2021 Sb., o některých požadavcích pro zápis do katalogu cloud computingu**
- **Vyhláška č. 315/2021 Sb., o bezpečnostních úrovních pro využívání cloud computingu orgány veřejné moci**

Směrnice EU

- **Směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii (Směrnice NIS I)**
- **Evropský parlament na svém jednání 10. listopadu 2022 a Rada Evropské unie na jednání 28. listopadu 2022 přijaly znění nové směrnice o opatřeních k zajištění vysoké společné úrovně kybernetické bezpečnosti v Unii, tzv. směrnice NIS2. Poté, co směrnice vstoupila v polovině ledna v platnost, začala členským státům EU běžet 21 měsíců dlouhá lhůta, během které musí transponovat tento předpis a změny z něj vyplývající do národních legislativ.**

Nový ZKB

- **Na základě implementace směrnice EU NIS2 připravil NÚKIB návrh nového ZKB včetně bezpečnosti dodavatelských řetězců a příslušných vyhlášek.**

- **Návrh nového ZKB včetně důvodových zpráv a návrhů vyhlášek byl začátkem února 2023 zveřejněn na stránkách NÚKIBu a předložen k veřejné diskuzi. Návrh prošel poté mezirezortním připomínkovým řízením. Nyní prochází legislativní radou vlády a následným schválením vládou. Vláda odešle návrh do Parlamentu ČR, kde bude projednán a schválen oběma komorami včetně příslušných výborů.**

- **V tomto okamžiku se jedná o návrh, který může doznat mnoha změn, ale musí implementovat NIS2.**

Problematika je dobře popsána NÚKIBem na adrese nis2.nukib.cz

Návrh nového ZKB

nZKB zavádí jediný typ povinné osoby a tou je poskytovatel regulované služby.

Poskytovatelem regulované služby je kdokoliv, kdo poskytuje alespoň jednu regulovanou službu, tedy službu, jejíž narušení by mohlo mít významný dopad na zabezpečení důležitých společenských nebo ekonomických činností a jejíž kritéria jsou ve vyhlášce o regulovaných službách.

nZKB definuje kritéria pro regulované služby:

- **pro identifikaci – organizace provádí posouzení a následnou registraci sama**
- **pro určení – NUKIB vede správní řízení o určení**

Návrh nového ZKB

Kritéria pro identifikaci regulované služby jsou stanovena v odvětvích

- **veřejná správa,**
- **energetika,**
- **výrobní průmysl,**
- **potravinářský průmysl,**
- **chemický průmysl,**
- **vodní hospodářství,**
- **odpadové hospodářství,**
- **doprava,**
- **digitální infrastruktura a služby,**
- **finanční trh,**
- **zdravotnictví,**
- **věda, výzkum a vzdělávání,**
- **poštovní a kurýrní služby,**
- **vojenský průmysl,**
- **vesmírný průmysl.**

Návrh nového ZKB

nZKB přiděluje poskytovatelům regulované služby tzv. režim povinností:

- **režim vyšších povinností – poskytovatelé podléhají NUKIBu/GOVCERTu**
- **režim nižších povinností – poskytovatelé podléhají národnímu CSIRTU(CZ NIC)**

Poskytovatel s více regulovanými službami, z nichž jedna je v režimu vyšších povinností, potom se tento režim vztahuje na všechny jím poskytované služby.

Současné IS podléhající regulaci NUKIB (asi 350 IS) automaticky se stávají regulovanou službou s vyšší povinností.

Odhadovaný počet poskytovatelů regulovaných služeb s režimem vyšších povinností je asi 6000.

Návrh nového ZKB

Další zásadní změny a novinky nZKB:

- **Komunikace bude prováděna přes portál NUKIB včetně registrace nahlášení kontaktních údajů, hlášení bezpečnostních incidentů a hlášení o provedených protiopatření**
- **Pro poskytovatele regulované služby je stanoven rozsah řízení kybernetické bezpečnosti.**
- **Seznam bezpečnostních opatření poskytovatele regulované služby je jiný pro různé režimy povinností.**
- **Hlášení incidentů dle režimu je povinností.**
- **Lokalizace**
- **Informování zákazníků o incidentech.**
- **Povinnosti vrcholového vedení (součást organizačních opatření).**
- **Povinnost plnit mechanismus řízení bezpečnosti dodavatelských řetězců.**
- **Regulovány jsou poskytovatelé služby registrace doménových jmen.**
- **Pokuty**
- **Stav kybernetického nebezpečí.**

Zajištění dostupnosti strategicky významné služby

Lokalizace primárních a podpůrných aktiv mimo území České republiky s sebou nese určitou míru rizika pro zajištění dostupnosti strategicky významných služeb v případě omezení dostupnosti nepostradatelných aktiv nacházejících se v zahraničí.

Je nutné zajistit dostupnost strategicky významných služeb z území České republiky.

Poskytovatel strategicky významné služby:
- má svobodu ve výběru prostředků, jakými tohoto cíle dosáhne,
- nastavuje dobu obnovení chodu služby i kvalitu služby,
- zajišťuje dostupnost z ČR alespoň v rámci nezbytného rozsahu stanoveném vyhláškou.

Není dostačující, aby poskytovatel zajistil dostupnost služeb poskytovaných z území mimo území České republiky pouze za využití standardních smluvních ujednání (typicky SLA), jelikož na tyto se nelze spoléhat v případě mimořádných událostí jako je válka či přírodní katastrofa.

Zajištění dostupnosti strategicky významné služby

Zajištění dostupnosti strategicky významné služby z území České republiky
- nevylučuje možnost poskytování těchto služeb a jejich řízení také z území mimo ČR;
- musí umožňovat obnovení dostupnosti služby a její další poskytování výhradně z území ČR bez použití aktiv mimo území ČR;
- může bylo řešeno rozdílně oproti standardnímu stavu, tedy například fyzicky bez využití ICT prostředků.

Od poskytovatele je požadováno otestování schopnosti zajistit poskytování strategicky významnou službu ve stanoveném čase a kvalitě z území České republiky.

Tato povinnost se vztahuje pouze na nejkritičtější a nejvíce strategické služby důležité pro chod státu a pouze na nezbytný rozsah těchto služeb stanovený vyhláškou (odvětví např. energetika, drážní a letecká doprava, telekomunikace, veřejná správa).

Zajištění dostupnosti služby je možné i mimo kyberprostor. Sám poskytovatel služby si definuje přípustnou míru snížení kvality poskytované služby

Bezpečnost dodavatelských řetězců

Česká chce realizovat strategickou kontrolu dodavatelských řetězců u nejkritičtějších služeb a tím
- reagovat na existence strategických hrozeb pocházejících z dodavatelského řetězce,
- prověřovat důvěryhodnost dodavatele,
- působit jak zpětně, tak do budoucna.

Mechanismus prověřování dodavatelského řetězce dopadne pouze na poskytovatele strategicky významných služeb (cca 150 subjektů). V rámci těchto poskytovatelů se vztahuje na bezpečnostně významnou dodávku, která směřuje:
- do části systému, kterou si poskytovatelé sami určí jako kritickou (aktiva s kritickým nebo vysokým dopadem na službu), nebo/i
- na funkci systému, kterou NÚKIB určí jako nepominutelnou.

Bezpečnostně významná dodávka je plnění směřující do kritické části stanoveného rozsahu spočívající v poskytnutí, vývoji, výrobě, sestavení, správě, provozu či servisu:
- technického prostředku nebo vybavení s výpočetní kapacitou;
- programového prostředku nebo vybavení, nebo
- informační či komunikační služby.

Bezpečnost dodavatelských řetězců

Prověřování bude zaměřeno na:
- dodavatele, kteří již svá plnění do infrastruktury pro poskytování strategicky významných služeb dodávají;
- jejich poddodavatele či potenciální dodavatele, mající vliv na konečný produkt.

V roce 2022 NÚKIB vydal „Doporučení pro hodnocení důvěryhodnosti dodavatelů technologií do 5G sítí v České republice“ (je na webu NÚKIB), kde je uvedeno:

…Snižování rizik spojených s dodavateli do 5G sítí pouze technickými prostředky je nedostatečné; hardware i software těchto technologických řešení jsou natolik komplexní, že je nelze efektivně technicky prověřit a eliminovat případné zranitelnosti. Ty v nich tak mohou zůstat dlouhodobě neodhaleny či do nich mohou být později zavedeny, například v rámci aktualizací. Důvěra v dodavatele je v tomto ohledu zásadní. Vliv právního a politického prostředí, ze kterého dodavatel pochází nebo kterým je ovlivňován, má na důvěryhodnost značný význam, a proto je nezbytné jej k zajištění bezpečnosti nejdůležitějších součástí 5G sítí zohlednit…

Dotazy?
Diskuze!