Vznik NUKIB, jeho činnosti a varování Huawei

Ing. Dušan Navrátil

NUKIB

- **Rozhodnutí vlády z prosince 2016 o vzniku samostatného úřadu NUKIB delimitací z NBÚ**
- **V prosinci 2016 v Poslanecké sněmovně Parlamentem ČR byla po prvním čtení novela ZKB (implementace směrnice EU - NIS I.)**
- **Pozměňovací poslanecký návrh předložený ve druhém čtení ve výboru pro bezpečnost definoval nový úřad – NUKIB**
- **Součástí pozměňovacího návrhu byla i novela Zákona o utajovaných informacích 412/2005 Sb.**
- **Novely schváleny v červnu 2017 Senátem Parlamentu ČR a podepsány prezidentem**
- **Platnost novely od 1. srpna 2017 – vznik NUKIB**
- **Leden – červenec 2017 - příprava delimitace NCKB, certifikace IS obsahujících utajované informace, Tempest, krypto a Galileo z NBU**
- **Leden – červenec 2017 – vytvoření nové obslužné sekcee – ekonomika, správa, vnitřní IT a právní věci ještě v rámci NBU a poté delimitováno**
- **Červen 2017 - novela zákona o státním rozpočtu – vlastní rozpočtová kapitola**
- **1. srpna 2017 vznik NUKIB**
- **Říjen 2017 – parlamentní volby**

NÚKIB

Ústřední orgán státní správy pro:

- **kybernetickou bezpečnost**
- **ochranu utajovaných informací v oblasti informačních a komunikačních systémů**
- **kryptografickou ochranu**
- **problematiku neveřejné služby v rámci družicového systému Galileo**

Sídlo v Brně (3 pracoviště – budoucí výstavba nové budovy v Černých Polích) a dvě pracoviště v Praze

NÚKIB

- **Ředitel jmenovaný vládou po projednání v příslušném výboru PS PČR, odpovědný premiérovi**
- **Ředitel se účastní zasedání BRS, výkonným předsedou RKB A VKB**
- **Právo legislativní iniciativy**
- **Celkem 330 pracovních míst**
- **Rozpočet 616 mil.**
- **Stálá komise PS PČR pro kontrolu NÚKIB**

NÚKIB

Struktura úřadu k 1.1.2023 (nejsou uvedeny obslužné útvary)

Sekce NCKB

- **Odbor vládní CERT**
- **Odbor regulace**

Sekce informačních systémů

- **Odbor bezpečnosti informačních technologií**
- **Oddělení bezpečnosti satelitních služeb**

Sekce strategických agent a spolupráce

- **Odbor mezinárodní spolupráce a EU**
- **Odbor cvičení a vzdělávání**
- **Odbor centrální analytiky**
- **Oddělení národních strategií politik**
- **Oddělení vědy, výzkumu a inovací**

NÚKIB

Činnosti odboru centrální analytiky:

- **Analýza a monitoring kybernetických hrozeb a trendů v kybernetické bezpečnosti**
- **Posuzování jejich politických kontextů či dopady materiálů.**
- **Ve spolupráci s CERT rozvíjí pokročilou analytickou kapacitu v podobě Cyber Threat Inteligence (CTI)**
- **Informační šetření**

NUKIB

Činnost oddělení výzkumu a inovací

Národní plán výzkumu v kybernetické a informační bezpečnosti

Dva zdroje financování:

- **Financováno z rozpočtu NÚKIB – vyčleněno na vědu a výzkum 20 mil. Kč – převážná většina v utajovaném režimu Tempest a krypto**
- **Bezpečnostní výzkum MV (řádově 500 mil Kč. pro všechny oblasti)**
  - **. Výzkumná potřeba státu – řešitelé jsou vybíráni veřejnou soutěží – řešení zůstává majetkem státu**
  - **. Nabídka tématu řešiteli – řešení zůstáva majetkem (příklad KYPO MU)**

Pozn 1. možné financování přes TAČR - zatím se nevyužívá

Pozn 2. Bezpečnostní výzkum MV může být i v utajeném režimu.

Pozn 3. Existuje i obranný výzkum MO – zatím se nevyužívá

NUKIB

NUKIB zajišťuje Národní koordinační centrum výzkumu a vývoje v oblasti kybernetické bezpečnosti (NCK) na základě nařízení EU 2021/887

NKC působí jako kontaktní místo PRO komunitu na národní úrovni, spolupracuje s CyberSecurity Hub (zapsaný ústav) – sdružení MU,VUT a ČVUT zabývající se kyberbezpečnostním výzkumem a je zároveň členem Digital Innovation Hun Network

NUKIB

Odbor bezpečnosti informačních technologií

Kryptografická ochrana

- **Aplikovaný výzkum a vývoj kryptografických prostředků**
- **Analýza a hodnocení šifrových systémů a kryptografických algoritmů určených k ochraně utajovaných informací**
- **Vývoj nových technologií a výrobních klíčových materiálů a kryptografických prostředků a vývoj v oblasti jejich zabezpečení proti neoprávněné manipulaci při převozu**

NUKIB

Odbor bezpečnosti informačních technologií

Certifikace informačních a komunikačních systémů

- **Certifikace systémů – 100 z toho 700 aktivních, 90% státní správa, z toho PT a T 15%, D-50%, V-35%**
- **Schvaluje změny v certifikovaných IS cirka 1000 ročně**
- **Tvorba standartů a metodik ochrany UI v IS**
- **Akreditace IS EU a NATO**

NUKIB

Odbor bezpečnosti informačních technologií

TEMPEST(Telecommunications Electronics Materials Protected from Emanating Spurious Transmissions)

- **Národní středisko pro měření kompromitujícího elektromagnetického vyzařování (KV) cca 200/rok**
- **Návrh metod a postupů hodnocení el. Zařízení, zabezpečené oblasti nebo objektu proti úniku UI prostřednictvím KV**
- **Certifikace stínících komor cca 20/r**
- **Kontroly jednacích místností k nepovolenému použití technických prostředků určených k získávání informací nebo KV**
- **Určování standardů v oblasti TEMPEST**

NUKIB

Odbor bezpečnosti informačních technologií

Šifrová služba

- **Výroba kryptografického materiálu KM) pro provoz kryptografických prostředků (KP)**
- **Evidence KM, pracovníků kryptografické ochrany včetně evidense kompromitace a ničení KM**
- **Národní středisko pro distribuci KM (NDA)**
- **Servis a údržba KP**

Nová výzva postkvantová kryptografie!!!!!!!!

„Varování Huawei“

17. prosince 2018 NUKIB vydal na základě § 18 ZKB Varování před používáním SW a HW společností Huawei Technologies a ZTE Corporation – používání technických a programových prostředků představuje hrozbu v oblasti kybernetické bezpečnosti.

Proč bylo vydáno?

- **Hrozba spočívá zejména v tom, že uvedené společnosti jsou srozuměny upřednostnit zájmy ČLR (KSČ) před zájmy uživatelů jejich technologií (zákazníků), s reálnou možností narušit bezpečnost dat.**
- **Politické a právní prostředí ČLR dává povinnost právnickým a fyzickým osobám podílet se na zpravodajské činnosti státu a napomáhat v prosazování jeho zájmu.**
- **Technologie uvedených společností jsou nebo se mohou nacházet se mohou nacházet v IS a KS strategického významu, přičemž jejich vliv na úroveň bezpečnosti těchto systémů je či může být značný mnohdy zásadní.**
- **Zjištění českých zpravodajských služeb o zpravodajských aktivitách ČLR vlivového a špionážního charakteru.**

„Varování Huawei“

Co to znamená?

- **Prostřednictvím varování NUKIB upozornil na existenci hrozby v oblasti kybernetické bezpečnosti, na kterou je nutno bezprostředně reagovat.**
- **Subjekty, které spadají pod ZKB jsou povinny se touto hrozbou zabývat a zohlednit ji v analýze rizik, kterou jsou v souladu se ZKB a příslušné vyhlášky, které jsou povinny pravidelně provádět.**
- **Varování neznamená bezpodmínečný zákaz používání daných technických a programových prostředků, ale nutnost zvážit případné bezpečnostní riziko související s jeho používáním.**
- **Dovolí-li to výsledky analýzy rizik, uvedené technické nebo programové prostředky je možno i nadále používat.**
- **Orgánům a osobám, kterým ZKB neukládá povinnost zavést a provádět bezpečnostní opatření, stejně jako široké veřejnosti, nezakládá varování žádnou povinnost.**

„Varování Huawei“

Co tedy dotčené subjekty měly udělat?

- **Na základě vydaného varování tedy musí povinné osoby v rámci zavedeného řízení rizik povézt (novou analýzu rizik), ve kterém zohlední hrozbu a následně na riziko reagovat přijetím bezpečnostního opatření, které musí být v souladu s nastavenými metrikami pro akceptovatelnost rizika a hodnotou daného rizika.**

- **Hrozba uvedená ve varování je definována jako velmi pravděpodobná až víceméně jistá. (stupeň 4 ze 4).**

- **Metodika k varováni vydána 4.1. 2018 – konkretizuje možné přístupy správců či provozatelů IS a KS v reakci na vydané varování.**

- **Pokud z analýzy rizik vyplyne riziko, které je neakceptovatelné dle ZKB a vyhlášky, je nutné přistoupit ke konkrétním opatřením. Může být například postupná náhrada daných technologických prvků a vyloučení společností týká z výběrových řízení.**

„Varování Huawei“

- **Dvě poznámky:**
- **V analýze rizik dochází k definování hodnoty hrozby, zranitelnosti a dopadu narušení aktiva. Díky výsledné hodnotě rizika organizace identifikuje, zda je nutné pro analyzované aktivum (to co chceme chránit, např. server, stanici , síťové prvky) zavádět opatření (tedy je více chránit) nebo, zda je riziko akceptovatelné (tedy není třeba potřeba opatření zavádět.**

- **Vztah varování k zákonu o zadávání veřejných zakázek (ZZVZ)- Zadavatel podle ZVZZ nesmí vytvářet při stanovování zadávacích podmínek „bezdůvodné překážky hospodářské soutěže“. Pokud je oprávněnou autoritou tj. NÚKIBem , vydáno varování dle ZKB, nelze pak přijetí vhodných bezpečnostních, kterými může být i vyloučení daných technologií, považováno za vytváření bezdůvodné překážky hospodářské soutěže.**

„Varování Huawei“

- **Proč bylo varování bylo vydáno „za pět minut dvanáct?**
- **V polovině roku ČTU měl vypsat výběrové řízení na provozování mobilních sítí 5.generace (5G)**
- **Pokud má ČR udržet si konkurenceschopnost a ekonomickou výkonnost budou 5G sítě tvořit páteř její ekonomiky.**
- **V případě, výrobce komponentů sítě 5G umožní přístup k zařízení třetí straně, získá tento aktér schopnost způsobit společnosti a ekonomice ČR masívní škody. I pouhé vědomí (či dokonce odůvodněné podezření) existence takové možnosti může mít dopad na svobodné a suverénní postavení ČR, jak v domácí tak zahraniční politice.**
- **Narušení bezpečnosti sítí 5G bude mít celospolečenské dopady v rovině ekonomické, společenské, strategické a vojenské. Takový efekt je v současné době srovnat snad je s výpadkem elektrické energie.**
- **Pokud bude mít cizí státní či nestátní aktér přístup k páteřním komponentům, může dojít i k manipulaci a pozměňování dat**

„Varování Huawei“

Reakce Číny

- **Návštěva premiéra v sídle HUAWAY – dopis ze stížností**
- **Aktivizace lobistů, včetně na nejvyšších mistech státu**
- **Strašení lobistů, že varování bude mít nedozírné následky pro ČR**
- **Setkání premiéra s čínským velvyslancem v Průhonicích**
- **Tisková zpráva velvyslance o setkání**
- **Pokusy o mediální kampaň**
- **Výhružný dopis vládě – vyhrožování arbitráží a škodou 40 miliard korun**

  (západní ambasadoři pečlivě sledovali so se bude dít)

NIC se NESTALO!

„Varování Huawei“

- **V podmínkách výběrového řízení na provozování mobilních sítí 5G byla věta: „Mobilní sítě 5G budou s vysokou pravděpodobností Kritickou informační infrastrukturou a bude se na ně vztahovat Zákon o kybernetické bezpečnosti.**

- **Připravuje se nové řešení uvedeného problému. NÚKIB dostal úkol vlády připravit Zákon o dodavatelských řetězcích.**

„Varování Huawei“

Mezinárodní souvislosti:

S nástupem technologií došlo k zásadnímu obratu v geopolitickém uvažování – rozhodujícím faktorem již není konkrétní území a vliv na něj, ale kontrola infrastruktury. S přechodem k digitalizované společnosti není potřeba kontrolovat území a politické prostředí formou vlády jedné strany či represemi pomocí fyzického útlaku. Celé státy je možné si podmanit kontrolou infrastruktury, která je digitalizovaná. Státní celky a společnost jsou zcela závislé na přenosu informací v době míru, ale především v době politických rozhodnutí a konfliktu. Toto si globální hráči (Rusko ?) uvědomili a měly by si to uvědomiti i menší státy, které jsou předmětem snah ČLR.

„Varování Huawei“

Mezinárodní souvislosti:

„ Spojence jsme“ ,podle George Masona, státního contractora pro obast čínského vlivu (USA), „Varováním zcela zaskočili a překvapili. Když bylo Varování vydáno, způsobilo jemně řečeno poprask v komunitě bezpečnostních složek a vlády, neboť měli za to, že ČR je jež ve sféře politického vlivu ČLR.“

Dle tvrzení Huawai zprávu o Varování četlo na světě 750 mil. lidí.

Američany a spojence překvapili principem Varování, který označili za novátorský a univerzální. V podstatě šlo o ukázku nejlepšího postupu (best practise). V té době se hodně hovořilo o technických důkazech. Varování primárně nepotřebovalo technické důkazy. Šlo cestou analýzy strategického zájmu a právního prostředí ve kterém se firmy pohybují. Technické důkazy byly pouze podpůrné.

„Varování Huawei“

- **Mezinárodní souvislosti:**
- **Před Varováním:**
- **Austrálie opatrně nejmenovitě nepřímo vyřadilo čínské firmy z 5G sítí.**
- **Francie v tichosti problém měla vyřešen zákonem o odposleších.**
- **USA – řada dílčích opatření**

- **Varování rozproudilo na „Západě“ intenzivní diskuzi, „došlo k prolomení ledu“.**
- **Názory se postupně se v jednotlivých státech postupně měnily. Intenzivní boj mezi „bezpečáky“ a „ekonomy“. Např. UK a Německo)**
- **USA – prezidentské dekrety**
- **Diskuze v Komisi EU**

„Varování Huawei“

Mezinárodní souvislosti:

Pražská konference o bezpečnosti sítí 5G – květen 2019 – doporučení nazvané „Prague Proposals“ (vymahatelnost práva, otevřenost, monitorovatelný dodavatelský řetězec, omezení státní podpory a podobně) vytvořilo další prostor pro debaty v rámci EU, NATO a OSN.

26.9.2019 – Doporučení Komise EU:

- **Posoudit bezpečnostní rizika ovlivňující 5G sítě**
- **Určit nejzranitelnější prvky**
- **Přezkoumat bezpečnostní požadavky a bezpečnostní hrozby**
- **Vzít v potaz technické i netechnické aspekty včetně politického rámce**

Dotazy?
Diskuze!