Národní bezpečnostní úřad
P.O.BOX 49
150 06 Praha 56

Věc : Připomínky k návrhu věcného záměru zákona o kybernetické bezpečnosti

Sdružení CZ.NIC velice uvítalo možnost vyjádřit se tímto způsobem k návrhu věcného záměru zákona o kybernetické bezpečnosti.

Jsme rádi, že jsme se mohli podílet na věcné, konstruktivní a v mnoha ohledech přínosné diskusi nad tímto důležitým dokumentem. Považujeme za správné a důležité, že NBÚ zpřístupnil navrhované znění záměru zákona veřejnosti, která měla dostatečnou dobu se s ním seznámit a následně ho připomínkovat.

Předpokládáme, že z těchto a dalších diskusí vzejdou zajímavé podněty, které mohou dále rozšířit význam a důležitost tohoto záměru. K tomu chceme přispět i my a proto jsme připravili seznam připomínek, které navrhujeme zohlednit ve věcném záměru. Jednotlivé podněty z naší strany jsou označeny čísly daných kapitol.

Kapitola 2.3.
Obáváme se, že možnost řešení kybernetické bezpečnosti pouze v rámci regulace orgánů veřejné správy nebyla dostatečně prozkoumána.

Jsme přesvědčeni o tom, že pro Českou republiku by bylo výhodné ve větší míře využít zkušeností, mechanismů a postupů, které byly v oblasti kybernetické bezpečnosti nasbírány a které se v praxi osvědčily. Považovali bychom za vhodnější, kdyby státní regulace tyto existující postupy pouze doplňovala tam, kde soukromoprávní či akademické působení nedává smysl nebo vůbec není možné.

Doporučujeme zvážit možnost rozdělení pravomocí a přenesení zodpovědností při ochraně kybernetického prostoru ČR mezi všechny zainteresované subjekty a využít jejich zkušenosti a odborný potenciál (Vládní CERT, Národní CERT, bezpečnostní složky státu, soukromé organizace zabývající se kybernetickou bezpečností, poskytovatelé služeb elektronických komunikací a elektronických služeb a jejich bezpečnostní týmy a vědecko-výzkumné organizace).

Pro aplikaci takovéto varianty by bylo možné využít stávající právní akty (zejména zák. č. 127/2005, 480/2004, TZK, TŘ….) a jednotlivým subjektům přiřknout pravomoci sloužící k ochraně zájmů ČR.

Z tohoto pohledu by potom zákon o kybernetické bezpečnosti mohl definovat základní pojmy a upravovat především Vládní CERT a jeho činnost a pravomoci vůči „státním“ sítím a informačním systémům.

Činnost Národního CERT týmu ani dalších „nestátních“ subjektů by pak regulaci NBÚ podléhat neměla, případně jen v omezené a přesně definované míře. Měla by být založena na spolupráci a na vzájemných formálních i neformálních dohodách (tak jak je obvyklé a osvědčuje se v dnešní praxi a jak je doporučováno

mezinárodními organizacemi, působícími na poli ochrany bezpečnosti kyberprostoru – ENISA, TERENA, FIRST).

Z našich zkušeností se jeví jako velmi nepravděpodobné, že by mohlo dojít k problémům s dodržováním závazků vůči NATO či EU. Sítě či systémy, které by regulaci nepodléhaly, sice mohou být (jako obecně jakákoliv síť) zdrojem závažných bezpečnostních incidentů, ale případná regulace jejich vyřešení negarantuje a téměř jistě ani neurychlí. Reagovat, hlásit bezpečnostní incidenty a tlačit zodpovědné osoby (subjekty) k odstranění a vyřešení problému lze i za současného stavu (a s dostupnými právními prostředky) a v praxi se tak i děje.

Námi navrhovaný postup je obecně založen na nutnosti spolupráce se soukromoprávními subjekty. Nepovažujeme za vhodné zahájit řešení kybernetické bezpečnosti aplikací co nejširší regulace, neboť je v praxi ověřeno, že odebírání pravomocí jednou svěřených státu či státním orgánům je výrazně komplikovanější, takže pokud by se regulace v budoucnu ukázala být naddimenzovanou, těžko se bude prosazovat její omezení.

Kapitola 6 :
Doporučujeme opustit termíny „národní / ústřední dohledové pracoviště“ a používat mezinárodně etablované termíny „Národní CERT“ (National CERT) a „Vládní CERT“ (Governmental CERT), které už zdomácněly a jsou běžně používány i v ČR – viz zprávy v médiích, výsledky vědecko-výzkumných aktivit, vystoupení na odborných konferencích, dokumenty typu *Strategie pro oblast kybernetické bezpečnosti České republiky, Usnesení vlády ČR č. 781 apod.*

Kapitola 7.2. :
Uložit povinnost hlášení kybernetických bezpečnostních událostí zákonem těm subjektům, které neprovozují systémy (služby) či sítě kritické informační či komunikační infrastruktury, by mohlo být výrazným zásahem do jejich činnosti.
Takovýto zásah pak de facto omezuje právo na informační sebeurčení. Doporučujeme tuto povinnost změnit tak, aby spolupráce byla dobrovolná. Tím by bylo umožněno, aby byla založena na konkrétní dohodě mezi všemi zúčastněnými stranami, která by reflektovala formu, četnost a další aspekty této spolupráce. Tento postup také koresponduje s původním účelem bezpečnostních týmů, neboť jejich úkolem je koordinace dobrovolné spolupráce subjektů, které mají o spolupráci a sdílení informací zájem.

Pro ty subjekty, které systémy či sítě kritické informační či komunikační infrastruktury provozují, by potom povinnost hlášení kybernetických bezpečnostních událostí bylo vhodné omezit pouze na tyto konkrétní části jejich systémů spadající do kritické informační a komunikační infrastruktury, a už nikoliv na všechny ostatní jimi provozované služby či sítě.

Doporučujeme zvážit možnost vztáhnout povinnost aplikovat protiopatření stanovená NBÚ pouze na správce informačních systémů veřejné správy (obecně na „pole působnosti“ budoucího Vládního CERT nebo její část).
U protiopatření, které má stanovovat NBÚ, v návrhu postrádáme jejich přesnější vymezení. I díky tomu by mohla vzniknout obava, že v praxi může jít o výrazné zásahy do systémů jednotlivých správců kritické informační a komunikační infrastruktury. Navíc bez detailní znalosti dané infrastruktury tato protiopatření

nemusí být kompatibilní s jejím aktuálním stavem, nebo dokonce mohou způsobit zcela opačný efekt – větší zranitelnost.

V praxi nařízení konkrétních zásahů bez znalosti konkrétního prostředí (nebo dokonce pouze jejich plošnou definici) považujeme za technicky jen velmi obtížně realizovatelné a potenciálně nebezpečné. Za určitých okolností ty navíc tato opatření mohla by být vnímána jako filtrování obsahu internetu, což je v přímém rozporu i s nedávnými rozhodnutími Evropského soudního dvora.

Dále doporučujeme věnovat pozornost definici „významných“ informačních systémů veřejné správy. Bylo by vhodné definovat je jak obecně, tak s ohledem na to, že „významnost“ jednotlivých systémů se může průběžně měnit.

Kapitola 8 :
Považujeme za žádoucí přesněji definovat odborná kriteria pro výběr provozovatele ústředního dohledového pracoviště a způsob výběru tohoto subjektu.

Minimálním standardem by podle našeho názoru mělo být provozování pracoviště typu CERT/CSIRT a akreditace takového pracoviště v odpovídajících mezinárodních strukturách (TERENA, FIRST)

Kapitola 10 :
Dle našeho názoru se řešení popsané ve VZ nedá považovat za minimalistické. Obáváme se, že nelze konstatovat, že zákon nezahrnuje přímé výkonné pravomoci státu. Státu má naopak podle znění VZ připadnout celá řada výkonných pravomocí, neboť bude požadovat plnění jistých minimálních bezpečnostních standardů po všech subjektech regulace.

Kapitola 15 :
Domníváme se, uváděné vymezení odpovědnosti za případnou škodu nedostatečně vystihuje případnou odpovědnost, neboť je možné si představit například případy, kdy:

1. Přes dodržení minimálních bezpečnostních standardů vznikne třetím osobám škoda,
2. stát vyhlásí stav kybernetického nebezpečí a subjekty budou postupovat dle protiopatření jim nařízených a dojde ke vzniku škody,
3. vyhlášená protiopatření budou zjevně nedostačující, nebo dokonce nevhodná.

Uvedené případy mohou nastat, avšak ne zcela splňují podmínky pro náhradu škody dle zák. č. 82/1998, zejména pak ust. § 3, 5 a násl.