VYHODNOTENIE MEDZIREZORTNÉHO PRIPOMIENKOVÉHO KONANIA

Pravidlá pre blokovanie útokov

Spôsob pripomienkového konania
Počet vznesených pripomienok, z toho zásadných 46 /8
Počet vyhodnotených pripomienok 46

Počet akceptovaných pripomienok, z toho zásadných 18 /3
Počet čiastočne akceptovaných pripomienok, z toho zásadných 7 /2
Počet neakceptovaných pripomienok, z toho zásadných 21 /3

Rozporové konanie (s kým, kedy, s akým výsledkom)
Počet odstránených pripomienok
Počet neodstránených pripomienok

Sumarizácia vznesených pripomienok podľa subjektov

Č.	Subjekt	Pripomienky do termínu	Pripomienky po termíne	Nemali pripomienky	Vôbec nezaslali
1.	Asociácia zamestnávatelských zväzov a združení Slovenskej republiky	1 (1o,0z)	0 (0o,0z)		
2.	Generálna prokuratúra Slovenskej republiky	1 (0o,1z)	0 (0o,0z)		
3.	Konferencia biskupov Slovenska	2 (2o,0z)	0 (0o,0z)		
4.	Ministerstvo financií Slovenskej republiky	4 (2o,2z)	0 (0o,0z)		
5.	Ministerstvo kultúry Slovenskej republiky	1 (1o,0z)	0 (0o,0z)		
6.	Ministerstvo obrany Slovenskej republiky	8 (7o,1z)	0 (0o,0z)		
7.	Ministerstvo práce, sociálnych vecí a rodiny Slovenskej republiky	1 (1o,0z)	0 (0o,0z)		

8.	Ministerstvo spravodlivosti Slovenskej republiky	1 (1o,0z)	0 (0o,0z)		
9.	Ministerstvo školstva, vedy, výskumu a športu Slovenskej republiky	1 (1o,0z)	0 (0o,0z)		
10.	Ministerstvo zdravotníctva Slovenskej republiky	3 (3o,0z)	0 (0o,0z)		
11.	Národná banka Slovenska	15 (15o,0z)	0 (0o,0z)		
12.	SK-NIC, a.s.	6 (3o,3z)	0 (0o,0z)		
13.	Úrad vlády Slovenskej republiky	2 (1o,1z)	0 (0o,0z)		
14.	Ministerstvo pôdohospodárstva a rozvoja vidieka Slovenskej republiky	0 (0o,0z)	0 (0o,0z)	x	
15.	Úrad pre verejné obstarávanie	0 (0o,0z)	0 (0o,0z)	x	
16.	Ministerstvo zahraničných vecí a európskych záležitostí Slovenskej republiky	0 (0o,0z)	0 (0o,0z)	x	
17.	Úrad pre normalizáciu, metrológiu a skúšobníctvo Slovenskej republiky	0 (0o,0z)	0 (0o,0z)	x	
18.	Úrad geodézie, kartografie a katastra Slovenskej republiky	0 (0o,0z)	0 (0o,0z)	x	
19.	Úrad jadrového dozoru Slovenskej republiky	0 (0o,0z)	0 (0o,0z)	x	
20.	Ministerstvo hospodárstva Slovenskej republiky	0 (0o,0z)	0 (0o,0z)	x	
21.	Protimonopolný úrad Slovenskej republiky	0 (0o,0z)	0 (0o,0z)	x	
22.	Ministerstvo vnútra Slovenskej republiky	0 (0o,0z)	0 (0o,0z)	x	
23.	Úrad priemyselného vlastníctva Slovenskej republiky	0 (0o,0z)	0 (0o,0z)	x	
24.	Ministerstvo životného prostredia Slovenskej republiky	0 (0o,0z)	0 (0o,0z)	x	
25.	Ministerstvo dopravy a výstavby Slovenskej republiky	0 (0o,0z)	0 (0o,0z)	x	
26.	Úrad podpredsedu vlády Slovenskej republiky pre investície a informatizáciu	0 (0o,0z)	0 (0o,0z)	x	

27.	Štatistický úrad Slovenskej republiky	0 (0o,0z)	0 (0o,0z)	x	
28.	Slovenská informačná služba	0 (0o,0z)	0 (0o,0z)		x
29.	Úrad na ochranu osobných údajov Slovenskej republiky	0 (0o,0z)	0 (0o,0z)		x
30.	Úrad pre reguláciu sieťových odvetví	0 (0o,0z)	0 (0o,0z)		x
31.	Správa štátnych hmotných rezerv Slovenskej republiky	0 (0o,0z)	0 (0o,0z)		x
32.	Národný bezpečnostný úrad	0 (0o,0z)	0 (0o,0z)		x
33.	Najvyšší kontrolný úrad Slovenskej republiky	0 (0o,0z)	0 (0o,0z)		x
34.	Najvyšší súd Slovenskej republiky	0 (0o,0z)	0 (0o,0z)		x
35.	Národná rada Slovenskej republiky	0 (0o,0z)	0 (0o,0z)		x
36.	Kancelária Ústavného súdu Slovenskej republiky	0 (0o,0z)	0 (0o,0z)		x
37.	Odbor aproximácie práva sekcie vládnej legislatívy Úradu vlády SR	0 (0o,0z)	0 (0o,0z)		x
38.	Slovenská poľnohospodárska a potravinárska komora	0 (0o,0z)	0 (0o,0z)		x
39.	Združenie miest a obcí Slovenska	0 (0o,0z)	0 (0o,0z)		x
40.	Splnomocnenec vlády Slovenskej republiky pre rómske komunity	0 (0o,0z)	0 (0o,0z)		x
41.	Konfederácia odborových zväzov Slovenskej republiky	0 (0o,0z)	0 (0o,0z)		x
42.	Republiková únia zamestnávateľov	0 (0o,0z)	0 (0o,0z)		x
43.	Úrad pre dohľad nad zdravotnou starostlivosťou	0 (0o,0z)	0 (0o,0z)		x
44.	Asociácia priemyselných zväzov	0 (0o,0z)	0 (0o,0z)		x
	Spolu	45 (37o,8z)	0 (0o,0z)		

Vyhodnotenie vecných pripomienok je uvedené v tabuľkovej časti.

Vysvetlivky k použitým skratkám v tabuľke:

O – obyčajná	A – akceptovaná
Z – zásadná	N – neakceptovaná
	ČA – čiastočne akceptovaná

Subjekt	Pripomienka	Typ	Vyh.	Spôsob vyhodnotenia
AZZZ SR	bez pripomienok	O	A	
GPSR	K časti 2, bod 2. 2 Navrhujeme v 3. fáze plánu aplikácie pravidiel blokovania presne konkretizovať profesné subjekty a subjekty, ktoré budú samostatné blokovanie aplikovať, s ktorými bude potrebné viesť odbornú diskusiu pre implementáciu pravidiel blokovania v národnom kybernetickom priestore. Všeobecné konštatovanie s presne nevymedzenými profesnými subjektmi a subjektmi, ktoré budú samotné blokovanie aplikovať, nedáva dostatočné informácie o ich postavení a dostatočné záruky o spôsobe ich výberu. Táto pripomienka je zásadná.	Z	A	
KBS	Na str. 29/31, podkapitola 2.4 Pravidlá blokovania IP adresných rozsahov publikovaním zoznamu, bez udania spôsobu blokovania, žiadame do podmienok zaradiť aj požiadavku v nasledovnom znení: „Prevádzkovatelia služby (základnej či digitálnej) pri blokovaní IP adresy primerane riešia zabezpečenie nekompromitovanej prevádzky z danej IP adresy.“ Odôvodnenie: Keďže v mnohých prípadoch na konkrétnych IP adresách je prevádzkovaných viacero služieb, či rôznorodého obsahu, bolo by vhodné do podmienok zaradiť aj požiadavku, aby prevádzkovatelia služby (základnej či digitálnej) pri blokovaní IP adresy primerane riešili zabezpečenie nekompromitovanej prevádzky z danej IP adresy. Napr. v prípade webových stránok vo väčšine prípadov ide len o kompromitáciu jedného, resp. malého počtu webov, pričom ostatné webové stránky z danej IP adresy sú z pohľadu kompromitácie nezávadné.	O	A	
KBS	Na strane 5/31, podkapitola 1.1 Potreba a dôvody blokovania, v predposlednom odseku, v súvislosti s textáciou: „Zamedzenie prístupu k škodlivému obsahu alebo na doménu, ktorá šíri škodlivý obsah, však nemožno považovať za zásah do práv a slobôd občanov, ale za nevyhnutné kroky, ktoré zamedzujú týmto používateľom	O	N	S duchom pripomienky súhlasíme. Na strane 5 v odseku 3 je však už škodlivý obsah definovaný ako "šírenie malvéru, existenciu riadiacich serverov pre botnety, phishingové stránky a podobne". Taktiež v kapitole 2.1 Pravidlá pre

	prístup k obsahu, ktorý by im mohol škodiť alebo priamo škodí.“ žiadame do textu explicitne uviesť definíciu/obsah pojmu „škodlivý obsah“. Odôvodnenie: aby sa zamedzilo riziku zneužitia blokovania pre cenzúru, žiadame v danom texte explicitne uviesť, čo je obsahom pojmu škodlivý obsah na účely predmetného materiálu.			blokovanie je jasne vymenované, aké typy obsahu alebo aktivít je možné blokovať ktoroukoľvek z navrhovaných techník.
MFSR	Ku kapitole 2.1.1 (Pravidlá pre blokovanie domén druhej úrovne na úrovni správcu národnej TLD): Chýbajú stanovené súvisiace pravidlá: - Z textu nie je zrejmé, čo podľa predkladateľa v praxi znamená „poskytnutie možnosti“ na odstránenie škodlivého obsahu z dotknutej domény. - Nie je stanovená lehota na odstránenie škodlivého obsahu. - Nie je stanovené, kto a na základe akého predpisu je zodpovedný za prípadné škody spôsobené blokovaným IP adresy, domény a subdomén, pripadne služieb. - Pri žiadosti majiteľa domény o odblokovanie domény nie je definované, aké dôkazy o odstránení škodlivého obsahu z domény sa požadujú a nie je stanovená lehota pre úrad na vybavenie žiadosti, ani lehota, do akej je správca domény povinný odblokovať doménu. - Textáciu vyššie uvedených pripomienok treba zohľadniť v kapitolách 2.1.2 a 2.1.3.	Z	ČA	- čiastočne akceptujeme: definovať poskytnutie možnosti. Poskytnutie možnosti je v súčasnosti riešené internými smernicami SK-CERT, ktoré upravujú komunikáciu so subjektami v procese riešenia incidentu. Tieto smernice sú natoľko komplikované a majúce len čiastočný presah s témou dokumentu, že ich nie je možné zapracovať. Doplnili sme však odkaz na to, že blokovaniu predchádza riadne riešenie incidentu. - neakceptujeme: lehoty. Jedná sa o dokument nelegislatívnej povahy, ktorý nemôže ukladať povinnosti. Lehoty vyplývajú z iných predpisov a líšia sa podľa závažnosti incidentu. - neakceptujeme: Zodpovednosť za škodu je riešená v zákone o KB, podľa ktorého nie je možné vylúčiť zodpovednosť štátu (zrejmé ustanovenie napríklad § 12 ods. 5, § 19 ods. 8) ani v kontexte reaktívnych opatrení vykonávaných v zmysle § 27 na základe rozhodnutia úradu, keďže v tomto prípade ide o situácie „eskalácie“ KBI, ergo aplikujeme ustanovenia zodpovednosti aj skôr citované. Úprava zodpovednosti v predmetnom návrhu materiálu nie je potrebná (a ani vhodná, keďže musí byť upravená na úrovni zákona, a teda tam aj upravená je) a vychádza priamo z právnej konštrukcie uvedenej v zákone o KB. Rovnako stále platí, že každý sa môže domáhať svojich práv v súdnom konaní. - akceptujeme: dôkazy o

				odstránení - bolo dopracovaných niekoľko ustanovení, ktoré adresujú tento problém.
MFSR	Ku kapitole 2.1.2 (Pravidlá pre blokovanie domén na úrovni ISP) všeobecne: Chýba úprava pravidiel tak, ako je stanovená v bode 2.1.1: - K odseku (Legislatívne podmienky): upozorňujeme, že nie všetci ISP (Internet service provider) spadajú pod zákon o kybernetickej bezpečnosti. - K § 19 ods. 6 3 (Prevádzkovateľ základnej služby): Uvedené platí iba pre : O2 Slovakia a.s., Orange Slovensko, a.s., Slovak Telekom, a.s., SWAN Mobile, a.s., SWAN, a.s., WebSupport, s.r.o. Ostatní ISP nie sú riešení. Nie je zrejmé, ako zabezpečí úrad ich spoluprácu. - K § 22 ods. 3 (Poskytovateľ digitálnej služby je povinný): - V zozname Poskytovateľov digitálnej služby nie je ani jeden ISP so službou výmenného uzlu na internete, službou systému doménových mien na internete. Nie je zrejmé, ako zabezpečí úrad ich spoluprácu.	O	N	NBÚ bude postupovať v zmysle platnej legislatívy. Pravidlá predpokladajú kooperáciu so subjektami, ktoré zapadajú do existujúceho rámca.
MFSR	Ku kapitole: 2.1.3 (Pravidlá pre blokovanie IP adresných rozsahov pomocou BGP): Táto kapitola hovorí iba o spôsobe implementácie v súčinnosti s ISP, ide o prekrývanie sa popisu úlohy s kapitolou 2.1.2. (Pravidlá pre blokovanie domén na úrovni ISP). Navrhujeme tieto textácie zosúladiť.	O	A	Textáciu 2.1.3 sme upravili v zmysle analýzy v bode 1.5.4, aby sa kapitoly neprekrývali.
MFSR	Všeobecne k materiálu: Obsah dokumentu v predloženom znení ide nad rámec splnomocnenia v zmysle úlohy Bezpečnostnej rady vlády SR, nakoľko upravuje aj jednotlivé oblasti škodlivého obsahu, ktoré nie sú v súčasnosti legislatívne zakázané. Z toho dôvodu ide tento materiál nad rámec úlohy stanovenej Bezpečnostnou radou vlády SR, nakoľko legislatívne sa opiera o zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o kybernetickej bezpečnosti“). Tento zákon však nerieši otázku posudzovania škodlivosti obsahu s výnimkou škodlivého kódu, ktorý vyvoláva kybernetický útok. Škodlivý kód je infiltrovaný do digitálneho obsahu (malware, phishing, atď.), nie je však sám o sebe digitálnym obsahom. Uvedená agenda boja proti škodlivému obsahu vychádza z úplne iných legislatívnych zdrojov (napr. návrh nariadenia Európskeho parlamentu a Rady o predchádzaní šíreniu teroristického obsahu online), než na ktorých je založený zákon o kybernetickej	Z	N	Zo zákona o kybernetickej bezpečnosti priamo vyplýva, že ústredný orgán plní úlohy jednotky CSIRT. Riešenie incidentov by nebolo možné bez technickej spôsobilosti rozhodnúť, či je obsah škodlivý, alebo nie. Nejedná sa v žiadnom prípade o posudzovanie ideologické či politické, ale o posudzovanie v zmysle taxonómie, uvedenej na strane 3 v kapitole Úvod a tiež na strane 21 v kapitole 2.1 pravidlá pre blokovanie.

	bezpečnosti (a to európska smernica o sieťovej a informačnej bezpečnosti NIS). Žiadame preto z celého materiálu vypustiť textáciu o škodlivom obsahu a upraviť ho v zmysle úlohy. Napr. celá kapitola 1.4 je venovaná digitálnemu obsahu a je preto bezpredmetná.			
MKSR	◦ Považujeme za nevyhnutné presne legislatívne vymedziť pojem „škodlivý obsah“. Vecnou podstatou predloženého materiálu (LP/2019/152) je totiž stanovenie pravidiel, ktorých vynucovanie má byť vyžadované formou rozhodnutia, ktoré uloží úrad (NBÚ) tomu, kto plní úlohy jednotky CSIRT, prevádzkovateľovi základnej služby a poskytovateľovi digitálnej služby (§ 27 ods. (3) zákona 69/2018 Z. z. o kybernetickej bezpečnosti). V materiáli popisované „blokovanie škodlivého obsahu“ vnímame ako nariadené „reaktívne opatrenie“ (§ 27 ods. (4) zákona 69/2018 Z. z. o kybernetickej bezpečnosti); ◦ Keďže zákon NR SR č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov termín „škodlivý obsah“ nedefinuje a nestanovuje ani postupy, ktorými sa z „nejakého obsahu“ stane „škodlivý obsah“, zastávame názor, že úradom (NBÚ) nariadené opatrenia (uložené formou rozhodnutia) musia rešpektovať existujúci právny rámec vymedzený Ústavou Slovenskej republiky. Z tohto pohľadu nevieme identifikovať existenciu zákonného mandátu pre NBÚ nariadeným reaktívnym opatrením obmedziť Ústavou Slovenskej republiky garantované základné ľudské práva a slobody (upravené najmä v čl. 19, čl. 22 a čl. 24 Ústavy SR) alebo politické práva (upravené najmä v čl. 26 a čl. 32 Ústavy SR); ◦ Praktické dôsledky prípadného nariadenia „blokovania škodlivého obsahu“ (najmä v situácii, keď je pojem „škodlivý obsah“ legislatívne nedefinovaný a prezentovaný len na základe „zvykového práva“ vychádzajúceho z „používanej taxonómie“) spĺňajú všetky pojmové znaky (minimálne) nariadenia cenzúry. Z prezentovanej definície „škodlivého obsahu“ totiž nie je možné zodpovedne posúdiť, či tento „škodlivý obsah“ je taký obsah, ktorý ohrozuje práva a slobody iných, bezpečnosť štátu, verejný poriadok, verejné zdravie a mravnosť. ◦ Vymedzenie pojmu „škodlivý obsah“ iba na základe „taxonómie, ktorú používa pri klasifikácii incidentov SK-CERT (Národná jednotka CSIRT)“ považujeme za nejednoznačné a nedostatočné z pohľadu oprávnenosti obmedzenia základných ľudských práv a slobôd, resp. politických práv upravených Ústavou SR.	O	N	O potrebe dodržať ústavné práva pojednáva veľká časť analýzy v úvode dokumentu. Navrhované opatrenia sa opierajú o ustanovenia platných zákonov.

MOSR	Ku kapitole 2.4 Materiál nepopisuje spôsob riešenia potreby blokovania elektronickej pošty. Problematika elektronickej pošty sa spomína v časti 1.3 Súčasný stav. Navrhujeme zapracovať do pravidiel aj možnosť ako vydať požiadavku na zablokovanie príjmu elektronickej pošty z určitých adries, alebo domén prípadne aj IP adries. Odôvodnenie: Prostredníctvom elektronickej pošty je vedené množstvo škodlivej aktivity, či už s charakterom zasiahnuť čo najviac obetí, ale aj pri cielených útokoch na konkrétne osoby.	O	A	
MOSR	Ku kapitole 2.4 Prípadné BLACKLISTY a iné dokumenty, ktoré vzniknú a budú obsahovať indikátory kompromitácie, ktoré sú prostredníctvom rôznych foriem blokované by mali byť aktívom, ktoré nie je verejne dostupné. Navrhujeme upraviť textáciu tak, aby bolo zrejmé, akým spôsobom budú BLACKLISTY distribuované. Odôvodnenie: Je nutné takéto aktívum chrániť, aby sa zamedzil prístup útočníkov k takýmto informáciám a teda možnosť realizovať opatrenia a zároveň aj útočníkom sledovať schopnosť kybernetickej obrany v rýchlosti prijatia reakcie na jeho aktivity.	O	A	
MOSR	Ku kapitole 2.4 Materiál sa nevenuje blokovaniu samotného DNS dotazu. Navrhujeme problematiku dopracovať. Odôvodnenie: Jedná sa o komunikácie smerujúce od infikovaného zariadenia vo forme DNS dotazov na server útočníka. Problémom je, že táto komunikácia nie je priama, ale je vybavovaná bežnými regulárnymi DNS servermi (Google, OpenDNS a mnohými inými), ktoré nemajú s útočníkom nič spoločné.	O	N	So znením pripomienky súhlasíme. Takúto komunikáciu je možné čiastočne blokovať aplikáciou inej uvedenej techniky "blokovanie konkrétnych doménových mien na úrovni ISP". Materiál predpokladá vykonateľnosť, teda nemôže očakávať súčinnosť DNS operátorov tretích strán mimo jurisdikcie SR. Zároveň nedefinuje viac granulárne techniky blokovania, ktoré by mohli mať dosah na CNC komunikáciu (napr. konkrétne DNS dopyty, blokovanie paketov podľa YARA pravidiel, blokovanie konkrétnych twitter účtov alebo Pastebin adries), z dôvodu príliš rozsiahleho, nedefinovateľného rozsahu možností a typov potrebného blokovania.

MOSR	Názov kapitoly 1. Analýza problematiky je mierne zavádzajúci a odporúčame ho premenovať napr. na Prehľad (alebo popis) problematiky z dôvodu, že uvedená kapitola nespĺňa atribúty riadnej analýzy, ale ide skôr o prehľad.	O	A	
MOSR	V kapitole 2. Návrh pravidiel pre blokovanie žiadame doplniť spoluprácu Národného bezpečnostného úradu s Vojenským spravodajstvom pri vydávaní rozhodnutí o blokovaní za účelom zabezpečenia kybernetickej obrany v prípadoch, ak bezpečnostné incidenty prekročia legislatívou stanovený stupeň závažnosti. Odôvodnenie: Centrum pre kybernetickú obranu SR musí prešetriť súvislosti, ktoré viedli k požiadavke na blokovanie IP adresy alebo domény a rovnako tak preveriť, či požadované IP adresy alebo domény nemajú súvislosť s inými kybernetickými incidentmi III. stupňa a to z dôvodu prevencie škodám, ktoré by mohli pre vyšetrovanie nastať samotným blokovaním alebo inými aktivitami popísanými v tomto dokumente. Žiadame preto zohľadniť platný legislatívny rámec pre kybernetickú obranu. Podľa § 27 ods. 10 zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti Národný bezpečnostný úrad informuje Vojenské spravodajstvo o bezpečnostných incidentoch, ktoré prekročia III. stupeň závažnosti. V zmysle § 2 ods. 2 zákona č. 319/2002 z. z. o obrane Slovenskej republiky sa obrana štátu zabezpečuje aj v kybernetickom priestore prostredníctvom opatrení zameraných na riešenie závažných kybernetických bezpečnostných incidentov, ktoré v tejto oblasti vykonáva Vojenské spravodajstvo. V § 18 ods. 2 toho istého zákona sa zároveň zavádza povinnosť osôb oprávnených na podnikanie poskytnúť Vojenskému spravodajstvu súčinnosť a informácie dôležité na zabezpečenie obrany štátu v kybernetickom priestore.	Z	A	
MOSR	V materiáli sa používa viacero cudzích výrazov, pričom pri niektorých existuje ich slovenský preklad. Odporúčame tieto cudzie, resp. aj odborné výrazy uvádzať v slovenskom jazyku alebo pri odborných výrazoch vytvoriť samostatnú prílohu k materiálu so zoznamom použitých odborných pojmov s ich vysvetlením.	O	ČA	Anglická terminológia je súčasťou odborného žargónu v tejto oblasti. Uznávame však, že niektoré pojmy je možné upraviť. Poslednou časťou dokumentu je zoznam použitých skratiek, ktorý sme doplnili.
MOSR	V úvode v štvrtom odseku uvedená taxonómia je všeobecne už zaužívaná aj inými subjektmi, a preto nie je dôvodné, prečo sa v tejto súvislosti uvádza len útvar SK-	O	N	Nakoľko Národná jednotka SK-CERT je útvarom Národného bezpečnostného úradu, ktorý plní úlohy Národnej jednotky CSIRT,

	CIRT.			odkazujeme na taxonómiu používanú na národnej úrovni, ktorú definuje práve SK-CERT. To, že ju požívajú aj iné jednotky CSIRT či iné bezpečnostné subjekty, textáciu nevylučuje, iba rozširuje.
MOSR	Vládna jednotka CSIRT.SK je v pôsobnosti Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu. Jednotka NACES (GOV CERT SK) uvádzaná v materiáli je taktiež v pôsobnosti Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu. Odporúčame uvádzať jednotný názov „jednotky CSIRT v pôsobnosti Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu“.	O	A	
MPSVRSR	• V časti 1.4 (Skúsenosti z iných krajín): navrhujeme doplniť, o akých respondentov v spomínanom prieskume išlo (boli to vládne organizácie, poskytovatelia pripojenia, používatelia internetových služieb?). • V častiach 2.1.1, 2.1.2 a 2.1.3: navrhujeme doplniť, do akého času od doručenia o blokovaní domény musí správca národnej TLD, resp. ISP začať blokovať doménu so škodlivým obsahom. • V častiach 2.1.1, 2.1.2 a 2.1.3: navrhujeme doplniť, do akého času po odstránení škodlivého obsahu musí úrad rozhodnúť o žiadosti o odblokovanie domény. • V podnadpise „2.4 Pravidlá blokovania IP adresných rozsahov...“ na str. 28: navrhujeme opraviť číslo kapitoly na „2.1.4 Pravidlá blokovania IP adresných rozsahov...“. • V časti 2.1.4: navrhujeme doplniť, že blacklist bude zverejňovaný v strojovo čitateľnom formáte kvôli možnosti jeho ďalšieho automatizovaného spracovania. • V časti 2.3, odsek 1. fáza – implementácia pravidiel na úrovni vládnej siete GOVNET: navrhujeme upresniť, kde budú popísané konkrétne pravidlá z tejto implementácie, nakoľko užívateľmi siete GOVNET sú ďalšie OVM. Tieto OVM by mali vedieť, akým spôsobom sa v GOVNETe bude aplikovať napr. blacklist popísaný v bode 2.1.4 (bude mať odporúčací charakter alebo IP rozsahy budú automaticky blokované na úrovni GOVNETu?). • Vzhľadom na fakt, že škodlivý obsah sa šíri aj prostredníctvom e-mailov, navrhujeme do materiálu doplniť aj pravidlá blokovania e-mailových služieb (e-mailových adries).	O	ČA	Ďakujeme za pripomienky. - neakceptujeme: autor a respondenti prieskumu. S textom pripomienky súhlasíme, autor štúdie je však v texte uvedený a ďalšie informácie je možné dohľadať z pôvodnej štúdie - neakceptujeme: rýchlosť blokovania. Keďže sa jedná o materiál nelegislatívnej povahy, nemôže ukladať povinnosti iným subjektom - akceptujeme: oprava čísla kapitoly - akceptujeme: strojovo čitateľný formát blokovacích pravidiel (zapracované na viacerých miestach dokumentu) - neakceptujeme: upresnenie blokovania Govnet. V prípade blokovania na úrovni siete Govnet sa jedná o blokovanie v core sieti, ktoré už reálne prebieha na základe operatívnej činnosti prevádzkovateľa siete Govnet. Súčinnosť uzlov nie je v súčasnosti vyžadovaná a neevidujeme sťažnosti používateľov siete Govnet na tento stav. - akceptujeme: e-mail doplnený.

MSSR	K doložke vybraných vplyvov, bodu 9: I) Upozorňujeme, že s účinnosťou od 1. marca 2019 má doložka vybraných vplyvov v zmysle § 7 ods. 3 písm. b) zákona č. 400/2015 Z. z. o tvorbe právnych predpisov a o Zbierke zákonov Slovenskej republiky a o zmene a doplnení niektorých zákonov obsahovať aj informáciu o predpokladaných vplyvoch na manželstvo, rodičovstvo a rodinu. V tejto súvislosti odporúčame túto časť doplniť do doložky vybraných vplyvov. II) Pokiaľ je v časti 9 uvedené, že materiál nemá žiadne vplyvy na rozpočet verejnej správy, neuvádza sa odpoveď na podotázku, či má materiál pozitívne/žiadne/negatívne rozpočtovo zabezpečené vplyvy. V tejto súvislosti odporúčame odstrániť v podotázke označenie pri možnosti „žiadne". III)Pokiaľ je v časti 9 uvedené, že materiál nemá žiadne vplyvy na podnikateľské prostredie, neuvádza sa odpoveď na podotázku, či má materiál pozitívne/žiadne/negatívne na MPS. V tejto súvislosti odporúčame odstrániť v podotázke označenie pri možnosti „žiadne".	O	A	
MŠVVaŠSR	K vlastnému materiálu: Navrhujeme upraviť bod 2.1.1. - Pravidlá pre blokovanie domén druhej úrovne na úrovni správcu národnej TLD. Nesúhlasíme s daným bodom, nakoľko blokovanie domény na druhej úrovni sa môže realizovať až na základe rozhodnutia súdu a až následne predmetnú doménu Národný bezpečnostný úrad zablokuje. Nerešpektovanie tejto požiadavky môže spôsobiť škody na strane prevádzkovateľa domény ako aj ďalších zainteresovaných osôb.	O	N	- Tento dokument nepojednáva o blokovaní nelegálnych webov na základe rozhodnutia súdu, iniciované MF SR, ale o reakcii na prebiehajúci kybernetický bezpečnostný incident (KBI). Pri prebiehajúcich útokoch (napríklad aktívna phishingová kampaň) je najrýchlejšia možná technická reakcia nevyhnutná na zabezpečenie kybernetickej bezpečnosti. Nejedná sa tiež o permanentné blokovanie, ale o zamedzenie útoku. Zároveň blokovaniu predchádza v zmysle predkladaného materiálu niekoľko ďalších krokov a dokument navrhuje viacero rôznych techník a poukazuje na možné riziká práve preto, aby bolo možné vybrať najmenej invazívny spôsob. - Zodpovednosť za škodu je riešená v zákone o KB, podľa ktorého nie je možné vylúčiť zodpovednosť štátu (zrejmé ustanovenie napríklad § 12 ods. 5, § 19 ods. 8) ani v kontexte reaktívnych opatrení vykonávaných v zmysle § 27 na základe rozhodnutia úradu, keďže v tomto

				prípade ide o situácie „eskalácie“ KBI, ergo aplikujeme ustanovenia zodpovednosti aj skôr citované. Úprava zodpovednosti v predmetnom návrhu materiálu nie je potrebná (a ani vhodná, keďže musí byť upravená na úrovni zákona, a teda tam aj upravená je) a vychádza priamo z právnej konštrukcie uvedenej v zákone o KB. Rovnako stále platí, že každý sa môže domáhať svojich práv v súdnom konaní.
MZSR	Ministerstvo zdravotníctva Slovenskej republiky k Pravidlám pre blokovanie útokov uplatňuje túto pripomienku: - v bode 1.2 "Riziká blokovania" žiadame špecifikovať, kto bude znášať zodpovednosť za škodu z hľadiska trestného konania – či Národný bezpečnostný úrad alebo súčinný orgán verejnej správy - pripomienka je obyčajná.	O	N	Zodpovednosť za škodu je riešená v zákone o KB, podľa ktorého nie je možné vylúčiť zodpovednosť štátu (zrejmé ustanovenie napríklad § 12 ods. 5, § 19 ods. 8) ani v kontexte reaktívnych opatrení vykonávaných v zmysle § 27 na základe rozhodnutia úradu, keďže v tomto prípade ide o situácie „eskalácie“ KBI, ergo aplikujeme ustanovenia zodpovednosti aj skôr citované. Úprava zodpovednosti v predmetnom návrhu materiálu nie je potrebná (a ani vhodná, keďže musí byť upravená na úrovni zákona, a teda tam aj upravená je) a vychádza priamo z právnej konštrukcie uvedenej v zákone o KB. Rovnako stále platí, že každý sa môže domáhať svojich práv v súdnom konaní.
MZSR	Materiál by mal obsahovať aj tému blokovania škodlivých mailov.	O	A	
MZSR	Pripomienka zaslaná mimo portálu Slov-Lex: V bode 1.2 Riziká blokovania žiadame špecifikovať, kto bude znášať zodpovednosť za škodu z hľadiska trestného konania - či Národný bezpečnostný úrad alebo súčinný orgán verejnej správy.	O	N	- Zodpovednosť za škodu je riešená v zákone o KB, podľa ktorého nie je možné vylúčiť zodpovednosť štátu (zrejmé ustanovenie napríklad § 12 ods. 5, § 19 ods. 8) ani v kontexte reaktívnych opatrení vykonávaných v zmysle § 27 na základe rozhodnutia úradu, keďže v tomto prípade ide o situácie „eskalácie“ KBI, ergo

				aplikujeme ustanovenia zodpovednosti aj skôr citované. Úprava zodpovednosti v predmetnom návrhu materiálu nie je potrebná (a ani vhodná, keďže musí byť upravená na úrovni zákona, a teda tam aj upravená je) a vychádza priamo z právnej konštrukcie uvedenej v zákone o KB. Rovnako stále platí, že každý sa môže domáhať svojich práv v súdnom konaní.
NBS	V Predkladacej správe a Doložke vybraných vplyvov sa uvádza že „Materiál nemá žiadne vplyvy na rozpočet verejnej správy, na podnikateľské prostredie, žiadne sociálne vplyvy, žiadne vplyvy na životné prostredie, žiadne vplyvy na informatizáciu spoločnosti a na služby verejnej správy pre občana.“ Navrhujeme tieto vplyvy prehodnotiť z dôvodu, že minimálne na služby verejnej správy pre občana dokument vplyv má, keďže dokument popisuje možnosť znemožnenia prístupu občanov k službám verejnej správy (napr. k ústrednému portálu verejnej správy slovensko.sk) v prípade, že je občan zasiahnutý blokovaním. Napríklad aj vo vlastnom materiáli v kategórii „granularita blokovania (nezablokujem, čo nechcem)“ v popise techník a v časti 1.2 Riziká blokovania je pod bodom „škody môžu byť spôsobené aj subjektu, ktorý nie je priamo zodpovedný za infraštruktúru šíriacu škodlivý obsah“ uvedený príklad blokovania IP adresy, zdieľanej viacerými používateľmi internetu, čo zapríčiní okrem zablokovania škodlivej IP adresy aj zablokovanie prístupu na internet užívateľom alebo zariadeniam, ktoré nie sú infikované a nevykonávajú škodlivú činnosť.“.	O	N	Účelom blokovania nie je brániť občanom v legitímnom prístupe na služby vrátane portálu slovensko.sk. Dokument poskytuje viacero nástrojov na blokovanie práve z dôvodu, aby bolo možné vybrať ten spôsob, ktorý je pre danú kybernetickú hrozbu najefektívnejší. Účelom časti dokumentu, ktorá zmieňuje riziká blokovania je práve to, aby si ich blokujúci subjekt pri výbere techniky blokovania uvedomoval a zahrnul ich do rozhodovacieho procesu. Záverom, dokument tiež definuje, že pri blokovaní ide o krajnú možnosť po vyčerpaní všetkých ostatných alternatív.
NBS	Vlastný materiál: Doporučujeme upresniť, čo sa bude diať v prípade, že ISP neimplementuje blokovanie v súlade s rozhodnutím národnej autority pre kybernetickú bezpečnosť.	O	N	Ide o materiál nelegislatívnej povahy, bez možnosti ukladať povinnosti subjektom.
NBS	Vlastný materiál: Navrhujeme pri technikách, ktoré používajú blokovanie pomocou IP adries upresniť, či budú používané IPv4 adresy alebo aj IPv6 adresy.	O	A	V slovníku použitých skratiek v závere dokumentu bola doplnená jednoznačná definícia IP adresy.

NBS	Vlastný materiál: Navrhujeme uviesť, akým spôsobom môže subjekt, ktorý vlastní doménu blokovanú technikou „2.4 Pravidlá blokovania IP adresných rozsahov publikovaním zoznamu, bez udania spôsobu blokovania“ rozporovať tento fakt a dozvedieť sa dôvody, prečo bola ním vlastnená doména zaradená na zoznam blokovaných domén.	O	A	Ako je uvedené v samotnom materiáli, "Úrad neposkytuje informácie o IP adresách, doménach a URL v blacklistoch nad rámec informácie, že sa jedná o indikátory, ktoré sú spojené so šírením škodlivého obsahu alebo sa na týchto indikátoroch nachádza škodlivý obsah". Toto ustanovenie je zavedené z dôvodu, že niektoré zdroje indikátorov sú neverejné. Napriek tomu je možné konktatovať SK-CERT a takéto prípady budú riešené na individuálnej báze. Toto bolo zapracované.
NBS	Vlastný materiál: Upozorňujeme, že vysvetlenie skratky „DDoS (Distributed Denial of Service) alebo tiež tzv. reflektívne útoky nie je správne. Reflektívne útoky sú len podskupina DDoS útokov (https://en.wikipedia.org/wiki/Denial-of-service_attack#Attack_techniques). Na DDoS útoku sa môžu podieľať aj legitímne súčasti infraštruktúry, napr. DNS servery (https://en.wikipedia.org/wiki/Denial-of-service_attack#Amplification), nemusí ísť o botnet.	O	A	
NBS	Vlastný materiál: Časť 2.1.2: Explicitne uviesť, že ide len o blokovanie domén v TLD .sk. Odôvodnenie: Aktuálne znenie zvádza k domnienke, že Národná jednotka CSIRT bude komunikovať s majiteľmi ľubovoľných domén a vynucovať blokovanie aj u zahraničných ISP, prípadne pri tom aplikovať legislatívne podmienky SR.	O	N	Textáciu sme zmenili na TLD, ale keďže nie je vylúčená budúca existencia iných TLD v pôsobnosti SK legislatívy, nechceme zúžiť definíciu na doménu .sk. Vzhľadom k tomu, že SK-CERT koná výlučne v rámci platnej legislatívy, blokovanie zahraničných TLD vylučujeme, čo je aj uvedené v poznámke v tabuľke v kapitole 1.5.1.
NBS	Vlastný materiál: Doplniť do dokumentu kvantifikáciu očakávaného počtu domén, IP adries, IP adresných rozsahov a pod., ktoré budú ISP musieť blokovať resp. následne opätovne odblokovať. Odôvodnenie: Pri veľkom počte záznamov môže ísť o nezanedbateľnú agendu na strane ISP. Predpokladáme, že Národná jednotka	O	N	Nakoľko štatistika nutnosti/možností blokovania sa mení v reálnom čase a nie je dostatočne predikovateľná, nie je možné zapracovať takú verziu kvantifikovaného prehľadu, aby bez dohadov prezentoval súčasný alebo budúci stav.

	CSIRT disponuje dostatkom údajov, aby dokázala vyhodnotiť očakávaný počet.			
NBS	Vlastný materiál: Navrhujeme doplniť metodiku, ako sa po úspešnom odstránení škodlivého obsahu z domén/IP adries, resp. úspešnej aplikácii nápravných opatrení odstráni blokovanie. Minimálne pravidelné prehodnotenie rozsahu blokovania.	O	A	
NBS	Vlastný materiál: Navrhujeme doplniť povinnosť informovať verejnosť o blokovaných doménach a IP adresách, vrátane dôvodov blokovania (centrálne miesto, nie web stránky jednotlivých subjektov). Odôvodnenie: Informácia o nedostupnosti domén, IP adries a adresných rozsahov z dôvodu blokovania by mala byť verejne dostupná. Najmä ak niektoré metódy blokovania môžu mať nežiadúci vedľajší efekt, ako konštatuje aj samotný materiál.	O	N	Princíp materiálu túto možnosť nepredpokladal a pripomienka je v rozpore s inými prijatými pripomienkami.
NBS	Vlastný materiál: Navrhujeme upresniť v bode 1.5.2 Blokovanie domén druhej úrovne na úrovni správcu národnej TLD“, aký je predpokladaný čas aplikovania blokovania pri technike použitím metódy „Blokovanie by vykonával správca top level domény .sk vyradením domény druhej úrovne z DNS.“ Odôvodnenie: DNS záznamy sa v DNS serveroch ukladajú (cachujú) s dobou platnosti (time-to-live) najčastejšie 86400 sekúnd=1 deň, teda aj pri vyradení predmetného DNS záznamu druhej úrovne zo záznamov DNS servera správcu top level domény .sk by vyradená doména bola stále po nejakú dobu prekladaná na svoju IP adresu z pamäti (cache) DNS serverov nižšej úrovne a teda prístupná.	O	ČA	Uvedomujeme si technické obmedzenia tejto metódy blokovania. Keďže je však na individuálnom rozhodnutí každého prevádzkovateľa DNS, aké dlhé doby TTL uvedie vo svojej zóne, nie je možné z našej strany ovplyvniť čas aktivácie blokovania. Problematiku sme do dokumentu zahrnuli.
NBS	Vlastný materiál: Navrhujeme upresniť, kde bude pri technike „1.5.7 Blokovanie IP adresných rozsahov publikovaním zoznamu, bez udania spôsobu blokovania“ publikovaný uvedený zoznam, či bude tento zoznam v digitálnej alebo tlačenej podobe, či bude tento zoznam strojovo čitateľný a v akej lehote bude mať ISP povinnosť implementovať blokovanie podľa tohto zoznamu od okamihu jeho publikácie alebo aktualizácie.	O	ČA	Strojovo čitateľný formát bol zapracovaný. Ostatné body nie sú predmetom tejto analýzy.

NBS	Vlastný materiál: Navrhujeme uviesť pri technike „1.5.11 Blokovanie prostriedkami endpoint security (firewall, antivírus, antimalware a podobne)“ či sa predpokladá, že každý koncový uzol (napr. router, počítač alebo iné zariadenie) bude mať nainštalovaný a aktívny antivírusový program, isté (nešpecifikované) anti-malware riešenie, firewall a podobne.	O	N	Dokument nepredpisuje použitie konkrétneho hardvéru alebo softvéru, ale len analyzuje jednotlivé techniky. V pláne implementácie sa výslovne uvádza potreba ďalšej odbornej diskusie.
NBS	Vlastný materiál: Navrhujeme v bodoch „1.5.5 Blokovanie IP adresných rozsahov pomocou firewallových pravidiel“ a „1.5.6 Blokovanie IP, protokolu a portu pomocou firewallových pravidiel“ upresniť, kto bude znášať náklady, keďže je potrebné mať a spravovať takéto zariadenie na strane ISP. Robustné riešenie môže vyžadovať investície na nákup a prevádzku takéhoto zariadenia na strane ISP.	O	N	Nakoľko ide o materiál nelegislatívnej povahy bez zaviazania konkrétnych subjektov k určitému konaniu (napr. investícii), predpokladá sa využitie už existujúcich infraštruktúrnych prvkov ISP.
NBS	Vlastný materiál: Upozorňujeme, že pri technike „1.5.4 Blokovanie IP adresných rozsahov pomocou BGP“ je implementácia alternatívy 1 aj alternatívy 2 pomerne zložitá, hodnotenie pre kritérium „jednoduchosť implementácie“ by malo mať menej hviezdičiek.	O	N	Zložitosť implementácie neposudzujeme len z pohľadu technickej náročnosti, ale zo širšieho pohľadu na odhadovaný počet potrebných spolupracujúcich subjektov a náročnosť komunikácie a koordinácie. V tomto prípade predpokladáme jednorazovú inštaláciu a konfiguráciu, na základe ktorej bude môcť blokovanie prebiehať strojovo. Do dokumentu sme doplnili podrobnejší popis jednotlivých atribútov analýzy.
NBS	Vlastný materiál: V časti „2.1.1 Pravidlá pre blokovanie domén druhej úrovne na úrovni správcu národnej TLD“ sa na viacerých miestach uvádza „ak škodlivý obsah nebol odstránený do určenej lehoty, úrad vydá rozhodnutie o blokovaní domény“. Navrhujeme upresniť, aká je predpokladaná dĺžka tejto lehoty (hodiny, dni, …).	O	N	Lehoty vyplývajú z iných predpisov a líšia sa podľa závažnosti incidentu.
SK-NIC	K 1.5.1, blokovanie domén druhej úrovne: Absentuje blokovanie na úrovni registrátora a blokovanie na inej ako na priamej druhej úrovni domén, či už tretej a ďalšej alebo ktoré sú napr. v tvare /subdomena za hlavnou doménou. Názov tejto	O	A	

	činnosti je všeobecný, ale popis v časti „Poznámky“ je zúžený, správne by malo byť „blokuje len domény danej TLD“, čo úzko súvisí aj s tým, že ak má ísť o flexibilný materiál, je nutné uvažovať aj o budúcich možných gTLD variantách ako napr. .bratislava obdobne ako existuje napr. .brussels alebo slovenských registrátorov pre iné TLD.			
SK-NIC	K 1.5.1: Úplne absentuje najštandardnejší postup, tzv. "notice and take-down", t.j. stiahnutie obsahu na úrovni poskytovateľa obsahu alebo poskytovateľa platformy na jeho poskytovanie, čo je de facto takisto zablokovanie, ktoré je principiálne najefektívnejšie.	O	N	S textom súhlasíme. Rieši ho ustanovenia 2.1.1, "blokovaniu musí predchádzať...".
SK-NIC	K 2.1.1, časť legislatívne podmienky Popísané je relevantné iba čiastočne, nakoľko sa jedná o opatrenia a kybernetické bezp. incidenty, ktoré vyplývajú z činnosti prevádzkovateľa základnej služby a v rámci jeho činnosti, t.j. v zmysle pôvodného zámeru daných ustanovení, nie ktoré spôsobuje niekto iný niekomu inému, využívajúc k tomu verejný nástroj tretieho subjektu, navyše uvedené ustanovenia v súčasnej podobe nespĺňajú ani žiadnym spôsobom negarantujú podmienky uvedené v 2.1 – uvedené je nutné v zákone rovnako ako v inej legislatíve upravujúcej túto problematiku riešiť explicitným spôsobom so všetkými aspektmi. Táto pripomienka je zásadná.	Z	N	Interpretácia SK-NIC vychádza z predpokladu, že tretí subjekt nie je účastníkom incidentu. Ako prevádzkovateľ infraštruktúry, ktorá sa používa na útok, je však účastníkom incidentu aj táto tretia strana. To umožňuje využiť ustanovenia zákona na vyžiadanie súčinnosti a vykonanie potrebných opatrení.
SK-NIC	K 2.1.1, časť podmienky, posledná odrážka: Uvedené nie je dostatočné – držiteľ sa môže vzdať práva k doméne, kto potom požiada resp. preukáže odstránenie obsahu? Aktuálny návrh je v takomto prípade nevykonateľný. Je nutné doplniť aj samostatnú zaniknuteľnosť blokovania z dôvodu prejdenia primeraného časového úseku. Táto pripomenka je zásadná. Ako poznámka - z praktického pohľadu nie je zrejmé, ako sa preukáže napr. odstránenie konkrétnej stránky webového sídla, keď webové sídlo nie je kvôli zablokovaniu zobraziteľné + ak držiteľ domény napr. iba spravuje nejakú platformu, ale nevytvára obsah, nemusí byť schopný čokoľvek v súvislosti s obsahom preukázať, je preto vhodné doplniť príklady tohto úkonu.	Z	ČA	K jednotlivým častiam: - neakceptujeme: Ak sa držiteľ formálne vzdá práva k doméne, ale táto je naďalej technicky prevádzkovaná, pravdepodobne nemá záujem na odstránení obsahu, teda dôvody blokovania pretrvávajú. - akceptujeme: Požadovaný dôkaz môže v tomto prípade byť aj prehlásenie o odstránení škodlivého obsahu, tak ako je zvykom pri blacklistoch na nevyžiadanú poštu alebo v reakciách na oznámenie o prítomnosti phishingovej stránky. Odstránenie obsahu vie SK-CERT technicky otestovať nastavením IP adresy servera do súboru hosts. - neakceptujeme:

				či držiteľ domény prevádzkuje alebo neprevádzkuje samotnú platformu je z hľadiska blokovania útoku irelevantné. V mantineloch technickej reakcie na incident, čo je zameranie celého predkladaného dokumentu, je potrebné predovšetkým zamedziť napr. prístupu na phishingovú stránku, nie venovať sa atribúcii alebo identifikácii príslušného subjektu. Predpokladáme, že ako subjekt, ktorý si objednal a platí za doménu, bude mať tento subjekt kontakt s technickým prevádzkovateľom a potrebné informácie bude schopný získať.
SK-NIC	K 2.1: K pravidlám pre blokovanie je nutné doplniť, že „nesmú vzniknúť neprimerané náklady v dôsledku možného vyžadovania expresného vykonania zablokovania“. Okrem toho je nutné doplniť dve nové odrážky: - „Jednoznačné časové ohraničenie (!) – blokovanie nemôže byť naveky, t.j. bezdôvodne – blokujú sa principiálne adresy, t.j. ako keby ste mali naveky zablokovanú ulicu, aj keď chránený konvoj už tade prešiel pred rokmi, pričom každá adresa je unikátna a jej použitie je iba temporálne. - “Jednoznačná zodpovednosť za škodu, ktorú nesmie niesť subjekt, ktorý vykonáva blokovanie na príkaz tretej strany.“ Táto pripomienka je zásadná	Z	N	- neakceptujeme: pri blokovaní neočakávame neprimerané náklady, úprava zoznamu generovaných domén je činnosť, ktorú tieto subjekty vykonávajú na dennej báze a s veľmi rýchlou reakčnou dobou už teraz - neakceptujeme: ak hrozba pretrváva, časové ohraničenie nemá zmysel; - zodpovednosť za škodu: rozumieme textu pripomienky. Pripomienku nie je možné akceptovať z dôvodu - Zodpovednosť za škodu je riešená v zákone o KB, podľa ktorého nie je možné vylúčiť zodpovednosť štátu (zrejmé ustanovenie napríklad § 12 ods. 5, § 19 ods. 8) ani v kontexte reaktívnych opatrení vykonávaných v zmysle § 27 na základe rozhodnutia úradu, keďže v tomto prípade ide o situácie „eskalácie“ KBI, ergo aplikujeme ustanovenia zodpovednosti aj skôr citované. Úprava zodpovednosti v predmetnom návrhu materiálu nie je potrebná (a ani vhodná, keďže musí byť upravená na úrovni zákona, a teda tam aj upravená je) a vychádza priamo z právnej konštrukcie uvedenej v zákone o KB.

				Rovnako stále platí, že každý sa môže domáhať svojich práv v súdnom konaní.
SK-NIC	Všeobecne: Materiál obsahuje rôzne nejasnosti a nepresnosti, ktoré rozhodne odporúčame upraviť: K úvodu: Nie je zrejmé, čoho taxonómia to vlastne je? Heslá nie sú škodlivý kód ani incident (iba jeho únik či zmena), infraštruktúra je nástroj alebo napadnuté aktívum, škodlivý kód je len nástroj, nie však incident atď. Odporúčame preformulovať. V celom texte materiálu takisto odporúčame vzhľadom na ďalšie právne implikácie opraviť nesprávny pojem "majiteľ domény" správnym pojmom "držiteľ domény". K 1.2, príliš široké blokovanie: Odporúčame doplniť prax, že z pohľadu toho, že v reťazci služieb napr. na internete je vždy nutné začínať čo najbližšie k obsahu a blokovanie domény či IP je až posledný rezort, keďže je tam veľká šanca na významné až kritické kolaterálne dopady. Pre lepšie uvedomenie si dopadov odporúčame doplniť aj „napr. e-mailová komunikácia, vrátane všetkých klientov a používateľov danej domény, kde môže pri veľkých portáloch či napr. cloud službách ísť rádovo o stovky, tisíce či ešte viac klientov". K 1.3, 2. odsek: Odporúčame upraviť chybné vyjadrenie v súvislosti so zákonom č. 171/2005 Z. z. - neblokujú domény, ale webové sídla, čo je zásadný rozdiel od domény a takisto je veľký rozdiel či je blokovanie uskutočnené na úrovni webhostingu, poskytovateľa internetu alebo napr. registrátora či registra domény, , čo tu nie je žiadnym spôsobom rozobraté. K 1.5.2: Tabuľka: Nie je zrejmé, čo sa v tomto prípade rozumie jednoduchosťou implementácie – implementácie kým? Nevýhody: Na konci prvej odrážky odporúčame doplniť „čím môže prísť k značným škodám". Odporúčame aj doplniť novú odrážku: „Blokovanie má časovú retenciu v závislosti od lokálnych nastavení aktualizácie DNS u poskytovateľov lokálnych DNS serverov, rádovo môže ísť aj o dni". K 1.5.3: Text „na ktoré smeruje záznam z SK-NIC" navrhujeme zmeniť na „na ktoré smeruje záznam daného správcu TLD" – jednak sa v ďalšom texte nerozprávame iba o .sk a zároveň slovenskí ISP resolvujú aj iné TLD ako .sk". K 2.2 Nie je zrejmé, ako do tohto dokumentu spadajú služby ako voda či zdravotná starostlivosť, keďže nie sú žiadnym zo subjektov konajúcim podľa predchádzajúcich kapitol. Odporúčame zvážiť vypustenie fázy 2, resp. jej zlúčenie s fázou 3.	O	ČA	- neakceptujeme: taxonómia nepojednáva o škodlivom kóde, ale o škodlivom obsahu. V tomto duchu je treba chápať aj zverejnené uniknuté heslá, ktorých včasným zneprístupnením možno minimalizovať počet a dopady incidentov s únikom spojených. - akceptujeme: držiteľ domény - čiastočne akceptujeme: o negatívnych dopadoch pojednáva dokument dostatočne. Príklad sme doplnili. - akceptujeme: webové sídla - akceptujeme: dovysvetlenie pojmov v analýze blokovacích techník - neakceptujeme: doplniť ""čím môže dôjsť k značným škodám"" - riziko škôd je podrobne opísané v kapitole 1.2 riziká blokovania a do technickej analýzy techník nepatrí. - akceptujeme: retencia DNS (rozšírená navyše o odkaz na DNS cache) - akceptujeme: zmena SK-NIC na správcu TLD - neakceptujeme: vypustenie fázy 2. Táto fáza je pre dokument zásadná.

ÚVSR	K uzneseniu BR SR: Zo znenia bodu II. uznesenia Bezpečnostnej rady SR navrhujeme vypustiť slová „riaditeľovi Národného bezpečnostného úradu“ a „riaditeľovi Slovenskej informačnej služby“ a uvedené slová odporúčame presunúť do bodu III. uznesenia Bezpečnostnej rady SR. Odôvodnenie: Bezpečnostná rada SR môže v zmysle Čl. 6 ods. 3 písm. a) Smernice na prípravu a predkladanie materiálov na rokovanie Bezpečnostnej rady SR ukladať úlohy iba svojim členom a riaditeľ Národného bezpečnostného úradu ani riaditeľ Slovenskej informačnej služby nie sú členmi Bezpečnostnej rady SR.	Z	A	Uznesenie Bezpečnostnej rady SR upravené.
ÚVSR	Všeobecne: Chýba možnosť blokovať jednotlivú email adresu. Žiadame doplniť. Odôvodnenie: V materiáli navrhované možnosti by blokovali všetku email komunikáciu z daného serveru, čo môže byť v jednotlivých prípadoch neprimerané.	O	A	