NÁRODNÝ
BEZPEČNOSTNÝ
ÚRAD

Pravidlá pre blokovanie útokov

Obsah

Úvod

Škodlivej aktivity na Internete z roka na rok pribúda. Zároveň rastie sofistikovanosť útokov a s neustále prebiehajúcou informatizáciou spoločnosti aj riziká, spojené s úspešne vykonanými útokmi. Reakcia na rôzne typy škodlivej aktivity spadá do kompetencie rôznych štátnych orgánov.

Množstvo útokov je vykonávaných buď plošne (napríklad phishingové kampane, lákajúce veľké množstvo používateľov kliknúť na rozoslanú linku), alebo na svoju činnosť využíva identifikovateľný škodlivý obsah alebo sieťovú infraštruktúru (napríklad riadiace servery botnet sietí, DNS servery k nim smerujúce, zariadenia vykonávajúce DDOS útoky a podobne).

Z tohto dôvodu mnohé krajiny zavádzajú legislatívne podmienky a technické prostriedky na blokovanie nežiadúceho obsahu, IP adries, domén, URL, súborov a podobne.

Podľa taxonómie, ktorú používa pri klasifikácii incidentov SK-CERT (Národná jednotka CSIRT), je možné škodlivý obsah a s ním spojenú infraštruktúru rozdeliť do týchto kategórií:

- Škodlivý kód (vírus, malvér, ransomvér)
- Infraštruktúra, umožňujúca
    - rozosielanie nevyžiadanej pošty
    - neoprávnené získavanie informácií: skenovanie sietí, odpočúvanie, sociálne inžinierstvo, phishing
- Podporný software, údaje a infraštruktúra umožňujúca pokusy o prienik, DoS, DDoS útoky alebo iné aktívne útoky, vrátane
    - riadiacich serverov (command and control servery)
    - uzlov siete botnet
    - obsahu, zneužívajúceho prostriedky používateľov bez ich vedomia (crypto minery)
- Verejne prístupné citlivé údaje ako sú heslá, šifrovacie kľúče, čísla kreditných kariet, osobné údaje

Národný bezpečnostný úrad (ďalej len „úrad“) v súlade s *Akčným plánom realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020 a* s *Plánom práce Bezpečnostnej rady Slovenskej republiky na rok 2017* vypracoval materiál *Pravidlá pre blokovanie útokov.*

Vypracovanie materiálu úradu vyplynulo z:

1. úlohy č. 3.5. Tabuľky úloh Akčného plánu realizácie Koncepcie kybernetickej bezpečnosti Slovenskej republiky na roky 2015-2020, ktorý bol schválený uznesením vlády Slovenskej republiky č. 93/2016 v znení uznesenia vlády Slovenskej republiky č. 62/2018 a

2. Plánu práce Bezpečnostnej rady Slovenskej republiky na rok 2017, schváleného uznesením vlády Slovenskej republiky č. 51 z 25. januára 2017, z ktorého vyplynula pre ministra financií úloha č. 8 - predložiť v mesiaci december 2017 na rokovanie Bezpečnostnej rady Slovenskej republiky materiál *Pravidlá pre blokovanie útokov*. Uznesením vlády Slovenskej republiky č. 62 z 31. januára 2018 k návrhu na zrušenie a zmenu niektorých úloh z uznesení vlády Slovenskej republiky bolo bodom B.14. zmenené gestorstvo predmetnej úlohy z ministra financií na riaditeľa úradu a bodom B.15. bol zmenený termín predloženia materiálu z mesiaca december 2017 na mesiac december 2018.

Cieľom materiálu je zaviesť pravidlá pre blokovanie útokov za účelom zvýšenia obranyschopnosti Slovenskej republiky (ďalej len „SR“) voči kybernetickým útokom na významné informačné systémy z externého prostredia (internetu), najmä voči šíreniu škodlivého kódu zo sietí infikovaných počítačov a šíreniu škodlivej aktivity z IP adresného rozsahu SR. Materiál je rozdelený do dvoch častí. Prvá časť obsahuje analýzu súčasného stavu, porovnanie skúseností z iných krajín a analýzu dostupných blokovacích techník. Druhá časť obsahuje návrh pravidiel pre blokovanie škodlivého obsahu vrátane plánu ich aplikácie.

1. Popis problematiky

1.1 Potreba a dôvody blokovania

Ako vzrastá dôležitosť internetu a zariadení pripojených na internet, vzrastá aj miera počítačovej kriminality a objem škodlivého obsahu. Pre útočníkov sú zaujímavé citlivé či osobné údaje, ale aj výpočtová sila napadnutej techniky. Tak, ako rastie počet útokov, vyvíjajú sa aj spôsoby a sofistikovanosť ich prevedenia. Vystopovanie páchateľov, zabezpečovanie dôkazov či ohraničenie škodlivého následku je čoraz zložitejšie.

Blokovanie infikovaných domén a IP adries je nutné považovať za reaktívne opatrenie vedúce k zamedzeniu prístupu k škodlivému obsahu. Dôvody, prečo využiť tento prostriedok môžeme zhrnúť do niekoľkých bodov:

1. **Ochrana používateľov napadnutých služieb a nevedomých používateľov podvodných služieb** - ak je na šírenie škodlivého obsahu, vylákanie údajov alebo na ilegálne aktivity zneužitá legitímna doména alebo služba, zablokovanie obsahu alebo konkrétneho URL zabezpečí ochranu používateľov, ktorí túto službu alebo doménu využívajú.

2. **Zmiernenie alebo zamedzenie škodlivých následkov** - blokovaním domén a IP adries so škodlivým obsahom či phishingom je možné takisto dosiahnuť zmierňovanie následkov v podobe menšieho dopadu na potenciálne obete, resp. zasiahnutých používateľov. Takisto včasným blokovaním možno zabezpečiť úplné zamedzenie škodlivých následkov, pretože nemusí dôjsť napríklad k stiahnutiu škodlivého obsahu alebo k dokončeniu všetkých fáz phishingovej kampane.

3. **Zastavenie šírenia škodlivého obsahu** - v tomto bode rozumieme najmä šírenie malvéru, existenciu riadiacich serverov pre botnety, phishingové stránky a podobne. Domény a IP adresy s takýmto obsahom sú využívané útočníkmi na nelegitímne ciele a ich blokovanie zamedzuje ďalšiemu šíreniu takéhoto škodlivého obsahu.

Téma blokovania internetového obsahu, domén a IP adries je citlivá a často spájaná s pojmom cenzúra. Je preto potrebné brať na zreteľ dôvody, ako aj spôsob či rozsah takéhoto blokovania. Hlavným dôvodom pre blokovanie by mala byť vždy ochrana záujmov a práv používateľov internetu, teda občanov, ktorých sloboda a práva by sa nemali obmedzovať ani vo virtuálnom priestore. 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 prístup k obsahu, ktorý by im mohol škodiť alebo priamo škodí.

Ďalším dôležitým aspektom blokovania je ochrana zariadení a služieb, ktoré sú poskytované koncovým užívateľom. Ako je uvedené vyššie, útočníkovi nemusí ísť exaktne o údaje používateľa, ale aj o výpočtovú silu zariadenia, ktoré používateľ vlastní. Nejde však iba o osobné počítače či mobilné zariadenia. Zahrnúť sem môžeme podpornú infraštruktúru, ako aj celé spektrum internetu vecí, teda zariadení pripojených na internet poskytujúcich určitý druh služby, ktoré sa po infikovaní škodlivým kódom alebo prelomením ochrany zo strany útočníka môžu stať užitočným nástrojom na

vykonávanie kybernetických útokov (DDoS útoky, šírenie malvéru, šírenie phishingových e-mailov a podobne).

Blokovanie útočníka alebo škodlivého obsahu je však len jedným z mnohých krokov v procese riešenia kybernetických bezpečnostných incidentov. Konkrétny proces je závislý od typu hrozby a viacerých faktorov, napríklad krajiny útočníka a obete. Blokovaniu môže napríklad predchádzať pokus o kontakt s prevádzkovateľom danej IP adresy alebo domény a odstránenie škodlivého obsahu, prípadne môže byť nasledované krokmi, vedúcimi k odstráneniu následkov, lepšiemu zabezpečeniu a obnove funkčnosti napadnutých systémov a podobne. Tieto úkony vykonávajú jednotliví prevádzkovatelia postihnutých služieb a zariadení, vrátane štátnej a verejnej správy, súkromného sektora a občanov.

Schopnosť efektívne blokovať, ako aj schopnosť efektívne vykonávať ďalšie kroky potrebné pre riešenie kybernetických bezpečnostných incidentov, si vyžaduje na národnej úrovni spoluprácu národnej autority pre kybernetickú bezpečnosť a sektorových autorít s poskytovateľmi hostingových a doménových služieb, s poskytovateľmi internetu a s ďalšími partnermi.

Vzhľadom ku globálnemu charakteru komunikačných sietí je potrebné pre ochranu kybernetického priestoru SR spolupracovať aj na nadnárodnej úrovni s partnermi, ktorí sú schopní zasiahnuť voči hrozbám pochádzajúcich z ich krajín, ktoré smerujú do kybernetického priestoru SR. Takáto spolupráca však predpokladá vysokú mieru reciprocity.

Keďže rôzne techniky, rozobrané podrobne v kapitole *Analýza blokovacích techník*, majú schopnosť blokovať jednotlivé typy hrozieb, ale neexistuje jedna technika, ktorá by naraz dokázala efektívne splniť všetky účely blokovania, je potrebné využiť kombináciu týchto techník, ktorá umožní:

- blokovanie prístupu na škodlivý obsah nachádzajúci sa kdekoľvek na svete z kybernetického priestoru SR,
- blokovanie prístupu na škodlivý obsah nachádzajúci sa v kybernetickom priestore SR z celého internetu,
- blokovanie útokov smerujúcich odkiaľkoľvek do kybernetického priestoru SR,
- blokovanie útokov smerujúcich z kybernetického priestoru SR kamkoľvek.

1.2 Riziká blokovania

Niektoré riziká a negatívne dopady blokovania sa týkajú všetkých mysliteľných techník. Iné sú závislé od konkrétnej použitej techniky. Identifikované riziká sú:

- Riziko vzniku škôd
    - pri blokovaní prístupu na IP adresu budú neprístupnené všetky služby prevádzkované na tej istej IP adrese, a to aj iné typy služieb ako služba, ktorá bola blokovaná
        - Príklad: blokovanie IP adresy webového servera nutne spôsobí znefunkčnenie iných webových stránok, ktoré zdieľajú tú istú IP adresu. Prevádzka viacerých stránok na tej istej IP adrese je bežnou praxou. Dopad: nefunkčnosť stránky organizácie môže mať za

následok ušlý zisk v podobe nezrealizovaných objednávok, stratu dôveryhodnosti organizácie, či v prípade automatizovaných komunikačných rozhraní stratu dát.

- Príklad: blokovanie IP adresy, na ktorej je prevádzkovaný DNS server, môže spôsobiť nefunkčnosť všetkých domén, ktoré túto IP adresu používajú ako DNS server.
- Príklad: blokovanie IP adresy alebo domény veľkého portálu alebo cloudovej služby môže znefunkčniť e-mailovú komunikáciu pre rádovo stovky, tisíce či ešte viac klientov.

- škody môžu byť spôsobené aj subjektu, ktorý nie je priamo zodpovedný za infraštruktúru šíriacu škodlivý obsah
  - Príklad: prevádzkovateľ služby web hostingu zablokuje prístup na stránky svojho zákazníka. Zákazník nezaplatí poplatok za dané obdobie na základe nedodania objednanej služby.
  - Príklad: blokovanie IP adresy, zdieľanej viacerými používateľmi internetu, zapríčiní okrem zablokovania škodlivej IP adresy aj zablokovanie prístupu na internet užívateľom alebo zariadeniam, ktoré nie sú infikované a nevykonávajú škodlivú činnosť.

- Blokovanie môže mať za následok aj znefunkčnenie služieb s dopadom na život, zdravie a majetok občanov
  - Príklad: znefunkčnenie tiesňovej linky prevádzkovanej cez IP telefóniu.
  - Príklad: znefunkčnenie bezpečnostných systémov - kamera, senzor, alarm.
- Príliš široké blokovanie
  - Príklad: pri blokovaní celého prístupu na doménu druhej úrovne budú zneprístupnené všetky URL, ktoré daná doména poskytuje, ako aj iné typy služieb ako služba, ktorá má byť zablokovaná.
- Nesprávne alebo neoprávnené blokovanie
  - niektoré udalosti vyhodnotené ako útok môžu byť v skutočnosti objednané penetračné testy alebo plošné skenovanie národného kybernetického priestoru bezpečnostnými výskumníkmi, ktorí sa snažia identifikovať problémy za účelom informovania a lepšej ochrany koncových používateľov. Tieto prípady nie je možné systematicky odlíšiť od skutočnej škodlivej aktivity,
  - pretože blokovanie ako také nie je automatizovanou činnosťou a rozhodnutie vykonáva človek, môže dôjsť k zablokovaniu takého obsahu, ktorý nie je škodlivý - napríklad preklep v názve domény, blokovanie inej IP z dôvodu omylu v číslach a podobne.
- Riziko ľahkého obídenia blokovania
  - dobre motivovaný útočník dokáže nájsť spôsob ako obísť blokovaciu techniku a škodlivý obsah šíriť ďalej. Konkrétne spôsoby závisia od použitej blokovacej techniky a obtiažnosť obídenia blokovania sa môže pre jednotlivé techniky líšiť.

- Neželaná podpora používateľov v hľadaní spôsobov ako blokovanie obísť
    - pri blokovaní obsahu, ktorý je používateľmi žiadaný, je možné predpokladať rozširovanie využitia anonymizačných služieb, čo má z dlhodobého hľadiska negatívny dopad na schopnosť chrániť používateľov pred škodlivým obsahom.
- Blokovanie neodstraňuje škodlivý obsah
    - to, že IP adresa alebo doména so škodlivým obsahom budú zablokované nerieši reálnu existenciu tohto obsahu a potrebu jeho odstránenia.
- Strata dôvery v transparentnosť a slobodu
    - používatelia môžu vnímať zablokovanie, aj keď škodlivého obsahu, ako narušenie slobody internetu alebo svojich vlastných osobných slobôd.
- Možné narušenie súkromia
    - niektoré spôsoby blokovania si vyžadujú zásah alebo nazeranie do prenášaných informácií používateľov, čo zvyšuje riziko narušenia súkromia a slobody používateľov na internete.

1.3 Súčasný stav blokovania v SR

V rámci slovenských reálií je blokovanie škodlivého obsahu, domén a IP adries v súčasnosti aplikované len na špecifické oblasti a prostredia. Jednotná koncepcia blokovania, aplikovateľná vo všetkých prípadoch a naprieč celým národným kybernetickým priestorom, však neexistuje.

Blokovanie v najväčšej miere a s jasne definovanou legislatívnou podporou využíva Finančná správa, ktorá blokuje webové sídla, ktoré poskytujú tzv. „zakázanú ponuku“ (§ 2 písm. u) zákona č. 171/2005 Z. z. o hazardných hrách a o zmene a doplnení niektorých zákonov - propagovanie hazardnej hry alebo prevádzkovanie hazardnej hry dostupnej na území SR bez licencie podľa tohto zákona prostredníctvom elektronickej komunikačnej siete). Toto blokovanie typicky využíva techniku blokovania konkrétnych doménových mien na úrovni ISP. Podľa § 15b ods. 7 a nasl. zákona č. 171/2005 Z. z. sú právnické alebo fyzické osoby, ktoré poskytujú elektronické komunikačné siete alebo služby povinné na základe príkazu súdu vydaného na základe žiadosti Finančného riaditeľstva SR zamedziť prístup k webovému sídlu, prostredníctvom ktorého sa poskytuje zakázaná ponuka, teda hazardné hry bez licencie.

Blokovanie škodlivého obsahu a indikátorov kompromitácie (IP adresy, domény, e-mailové adresy a podobne) prebieha aj na úrovni vládnej siete GOVNET, ktorú má v správe Národná agentúra pre sieťové a elektronické služby (NASES). Toto blokovanie je zamerané výlučne na ochranu vládnej siete a jej používateľov pred škodlivým obsahom a útokmi a prebieha na základe zistení z bezpečnostného monitoringu, ktorý vykonávajú jednotky CSIRT v pôsobnosti Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu. Na základe výstupov a odporúčaní tejto CSIRT jednotky sú jednotlivé škodlivé indikátory alebo obsah zablokované len na úrovni vládnej siete a ovplyvňujú komunikáciu z/do uzlov v sieti GOVNET. Podobné blokovanie prebieha na úrovni viacerých organizácií z rôznych sektorov.

Blokovanie škodlivého obsahu (malvér, vírusy) na úrovni koncových používateľov a pracovných staníc je široko dostupné a využívané, najčastejšie vo forme rôznych komerčných antivírusových produktov. Existujú však aj používatelia, ktorí antivírusové programy nepoužívajú a nezanedbateľná časť používateľov nemá nastavené automatické aktualizácie produktov a vzoriek. Táto oblasť nie je nijako harmonizovaná a regulovaná. Neexistuje mechanizmus ako túto infraštruktúru plošne využívať na adresné blokovanie škodlivej aktivity naprieč rôznymi výrobcami a produktami.

Blokovanie nevyžiadanej pošty je realizované na poštových serveroch a využíva kombináciu viacerých techník, vrátane reputačných databáz, signatúr a štatistických pravidiel. Blokovanie je vykonávané u poskytovateľov e-mailových služieb a slovenskí občania aj firmy často využívajú aj zahraničných poskytovateľov služieb, napríklad gmail. Táto oblasť nie je nijako harmonizovaná a regulovaná, pričom je nereálne predpokladať schopnosť vymôcť prípadné regulácie u zahraničných poskytovateľov.

Blokovanie DDoS útokov nie je široko rozšírené a využívajú ho prevažne veľké inštitúcie. Časť blokovania je riešená zariadeniami na sieťovom bezpečnostnom perimetri organizácií, prípadne u poskytovateľa pripojenia do internetu. Časť blokovania je realizovaná cloudovými službami. Táto oblasť nie je nijako harmonizovaná ani regulovaná.

1.4 Skúsenosti z iných krajín

Potreba a dôvody blokovania neobchádzajú žiadnu z krajín, kde je rozvinutá digitálna a internetová infraštruktúra. Jednotlivé krajiny si volia spôsob a nachádzajú dôvody, ako sa vysporiadať jednak s globálnymi hrozbami a škodlivým obsahom (detská pornografia, nelegálny predaj zbraní a drog na internete, porušovanie autorských práv a podobne) a jednak so špecifikami jednotlivých krajín.

V roku 2018 japonská organizácia Japan Network Information Center uskutočnila prieskum, ktorý sa týkal situácie blokovania webového obsahu vo svete. Na tento prieskum odpovedalo 104 respondentov zo 49 krajín. Boli položené nasledujúce otázky s výsledkom:

1. **Je vo vašej krajine zavedené blokovanie webového obsahu?**

   71.2% opýtaných odpovedalo áno (74 respondentov)

   26.9% odpovedalo nie (28 respondentov)

   1.9% odpovedalo neviem (2 respondenti)

2. **Ak je vo vašej krajine zavedené blokovanie webového obsahu, aké sú použité techniky blokovania?**

   61.5% DNS Blokovanie (48 respondentov)

   41% Blokovanie IP adries a portov (32 respondentov)

   9% Blokovanie založené na hĺbkovej inšpekcii paketov (7 respondentov)

   43.6% Blokovanie URL (34 respondentov)

   15.4% Blokovanie platforiem (12 respondentov)

23.1% Blokovanie viacerými spôsobmi uvedenými vyššie (18 respondentov)

3. Je blokovanie webového obsahu vo vašej krajine legislatívne vymedzené?

51.9% odpovedalo áno (54 respondentov)

41.3% odpovedalo nie (43 respondentov)

6.7% odpovedalo neviem (7 respondentov)

Tabuľka nižšie uvádza konkrétne príklady blokovania v jednotlivých krajinách, ktoré sa zúčastnili prieskumu:

Krajina	**Blokovanie**	**Objekt blokovania**	**Diskusia k blokovaniu**
Argentína	Áno	Hazardné hry Zločiny Drogy Zbrane UBER - ako ilegálna forma dopravy	V Argentíne prebieha diskusia a príprava zákona o zodpovednosti prevádzkovateľov online služieb (Law on Intermediary Liabilities), ktorý predpokladá, že len Federálny súd môže nariadiť blokovanie alebo filtrovanie na internete
Arménsko	Nie		Áno, prebieha diskusia o blokovaní webov s hazardnými hrami, ktoré v Arménsku prevádzkujú svoje služby bez licencie
Austrália	Áno	Porušenia autorských práv	Áno, prebieha diskusia
Bangladéš	Áno	Pornografia Hazardné hry Nelegálny obchod so zbraňami a drogami Zločiny Politické dôvody Nenávistné a diskriminačné prejavy Zásahy do súkromia	Zákon o digitálnej bezpečnosti (Digital Security Act)
Belgicko	Áno	Každý obsah, ktorý je pri vyšetrovaní verejnej autority vyhodnotený ako ilegálny	
Brazília	Áno	Zločiny Drogy Zbrane Phishing Ohrozovanie detí	Prebiehajú diskusie o ďalších formách blokovania
Buthán	Nie		Bez diskusie
Čile	Nie		Áno, pred časom sa vytvoril projekt, ako blokovať aplikácie ako Uber, ktoré nie sú v Čile regulované
Česká republika	Áno	Hazardné hry - len tie bez oficiálneho povolenia	Diskusie v minulosti boli zamerané proti blokovaniu

Estónsko	Áno	Hazardné hry Iné ilegálne aktivity môžu byť blokované pomocou DNS podľa uváženia registra, ak je takáto aktivita nahlásená verejnými orgánmi na presadzovanie práva alebo CERTom	
Filipíny	Áno	Pornografia - hlavne detská pornografia	
Fínsko	Nie	Porušovanie autorských práv Ilegálne e-shopy s alkoholom Pornografia Hazardné hry Zásahy do súkromia	
Francúzsko	Áno	Obhajovanie a schvaľovanie terorizmu Nabádanie k terorizmu Detská pornografia	
Holandsko	Áno	Porušovanie autorských práv	
India	Áno	Pornografia hazardné hry Zločiny Drogy Zbrane Porušovanie hospodárskej súťaže Porušovanie autorských práv Politické dôvody Nenávistné a diskriminačné prejavy Čokoľvek, čo nariadi súd	
Izrael	Áno	Pornografia Pedofília	
Južná Afrika	Nie		
Južná Kórea	Áno	Pornografia Hazardné hry Zločiny Drogy Zbrane Porušovanie autorských práv Zásahy do súkromia Politické dôvody Nenávistné a diskriminačné prejavy	
Kambodža	Áno	Politické dôvody	Bez ďalšej diskusie
Kanada	Nie		Prebiehajú diskusie, ale zatiaľ bez legislatívneho výstupu
Kiribati	Nie		Diskusie prebiehajú
Litva	Áno	Hazardné hry	

Lotyšsko	Áno	Hazardné hry Nelicencované online televízie Objekty súvisiace s bezpečnosťou informačných technológií	
Malajzia	Áno	Pornografia Zločiny Drogy Zbrane Zásahy do súkromia Politické dôvody Nenávistné a diskriminačné prejavy	
Mexiko	Nie		
Nemecko	Áno	Porušovanie autorských práv	Prebiehajú diskusie, ako predchádzať pomocou blokovania terorizmu a detskej pornografii
Nepál	Áno	Pornografia Zločiny Drogy Zbrane Politické dôvody Hanobenie alebo pohoršujúci obsah narúšajúci slobodu jednotlivca	
Nórsko	Áno	Pornografia Porušovanie autorských práv	
Nový Zéland	Áno	Detská pornografia Pornografia - použitie blacklistov je dobrovoľné	
Pakistan	Áno	Pornografia Hazardné hry Zločiny Drogy Zbrane Zásahy do súkromia Politické dôvody Nenávistné a diskriminačné prejavy	
Poľsko	Áno	Hazardné hry	Po skúsenostiach s blokovaním hazardných stránok viacero štátnych orgánov diskutuje o potrebe blokovania, napríklad Ministerstvo zdravotníctva o blokovaní stránok predávajúcich ilegálne lieky a drogy
Portoriko	Nie		Prebiehajú diskusie s legislatívnymi orgánmi
Rusko	Áno	Pornografia Hazardné hry Zločiny Drogy Zbrane Porušovanie hospodárskej	

		súťaže Porušovanie autorských práv Zásahy do súkromia Politické dôvody Nenávistné a diskriminačné prejavy	
Singapur	Áno	Pornografia Hazardné hry Zločiny Drogy Zbrane Porušovanie autorských práv Politické dôvody Nenávistné a diskriminačné prejavy Falošné správy a podvodné stránky	
Slovensko	Áno	Hazardné hry	
Slovinsko	Áno	Hazardné hry Daňové úniky	
Spojené arabské emiráty	Áno	Pornografia Zločiny Drogy Zbrane Porušovanie autorských práv Politické dôvody Nenávistné a diskriminačné prejavy	
Spojené štáty americké	Áno	Detská pornografia Hazardné hry Zločiny Drogy Zbrane Porušovanie autorských práv Zásahy do súkromia Malvér	
Srí Lanka	Áno	Politické dôvody Nenávistné a diskriminačné prejavy	Prebieha ďalšia diskusia
Španielsko	Áno	Hazardné hry Zločiny Drogy Zbrane Porušovanie autorských práv Politické dôvody Nenávistné a diskriminačné prejavy	
Švajčiarsko	Áno	Hazardné hry Detská pornografia	
Švédsko	Nie		
Tajwan	Nie		

Taliansko	Áno	Pornografia hazardné hry Zločiny Drogy Zbrane Porušovanie autorských práv	
Thajsko	Áno	Pornografia Hazardné hry Zločiny Drogy Zbrane Porušovanie autorských práv Politické dôvody	Blokovanie bude súčasť nového zákona o duševnom vlastníctve
Uganda	Áno	Politické dôvody Zdaňovanie instant messaging služieb	
Uruguaj	Áno	Hazardné hry Porušovanie autorských práv	
Veľká Británia	Áno	Pornografia - blokované sú pornografické stránky, ktoré neobsahujú overenie veku používateľov, takisto sú blokované stránky s detskou pornografiou Porušovanie autorských práv Zásahy do súkromia	

1.5 Analýza blokovacích techník

Tu uvedená analýza posudzuje jednotlivé techniky blokovania z nasledovných pohľadov:

- Účinnosť blokovania komunikácie prichádzajúcej na blokovanú adresu: aká je účinnosť techniky na zastavenie útoku alebo hrozby, ak spojenia, útok, komunikácia smeruje na danú adresu.
- Účinnosť blokovania komunikácie odchadzajúcej z blokovanej adresy: aká je účinnosť techniky na zastavenie útoku alebo hrozby, ak spojenia, útok, komunikácia pochádza z danej adresy
    - Príklad: zablokovanie domény je veľmi účinné na mitigáciu phishingovej kampane, ktorá túto doménu využíva na zber dát, ale vôbec nie je účinné proti Denial of Service útokom, pochádzajúcim z IP adresy, ktorá má pridelené doménové meno v tejto doméne (úspešnosť útoku sa nespolieha na funkčnosť DNS).
- Jednoduchosť implementácie: globálny, nie iba technický, pohľad na náročnosť nasadenia nového blokovacieho pravidla pomocou tejto techniky.
    - Príklad: ak je blokovanie vykonávané jediným subjektom, implementácia je pomerne jednoduchá. Ak je na blokovanie potrebná súčinnosť všetkých používateľov Internetu, alebo je potrebné konfigurovať desiatky najrozličnejších technológií, alebo sa vyžaduje súčinnosť zahraničných subjektov, implementáciu možno považovať za zložitú.
- Kvalita pokrytia: „viem zablokovať, čo potrebujem“. indikátor ukazuje, nakoľko je táto technika účinná pre všetky mysliteľné varianty vstupov.
- Granularita pokrytia: „nezablokujem, čo nechcem“. Indikátor ukazuje, ako presná a jemná je blokovacia technika, aby zablokovala len škodlivý obsah.

1.5.1 Stručný prehľad analyzovaných techník

technika	účinnosť blokovania komunikácie prichádzajúcej na blokovanú adresu	účinnosť blokovania komunikácie odchádzajúcej z blokovanej adresy	jednoduchosť implementácie	kvalita pokrytia (viem zablokovať, čo potrebujem)	granularita blokovania (nezablokujem, čo nechcem)	poznámky
	(škodlivý kód, phishingová stránka, C&C)	(DDoS, spam a scam, skenovanie, pokusy o prienik)	(na významnú časť konštituencie)			
Blokovanie domén druhej úrovne na úrovni správcu TLD	★★★★☆	☆☆☆☆☆	★★★★★	★☆☆☆☆	★☆☆☆☆	blokuje len TLD v jurisdikcii blokujúceho subjektu
Blokovanie konkrétnych doménových mien na úrovni ISP	★★★☆☆	☆☆☆☆☆	★★★☆☆	★★★★☆	★★★☆☆	
Blokovanie konkrétnych URL na webových serveroch	★★★★★	☆☆☆☆☆	★☆☆☆☆	★☆☆☆☆	★★★★★	servery musia spadať do jurisdikcie blokujúceho subjektu
Blokovanie konkrétnych URL na proxy serveroch	★★★★★	☆☆☆☆☆	☆☆☆☆☆	☆☆☆☆☆	★★★★★	nie každý má proxy, nemožné vynútiť
Blokovanie e-mailového účtu na	★★★★★	★★★★★	★☆☆☆☆	★☆☆☆☆	★★★★☆	Poštový server musí spadať

príslušnom poštovom serveri						do jurisdikcie blokujúceho subjektu
Blokovanie e-mailovej adresy na relay serveroch a iných poštových serveroch	★★★★★	★★★★★	☆☆☆☆☆	☆☆☆☆☆	★★★★★	

Blokovanie IP adresných rozsahov pomocou BGP	★★★★★	★★☆☆☆	★★★★☆	★★★★☆	★★☆☆☆	ľahko nasaditeľné spoluprácou s konečným počtom ISP
Blokovanie IP adresných rozsahov pomocou firewallových pravidiel	★★★★★	★★★★★	★★☆☆☆	★★★★☆	★★☆☆☆	neexistuje „centrálny firewall“, jeho nasadenie by mohlo byť kontroverzné, ISP majú firewally rôznych výrobcov
Blokovanie IP, protokolu a portu pomocou firewallových pravidiel	★★★★★	★★★★★	★☆☆☆☆	★★★★★	★★★☆☆	neexistuje „centrálny firewall“, jeho nasadenie by mohlo byť kontroverzné, ISP majú firewally rôznych výrobcov, niektoré nepodporujú L4+ blokovanie
Blokovanie IP adresných rozsahov, domén, URL a mailových adries publikovaním zoznamu, bez udania spôsobu blokovania	★★★★★	★★★★★	★★☆☆☆	★★★★☆	★★☆☆☆	bez konkrétnych metodík a usmernení veľmi obtiažne na implementáciu

Blokovanie prístupu koncového uzlu resp. používateľa (sprostredkovane)	★★★★★	★★★★★	★★★★☆	★☆☆☆☆	☆☆☆☆☆	

Blokovanie prostriedkami endpoint security (firewall, antivírus, antimalware a podobne)	★★★★★	★★★★★	☆☆☆☆☆	★★★★★	★★★★★	veľa rôznych výrobcov zariadení, neistá rýchlosť aktualizácií, možnosť implementovať vo vybraných sektoroch

1.5.2 Blokovanie domén druhej úrovne na úrovni správcu TLD

účinnosť blokovania prichádzajúcej komunikácie	★★★★☆
účinnosť blokovania odchádzajúcej komunikácie	☆☆☆☆☆
jednoduchosť implementácie	★★★★★
kvalita pokrytia (viem zablokovať, čo potrebujem)	★☆☆☆☆
granularita blokovania (nezablokujem, čo nechcem)	★☆☆☆☆

Technický princíp blokovania

- Blokovanie by vykonával správca TLD alebo prevádzkovateľ DNS serverov pre túto TLD vyradením domény druhej úrovne z DNS.

Výhody

- Blokovanie vykonáva len jeden subjekt.
- Blokovanie univerzálne funguje pre používateľov z celého sveta.

Nevýhody

- Blokovanie znefunkční celú doménu druhej úrovne, čo môže predstavovať desiatky subdomén, stovky serverov a tisíce služieb. Okrem znefunkčnenia, napríklad konkrétneho webu, nebude na doménu možné prijímať e-mail (môže znemožniť komunikáciu so zablokovaným subjektom) a nebudú fungovať žiadne iné služby prevádzkované na doméne (VPN prístup pre vzdialených zamestnancov či prepojenie pobočiek, IP telefónia založená na doménovom mene a mnohé iné).
- Blokovanie postihuje len domény TLD v jurisdikcii blokujúceho subjektu, nemožnosť blokovať iné TLD.
- Blokovanie je možné ľahko obísť statickým záznamom v hosts (vyžaduje to však akciu na strane každého používateľa).
- Blokovanie má časovú retenciu v závislosti od lokálnych nastavení aktualizácie DNS u poskytovateľov lokálnych DNS serverov a od aktuálneho stavu DNS cache na serveroch používateľov. Blokovanie sa v najhoršom prípade môže prejaviť niektorým používateľom okamžite, iným však s latenciou niekoľko hodín až dní.

Záver

- Možnosť nasadiť túto techniku je veľmi jednoduchá, pretože blokovanie technicky vykonáva jeden subjekt.
- Blokovanie funguje len pre prichádzajúcu komunikáciu a len pre slovenské domény, ale chráni používateľov kdekoľvek na svete.
- Negatívne následky blokovania a riziko vzniku vedľajších škôd sú pri tejto technike pomerne vysoké, preto má byť použitá len v nevyhnutných prípadoch.

1.5.3 Blokovanie konkrétnych doménových mien na úrovni ISP

účinnosť blokovania prichádzajúcej komunikácie	★★★☆☆
účinnosť blokovania odchádzajúcej komunikácie	☆☆☆☆☆
jednoduchosť implementácie	★★★☆☆
kvalita pokrytia (viem zablokovať, čo potrebujem)	★★★★☆
granularita blokovania (nezablokujem, čo nechcem)	★★★☆☆

Technický princíp blokovania

- Blokovanie ľubovoľného doménového mena alebo subdomény na úrovni ISP a iných prevádzkovateľov DNS serverov.
- Technicky je možné blokovať
    - odpoveďou NXDOMAIN (doména neexistuje),
    - odpoveďou smerujúcou na vyhradený server vysvetľujúci dôvody blokovania,
    - odpoveďou 127.0.0.1 alebo inou odpoveďou smerujúcou na inú IP adresu (neodporúčané).
- Toto je možné realizovať
    - na primárnych DNS serveroch, na ktoré smeruje záznam daného správcu TLD (lenže prevádzkovateľ DNS nemusí spolupracovať, napríklad server vôbec nemusí byť v SR, alebo doba expirácie, TTL, na doméne môže byť nastavená na veľmi dlhú dobu),
    - blokovaním na úrovni ISP (prakticky výrazne funkčnejšie riešenie).

Výhody

- Blokovanie ľubovoľnej domény, nielen .SK.
- Blokuje jediné konkrétne doménové meno.

Nevýhody

- Neumožňuje blokovanie konkrétneho URL, ale blokuje vždy celú adresu.
- Blokuje iné služby prevádzkované na tom istom serveri.
- Blokovanie možno veľmi ľahko obísť nastavením vlastného DNS servera alebo záznamom do súboru hosts.

1.5.4 Blokovanie IP adresných rozsahov pomocou BGP

účinnosť blokovania prichádzajúcej komunikácie	★★★★★
účinnosť blokovania odchádzajúcej komunikácie	★★☆☆☆
jednoduchosť implementácie	★★★★☆
kvalita pokrytia (viem zablokovať, čo potrebujem)	★★★★☆
granularita blokovania (nezablokujem, čo nechcem)	★★☆☆☆

Technický princíp blokovania

BGP je protokol, ktorým komunikujú smerovače v chrbticovej sieti internet, aby si vymieňali informácie o cestách, kde

- alternatíva 1: poskytovatelia budú na výmenných bodoch vytvárať novú BGP session voči schváleným blokovacím serverom. Tento server bude publikovať špeciálne smerovacie pravidlo pre všetky IP adresy určené na blokovanie,
- alternatíva 2: poskytovatelia budú na svojich výmenných bodoch sami aplikovať sadu smerovacích pravidiel podľa publikovaného zoznamu.

Výhody

- Umožňuje blokovať jednotlivé IP adresy aj celé rozsahy.
- Technicky je blokovanie obtiažne obísť (potrebná VPN ku zahraničnému poskytovateľovi, ktorý filter neaplikuje).

Nevýhody

- Neblokuje DDoS útoky ako UDP, syn flood.

1.5.5 Blokovanie IP adresných rozsahov pomocou firewallových pravidiel

účinnosť blokovania prichádzajúcej komunikácie	★★★★★
účinnosť blokovania odchádzajúcej komunikácie	★★★★★
jednoduchosť implementácie	★★☆☆☆
kvalita pokrytia (viem zablokovať, čo potrebujem)	★★★★☆
granularita blokovania (nezablokujem, čo nechcem)	★★☆☆☆

Technický princíp blokovania

- Blokovanie prebieha na úrovni perimetrového bezpečnostného zariadenia (firewall), možno blokovať IP adresy a IP adresné rozsahy na odchádzajúcej a prichádzajúcej komunikácii.
- Blokuje ISP, ktorý je o to požiadaný.

Výhody

- Blokovanie oboch smerov komunikácie.
- Blokovanie je veľmi ťažké alebo nemožné obísť.
- Technologicky neutrálny spôsob blokovania (nezáleží na technológií ISP).

Nevýhody

- Pre efektivitu nutné zaviesť u viacerých ISP, pretože neexistuje „národný firewall“.

1.5.6 Blokovanie IP, protokolu a portu pomocou firewallových pravidiel

účinnosť blokovania prichádzajúcej komunikácie	★★★★★
účinnosť blokovania odchádzajúcej komunikácie	★★★★★
jednoduchosť implementácie	★☆☆☆☆
kvalita pokrytia (viem zablokovať, čo potrebujem)	★★★★★
granularita blokovania (nezablokujem, čo nechcem)	★★★☆☆

Technický princíp blokovania

- Obdobný princíp ako pri blokovaní IP adresných rozsahov pomocou firewallových pravidiel. Rozdiel je len v užšej špecifikácii čo blokovať, teda až do úrovne protokolu a portu.

Výhody

- Lepšia granularita blokovania.
- Zníženie rizika nežiadúcich efektov.
- Technologicky neutrálny spôsob blokovania (nezáleží na technológií ISP).

Nevýhody

- Pre efektivitu nutné zaviesť u viacerých ISP, pretože neexistuje „národný firewall“.
- ISP musí umožňovať blokovanie na 4. vrstve ISO OSI.

1.5.7 Blokovanie IP adresných rozsahov, domén, URL a mailových adries publikovaním zoznamu, bez udania spôsobu blokovania

účinnosť blokovania prichádzajúcej komunikácie	★★★★★
účinnosť blokovania odchádzajúcej komunikácie	★★★★★
jednoduchosť implementácie	★★☆☆☆
kvalita pokrytia (viem zablokovať, čo potrebujem)	★★★★☆
granularita blokovania (nezablokujem, čo nechcem)	★★☆☆☆

Technický princíp blokovania

- Národná autorita pre kybernetickú bezpečnosť vypublikuje strojovo čitateľné zoznamy IP adries, domén, URL a mailových adries na blokovanie.
- ISP tieto zoznamy automatickým spôsobom pravidelne začlenia do svojich blokovacích pravidiel.

Výhody

- Jednoduchý a operatívny spôsob zmien v IP adresách doménach, URL a mailových adresách, ktoré majú byť blokované.
- Technologicky neutrálny spôsob blokovania (nezáleží na technológií ISP).

Nevýhody

- Nie je zaručené, že zoznam bude včasne a správne implementovaný u každého ISP.

1.5.8 Blokovanie konkrétnych URL na webových serveroch

účinnosť blokovania prichádzajúcej komunikácie	★★★★★
účinnosť blokovania odchádzajúcej komunikácie	☆☆☆☆☆
jednoduchosť implementácie	★☆☆☆☆
kvalita pokrytia (viem zablokovať, čo potrebujem)	★☆☆☆☆
granularita blokovania (nezablokujem, čo nechcem)	★★★★★

Technický princíp blokovania

- URL budú blokované konfiguráciou konkrétneho webového servera, ktorý pri obdržaní požiadavky na dané URL vráti miesto pôvodnej odpovede či už chybový kód, alebo presmerovanie na inú URL so správou, prečo je prístup na blokovanú URL obmedzený.

Výhody

- Možnosť zablokovania len konkrétnej URL adresy bez ovplyvnenia celého webu.
- Nemožné obísť blokovanie.

Nevýhody

- Možnosť blokovania len webových služieb.
- Blokovanie postihuje len web servery, ktoré spadajú do konštituencie SK-CERT.
- Útočník môže škodlivý obsah umiestniť na inú URL v rámci webovej stránky a vyhnúť sa tak blokovaniu.

1.5.9 Blokovanie konkrétnych URL na proxy serveroch

účinnosť blokovania prichádzajúcej komunikácie	★★★★★
účinnosť blokovania odchádzajúcej komunikácie	☆☆☆☆☆
jednoduchosť implementácie	☆☆☆☆☆
kvalita pokrytia (viem zablokovať, čo potrebujem)	☆☆☆☆☆
granularita blokovania (nezablokujem, čo nechcem)	★★★★★

Technický princíp blokovania

- URL budú blokované konfiguráciou konkrétneho proxy servera, ktorý pri obdržaní požiadavky na dané URL vráti miesto pôvodnej odpovede či už chybový kód, alebo presmerovanie na inú URL so správou, prečo je prístup na blokovanú URL obmedzený.

Výhody

- Vysoká granularita blokovania.
- Možnosť zablokovania len konkrétnej URL adresy bez ovplyvnenia celého webu.

Nevýhody

- Blokovanie je možné obísť nastavením iného proxy servera.
- Blokovať možno len webové služby.
- Útočník môže škodlivý obsah umiestniť na inú URL v rámci webovej stránky a vyhnúť sa blokovaniu.
- Používateľ musí mať proxy server - typicky dostupné len v korporátnych prostrediach.
- Problematická distribúcia zakázaných URL na jednotlivé proxy servery.
- Pri šifrovanej komunikácii a použití metódy CONNECT nie je možné na proxy serveri blokovať jednotlivé konkrétne URL.

1.5.10 Blokovanie prístupu koncového uzlu, resp. používateľa

účinnosť blokovania prichádzajúcej komunikácie	★★★★★
účinnosť blokovania odchádzajúcej komunikácie	★★★★★
jednoduchosť implementácie	★★★★☆

kvalita pokrytia (viem zablokovať, čo potrebujem)	★☆☆☆☆
granularita blokovania (nezablokujem, čo nechcem)	☆☆☆☆☆

Technický princíp blokovania

- Blokovanie vykoná ISP, ktorý má koncový uzol vo svojej sieti.

Výhody

- Vysoká účinnosť blokovania komunikácie z/do koncového uzla.
- Jednoducho implementovateľné zo strany ISP.

Nevýhody

- Možnosť zablokovať len koncové uzly v rámci slovenského kybernetického priestoru.
- Vysoké riziko vzniku nežiaducich škôd, pretože za blokovaným uzlom sa môže nachádzať viacero zariadení, služieb alebo používateľov.

1.5.11 Blokovanie prostriedkami endpoint security (firewall, antivírus, antimalware a podobne)

účinnosť blokovania prichádzajúcej komunikácie	★★★★★
účinnosť blokovania odchádzajúcej komunikácie	★★★★★
jednoduchosť implementácie	☆☆☆☆☆
kvalita pokrytia (viem zablokovať, čo potrebujem)	★★★★★
granularita blokovania (nezablokujem, čo nechcem)	★★★★★

Technický princíp blokovania

- Blokovanie je vykonávané prostredníctvom softvérových alebo hardvérových nástrojov, ktoré sú prevádzkované v rámci jednotlivých sietí.

Výhody

- Možnosť blokovať viacero indikátorov súčasne jedným nástrojom.
- Možnosť využívať aj bezplatné nástroje.

Nevýhody

- Obtiažna koordinácia s autormi AV produktov. Nie je zaručené, že škodlivé indikátory budú blokovať všetky softvérové a hardvérové nástroje.

- Nie každý používateľ používa nástroje endpoint security, takisto nie každý používateľ má tieto nástroje aktualizované a obohatené aktuálnymi indikátormi.

1.5.12 Blokovanie e-mailového účtu na príslušnom poštovom serveri

účinnosť blokovania prichádzajúcej komunikácie	★★★★★
účinnosť blokovania odchádzajúcej komunikácie	★★★★★
jednoduchosť implementácie	★☆☆☆☆
kvalita pokrytia (viem zablokovať, čo potrebujem)	★☆☆☆☆
granularita blokovania (nezablokujem, čo nechcem)	★★★★☆

Technický princíp blokovania

- Odosielanie e-mailu a vyberanie e-mailu zo schránky znefunkční jej prevádzkovateľ formou zablokovania používateľského účtu alebo dočasnej zmeny hesla.

Výhody

- Vysoká granularita blokovania
- Možnosť zablokovania jednej e-mailovej adresy

Nevýhody

- Subjekt, ktorý prevádzkuje e-mailovú adresu, musí byť v jurisdikcii SR
- Rôzne techniky blokovania na rôznych poštových serveroch

1.5.13 Blokovanie e-mailovej adresy na relay serveroch a iných poštových serveroch

účinnosť blokovania prichádzajúcej komunikácie	★★★★★
účinnosť blokovania odchádzajúcej komunikácie	★★★★★
jednoduchosť implementácie	☆☆☆☆☆
kvalita pokrytia (viem zablokovať, čo potrebujem)	☆☆☆☆☆
granularita blokovania (nezablokujem, čo nechcem)	★★★★★

Technický princíp blokovania

- E-maily budú blokované podľa adresy odosielateľa alebo prijímateľa filtrom na poštových serveroch ISP, organizácií a relay serveroch.

Výhody

- Vysoká granularita blokovania
- Možnosť zablokovania jednej e-mailovej adresy

Nevýhody

- Na celonárodnej úrovni nemožné skoordinovať konfiguráciu všetkých poštových serverov. Nie je známe, ako určiť optimálny zoznam serverov, ktorý maximalizuje pomer ochránených používateľov voči počtu potrebných administratívnych a konfiguračných zásahov. Riešenie je možné použiť v užšie definovaných prostrediach, kde sú na to vybudované predpoklady.

2. Návrh pravidiel pre blokovanie

2.1 Pravidlá pre blokovanie

Samotné pravidlá pre blokovanie musia spĺňať nasledujúce požiadavky:

- **Zákonné predpoklady** - blokovanie musí mať oporu v legislatíve.
- **Jasná formulácia** - pravidlá musia byť jasne formulované bez možnosti alternatívneho výkladu.
- **Jednoznačné právomoci** - pravidlá musia obsahovať, kto má právomoc vydať rozhodnutie o blokovaní.
- **Adresnosť** - z pravidiel musí byť jasne vymedzený subjekt, ktorý bude vykonávať blokovanie.
- **Jednoduchá implementácia** - s blokovaním nesmú vzniknúť také náklady, ktoré by prevyšovali samotný účel blokovania.

V rámci jednotlivých techník sa pravidlá pre ich nasadenie líšia. Pre všetky pravidlá však platí, že blokovať možno:

- IP adresu, doménu alebo URL, na ktorých sa nachádza:
    - phishingová stránka alebo server riadiaci phishingové aktivity,
    - škodlivý kód,
    - riadiaci server pre riadenie botnetovej siete.
- IP adresu alebo doménu, prostredníctvom ktorej sa vykonáva:
    - DDoS útok,
    - skenovanie,
    - bruteforce útoky alebo pokusy,
    - pokusy o prienik.

V rámci pravidiel, platných pre celý národný kybernetický priestor nie je možné aplikovať všetky techniky blokovania škodlivého obsahu. Je potrebné určiť a vybrať techniky, ktoré sú najúčinnejšie a najľahšie implementovateľné so vzťahom na čo najvyššiu elimináciu rizík, spojenú s blokovaním domén.

2.1.1 Pravidlá pre blokovanie domén druhej úrovne na úrovni správcu národnej TLD

Subjekt, ktorý môže rozhodnúť o blokovaní: Úrad ako národná autorita pre kybernetickú bezpečnosť.

Podmienky

- Blokovanie domény na úrovni správcu národnej TLD je krajným prostriedkom riešenia kybernetického bezpečnostného incidentu, najmä pri závažných kybernetických bezpečnostných incidentoch II. a III. stupňa a incidentoch s cezhraničným presahom.
- Blokovaniu musí predchádzať:
    - Evidencia a riešenie incidentu Národnou jednotkou CSIRT v zmysle platnej legislatívy a interných postupov, vrátane eskalačných a komunikačných mechanizmov medzi jednotlivými zložkami, ktorých účasť na riešení incidentu vyžaduje platná legislatíva,
    - po zistení škodlivého obsahu na dotknutej doméne informovanie Národnej jednotky CSIRT,
    - komunikácia Národnej jednotky CSIRT s držiteľom a prevádzkovateľom domény,
    - poskytnutie možnosti na odstránenie škodlivého obsahu z dotknutej domény,
    - ak škodlivý obsah nebol odstránený do určenej lehoty, úrad vydá rozhodnutie o blokovaní domény,
    - rozhodnutie úrad oznámi správcovi národnej TLD, ktorý je povinný blokovať doménu so škodlivým obsahom.
- V prípade odstránenia škodlivého obsahu pred uplynutím lehoty úrad nevydá rozhodnutie o blokovaní a v súčinnosti s držiteľom a prevádzkovateľom domény pokračuje v ďalších fázach riešenia a koordinácie riešenia kybernetického bezpečnostného incidentu.
- Ak prišlo k blokovaniu domény a škodlivý obsah bol z domény odstránený, držiteľ domény môže požiadať úrad o odblokovanie domény. Súčasťou takejto žiadosti musia byť dôkazy o odstránení škodlivého obsahu z domény. Úrad takejto žiadosti, na základe predložených dôkazov, môže vyhovieť alebo žiadosť zamietnuť. O vyhovení žiadosti alebo jej zamietnutí vydá rozhodnutie, ktoré zašle správcovi národnej TLD.

Legislatívne podmienky

Zákon č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „zákon o kybernetickej bezpečnosti“).

§ 5 ods. 1 písm. p) - úrad zabezpečuje a zodpovedá za koordinované riešenie kybernetických bezpečnostných incidentov na národnej úrovni,

§ 19 ods. 6 - Prevádzkovateľ základnej služby je ďalej povinný:

a) riešiť kybernetický bezpečnostný incident,

b) bezodkladne hlásiť závažný kybernetický bezpečnostný incident,

c) spolupracovať s úradom a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu,

§ 22 ods. 3 - Poskytovateľ digitálnej služby je povinný:

a) hlásiť každý kybernetický bezpečnostný incident, ak disponuje informáciami, na základe ktorých je spôsobilý identifikovať, či má tento kybernetický bezpečnostný incident podstatný vplyv podľa osobitného predpisu, a to bezodkladne po jeho zistení,

b) riešiť hlásený kybernetický bezpečnostný incident,

c) spolupracovať s úradom pri riešení hláseného kybernetického bezpečnostného incidentu.

§ 27 ods. 1 - V prípade závažného kybernetického bezpečnostného incidentu alebo jeho hrozby môže úrad

a) vyhlásiť výstrahu a varovanie pred závažným kybernetickým bezpečnostným incidentom,

b) uložiť povinnosť riešiť kybernetický bezpečnostný incident,

c) uložiť povinnosť vykonať reaktívne opatrenie,

d) požadovať návrh opatrení a vykonanie opatrení určených na zabránenie ďalšieho pokračovania, šírenia a opakovaného výskytu závažného kybernetického bezpečnostného incidentu (ďalej len „ochranné opatrenie“).

§ 27 ods. 7 - Ochranné opatrenie prijíma prevádzkovateľ základnej služby na základe analýzy riešeného závažného kybernetického bezpečnostného incidentu.

§ 27 ods. 8 - Prevádzkovateľ základnej služby je na výzvu úradu v určenej lehote povinný predložiť navrhované ochranné opatrenie na schválenie. Úrad rozhodnutím navrhované opatrenie schváli a určí lehotu na jeho vykonanie. **V prípade, ak prevádzkovateľ základnej služby nenavrhne ochranné opatrenie v určenej lehote alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je prevádzkovateľ základnej služby povinný spolupracovať s úradom, ústredným orgánom a s tým, kto prevádzkuje jednotku CSIRT, na jeho návrhu.**

2.1.2 Pravidlá pre blokovanie domén na úrovni ISP

Subjekt, ktorý môže rozhodnúť o blokovaní: Úrad ako národná autorita pre kybernetickú bezpečnosť.

Podmienky

- Blokovanie domény na úrovni ISP je krajným prostriedkom riešenia kybernetického bezpečnostného incidentu.
- Blokovaniu musí predchádzať:
    - Evidencia a riešenie incidentu Národnou jednotkou CSIRT v zmysle platnej legislatívy a interných postupov, vrátane eskalačných a komunikačných mechanizmov medzi jednotlivými zložkami, ktorých účasť na riešení incidentu vyžaduje platná legislatíva,

- po zistení škodlivého obsahu na dotknutej doméne akejkoľvek úrovne informovanie Národnej jednotky CSIRT,
- komunikácia Národnej jednotky CSIRT s držiteľom a prevádzkovateľom domény,
- poskytnutie možnosti na odstránenie škodlivého obsahu z dotknutej domény,
- ak škodlivý obsah nebol odstránený do určenej lehoty, úrad vydá rozhodnutie o blokovaní domény,
- rozhodnutie sa oznámi ISP, ktorý je povinný blokovať doménu so škodlivým obsahom,
- ISP presmeruje škodlivú doménu na špeciálnu stránku, na ktorej sú vysvetlené dôvody blokovania dotknutej domény.

- V prípade odstránenia škodlivého obsahu pred uplynutím lehoty úrad nevydá rozhodnutie o blokovaní a v súčinnosti s držiteľom a prevádzkovateľom domény pokračuje v ďalších fázach riešenia a koordinácie riešenia kybernetického bezpečnostného incidentu.

- Ak prišlo k blokovaniu domény a škodlivý obsah bol z domény odstránený, držiteľ domény môže požiadať úrad o odblokovanie domény. Súčasťou takejto žiadosti musia byť dôkazy o odstránení škodlivého obsahu z domény. Úrad takejto žiadosti, na základe predložených dôkazov a vlastnej analýzy, môže vyhovieť alebo žiadosť zamietnuť. O vyhovení žiadosti alebo jej zamietnutí vydá rozhodnutie, ktoré zašle ISP, ktorý doménu zablokoval.

<u>Legislatívne podmienky</u>

Zákon o kybernetickej bezpečnosti:

§ 5 ods. 1 písm. p) - úrad zabezpečuje a zodpovedá za koordinované riešenie kybernetických bezpečnostných incidentov na národnej úrovni,

§ 19 ods. 6 - Prevádzkovateľ základnej služby je ďalej povinný:

a) riešiť kybernetický bezpečnostný incident,

b) bezodkladne hlásiť závažný kybernetický bezpečnostný incident,

c) spolupracovať s úradom a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu,

§ 22 ods. 3 - Poskytovateľ digitálnej služby je povinný:

a) hlásiť každý kybernetický bezpečnostný incident, ak disponuje informáciami, na základe ktorých je spôsobilý identifikovať, či má tento kybernetický bezpečnostný incident podstatný vplyv podľa osobitného predpisu, a to bezodkladne po jeho zistení,

b) riešiť hlásený kybernetický bezpečnostný incident,

c) spolupracovať s úradom pri riešení hláseného kybernetického bezpečnostného incidentu.

§ 27 ods. 1 - V prípade závažného kybernetického bezpečnostného incidentu alebo jeho hrozby môže úrad

a) vyhlásiť výstrahu a varovanie pred závažným kybernetickým bezpečnostným incidentom,

b) uložiť povinnosť riešiť kybernetický bezpečnostný incident,

c) uložiť povinnosť vykonať reaktívne opatrenie,

d) požadovať návrh ochranných opatrení a vykonanie ochranných opatrení.

§ 27 ods. 7 - Ochranné opatrenie prijíma prevádzkovateľ základnej služby na základe analýzy riešeného závažného kybernetického bezpečnostného incidentu.

§ 27 ods. 8 - Prevádzkovateľ základnej služby je na výzvu úradu v určenej lehote povinný predložiť navrhované ochranné opatrenie na schválenie. Úrad rozhodnutím navrhované opatrenie schváli a určí lehotu na jeho vykonanie. **V prípade, ak prevádzkovateľ základnej služby nenavrhne ochranné opatrenie v určenej lehote alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je prevádzkovateľ základnej služby povinný spolupracovať s úradom, ústredným orgánom a s tým, kto prevádzkuje jednotku CSIRT, na jeho návrhu.**

2.1.3 Pravidlá pre blokovanie IP adresných rozsahov pomocou BGP

Subjekt, ktorý môže rozhodnúť o blokovaní: Úrad ako národná autorita pre kybernetickú bezpečnosť.

Podmienky

- Blokovanie IP adries a IP adresných rozsahov pomocou BGP je krajným prostriedkom riešenia kybernetického bezpečnostného incidentu.

Blokovaniu musí predchádzať:

  - Evidencia a riešenie incidentu Národnou jednotkou CSIRT v zmysle platnej legislatívy a interných postupov, vrátane eskalačných a komunikačných mechanizmov medzi jednotlivými zložkami, ktorých účasť na riešení incidentu vyžaduje platná legislatíva,
  - po zistení škodlivého obsahu na dotknutej IP adrese alebo v rámci IP adresného rozsahu informovanie Národnej jednotky CSIRT,
  - komunikácia Národnej jednotky CSIRT s držiteľom a prevádzkovateľom IP adresy alebo IP adresného rozsahu,
  - poskytnutie možnosti na odstránenie škodlivého obsahu z dotknutej IP adresy prípadne IP adresného rozsahu (napríklad viac zasiahnutých IP adries v jednom IP adresnom rozsahu),
  - ak škodlivý obsah nebol odstránený do určenej lehoty, úrad vydá rozhodnutie o blokovaní IP adresy alebo IP adresného rozsahu a vytvorí na blokovacom serveri pravidlo, ktoré preberú smerovače ISP, ktoré majú s blokovacím serverom BGP peering,

- V prípade odstránenia škodlivého obsahu pred uplynutím lehoty úrad nevydá rozhodnutie o blokovaní a v súčinnosti s držiteľom a prevádzkovateľom IP adresy alebo IP adresného rozsahu pokračuje v ďalších fázach riešenia a koordinácie riešenia kybernetického bezpečnostného incidentu.

- Ak prišlo k blokovaniu IP adresy alebo IP adresného rozsahu a škodlivý obsah bol odstránený, držiteľ IP adresy alebo IP adresného rozsahu môže požiadať úrad o odblokovanie. Súčasťou takejto žiadosti musia byť dôkazy o odstránení škodlivého obsahu. Úrad takejto žiadosti, na základe predložených dôkazov a vlastnej analýzy, môže vyhovieť alebo žiadosť zamietnuť. O vyhovení žiadosti alebo jej zamietnutí vydá rozhodnutie, ktoré implementuje odstránením pravidla na blokovacom serveri.

Legislatívne podmienky

Zákon o kybernetickej bezpečnosti:

§ 5 ods. 1 písm. p) - úrad zabezpečuje a zodpovedá za koordinované riešenie kybernetických bezpečnostných incidentov na národnej úrovni,

§ 19 ods. 6 - Prevádzkovateľ základnej služby je ďalej povinný:

a) riešiť kybernetický bezpečnostný incident,
b) bezodkladne hlásiť závažný kybernetický bezpečnostný incident,
c) spolupracovať s úradom a ústredným orgánom pri riešení hláseného kybernetického bezpečnostného incidentu a na tento účel im poskytnúť potrebnú súčinnosť, ako aj informácie získané z vlastnej činnosti dôležité pre riešenie kybernetického bezpečnostného incidentu,

§ 22 ods. 3 - Poskytovateľ digitálnej služby je povinný:

a) hlásiť každý kybernetický bezpečnostný incident, ak disponuje informáciami, na základe ktorých je spôsobilý identifikovať, či má tento kybernetický bezpečnostný incident podstatný vplyv podľa osobitného predpisu, a to bezodkladne po jeho zistení,
b) riešiť hlásený kybernetický bezpečnostný incident,
c) spolupracovať s úradom pri riešení hláseného kybernetického bezpečnostného incidentu.

§ 27 ods. 1 - V prípade závažného kybernetického bezpečnostného incidentu alebo jeho hrozby môže úrad

a) vyhlásiť výstrahu a varovanie pred závažným kybernetickým bezpečnostným incidentom,
b) uložiť povinnosť riešiť kybernetický bezpečnostný incident,
c) uložiť povinnosť vykonať reaktívne opatrenie,
d) požadovať návrh ochranných opatrení a vykonanie ochranných opatrení.

§ 27 ods. 7 - Ochranné opatrenie prijíma prevádzkovateľ základnej služby na základe analýzy riešeného závažného kybernetického bezpečnostného incidentu.

§ 27 ods. 8 - Prevádzkovateľ základnej služby je na výzvu úradu v určenej lehote povinný predložiť navrhované ochranné opatrenie na schválenie. Úrad rozhodnutím navrhované opatrenie schváli a určí lehotu na jeho vykonanie. **V prípade, ak prevádzkovateľ základnej služby nenavrhne ochranné opatrenie v určenej lehote alebo ak je navrhované ochranné opatrenie zjavne neúspešné, je prevádzkovateľ základnej služby povinný spolupracovať s úradom, ústredným orgánom a s tým, kto prevádzkuje jednotku CSIRT, na jeho návrhu.**

2.1.4 Pravidlá blokovania IP adresných rozsahov, domén, URL a mailových adries publikovaním zoznamu, bez udania spôsobu blokovania

Subjekt, ktorý vydáva zoznam: Úrad ako národná autorita pre kybernetickú bezpečnosť.

Podmienky

- Úrad prostredníctvom národnej jednotky CSIRT monitoruje, agreguje a analyzuje indikátory kompromitácie vrátanie IP adries, domén a URL so škodlivým obsahom.

- Úrad pravidelne vydáva blacklisty s obsahom IP adries, domén a URL a mailových adries v strojovo čitateľnom formáte spolu s odporúčaním pre blokovanie týchto indikátorov z dôvodu ich škodlivosti.
- Úrad blacklisty distribuuje s prihliadnutím na dôvernosť údajov z blacklistov, ako aj aktív držiteľa alebo prevádzkovateľa, na ktorého IP adrese alebo doméne sa škodlivý obsah nachádza.
- 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.
- Ak sa úrad dozvie v rámci svojej analytickej činnosti, že na IP adrese, doméne alebo URL, ktorú zaradil do blacklistu, sa už škodlivý obsah nenachádza, vydá revíziu blacklistu, v ktorom sa už táto IP adresa, doména alebo URL nenachádza.
- Prevádzkovatelia základnej služby alebo poskytovatelia digitálnej služby pri blokovaní IP adresy primerane riešia zabezpečenie nekompromitovanej prevádzky z danej IP adresy.
- Ak je v blackliste uvedená IP adresa, doména, URL alebo e-mail, ktoré nie sú škodlivým obsahom alebo škodlivý obsah neobsahujú, držiteľ alebo správca môže predložiť národnej jednotke CSIRT jednoznačné dôkazy, ktoré takéto tvrdenia preukazujú. Národná jednotka CSIRT uvedenú IP adresu, doménu, URL alebo e-mail vyradí z blacklistu.

Legislatívne podmienky

Zákon o kybernetickej bezpečnosti:

§ 5 ods.1 písm. c) - úrad určuje zásady predchádzania kybernetickým bezpečnostným incidentom a zásady ich riešenia,

§ 5 ods. 1 písm. p) - zabezpečuje a zodpovedá za koordinované riešenie kybernetických bezpečnostných incidentov na národnej úrovni,

§ 5 ods. 1 písm. r) - úrad zasiela včasné varovania,

§ 27 ods. 1 - V prípade závažného kybernetického bezpečnostného incidentu alebo jeho hrozby môže úrad

a) vyhlásiť výstrahu a varovanie pred závažným kybernetickým bezpečnostným incidentom,

b) uložiť povinnosť riešiť kybernetický bezpečnostný incident,

c) uložiť povinnosť vykonať reaktívne opatrenie,

d) požadovať návrh ochranných opatrení a vykonanie ochranných opatrení.

2.2 Pravidlá pre obnovenie stavu pred blokovaním

Blokovanie škodlivého obsahu musí určovať aj pravidlá v prípade, ak bude škodlivý obsah odstránený a teda pominú dôvody na blokovanie.

Držiteľ alebo správca IP adresy alebo domény môže požiadať o odblokovanie, ak dostatočne preukáže, že sa na IP adrese alebo doméne škodlivý obsah už nenachádza. Takéto preukázanie je v niektorých prípadoch možné aj vyhlásením zo strany držiteľa alebo správcu IP adresy alebo domény o odstránení škodlivého obsahu.

Subjekt, ktorý blokovanie nariadil, je oprávnený pravidelne kontrolovať blokovaný obsah, ak je to z povahy technického riešenia možné. Ak sa počas tejto kontroly preukáže, že blokovanie už nie je potrebné z dôvodu absencie škodlivého obsahu, vykoná kroky k odblokovaniu:

1. subjekt, ktorý blokovanie nariadil, informuje subjekt, ktorý blokoval, že pominuli dôvody na blokovanie.
2. subjekt, ktorý blokoval škodlivý obsah, IP adresu alebo doménu odblokuje a informuje držiteľa a správcu.

2.3 Plán aplikácie pravidiel blokovania

Aplikácia pravidiel blokovania musí mať svoju postupnosť, a to najmä z hľadiska veľkosti prostredia, do ktorého majú byť aplikované, rozsahu legislatívnych zmien, ako aj z hľadiska nutnosti zabezpečenia náležitej technologickej infraštruktúry. Pre úspešnú implementáciu pravidiel je potrebné dodržať postupnosť jednotlivých fáz implementácie pravidiel do národného kybernetického priestoru:

1. fáza - implementácia pravidiel na úrovni vládnej siete GOVNET - jednotlivé pravidlá je v prvej fáze nutné aplikovať za účelom ochrany vládnej siete, pretože v rámci tejto siete je implementácia ucelených pravidiel jednoduchšia z technického aj legislatívneho hľadiska. V prvej fáze je teda možné otestovať limity jednotlivých pravidiel, procesy blokovania ako aj technologické prevedenie. Blokovanie sa v sieti GOVNET už využíva najmä na zablokovanie prichádzajúceho škodlivého obsahu, teda implementácia ostatných pravidiel bude jednoduchšia.
2. fáza - implementácia pravidiel na úrovni prevádzkovateľov základných služieb - ochrana informačnej infraštruktúry významných alebo kritických služieb nie len na úrovni štátu, ale aj pri poskytovaní významných služieb (elektrická energia, voda, zdravotná starostlivosť a podobne) je jednou zo základných pilierov bezpečnej spoločnosti. Preto implementáciu pravidiel blokovania na tejto úrovni možno považovať za krok, ktorý smeruje k zabezpečeniu vysokej miery bezpečnosti služieb a sietí prevádzkovateľov základných služieb.
3. fáza - implementácia pravidiel na celonárodnej úrovni - v národnom kybernetickom priestore je možné implementovať pravidlá blokovania až po odbornej diskusii s profesnými subjektami (Národná jednotka CSIRT – SK-CERT, jednotky CSIRT v pôsobnosti Úradu podpredsedu vlády Slovenskej republiky pre investície a informatizáciu, Policajný zbor SR, zástupcovia prevádzkovateľov základných služieb a poskytovateľov digitálnych služieb, akademická obec) a subjektami, ktoré budú samotné blokovanie aplikovať. To so sebou prináša aj zmeny v legislatíve, vydávanie metodík, úzku národnú spoluprácu a zodpovedajúce technologické zabezpečenie.

Použité skratky

BGP (Border Gateway Protocol) je štandardizovaný protokol vonkajšej brány určený na výmenu informácií o smerovaní a dostupnosti medzi autonómnymi systémami (AS) na internete.

CSIRT Tím na odozvu na incidenty v oblasti počítačovej bezpečnosti (CSIRT) je organizácia, ktorá dostáva správy o narušení bezpečnosti, vykonáva analýzy výkazov a reaguje na odosielateľov. CSIRT môže byť samostatnou organizáciou alebo ad hoc zhromaždením.

CERT je registrovaná ochranná známka Univerzity Carnegie Mellon (USA) používaná najmä pre národne CSIRTy.

DDoS (Distributed Denial of Service) je typ útoku, ktorého cieľom je zneprístupnenie alebo znefunkčnenie služby prevádzkovateľa. Princíp DDoS útokov spočíva vo využití viacerých zariadení, ktoré sú zapojené do tzv. siete internetových robotov (botnet) alebo zle nakonfigurovaných zariadení, ktoré umožňujú amplifikáciu útoku. Tieto zariadenia zasielajú súbežne svoje požiadavky na cieľ útočníka a ten z dôvodu veľkého dopytu prestane poskytovať službu.

DNS (Domain Name System) - je to hierarchický systém doménových mien, ktorý je realizovaný servermi DNS a protokolom rovnakého mena, ktorým si vymieňajú informácie. Jeho hlavnou úlohou a príčinou vzniku sú vzájomné prevody doménových mien a IP adries uzlov siete.

IP adresa - Internet Protocol address (adresa Internetového protokolu) - jedinečná číselná adresa, ktorá umožňuje jednoznačne identifikovať zariadenie pripojené v sieti a umožňuje tak komunikáciu medzi zariadeniami. Ak sa v texte nachádza skratka IP adresa, myslia sa tým aj IPv4 aj IPv6 adresy.

ISO OSI (Open Systems Interconnection model) je koncepčný model, ktorý charakterizuje a štandardizuje komunikačné funkcie telekomunikačného alebo výpočtového systému bez ohľadu na jeho vnútornú štruktúru a technológiu. Jeho cieľom je interoperabilita rôznych komunikačných systémov so štandardnými protokolmi. Model rozdeľuje komunikačný systém na abstrakčné vrstvy. Pôvodná verzia modelu definovala sedem vrstiev.

ISP (Internet service provider) Je to telekomunikačná firma - poskytovateľ internetového pripojenia.

TLD (Top Level Domain) Internetová doména najvyššej úrovne.

UDP (User Datagram Protocol) je nespojový datagramový protokol. Označuje sa ako „best effort“ protokol – protokol, ktorý neoveruje, či pakety prišli do cieľa a neposkytuje záruku, že prídu v poradí.

URL - Uniform Resource Locator (univerzálny ukazovateľ na zdroj) - ide v podstate o adresu webovej stránky.

VPN - (virtual private network) - Virtuálna privátna sieť. Je to prostriedok k pripojeniu niekoľko počítačov prostredníctvom (verejnej) nedôveryhodnej počítačovej siete.