

Návrh
Vyhláška
Národného bezpečnostného úradu
z2022

ktorou sa ustanovujú pravidlá blokovania

Národný bezpečnostný úrad podľa § 32 ods. 1 písm. i) zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov v znení zákona č. .../2022 Z. z. (ďalej len „zákon“) ustanovuje:

§ 1

- (1) Táto vyhláška ustanovuje pravidlá blokovania
- a) domén druhej úrovne na úrovni správcu národnej domény najvyššej úrovne (TLD),
 - b) domén na úrovni poskytovateľa internetového pripojenia (ISP),
 - c) IP adresných rozsahov pomocou smerovacieho protokolu Border Gateway Protocol (BGP),
 - d) IP adresných rozsahov, domén, funkčných priamych odkazov vo forme Uniform Resource Locator (URL) a mailových adries publikovaním zoznamu, bez udania spôsobu blokovania.
- (2) Blokovat' možno najmä
- a) adresu sieťového protokolu Internet Protocol (IP), doménu alebo URL, na ktorých sa nachádza
 - 1. phishingová stránka alebo server riadiaci phishingové aktivity,
 - 2. škodlivý kód alebo škodlivá aktivita,
 - 3. riadiaci server pre riadenie botnetovej siete a
 - b) IP adresu alebo doménu, prostredníctvom ktorej sa vykonáva
 - 1. útok typu Distributed Denial of Service (DDoS),
 - 2. skenovanie,
 - 3. bruteforce útoky alebo pokusy,
 - 4. pokusy o prienik.

§ 2

(1) Blokovanie domény na úrovni správcu národnej TLD sa využíva pri závažných kybernetických bezpečnostných incidentoch II. a III. stupňa a incidentoch s cezhraničným presahom, ak je zo všetkých okolností zrejmé, že postupom podľa osobitných predpisov nedôjde k bezodkladnému uskutočneniu nápravy, a účel nie je možné dosiahnuť inak.

- (2) Blokovaniu predchádza
- a) informovanie Národnej jednotky CSIRT o zistení škodlivého obsahu na dotknutej doméne,
 - b) evidovanie a riešenie incidentu Národnou jednotkou CSIRT podľa zákona a interných postupov, vrátane eskalačných a komunikačných mechanizmov medzi jednotlivými zložkami, ktorých účasť na riešení incidentu vyžaduje zákon,

- c) komunikácia Národnej jednotky CSIRT s držiteľom a prevádzkovateľom domény,
- d) umožnenie držiteľovi alebo prevádzkovateľovi domény odstránenie škodlivého obsahu z dotknutej domény v určenej lehote.

(3) Ak dôjde k odstráneniu škodlivého obsahu pred uplynutím určenej lehoty v súčinnosti s držiteľom alebo prevádzkovateľom domény sa pokračuje v ďalších fázach riešenia a koordinácie riešenia kybernetického bezpečnostného incidentu.

(4) Ak škodlivý obsah nie je odstránený do určenej lehoty, vydá sa rozhodnutie o blokovaní domény podľa § 27b zákona, na základe ktorého správca národnej TLD vykoná blokovanie domény.

§ 3

(1) Blokovanie domény na úrovni ISP sa využíva, ak je zo všetkých okolností zrejmé, že postupom podľa osobitných predpisov nedôjde k bezodkladne k náprave, a účel nie je možné dosiahnuť inak.

- (2) Blokovaniu predchádza
- a) informovanie Národnej jednotky CSIRT o zistení škodlivého obsahu na dotknutej doméne,
 - b) evidovanie a riešenie incidentu Národnou jednotkou CSIRT podľa zákona a interných postupov, vrátane eskalačných a komunikačných mechanizmov medzi jednotlivými zložkami, ktorých účasť na riešení incidentu vyžaduje zákon,
 - c) komunikácia Národnej jednotky CSIRT s držiteľom a prevádzkovateľom domény na úrovni ISP,
 - d) umožnenie držiteľovi alebo prevádzkovateľovi domény odstránenie škodlivého obsahu z dotknutej domény na úrovni ISP v určenej lehote.

(3) Ak dôjde k odstráneniu škodlivého obsahu pred uplynutím určenej lehoty v súčinnosti s držiteľom alebo prevádzkovateľom domény sa pokračuje v ďalších fázach riešenia a koordinácie riešenia kybernetického bezpečnostného incidentu.

(4) Ak škodlivý obsah nie je odstránený do určenej lehoty, vydá sa rozhodnutie o blokovaní domény na úrovni ISP podľa § 27b zákona, na základe ktorého ISP presmeruje škodlivú doménu na špeciálnu internetovú stránku, na ktorej sa vysvetlia dôvody blokovania dotknutej domény.

§ 4

(1) Blokovanie IP adries a IP adresných rozsahov pomocou BGP sa využíva, ak je zo všetkých okolností zrejmé, že postupom podľa osobitných predpisov nedôjde k bezodkladnému uskutočneniu nápravy, a účel nie je možné dosiahnuť inak.

- (2) Blokovaniu predchádza
- a) informovanie Národnej jednotky CSIRT o zistení škodlivého obsahu na dotknutej doméne
 - b) evidovanie a riešenie incidentu Národnou jednotkou CSIRT podľa zákona a interných postupov, vrátane eskalačných a komunikačných mechanizmov medzi jednotlivými zložkami, ktorých účasť na riešení incidentu vyžaduje zákon,

- c) komunikácia Národnej jednotky CSIRT s držiteľom a prevádzkovateľom IP adresy alebo IP adresného rozsahu,
- d) umožnenie odstránenia škodlivého obsahu z dotknutej IP adresy alebo IP adresného rozsahu (napríklad viac zasiahnutých IP adries v jednom IP adresnom rozsahu).

(3) Ak dôjde k odstráneniu škodlivého obsahu pred uplynutím určenej lehoty v súčinnosti s držiteľom alebo prevádzkovateľom domény sa pokračuje v ďalších fázach riešenia a koordinácie riešenia kybernetického bezpečnostného incidentu.

(4) Ak škodlivý obsah nie je odstránený do určenej lehoty, vydá sa rozhodnutie o blokovanií IP adresy alebo IP adresného rozsahu podľa § 27b zákona, na základe ktorého ISP blokuje IP adresu alebo IP adresný rozsah so škodlivým obsahom prostredníctvom BGP protokolu.

§ 5

Účely blokovania IP adresných rozsahov, domén, URL a mailových adries sa pravidelne zverejňujú v zoznamoch (blacklisty), ktoré

- a) vychádzajú z monitoringu, agregácie a analýzy indikátorov kompromitácie vrátane IP adries, domén a URL so škodlivým obsahom,
- b) obsahujú IP adresy, domény, URL a mailové adresy v strojovo čitateľnom formáte spolu s odporúčaním pre blokovanie týchto indikátorov z dôvodu ich škodlivosti
- c) zohľadňujú dôvernosť údajov, ako aj aktív držiteľa alebo prevádzkovateľa, na ktorého IP adrese alebo doméne sa škodlivý obsah nachádza,
- d) obsahujú len informácie o indikátoroch, ktoré sú spojené so šírením škodlivého obsahu alebo sa na týchto indikátoroch nachádza škodlivý obsah,
- e) sa revidujú po odstránení škodlivého obsahu z IP adresy, domény alebo URL.

§ 6

Táto vyhláška nadobúda účinnosť dňom vyhlásenia.