**....**

**V YHLÁŠKA**

**Národného bezpečnostného úradu**

z ............

**Pravidlá blokovania**

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

## **§ 1**

## **Pravidlá pre blokovanie**

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.

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.

###

### **§2**

### **Pravidlá pre blokovanie domén druhej úrovne na úrovni správcu národnej TLD**

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:
	+ po zistení škodlivého obsahu na dotknutej doméne informovanie Národnej jednotky CSIRT,
	+ komunikácia Národnej jednotky CSIRT s majiteľom 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 majiteľom 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, majiteľ 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.

###

### **§ 3**

### **Pravidlá pre blokovanie domén na úrovni ISP**

Podmienky

* Blokovanie domény na úrovni ISP je krajným prostriedkom riešenia kybernetického bezpečnostného incidentu.
* Blokovaniu musí predchádzať:
	+ po zistení škodlivého obsahu na dotknutej doméne akejkoľvek úrovne informovanie Národnej jednotky CSIRT,
	+ komunikácia Národnej jednotky CSIRT s majiteľom 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 majiteľom 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, majiteľ 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.

### **§4**

### **Pravidlá pre blokovanie IP adresných rozsahov pomocou BGP**

Podmienky

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

Blokovaniu musí predchádzať:

* + po zistení škodlivého obsahu na dotknutej IP adrese alebo v rámci IP adresného rozsahu informovanie Národnej jednotky CSIRT,
	+ komunikácia Národnej jednotky CSIRT s majiteľom 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,
	+ rozhodnutie sa oznámi ISP, ktorý je povinný blokovať IP adresu alebo IP adresný rozsah so škodlivým obsahom prostredníctvom BGP protokolu.
* V prípade odstránenia škodlivého obsahu pred uplynutím lehoty úrad nevydá rozhodnutie o blokovaní a v súčinnosti s majiteľom 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, majiteľ 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 zašle ISP, ktorý IP adresu alebo IP adresný rozsah zablokoval.

###

### **§5**

### **Pravidlá blokovania IP adresných rozsahov publikovaním zoznamu, bez udania spôsobu blokovania**

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 spolu s odporúčaním pre blokovanie týchto indikátorov z dôvodu ich škodlivosti.
* 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.

**§ 6**

Táto vyhláška nadobúda účinnosť ........

**Roman Konečný v. r.**