OPATRENIE

Telekomunikačného úradu Slovenskej republiky

z 18. mája 2012, č. O-30/2012,

ktorým sa ustanovujú podrobnosti o udržiavaní bezpečnosti a integrity verejných elektronických komunikačných sietí alebo verejných elektronických komunikačných služieb

Telekomunikačný úrad Slovenskej republiky (ďalej len „úrad“) podľa § 64 ods. 7 zákona č.351/2011 Z. z. o elektronických komunikáciách (ďalej len „zákon“) ustanovuje:

§ 1
ZÁKLADNÉ USTANOVENIA

(1) Na ochranu bezpečnosti alebo udržanie integrity elektronickej komunikačnej siete (ďalej len „sieť“) alebo elektronickej komunikačnej služby (ďalej len „služba“) podnik poskytujúci verejné siete alebo verejné služby na základe všeobecného povolenia na poskytovanie sietí a služieb a oznámenia podľa § 15 zákona (ďalej len „podnik“) prijíma a dodržuje technické a organizačné opatrenia (ďalej len „bezpečnostné opatrenie“) najmenej v rozsahu minimálnych bezpečnostných opatrení podľa § 2.

(2) Bezpečnosť siete je súbor opatrení na prevenciu a monitorovanie neoprávneného vstupu do siete, zneužitia, úpravy a prístupu k dátam v sieti. Integrita siete je schopnosť siete ponechať si svoje špecifické vlastnosti z hľadiska výkonu a funkčnosti.

(3) Bezpečnostný incident je každá udalosť narušujúca akýmkoľvek spôsobom bezpečnosť sietí alebo služieb alebo integritu sietí, ktorých sa týka.

(4) Podnik uplatňuje bezpečnostné opatrenia na všetky svoje aktíva[1)], ktorých narušenie alebo zlyhanie môže mať významný negatívny účinok na bezpečnosť alebo integritu sietí alebo služieb poskytovaných podnikom. Bezpečnostné opatrenia prijíma podnik v rozsahu primeranom k riziku ohrozenia aktív podľa bezpečnostnej politiky podniku.

§ 2
MINIMÁLNE BEZPEČNOSTNÉ OPATRENIA

(1) Minimálne bezpečnostné opatrenia pre jednotlivé oblasti bezpečnosti stanovujú základné parametre pre udržiavanie integrity siete a sú obsahom zdokumentovaných bezpečnostných politík podniku.

(2) Minimálne bezpečnostné opatrenia pre riadenie bezpečnosti a manažment rizík sú

a) vypracovanie, schválenie, uplatňovanie a aktualizovanie bezpečnostnej politiky podniku,

b) vypracovanie rámca na identifikáciu a riadenie bezpečnostných rizík podniku a jeho udržiavanie,

c) stanovenie organizačnej štruktúry riadenia bezpečnosti, definovanie bezpečnostných úloh a zodpovedností zamestnancov podniku a iných strán, ktoré vykonávajú činnosti pre podnik na základe zmluvných vzťahov (ďalej len „tretia strana“),

d) stanovenie bezpečnostných požiadaviek na siete alebo služby poskytované podniku tretími stranami.

[1)] § 2 ods. 4 písm. i) zákona č. 431/2002 Z. z. o účtovníctve v znení neskorších predpisov.

e) prijatie postupov na riadenie aktív súvisiacich s prevádzkou sietí a služieb podniku

(3) Minimálne bezpečnostné opatrenia pre personálnu bezpečnosť sú

a) oboznámenie zamestnancov podniku a tretích strán s bezpečnostnou politikou podniku v rozsahu potrebnom na výkon ich činnosti pre podnik, spravidla na základe zmluvy,

b) organizovanie školení pre zamestnancov podniku na udržanie a zdokonaľovanie ich bezpečnostných znalostí a zručností,

c) vypracovanie bezpečnostných postupov súvisiacich s personálnymi zmenami zamestnancov podniku alebo so zmenami v zmluvných vzťahoch s tretími stranami,

d) vypracovanie postupov na disciplinárne konania vo vzťahu k zamestnancom, ktorí spôsobili narušenie bezpečnosti alebo integrity sietí alebo služieb podniku.

(4) Minimálne bezpečnostné opatrenia pre bezpečnosť systémov a zariadení sú

a) zaistenie fyzickej bezpečnosti a bezpečnosti prostredia pre zariadenia a infraštruktúru sietí a služieb,

b) zabezpečenie ochrany pred výpadkom napájania a podporných prostriedkov, od ktorých závisí prevádzka sieťových a informačných systémov,

c) riadenie prístupu do sieťových a informačných systémov, ak je to technicky možné.

(5) Minimálne bezpečnostné opatrenia pre riadenie prevádzky sú

a) vypracovanie prevádzkových postupov a určenie zodpovednosti na riadenie prevádzky sieťových a informačných systémov,

b) vytvorenie postupov na riadenie zmien a aktualizácií sieťových a informačných systémov.

(6) Minimálne bezpečnostné opatrenia pre manažment bezpečnostných incidentov sú

a) uplatňovanie systému bezpečnosti, vypracovanie štandardov a postupov manažmentu bezpečnostných incidentov,

b) zavedenie monitorovacích a kontrolných postupov na odhalenie bezpečnostných incidentov,

c) vypracovanie postupov reakcie na rôzne druhy bezpečnostných incidentov,

d) vypracovanie postupov na ohlasovanie bezpečnostných incidentov v rámci podniku a postupov na komunikáciu s obchodnými partnermi, účastníkmi a verejnosťou.

(7) Minimálne bezpečnostné opatrenia pre riadenie dostupnosti sietí a služieb podniku sú

a) vypracovanie stratégie a krízových plánov na zabezpečenie dostupnosti sietí alebo služieb po narušení alebo zlyhaní kritických procesov podniku,

b) vytvorenie a udržiavanie záložných prostriedkov na obnovu sietí alebo služieb po narušení alebo zlyhaní kritických procesov podniku, ak je to technicky možné.

(8) Minimálne bezpečnostné opatrenia pre monitorovanie, testovanie bezpečnosti a bezpečnostné audity sú

a) vytvorenie postupov na monitorovanie a zaznamenávanie činností obsluhy sieťových a informačných systémov,

b) vypracovanie postupov na preverenie záloh a precvičovanie krízových plánov,

c) vypracovanie politiky na posúdenie a testovanie zabezpečenia špecifikovaných aktív podniku a testovacích scenárov,

d) uskutočňovanie interných bezpečnostných auditov.

§ 3

Cieľom oznamovacej povinnosti podnikov podľa § 64 ods. 3 zákona pri narušení bezpečnosti alebo integrity s významným vplyvom na prevádzku sietí alebo služieb je poskytnúť úradu podstatné informácie o vzniknutých bezpečnostných incidentoch podľa prílohy č. 1 na

a) sledovanie výskytu bezpečnostných incidentov a reakcií podnikov na tieto incidenty na národnej úrovni, s cieľom zamedziť opakovaniu bezpečnostných incidentov a chrániť záujmy koncových užívateľov,

b) informovanie Európskej agentúry pre bezpečnosť sietí a informácií (ENISA)[2)] o vzniku bezpečnostných incidentov podliehajúcich hláseniu, ako aj informovanie zainteresovaných domácich podnikov a partnerských regulačných orgánov v členských štátoch Európskej únie a štátoch, ktoré sú zmluvnými stranami Dohody o Európskom hospodárskom priestore.

HLÁSENIE BEZPEČNOSTNÝCH INCIDENTOV

§ 4

(1) Bezpečnostný incident oznamuje podnik úradu prostredníctvom hlásenia bezpečnostného incidentu v elektronických komunikáciách podľa prílohy č. 1 (ďalej len „hlásenie“). Podnik podáva úradu hlásenie bezodkladne po zistení významného bezpečnostného incidentu.

(2) Hláseniu nepodliehajú plánované výpadky siete v rámci výluky určené na údržbu, rozvoj siete a iné technické zásahy, ktoré obmedzia poskytovanie služieb účastníkom.

(3) Hláseniu podliehajú len tie bezpečnostné incidenty, ktoré majú významný vplyv na prevádzku sietí alebo služieb poskytovaných podnikom (ďalej len „významný bezpečnostný incident“).

(4) Parametre na posúdenie, či ide o významný bezpečnostný incident, sú uvedené v prílohe č. 2.

(5) Pokiaľ do doby odoslania hlásenia nepominuli účinky incidentu alebo nedošlo k ukončeniu nápravných opatrení, podnik

a) odošle neúplne vyplnené hlásenie, v ktorom vyznačí identifikátor neukončeného hlásenia,

b) po obnove normálnej prevádzky siete alebo služby pošle úradu bezodkladne, najneskôr však do piatich dní, ďalšie hlásenie s vyznačeným indikátorom doplnkového hlásenia týkajúce sa predmetného incidentu, doplnené o chýbajúce skutočnosti a rozsah vykonaných nápravných opatrení.

(6) Hlásenie sa podáva elektronicky s využitím šifrovania alebo iným náhradným spôsobom podľa pokynov úradu pri poskytnutí údajov podľa § 5.

§ 5

(1) Podnik do 30 dní od nadobudnutia účinnosti tohto opatrenia alebo od začatia poskytovania siete alebo služby oznámi úradu písomne údaje o kontaktnej osobe v oblasti bezpečnosti a integrity sietí alebo služieb (ďalej len „kontaktná osoba“) v rozsahu

a) meno, priezvisko,

b) telefónne číslo a adresa elektronickej pošty,

c) adresa na zasielanie listinných dokumentov.

(2) Podnik písomne oznamuje úradu bezodkladne každú zmenu v údajoch kontaktnej osoby.

[2)] Nariadenie Európskeho parlamentu a Rady (ES) č. 460/2004 z 10. marca 2004 o zriadení Európskej agentúry pre bezpečnosť sietí a informácií (ENISA) v platnom znení.

§ 6

POSKYTOVANIE INFORMÁCIÍ

Podnik na žiadosť úradu poskytuje podstatné informácie na posúdenie bezpečnosti a integrity svojich sietí a služieb v písomnej forme do 60 dní od doručenia žiadosti. Za podstatné informácie sa považujú

a) informácie o plnení minimálnych bezpečnostných požiadaviek podľa § 2 potrebných na posúdenie bezpečnosti alebo integrity svojich služieb a sietí vrátane zdokumentovaných bezpečnostných politík podniku,

b) osvedčenie o vykonaní bezpečnostného auditu týkajúce sa bezpečnosti sietí a služieb podniku,

c) aktíva podniku, na ktoré sa uvedené opatrenia vzťahujú.

§ 7

Toto opatrenie nadobúda účinnosť 1. júla 2012.

Ladislav Mikuš

predseda Telekomunikačného úradu Slovenskej republiky

Príloha č. 1 k opatreniu č. O-30/2012

FORMULÁR HLÁSENIA BEZPEČNOSTNÉHO INCIDENTU

HLÁSENIE BEZPEČNOSTNÉHO INCIDENTU V ELEKTRONICKÝCH KOMUNIKÁCIÁCH

pre Telekomunikačný úrad Slovenskej republiky

Poradové číslo: ..... Dátum: .....

☐ Neukončené hlásenie

☐ Doplňujúce hlásenie k hláseniu číslo ..... zo dňa: .....

1 Identifikácia podniku		
1.1 Názov:		
1.2 IČO:		
1.3 Kontaktná osoba:	tel.č.:	e-mailová adresa:

2 Časové údaje incidentu	
2.1 Zistenie incidentu dátum: čas:	2.3 Ukončenie incidentu dátum: čas:
2.2 Vznik incidentu dátum: čas:	2.4 Obnova prevádzky s náhradnými prostriedkami dátum: čas:
	2.5 Úplná obnova prevádzky dátum: čas:

3 Príčiny incidentu a nápravné opatrenia			
3.1 Prvotná príčina			
3.1.1 Prírodná katastrofa	☐	3.1.4 Technická/programová porucha	☐
3.1.2 Ľudský omyl	☐	3.1.5 Externé zlyhanie	☐
3.1.3 Úmyselný útok	☐	3.1.6 Iné	☐
3.2 Opis incidentu:			
3.3 Vykonané nápravné opatrenia:			
3.4 Opatrenia na zamedzenie opakovania incidentu:			

4 Následky bezpečnostného incidentu
4.1 Prvotne zasiahnuté aktíva:
4.2 Narušené siete 4.2.1 Pevná ☐ 4.2.3 Družicová ☐ 4.2.2 Mobilná ☐ 4.2.4 Iná ☐ uveďte:
4.3 Narušené služby 4.3.1 Telefónna ☐ 4.3.2 Iná hlasová ☐ uveďte: 4.3.3 Prenájom okruhov ☐ 4.3.4 Prenos dát ☐ uveďte: 4.3.5 Prístup k internetu ☐ 4.3.6 Tiesňové volania ☐ 4.3.7 Iná ☐ uveďte:
4.4 Postihnuté územie/región:
4.5 Informované podniky a účastníci:
4.6 Účastníci 4.6.1 Celkový počet účastníkov služby : 4.6.2 Percento zasiahnutých účastníkov: 4.6.3 Dôležití účastníci ☐ uveďte:
5 Poznámky

Pokyny na vyplňovanie hlásenia:

Poradové číslo: Uvedie sa poradové číslo hlásenia o narušení bezpečnosti v priebehu dňa.

Dátum: Uvedie sa dátum odosielania hlásenia.

Neukončené hlásenie: Označí sa, ak podnik do doby odoslania hlásenia neodstránil úplne následky narušenia bezpečnosti alebo predpokladá neskoršie zaslanie doplňujúcich informácií k bezpečnostnému incidentu.

Doplňujúce hlásenie: Označí sa v prípade, ak ide o doplňujúce hlásenie k hláseniu identifikovanému číslom a dátumom, ktorý sa uvedie v položke „*k hláseniu číslo:... zo dňa:....* “. Doplňujúce hlásenie obsahuje vzhľadom k pôvodnému neukončenému hláseniu nielen nové údaje, ale aj všetky údaje uvedené v pôvodnom hlásení, v prípade potreby aktualizované.

1.1 Názov: Uvedie sa názov podniku

1.2 IČO: Uvedie sa identifikačné číslo organizácie.

1.3 Kontaktná osoba: Uvedie sa meno, priezvisko a kontaktné údaje (tel. č. – telefónne číslo, e-mailová adresa) osoby, ktorá posiela hlásenie a je zodpovedná za jeho obsah (určená kontaktná osoba podniku, prípadne jej zástupca).

2.1 Zistenie narušenia: Uvedie sa dátum a čas zistenia bezpečnostného incidentu.

2.2 Vznik narušenia: Uvedie sa dátum a čas vzniku bezpečnostného incidentu (pokiaľ sú tieto údaje známe).

2.4. Obnova prevádzky s náhradnými prostriedkami: Ak vplyvom narušenia bezpečnosti došlo k prerušeniu prevádzky siete alebo služby, uvedie sa dátum a čas obnovy prevádzky siete alebo poskytovania služby s použitím náhradných prostriedkov.

2.5. Úplná obnova prevádzky: Uvedie sa dátum a čas úplného uvedenia aktív podniku do stavu pred narušením bezpečnosti.

3.1 Prvotná príčina: Vyznačí sa prvotná príčina, ktorá vyvolala narušenie bezpečnosti, ako jedna zo základných príčin 3.1.1 až 3.1.5.a iné príčiny 3.1.6.

3.2 Opis incidentu: Uvedie sa opis bezpečnostného incidentu s využitím príkladov podkategórií prvotných príčin, prípadne uvedením ďalších detailov príčiny bezpečnostného incidentu. Podkategórie základných prvotných príčin môžu byť napríklad:

1. Prírodná katastrofa:
    a) extrémy počasia (možné spresniť - búrka, snehová kalamita, víchrica,...),
    b) zemetrasenie,
    c) zosuv pôdy,
    d) povodeň,
    e) požiar,
    f) účinky kozmických javov (magnetické búrky, slnečné erupcie,...)
    g) pandémia a iné.
2. Ľudský omyl:
    a) chybné rozmiestnenie alebo konfigurácia
        - sieťových zariadení,
        - platforiem,
        - aplikácií,
        - záloh,
        - databáz.

b) nesprávny postup

- nastavenia konfiguračných parametrov,
- riadenia prístupu a priradenie identity a pod.

3. Úmyselný útok:
   a) neoprávnený logický prístup k sieťovým a informačným systémom a s ním spojené manipulovanie s dátami, aplikáciami, procesmi, dokumentáciou, prenášanými informáciami a pod.,
   b) útok na informačné systémy, vírusy, spyware a pod.,
   c) náhle zvýšenie prevádzky v sieti (spamy, cielené útoky),
   d) neoprávnený fyzický prístup k technickému vybaveniu a do zariadení s umiestnenými informačnými systémami,
   e) krádež zariadení alebo médií a iné.
4. Technická/programová porucha:
   a) chyba technického vybavenia,
   b) chyba programu a pod.
5. Externé zlyhanie:
   a) porucha zapríčinená osobami tretej strany (napr. preseknutie kábla...),
   b) zlyhanie externého procesu s účinkom na podnikový proces,
   c) zlyhanie dodávateľov a pod.

3.3 Vykonané nápravné opatrenia: Uvedú sa činnosti, ktoré podnik vykonal po zistení bezpečnostného incidentu a opatrenia na obnovu siete alebo služby (aj s využitím náhradných prostriedkov).

3.4 Opatrenia na zamedzenie opakovania incidentu: Uvedie sa opis opatrení, ktoré podnik prijal na minimalizovanie úrovne rizika opakovania bezpečnostného incidentu.

4.1 Prvotne zasiahnuté aktíva: Uvedú sa tie aktíva podniku, ktoré boli prvotne zasiahnuté bezpečnostným incidentom (nie aktíva následne zasiahnuté reťazovou reakciou, ktorá môže končiť napríklad nedostupnosťou určitej služby).

4.2. Narušené siete: Označia sa siete 4.2.1 až 4.2.4, pri ktorých došlo k narušeniu bezpečnosti alebo strate integrity. Pokiaľ sa zvolí položka 4.2.4 (iná), uvedie sa aj spresnenie, o akú sieť sa jedná.

4.3. Narušené služby: Označia sa služby 4.3.1 až 4.3.7 (aj viac súčasne), ktoré sa vplyvom narušenia bezpečnosti stali nedostupné (úplne alebo so zníženou kvalitou) pre koncových užívateľov. Pri položkách 4.3.2 (iná hlasová, napríklad VoIP, tranzit volaní a pod.), 4.3.4 (prenos dát, napríklad MMS, SMS, e-mail a iné) a 4.3.7 (iná) sa uvedie aj spresnenie, o akú službu sa jedná.

4.4 *Postihnuté územie/región*: Predstavuje minimálne tri navzájom susediace primárne oblasti pre fixnú sieť a minimálne tri navzájom susediace základňové stanice pre mobilnú sieť. Ak nastali, uvedú sa účinky bezpečnostného incidentu na siete alebo služby aj iných podnikov.

4.5 *Informované podniky a účastníci:* Uvedú sa podniky a účastníci (rámcovo, napr. všetci účastníci služby ..., v lokalite...), ktorí boli informovaní o narušení bezpečnosti.

4.6.1 *Celkový počet účastníkov služby:* Uvedie sa celkový počet účastníkov služby, ktorá bola zasiahnutá bezpečnostným incidentom.

4.6.2 *Percento zasiahnutých účastníkov:* Uvedie sa percento zasiahnutých účastníkov z celkového počtu účastníkov služby. Ak nie je možné zistiť presný počet zasiahnutých účastníkov, napríklad pri službách poskytovaných prostredníctvom mobilných sietí, uvedie sa ich kvalifikovaný odhad.

4.6.3 *Dôležití účastníci:* Ak ide o dôležitých účastníkov, označí sa indikátor a uvedie sa spresnenie, o koho sa jedná.

5 *Poznámky:* Uvedú sa ďalšie doplňujúce informácie k bezpečnostnému incidentu, nápravným opatreniam a pod., ktoré podnik považuje za dôležité pre úrad, iné podniky alebo medzinárodné inštitúcie v záujme zdokonaľovania bezpečnosti sietí alebo služieb.

Príloha č. 2 k opatreniu č. O-30/2012

PARAMETRE URČUJÚCE VÝZNAMNÝ BEZPEČNOSTNÝ INCIDENT

Parametre na posúdenie významného bezpečnostného incidentu:

1. celkový počet účastníkov podniku,
2. percento postihnutých účastníkov služby, ktoré vyjadruje percento účastníkov postihnutých účinkami bezpečnostného incidentu z celkového počtu účastníkov,
3. trvanie účinku bezpečnostného incidentu; doba, počas ktorej bola narušená bezpečnosť siete alebo služby alebo počas ktorej bola služba koncovým užívateľom nedostupná alebo poskytovaná s výrazne zníženou úrovňou kvality oproti bežným prevádzkovým podmienkam (ďalej len „nedostupnosť služby“),
4. veľkosť postihnutého územia alebo regiónu,
5. nedostupnosť služby tiesňových volaní; doba, počas ktorej je služba tiesňových volaní nedostupná pre koncových užívateľov,
6. nedostupnosť služby pre dôležitých účastníkov služby; doba, počas ktorej je služba nedostupná pre dôležitých účastníkov, pričom za dôležitých účastníkov sa pokladajú
   - ministerstvá a ostatné ústredné orgány štátnej správy,
   - mestá a samosprávne kraje.

Významným bezpečnostným incidentom je narušenie bezpečnosti siete alebo služby alebo strata integrity siete pre podnik, ktorý má viac ako 2000 účastníkov, pri ktorých:

1. hodnota parametra počet postihnutých účastníkov a súčasne hodnota parametra trvanie účinku bezpečnostného incidentu je v oblasti významných bezpečnostných incidentov podľa tabuľky 1.

	1 h < D < 2 h	2 h < D < 4 h	4 h < D < 6 h	6 h < D < 8 h	D > 8 h
1 % < n ≤ 2%					▨
2 % < n ≤ 5 %				▨	▨
5 % < n ≤ 10 %			▨	▨	▨
10 % < n ≤ 15 %		▨	▨	▨	▨
n > 15 %	▨	▨	▨	▨	▨

vysvetlivky: n - počet postihnutých účastníkov,
D - trvanie účinku bezpečnostného incidentu v hodinách,
▨ - oblasť významných bezpečnostných incidentov

Tabuľka 1- Medzné hodnoty parametrov - počet postihnutých účastníkov a trvanie účinku bezpečnostného incidentu.

2. nedostupnosť služby tiesňových volaní pre viac ako 0,1 % účastníkov trvá dlhšie ako 1 hodinu,
3. nedostupnosť služby pre dôležitých účastníkov trvá dlhšie ako 2 hodiny,
4. nedostupnosť služby na území najmenej jednej primárnej oblasti pre pevné siete a oblasť najmenej troch navzájom susediacich základňových staníc pre mobilné siete.