Príloha č. 6

Bezpečnostné politiky a bezpečnostné opatrenia ma zabezpečenie kybernetickej bezpečnosti

Základným poslaním Objednávateľa, ako prevádzkovateľa základnej služby podľa ust. § 3 písm. k) zákona č. 69/2018 Z.z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej len „**ZoKB**“), je bezpečná, spoľahlivá a efektívna preprava zemného plynu na územie Slovenskej republiky a na európske trhy. Objednávateľ garantuje prístup do prepravnej siete na území SR transparentným a nediskriminujúcim spôsobom a zabezpečuje komplexné služby v oblasti prepravy zemného plynu.

Súvisiacim poslaním Objednávateľa je spoľahlivo uspokojovať oprávnené požiadavky zákazníkov za každej situácie, v najvyššej kvalite a zodpovedajúcej cene, za súčasného plnenia opatrení na ochranu života a zdravia osôb, životného prostredia a majetkových hodnôt.

Úspešné plnenie poslania Objednávateľa závisí aj od intenzívneho využívania sietí a informačných systémov, ktorých primeraná bezpečnosť je nutnou podmienkou ich efektívnej prevádzky.

Minimálne požiadavky na zabezpečenie bezpečnosti sietí a informačných systémov prevádzkovateľov základných služieb v kybernetickom priestore (ďalej tiež ako „**Kybernetická bezpečnosť**“) stanovuje ZoKB a ďalšie všeobecne záväzné predpisy vydané na vykonanie ZoKB. Na základe ZoKB bola do právneho poriadku SR prebratá Smernica Európskeho parlamentu a Rady (EÚ) 2016/1148 zo 6. júla 2016 o opatreniach na zabezpečenie vysokej spoločnej úrovne bezpečnosti sietí a informačných systémov v Únii.

Ochrana informácií a riadenie bezpečnosti systémov informačných technológií vo vnútri spoločností je tiež obsiahnutá v medzinárodnej technickej norme STN ISO/IEC 27000 Systémy riadenia informačnej bezpečnosti, ktorá vymedzuje základné bezpečnostné ciele smerovania bezpečnostných aktivít a zásady, požiadavky a opatrenia na ich splnenie.

V súlade so ZoKB a Vyhláškou Národného bezpečnostného úradu č. 362/2018 Z.z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení (ďalej len „**Vyhláška**“), Objednávateľ prijíma bezpečnostné politiky a všeobecné bezpečnostné opatrenia na zabezpečenie Kybernetickej bezpečnosti, ktorých účelom je stanoviť základné princípy, postupy a bezpečnostné ciele Objednávateľa.

I. Bezpečnostné politiky

Bezpečnostné politiky určujú ciele, ktoré je potrebné na základe výsledkov analýzy rizík Kybernetickej bezpečnosti dosiahnuť a základné smerovanie bezpečnostných aktivít v oblasti bezpečnosti sietí a informačných systémov Objednávateľa.

Hlavné ciele:

1) Minimalizovať možnosti narušenia prevádzky využívaných informačných sietí a informačných systémov.
2) Minimalizovať možné straty a dopady z narušenia prevádzky využívaných sietí a informačných systémov.

Následné ciele:

1) Zabezpečovať primeranými technickými, organizačnými a personálnymi opatreniami

ochranu klasifikovaných údajov (najmä osobné údaje, obchodné, daňové a telekomunikačné tajomstvo) v sieťach a informačných systémoch pred odcudzením, stratou, poškodením, neoprávneným prístupom, zmenou a rozširovaním, v súlade s požiadavkami legislatívy SR a interných riadiacich aktov.

2) Vybudovať ucelený Systém riadenia informačnej a komunikačnej bezpečnosti v súlade s najlepšími praktikami, napr. požiadavkami normy ISO/IEC 27002:2014, s odpovedajúcim technickým, organizačným a personálnym zabezpečením.

II. Bezpečnostné opatrenia

Zhotoviteľ prijíma a/alebo určuje úlohy, procesy, role a technológie v organizačnej, personálnej a technickej oblasti (pre účely tohto článku ďalej len „**Bezpečnostné opatrenia**“) v rozsahu Bezpečnostných opatrení prijatých Objednávateľom so zreteľom na najnovšie poznatky, náklady na vykonanie opatrení a na povahu, rozsah, kontext a účel predmetu plnenia podľa tejto Zmluvy a s cieľom predchádzať kybernetickým bezpečnostným incidentom a minimalizovať vplyv kybernetických bezpečnostných incidentov na kontinuitu prevádzkovania základnej služby Objednávateľa.

Bezpečnostné opatrenia sú realizované v závislosti od klasifikácie informácií a analýzy rizík v súlade s bezpečnostnými štandardami v oblasti informačnej a/alebo Kybernetickej bezpečnosti pre všetky siete a informačné systémy.

Bezpečnostné opatrenia zahŕňajú nasledovné opatrenia :

a) Definovanie systému riadenia informačnej bezpečnosti najmä v oblastiach:
   I. manažmentu digitálnej identity zamestnancov a technických zariadení,
   II. monitorovania prevádzky sietí a informačných systémov,
   III. ochrany sietí a informačných systémov pred počítačovými a ľudskými infiltráciami, spywarom a spamom,
   IV. zálohovania a archivácie údajov v elektronickej podobe,
   V. konfiguračného a zmenového manažmentu, distribúcie opráv a servisných balíkov pre operačné systémy, databázy a aplikácie,
   VI. manažmentu bezpečnostných incidentov
   VII. manažmentu zraniteľností informačných systémov a sietí

b) Vykonávanie riadenia prístupu k informačným systémom a sieťam na princípe najnižších možných privilégií, vykonávanie segmentácie sietí a ich oddeľovanie prostredníctvom bezpečnostných prvkov, riadenia vzdialeného prístupu s využitím up-to-date bezpečnostných technológií a ich nastavení, vykonávanie zodolňovania prvkov informačných systémov a sietí (napr. minimalizácia otvorených portov/spustených služieb, bezpečná konfigurácia prvkov).

c) Vykonávanie klasifikácie informácií a kategorizácia všetkých sietí a informačných systémov na základe významnosti, funkcie a účelu informácií a informačných systémov a s ohľadom na dôvernosť, integritu, dostupnosť.

d) Určenie minimálnej úroveň bezpečnosti pre jednotlivé informácie a kategórie sietí a informačných systémov podľa schválenej klasifikačnej schémy.

e) Priradenie vlastníctva ku všetkým aktívam, od ktorých závisí poskytovanie služieb, v zmysle určenia zodpovednosti konkrétnych osôb za správu a riadenie príslušných aktív.

f) Implementovanie Bezpečnostných opatrení počas celého životného cyklu všetkých prevádzkovaných sietí a informačných systémov, vrátane subsystémov, už od etapy špecifikácie a zadania.

g) Stanovenie zodpovednosti za Kybernetickú bezpečnosť.

h) Vykonávanie pravidelného testovanie funkčnosti implementovaných Bezpečnostných opatrení formou interného auditu alebo kontroly, externého auditu alebo penetračného testovania.

i) Vykonávanie loggingu a monitoringu najmä centrálnych sieťových prvkov, služieb prístupných do externých sietí, kritických interných aplikácií a infraštruktúrnych služieb, prístupu tretích strán Zhotoviteľa.

j) Vypracovanie, udržiavanie a testovanie plánov kontinuity činností pre všetky siete a informačné systémy.

k) Vykonávanie analýzy rizík pre všetky siete a informačné systémy v pravidelných intervaloch.

l) Identifikáciu zraniteľností prevádzkovaných systémov a sietí následné vykonávanie patch managementu.

m) Presadzovanie princípu „čistého stola“ – odkladanie dokumentov a médií s citlivými údajmi do vyhradených uzamykateľných priestorov po ukončení práce alebo pracovnej doby.

n) Presadzovanie princípu „potreba vedieť“ (need to know) – pristupovanie k dôverným informáciám a dokumentom oprávnených zamestnancov len keď to vyžadujú pracovné úlohy.

o) Oddeľovanie prevádzkových a bezpečnostných rolí v informačných systémoch a sieťach.

p) Oddeľovanie výkonných a kontrolných rolí.

q) Zvyšovanie bezpečnostného povedomie používateľov sietí a informačných systémov v rámci vzdelávacieho programu spoločnosti.