Metodické usmernenie pre OVM

(odporúčania pre proces verejného obstarávania auditu kybernetickej bezpečnosti a prípravu na audit kybernetickej bezpečnosti)

Obsah

1 Správa dokumentu

Tento dokument je metodickým materiálom slúžiacim pre potreby orgánov verejnej moci (ďalej aj „organizácia"), ktorý nie je povinný na použitie a ani nie je záväzný. Dokument je poskytnutý voľne a bezplatne na využitie podľa potrieb konkrétnej organizácie.

Vytvorený dokument je možné použiť i pre potreby vzdelávania pracovníkov organizácií v oblasti kybernetickej a informačnej bezpečnosti.

Vytvorený dokument nie je určený na ďalší predaj alebo akúkoľvek inú komerčnú či obchodnú činnosť.

Ministerstvo investícií, regionálneho rozvoja a informatizácie Slovenskej republiky (ďalej aj „MIRRI") nezodpovedá za nesprávne použitie predmetného dokumentu zo strany organizácie. Správne použitie a implementácia bezpečnostných opatrení je plne v kompetencii a zodpovednosti konkrétnej organizácie.

MIRRI si vyhradzuje právo na zmenu/úpravu predmetného dokumentu alebo čiastkových textov a tabuliek, a to v potrebnom rozsahu vrátane zmien verzií dokumentov. Dokument je výstupom pilotného projektu, na ktorý nadväzuje Reforma Štandardizácia technických a procesných riešení kybernetickej a informačnej bezpečnosti (Plán obnovy a odolnosti).

2 Úvod

2.1 Účel dokumentu

Účelom tohto dokumentu je poskytnúť odporúčania pre proces verejného obstarávania podľa zákona č. 343/2015 Z. z. o verejnom obstarávaní a o zmene a doplnení niektorých zákonov v znení neskorších predpisov (ďalej len „zákon o verejnom obstarávaní“), auditu kybernetickej bezpečnosti a prípravu na audit kybernetickej bezpečnosti (ďalej aj „audit“) podľa zákona č. 69/2018 Z. z. o kybernetickej bezpečnosti a o zmene a doplnení niektorých zákonov (ďalej aj „zákon o kybernetickej bezpečnosti“).

Súvisiacimi právnymi predpismi sú:

- vyhláška Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti a
- vyhláška Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

2.2 Rozsah platnosti

Tento dokument je platný pre všetkých zamestnancov organizácie a tiež všetky relevantné tretie strany.

3 Všeobecne o audite kybernetickej bezpečnosti

Auditom kybernetickej bezpečnosti sa overuje plnenie povinností podľa zákona a posudzuje sa zhoda prijatých bezpečnostných opatrení s požiadavkami podľa zákona a súvisiacich osobitných predpisov vzťahujúcich sa na bezpečnosť sietí a informačných systémov prevádzkovateľa základnej služby pre jednotlivé siete a informačné systémy základnej služby a pre tie, ktoré podporujú základné služby, s cieľom zabezpečiť požadovanú úroveň kybernetickej bezpečnosti a predchádzať kybernetickým bezpečnostným incidentom.

Auditom kybernetickej bezpečnosti sa identifikujú nedostatky pri zabezpečovaní kybernetickej bezpečnosti prevádzkovateľom základnej služby s cieľom prijať opatrenia na ich odstránenie a nápravu a na predchádzanie kybernetickým bezpečnostným incidentom.

Audit sa vykonáva

- každé dva roky, audit sa musí začať do dvoch rokov od vydania záverečnej správy o výsledkoch auditu a
- pri každej významnej zmene, najneskôr do dvoch mesiacov, odkedy má zmena významný vplyv na realizované bezpečnostné opatrenia.

Významným vplyvom sa rozumie najmä:

- vplyv na prijatú klasifikáciu informácií a kategorizáciu sietí a informačných systémov,
- zmena dopadových kritérií základnej služby,
- zmena alebo výmena informačného systému a prevádzkových parametrov základnej služby,
- zavedenie novej siete, nového informačného systému, od ktorých je závislá základná služba,
- zavedenie novej technológie, od ktorej je závislá základná služba alebo
- zmena systémovej architektúry alebo sieťovej topológie.

Audit kybernetickej bezpečnosti vykonáva certifikovaný audítor kybernetickej bezpečnosti podľa § 29 ods. 3 zákona o kybernetickej bezpečnosti (ďalej aj „audítor“). Na vykonanie auditu musí audítor spĺňať podmienky znalostného štandardu overené skúškou doloženou podľa odporúčaní medzinárodne akceptovaných technických noriem alebo iných, týmto štandardom vecne obdobných a všeobecne uznávaných postupov.

V záverečnej správe o výsledkoch auditu kybernetickej bezpečnosti sa hodnotí výsledok auditu a uvedú sa dôkazy, ktoré sa viažu k jednotlivým zisteniam auditu. Prílohou záverečnej správy o výsledkoch auditu je pri zistení nesúladu s požiadavkami na bezpečnosť sietí a informačných systémov aj správa o zistených nedostatkoch, pri ktorých sa uvádza termín vykonania nápravných opatrení na zabezpečenie súladu s požiadavkami na bezpečnosť sietí a informačných systémov. Nápravné opatrenia sa prijímajú tak, že je možné ich zahrnúť do záverečnej správy o výsledkoch auditu. Ak sú niektoré zistené nedostatky odstránené do termínu vyjadrenia prevádzkovateľa základnej služby k zisteniam auditu pred spracovaním záverečnej správy o výsledkoch auditu, je možné v tejto záverečnej správe o výsledkoch auditu konštatovať pre plnenie daných požiadaviek súlad s požiadavkami na bezpečnosť sietí a informačných systémov.

4 Odporúčania pre proces verejného obstarávania auditu kybernetickej bezpečnosti

Vzhľadom k povahe obstarávaných služieb sa predpokladá, že v prípade verejného obstarávania auditu kybernetcikej bezpečnosti pôjde – v prevažnej väčšine prípadov – o zákazku s nízkou hodnotou a verejné obstarávanie bude realizované podľa § 117 zákona o verejnom obstarávaní. V prípade zákazky s nízkou hodnotou sú pre organizáciu relevantné všetky body tejto kapitoly.

Poznámka: Najmä pri auditoch s nižším očakávaným počtom auditodní v zmysle vyhlášky Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti sa môže uplatniť § 1 ods. 15 zákona o verejnom obstarávaní. Ak organizácia uplatní uvedené ustanovenie zákona, postup uvedený v tejto kapitole nie je pre organizáciu aplikovateľný.

4.1 Základné pravidlá zadávania zákaziek s nízkymi hodnotami

Organizácia ako verejný obstarávateľ pri zadávaní zákazky s nízkou hodnotou:

- postupuje tak, aby vynaložené náklady na predmet zákazky boli hospodárne,
- v prípade, že vyzve na predloženie ponuky viac hospodárskych subjektov na účel zadania zákazky, vyzve tieto hospodárske subjekty na to určenou funkcionalitou elektronickej platformy,
- je povinný zabezpečiť dodržanie princípov rovnakého zaobchádzania a nediskriminácie
- je povinný postupovať v súlade s princípom transparentnosti a zdokumentovať celý priebeh verejného obstarávania tak, aby jeho úkony boli preskúmateľné bez ohľadu na použité prostriedky komunikácie
- v prípade, ak na zadanie zákazky využije elektronickú platformu, môže priebeh verejného obstarávania zdokumentovať prostredníctvom elektronickej platformy,
- môže umožniť predloženie ponuky v inom ako štátnom jazyku (ak verejný obstarávateľ umožní predloženie ponuky v inom jazyku, musí vždy umožniť predloženie ponuky aj v štátnom jazyku),
- môže postupovať podľa § 109 až 111 zákona o verejnom obstarávaní,
- je povinný odoslať na uverejnenie prostredníctvom na to určenej funkcionality elektronickej platformy výzvu na predkladanie ponúk a uskutočňovať komunikáciu v rámci zadávania zákazky s nízkou hodnotou vrátane predkladania ponúk prostredníctvom elektronickej platformy, ak predpokladaná hodnota zákazky na dodanie tovaru okrem potravín alebo zákazky na poskytnutie služby okrem služby uvedenej v prílohe č. 1 je rovnaká alebo vyššia ako 70 000 eur.

Organizácia pre účely verejného obstarávania auditu kybernetickej bezpečnosti aplikuje vlastné postupy, ktoré detailizujú zadávanie zákaziek s nízkymi hodnotami.

4.2 Základné náležitosti výzvy na predkladanie ponúk

Vo výzve na predkladanie ponúk organizácia ako verejný obstarávateľ uvedie najmä:

- predpokladanú hodnotu zákazky, množstvo alebo rozsah služieb (odporúčaný rozsah služieb je uvedený v bode 4.2.1 tohto dokumentu),
- lehotu na predkladanie ponúk (lehota nesmie byť kratšia ako sedem pracovných dní odo dňa odoslania výzvy na predkladanie ponúk),

- informácie o vyžadovaných podmienkach účasti a doklady, ktorými ich možno preukázať (odporúčané informácie o vyžadovaných podmienkach účasti a doklady sú uvedené v bode 4.2.2 tohto dokumentu),
- informácie potrebné na vypracovanie ponuky, predloženie ponuky a plnenie zmluvy (odporúčané informácie tohto charakteru sú uvedené v bode 4.2.3 tohto dokumentu),
- kritériá na vyhodnotenie ponúk a ich relatívnu váhu (odporúčaným kritériom je najnižšia cena).
- informáciu, či sa použije elektronická aukcia (je na zvážení verejného obstarávateľa, či bude aukcia použitá).

4.2.1 Odporúčaný rozsah služieb

Predmetom verejného obstarávania je obstaranie služieb auditu kybernetickej bezpečnosti s cieľom preveriť účinnosť prijatých bezpečnostných opatrení verejného obstarávateľa a plnenie požiadaviek stanovených zákonom č. 69/2018 Z. z. o kybernetickej bezpečnosti v platnom znení (ďalej len „Zákon“), príslušnej Vyhlášky Národného bezpečnostného úradu č. 362/2018 Z.z. (ďalej len „Vyhláška o bezpečnostných opatreniach”), ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení a Vyhlášky Národného bezpečnostného úradu č. 493/2022 Z.z. (ďalej len „Vyhláška o audite“) o audite kybernetickej bezpečnosti.

Uchádzač sa v rámci auditu kybernetickej bezpečnosti zaväzuje zabezpečiť výkon auditu prostredníctvom certifikovaného audítora kybernetickej bezpečnosti (ďalej len „Audítor kybernetickej bezpečnosti“) podľa Vyhlášky o audite, ktorý spĺňa všetky požiadavky na výkon auditu.

Uchádzač je oprávnený použiť na splnenie predmetu zákazky subdodávateľov, za predpokladu, že s nimi uzatvoril písomnú zmluvu a o zapojení subdodávateľa vopred informoval verejného obstarávateľa. Tým nie je dotknutá zodpovednosť Dodávateľa za splnenie predmetu tejto zmluvy.

Predmet zákazky sa bude považovať za splnený riadne a včas dňom predloženia Záverečnej správy o výsledkoch auditu kybernetickej bezpečnosti.

Uchádzač sa v rámci auditu kybernetickej bezpečnosti zaväzuje poskytnúť nasledovné služby:

a) v súlade so Štandardom na výkon auditu kybernetickej bezpečnosti vydanom Kompetenčným centrom kybernetickej bezpečnosti (ďalej len „Metodika auditu“) a v súlade s požiadavkami Zákona a Vyhlášky o bezpečnostných opatreniach výkon auditu kybernetickej bezpečnosti, a teda auditu sietí a informačných systémov verejného obstarávateľa ako prevádzkovateľa základnej služby, s cieľom preveriť účinnosť prijatých bezpečnostných opatrení a plnenie požiadaviek Zákona a Vyhlášky o bezpečnostných opatreniach, ktoré definujú príslušné požiadavky na prevádzkovateľa základnej služby. Audit kybernetickej bezpečnosti zahŕňa tieto požiadavky:

Posúdenie prijatia a dodržiavania všeobecných bezpečnostných opatrení vo forme úloh, procesov, rolí a technológií v organizačnej, personálnej a technickej rovine v oblastiach:

a) organizácie kybernetickej bezpečnosti a informačnej bezpečnosti,

b) riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti,

c) personálnej bezpečnosti,

d) riadenia prístupov,

e) riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,

f) bezpečnosti pri prevádzke informačných systémov a sietí,

g) hodnotenia zraniteľností a bezpečnostných aktualizácií,

h) ochrany proti škodlivému kódu,

i) sieťovej a komunikačnej bezpečnosti,

j) akvizície, vývoja a údržby informačných sietí a informačných systémov,

k) zaznamenávania udalostí a monitorovania,

l) fyzickej bezpečnosti a bezpečnosti prostredia,

m) riešenia kybernetických bezpečnostných incidentov,

n) kryptografických opatrení,

o) kontinuity prevádzky,

p) auditu, riadenia súladu a kontrolných činností.

Verejný obstarávateľ poskytne uchádzačovi všetky informácie a súčinnosť potrebnú pre splnenie predmetu zákazky.

Výstupom auditu kybernetickej bezpečnosti je Záverečná správa o výsledkoch auditu kybernetickej bezpečnosti v slovenskom jazyku (ďalej aj ako „Správa“) vypracovaná v súlade s požiadavkami Vyhlášky o audite. Správa bude mať nasledovnú štruktúru, pokiaľ z Vyhlášky o audite nevyplýva iná štruktúra a rozsah:

(a) Meno, priezvisko a číslo platného certifikátu audítora, dátum vyhotovenia a podpis audítora,

(b) Vymedzenie rozsahu vykonaného auditu kybernetickej bezpečnosti,

(c) Cieľ auditu kybernetickej bezpečnosti,

(d) Použité postupy a metodiky vykonaného auditu kybernetickej bezpečnosti,

(e) Zhrnutie zistení výsledkov auditu kybernetickej bezpečnosti a konštatovanie súladu alebo nesúladu s požiadavkami na bezpečnosť sietí a informačných systémov,

(f) Odporúčané nápravné opatrenia audítora pri zistení nedostatkov,

(g) Dokumenty, ktorými sú najmä:

1. Kópia certifikátu audítora,

2. Kópia žiadosti o výkon auditu podľa prílohy č. 1 Vyhlášky o audite,

3. Výpočet rozsahu trvania auditu a zdôvodnenie skrátenia alebo predĺženia,

4. Kontrolný záznam auditovaných bezpečnostných opatrení s vyjadrením prevádzkovateľa základnej služby so zisteniami auditu,

5. Harmonogram auditu,

6. Zoznam posúdenej dokumentácie,

7. Uvedenie a zdôvodnenie zmien a rozdielov priebehu auditu oproti plánovanému harmonogramu,

8. Zhodnotenie plnenia povinností podľa zákona a celkového stavu prijatých bezpečnostných opatrení každého informačného systému súvisiaceho so základnou službou, vyslovenie súladu alebo nesúladu s požiadavkami na bezpečnosť sieti a informačných systémov, a konkrétne uvedenie nedostatkov.

4.2.2 Odporúčané podmienky účasti a doklady

Odporúčané podmienky účasti a doklady pre zákazku typu audit kybernetickej bezpečnosti sú:

- osobné postavenie podľa § 32 ods. 1 písm. e) a f) zákona o verejnom obstarávaní (splnenie podmienok je možné preukázať zápisom v zozname hospodárskych subjektov):
  - § 32 ods. 1 písm. e) zákona o verejnom obstarávaní: uchádzač je oprávnený dodávať tovar, uskutočňovať stavebné práce alebo poskytovať službu,
  - § 32 ods. 1 písm. f) zákona o verejnom obstarávaní: uchádzač nemá uložený zákaz účasti vo verejnom obstarávaní potvrdený konečným rozhodnutím v SR a v štáte sídla, miesta podnikania alebo obvyklého pobytu
- predloženie certifikátu audítora kybernetickej bezpečnosti,
- zoznam zákaziek obdobného charakteru za predchádzajúce obdobie (je na rozhodnutí verejného obstarávateľa, či takýto zoznam bude požadovať),
- ak sa uplatňuje zákon č. 315/2016 Z. z. o registri partnerov verejného sektora a o zmene a doplnení niektorých zákonov v znení neskorších predpisov, organizácia by mala požadovať výpis z registra partnerov verejného sektora.

4.2.3 Informácie potrebné na vypracovanie ponuky, predloženie ponuky a plnenie zmluvy

Odporúča sa, aby verejný obstarávateľ k výzve priložil:

- vyplnený dotazník určený audítorovi kybernetickej bezpečnosti na určenie rozsahu trvania auditu,
- návrh zmluvy o vykonaní auditu kybernetickej bezpečnosti.

Dotazník určený audítorovi kybernetickej bezpečnosti na určenie rozsahu trvania auditu

Aby bol audítor kybernetickej bezpečnosti schopný určiť rozsah trvania auditu kybernetickej bezpečnosti v zmysle prílohy č. 2 vyhlášky Národného bezpečnostného úradu č. 493/2022 Z. z. o audite kybernetickej bezpečnosti, je potrebné, aby mu verejný obstarávateľ poskytoval najmenej nasledovné informácie:

- počet interných zamestnancov a zamestnancov externých dodávateľov zúčastňujúcich sa na prevádzke sietí a informačných systémov,
- kategorizáciu sietí a informačných systémov,
- systémovú architektúru prostredia (centralizovaný alebo decentralizovaný spôsob prevádzkovania informačných systémov),
- množstvo, rozsah a komplexnosť dokumentácie súvisiacej s prevádzkou informačného systému a zabezpečovaním bezpečnostných opatrení vrátane výsledkov predchádzajúcich auditov a vykonaných analýz rizík,
- počet tretích strán zúčastňujúcich sa na prevádzke informačných systémov,
- počet lokalít v ktorých nachádzajú siete a informačné systémy podporujúce prevádzku základnej služby.

Odporúčaný rozšírený rozsah údajov, na základe ktorých audítor kybernetickej bezpečnosti určí rozsah

trvania auditu kybernetickej bezpečnosti tvorí prílohu č. 1 tohto dokumentu.

Návrh zmluvy o vykonaní auditu kybernetickej bezpečnosti

Pri zadávaní zákazky s nízkou hodnotou sa v zmysle § 117 zákona o verejnom obstarávaní nevyžaduje písomná forma zmluvy okrem prípadov, v ktorých to vyžadujú osobitné predpisy. V prípade auditu kybernetickej bezpečnosti sa jednoznačne odporúča uzatvoriť zmluvu v písomnej forme.

Príklad návrhu zmluvy o vykonaní auditu kybernetickej bezpečnosti je súčasťou prílohy č. 2 tohto dokumentu. Uvedený príklad slúži len ako vzor, organizácia môže pokojne využiť vlastnú zaužívanú šablónu zmluvy pre zákazky s nízkymi hodnotami.

5 Odporúčania pre proces prípravy na audit kybernetickej bezpečnosti

Pred samotným procesom verejného obstarávania v rámci prípravnej fázy auditu kybernetickej bezpečnosti sa odporúča vykonať prípravnú rozdielovú analýzu súčasného stavu voči požiadavkám zákona o kybernetickej bezpečnosti a vyhláške Národného bezpečnostného úradu č. 362/2018 Z. z., ktorou sa ustanovuje obsah bezpečnostných opatrení, obsah a štruktúra bezpečnostnej dokumentácie a rozsah všeobecných bezpečnostných opatrení.

Účelom takejto prípravnej analýzy je ohodnotiť tieto domény kybernetickej bezpečnosti:

a) organizácie kybernetickej bezpečnosti a informačnej bezpečnosti,

b) riadenia rizík kybernetickej bezpečnosti a informačnej bezpečnosti,

c) personálnej bezpečnosti,

d) riadenia prístupov,

e) riadenia kybernetickej bezpečnosti a informačnej bezpečnosti vo vzťahoch s tretími stranami,

f) bezpečnosti pri prevádzke informačných systémov a sietí,

g) hodnotenia zraniteľností a bezpečnostných aktualizácií,

h) ochrany proti škodlivému kódu,

i) sieťovej a komunikačnej bezpečnosti,

j) akvizície, vývoja a údržby informačných sietí a informačných systémov,

k) zaznamenávania udalostí a monitorovania,

l) fyzickej bezpečnosti a bezpečnosti prostredia,

m) riešenia kybernetických bezpečnostných incidentov,

n) kryptografických opatrení,

o) kontinuity prevádzky,

p) auditu, riadenia súladu a kontrolných činností.

Príklad zoznamu oblastí a bezpečnostných opatrení, ktorý je vhodný pre účely prípravy na audit kybernetickej bezpečnosti tvorí prílohu č. 3 tohto dokumentu.

Odporúčaným krokom po vykonaní rozdielovej analýzy je implementácia najväčšieho možného počtu bezpečnostných opatrení v zmysle zákona o kybernetickej bezpečnosti v organizačnej, personálnej a technickej oblasti.

6 Prílohy

6.1 Príloha č. 1 – Dotazník určený audítorovi kybernetickej bezpečnosti na určenie rozsahu trvania auditu

Príloha 1 je samostatná príloha.

6.2 Príloha č. 2 – Príklad návrhu zmluvy o vykonaní auditu kybernetickej bezpečnosti

Príloha 2 je samostatná príloha.

6.3 Príloha č. 3 – Zoznam oblastí a bezpečnostných opatrení vhodný pre účely prípravy na audit kybernetickej bezpečnosti

Príloha 3 je samostatná príloha.