Specifikace díla

Provedení komplexního auditu stavu kybernetické bezpečnosti v celé organizaci Objednatele. Rozsah díla je dán zákonem č. 181/2014 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen „ZoKB“), a vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti, v platném znění (dále jen „VoKB“) a dalších souvisejících norem.
Dílem je hodnocení stupně shody zavedených opatření Objednatele se ZoKB a VoKB. Objednatel bude zkoumán z pohledu všech organizačních i technických opatření.

A. Dílo musí obsahovat tyto náležitosti:

1. Plán auditu, předložený Objednateli před zahájením vstupních konzultací podle bodu 1.2 písm. a) Smlouvy
2. Definici způsobu kontroly všech povinných činností
3. Harmonogram zahrnující minimálně tyto činnosti a milníky:
   a) Zahájení
   b) Vstupní konzultace
   c) Provedení auditu ověření shody s požadavky ZoKB a VoKB
   d) Prezentování auditu
   e) Zapracování připomínek
   f) Protokolární předání finální verze auditní zprávy
4. Provedení analýzy stávajícího stavu kybernetické bezpečnosti.
5. Poskytnutí relevantních hodnotících kritérií v souladu s VoKB a se ZoKB.
6. Ověření, že objednatel disponuje všemi potřebnými záznamy a dokumenty dle VoKB a ZoKB. V případě potřeby úprav dokumentů dodat návrh, jakým způsobem dokumenty upravit.
7. Posouzení bezpečnostní dokumentace kybernetické bezpečnosti podle § 30 ZoKB a přílohy č. 5 VoKB.
8. Posouzení organizace bezpečnosti podle § 6 VoKB a bezpečnostních rolí podle § 7 VoKB.
9. Posouzení souladu požadovaných technických a organizačních opatření dle VoKB.
10. Audit analýzy a řízení aktiv, který musí obsahovat všechny náležitosti § 4 VoKB a to minimálně v této struktuře:
    a) Ověření a analýza stávající metodiky pro identifikaci a hodnocení aktiv.
    b) Identifikace aktiv a jejich garantů.
    c) Určení vazeb mezi aktivy a hodnocení závislostí mezi nimi.
    d) Hodnocení důležitosti všech aktiv.

    Výstupem této části musí být:

    a) Metodika pro identifikaci a hodnocení aktiv
    b) Dokument zpráva o hodnocení aktiv
    c) Diagram vazeb jednotlivých aktiv a závislostí mezi nimi

11. Audit analýzy a řízení rizik, který musí obsahovat všechny náležitosti § 5 VoKB. Konkrétně se jedná o prověřením, případně zpracování:
    a) Stanovené metodiky pro identifikaci a hodnocení rizik a případné doporučení její úpravy
    b) Stanovených kritérií pro akceptovatelnost rizik a v případě potřeby doporučení jejich úprav
    c) Identifikace rizik
    d) Zprávy o hodnocení rizik
    e) Plánu zvládání rizik

Výstupem této části musí být:

a) Zhodnocení metodiky pro identifikaci a hodnocení rizik a případné návrhy na její úpravu
b) Zhodnocení Zprávy o hodnocení rizik a případné návrhy na její úpravu
c) Zhodnocení Plánu zvládání rizik a případné návrhy na její úpravu

12. Závěrečnou zprávu z auditu kybernetické bezpečnosti popisující jednotlivá auditní zjištění a z toho plynoucí soulad/nesoulad prostředí Objednatele s požadavky ZoKB a VoKB. Závěrečná zpráva musí dále obsahovat seznam a popis doporučených opatření, která musí Objednatel provést, aby všechny zjištěné nedostatky odstranil a byl tak plně v souladu se ZoKB a VoKB. Závěrečná zpráva z auditu musí obsahovat minimálně tyto náležitosti:
    a) Program a časový plán auditu
    b) Seznam auditovaných útvarů a účastníků
    c) Průběh auditu
    d) Závěry auditu – nápravná opatření, omezení, nevyřešené neshody
    e) Omezení, nevyřešené neshody,
    f) Oblasti, které nebyly pokryty a proč nemohly být pokryty

13. Součástí každého nápravného opatření musí být popis aktuálního stavu. Návrh nápravných opatření musí obsahovat jejich detailní popis včetně stanovení priorit pro jednotlivá nápravná opatření, která budou vyplývat ze zjištění auditu.

B. Analýza současného stavu kybernetické bezpečnosti v organizaci musí zahrnovat minimálně:
    1) Přehled všech provozovaných informačních systémů
    2) Přehled všech poskytovaných služeb
    3) Přehled veškeré technologické infrastruktury
    4) Hodnocení zavedených bezpečnostních opatření
    5) Přehled, analýzu a popis způsobu řízení aktiv
    6) Přehled, analýzu a popis způsobu řízení rizik
    7) Přehled všech požadavků dle struktury ZoKB a VoKB. U každého požadavku musí být uvedeno, do jaké míry je plněn. Konkrétně se musí jednat o jednu z níže uvedených možností:
        a) Nezavedeno
        b) V procesu zavádění
        c) Zavedeno
        d) Neaplikovatelné (včetně odůvodnění)
    8) Doporučení, jaká opatření má Objednatel přijmout, aby splňoval všechny požadavky ZoKB a VoKB, a to také s přihlédnutím k dosud známým „best practices“.

C. Ověření úplnosti a správného nastavení níže uvedené dokumentace:

Bezpečnostní politiky

1. Politika systému řízení bezpečnosti informací
2. Politika organizační bezpečnosti
3. Politika řízení dodavatelů
4. Politika klasifikace aktiv

5. Politika bezpečnosti lidských zdrojů
6. Politika řízení provozu a komunikací
7. Politika řízení přístupu
8. Politika bezpečného chování uživatelů
9. Politika zálohování a obnovy
10. Politika bezpečného předávání a výměny informací
11. Politika řízení technických zranitelností
12. Politika bezpečného používání mobilních zařízení
13. Politika poskytování a nabývání licencí programového vybavení a informací
14. Politika dlouhodobého ukládání a archivace informací
15. Politika ochrany osobních údajů
16. Politika fyzické bezpečnosti
17. Politika bezpečnosti komunikační sítě
18. Politika ochrany před škodlivým kódem
19. Politika nasazení a používání nástroje pro detekci kybernetických bezpečnostních událostí
20. Politika využití a údržby nástroje pro sběr a vyhodnocení kybernetických bezpečnostních událostí
21. Politika bezpečného používání kryptografické ochrany

Ostatní dokumentace

1. Metodika pro identifikaci a hodnocení aktiv a pro identifikaci a hodnocení rizik
2. Zpráva o hodnocení aktiv a rizik
3. Prohlášení o aplikovatelnosti
4. Plán zvládání rizik
5. Plán rozvoje bezpečnostního povědomí
6. Zvládání kybernetických bezpečnostních incidentů
7. Strategie řízení kontinuity činností
8. Přehled obecně závazných právních předpisů, vnitřních předpisů a jiných předpisů a smluvních závazků

D. Prověření míry plnění požadavků dle ZoKB § 5 - bezpečnostních opatření, konkrétně tato:

Organizační opatření:
a) systém řízení bezpečnosti informací Zhotovitel musí mimo jiné ověřit, že: • Jsou v ISMS zahrnuty všechny relevantní systémy a bezpečnostní opatření
b) řízení rizik Zhotovitel musí mimo jiné ověřit, že: • Seznam zranitelností obsahuje všechny možné zranitelnosti, • Mají identifikovaná rizika nastaveny hodnoty pro jednotlivé atributy rizik • Existují vazby rizik na aktiva, hrozby a zranitelnosti, • Je správně nastaven Plán zvládání rizik • Existují vazby aktivum-hrozba-zranitelnost • Jsou zohledněny relevantní hrozby, a je správně nastavena analýza a řízení rizik • Jsou evidovány všechny vazby rizik a významných dodavatelů

• Prohlášení o aplikovatelnosti obsahuje přehled bezpečnostních opatření, která nebyla aplikována, včetně odůvodnění a způsobu plnění opatření • Existuje vyhodnocení účinnosti ISMS a také seznam opatření dle VoKB, která nebylo možno zavést • Plán zvládání rizik obsahuje všechny potřebné náležitosti jako např. cíle a přínosy bezpečnostních opatření, určení odpovědných osob, zdrojů, a návaznosti na hodnocení rizik
c) bezpečnostní politika
d) organizační bezpečnost
e) stanovení bezpečnostních požadavků pro dodavatele
a) řízení aktiv <u>Zhotovitel musí mimo jiné ověřit, že:</u> • Jsou správně identifikována všechna primární a podpůrná aktiva, • Jsou mezi těmito aktivy evidovány správně všechny vazby, • Jsou hodnoceny důsledky jejich závislostí, • Jsou správně identifikováni garanti těchto aktiv
g) bezpečnost lidských zdrojů
h) řízení provozu a komunikací
i) řízení přístupu osob
j) akvizice, vývoj a údržba
k) zvládání kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů <u>Zhotovitel musí mimo jiné ověřit, že:</u> • Je popsán proces zjišťování, prošetřování a určování příčin kybernetických bezpečnostních incidentů a událostí
l) řízení kontinuity činností <u>Zhotovitel musí mimo jiné ověřit, že:</u> • Je správně nastavena metodika pro určení hodnot RTO a RPO
m) kontrola a audit kritické informační infrastruktury a významných informačních systémů
Technická opatření:
a) fyzická bezpečnost
b) nástroj pro ochranu integrity komunikačních sítí
c) nástroj pro ověřování identity uživatelů
d) nástroj pro řízení přístupových oprávnění
e) nástroj pro ochranu před škodlivým kódem
f) nástroj pro zaznamenávání činnosti informačního nebo komunikačního systému, jeho uživatelů a administrátorů
g) nástroj pro detekci kybernetických bezpečnostních událostí
h) nástroj pro sběr a vyhodnocení kybernetických bezpečnostních událostí
i) aplikační bezpečnost
j) kryptografické prostředky
k) nástroj pro zajišťování úrovně dostupnosti informací
l) bezpečnost průmyslových a řídících systémů

E. Zhotovitel prověří shodu níže uvedených opatření s VoKB:

Prověřovaná oblast:	
Organizační opatření :	
§ 3	Systém řízení bezpečnosti informací
§ 4	Řízení aktiv Zhotovitel musí mimo jiné ověřit, že: • Jsou správně identifikována všechna primární a podpůrná aktiva, • Jsou mezi těmito aktivy evidovány správně všechny vazby, • Jsou hodnoceny důsledky jejich závislostí, • Jsou správně identifikováni garanti těchto aktiv
§ 5	Řízení rizik Zhotovitel musí mimo jiné ověřit, že: • Seznam zranitelností obsahuje všechny možné zranitelnosti, • Mají identifikovaná rizika nastaveny hodnoty pro jednotlivé atributy rizik, • Existují vazby rizik na aktiva, hrozby a zranitelnosti, • Je správně nastaven Plán zvládání rizik, • Existují vazby aktivum-hrozba-zranitelnost, • Jsou zohledněny relevantní hrozby, a je správně nastavena analýza a řízení rizik, • Jsou evidovány všechny vazby rizik a významných dodavatelů.
§ 6	Organizační bezpečnost
§ 7	Bezpečnostní role
§ 8	Řízení dodavatelů Zhotovitel musí mimo jiné ověřit, že: • Existuje seznam všech významných dodavatelů a provozovatelů, a že jsou tito dodavatelé prokazatelně informováni o tom, že naplňují definici významného dodavatele/provozovatele • Probíhá pravidelné přezkoumání smluv u těchto dodavatelů/provozovatelů
§ 9	Bezpečnost lidských zdrojů
§ 10	Řízení provozu a komunikací
§ 11	Řízení změn Zhotovitel musí mimo jiné ověřit, že: Existuje popis významné změny Existuje dokumentace řízení významných změn Jsou přijímána opatření za účelem snížení všech nepříznivých dopadů spojených s významnými změnami Je zajištěno testování významných změn
§ 12	Řízení přístupu
§ 13	Akvizice, vývoj a údržba
§ 14	Zvládání kybernetických bezpečnostních událostí a incidentů Zhotovitel musí mimo jiné ověřit, že:

	• Je popsán proces zjišťování, prošetřování a určování příčin kybernetických bezpečnostních incidentů a událostí
§ 15	Řízení kontinuity činností Zhotovitel musí mimo jiné ověřit, že: • Je správně nastavena metodika pro určení hodnot RTO a RPO
§ 16	Audit kybernetické bezpečnosti
Technická opatření	
§ 17	Fyzická bezpečnost
§ 18	Bezpečnost komunikačních sítí
§ 19	Správa a ověřování identit
§ 20	Řízení přístupových oprávnění
§ 21	Ochrana před škodlivým kódem
§ 22	Zaznamenávání událostí informačního a komunikačního systému, jeho uživatelů a administrátorů
§ 23	Detekce kybernetických bezpečnostních událostí
§ 24	Sběr a vyhodnocování kybernetických bezpečnostních událostí
§ 25	Aplikační bezpečnost
§ 26	Kryptografické prostředky
§ 27	Zajišťování úrovně dostupnosti informací
§ 28	Průmyslové, řídicí a obdobné specifické systémy
§ 29	Digitální služby
Bezpečnostní politika a bezpečnostní dokumentace	
§ 30	Bezpečnostní politika a bezpečnostní dokumentace
Kybernetický bezpečnostní incident	
§ 31	Kategorizace kybernetických bezpečnostních incidentů
§ 32	Forma a náležitosti hlášení kybernetických bezpečnostních incidentů
Reaktivní opatření a kontaktní údaje	
§ 33	Reaktivní opatření
§ 34	Kontaktní údaje

F. Zhotovitel prověří, do jaké míry jsou vyřešena zjištění z auditů kybernetické bezpečnosti, které provedl útvar interního auditu Objednatele, a to včetně jejich proveditelnosti a slučitelnosti se ZoKB a VoKB. Za tímto účelem Objednatel předá Zhotoviteli veškeré dotčené audity. Jedná se o níže uvedená zjištění:

Číslo zjištění	Název zjištění
1	Ochrana před malwarem na síti
2	Bezpečností politiky (soulad se ZoKB, VoKB a aktuálním stavem KB v prostředí Objednatele)
3	Logování síťových událostí
4	Ochrana proti úniku informací (dat)
5	Penetrační testy
6	Řízení přístupu na síti
7	Řízení kybernetických bezpečnostních událostí a incidentů
8	Správa zranitelností

9	Šifrování mobilních zařízení typu notebook
10	Zabezpečení sítě (technologie 802.1X)
11	Pravidelné aktualizace serverových operačních systémů
12	Správa privilegovaných účtů