Specifikace předmětu plnění - požadavek VZP ČR na plnění dodavatele v rámci Smlouvy o poskytování služeb č. 1800769/4100053861

Název požadavku: Řízení přístupu a přístupových oprávnění dodavatele do vnitřní sítě VZP a k aktivům VZP ČR.

Stávající stav (dále uvedené vnitřní předpisy VZP ČR budou dodavateli poskytnuty po přijetí objednávky):

1. Platný, ale již zastaralý vnitřní předpis PŘ č. 3/2013 – „Postup při přidělování přístupových oprávnění do informačního systému VZP ČR pracovníků smluvních partnerů VZP ČR
2. Platný, ale již zastaralý vnitřní předpis PN ÚICT č. 05/2015 – „Postup při přidělování přístupových oprávnění do informačního systému VZP ČR pracovníkům smluvních partnerů VZP ČR“
3. Platný vnitřní předpis PN ÚICT 1/2016 - „Detailní bezpečnostní politika pro ICT VZP ČR“, který obsahuje Přílohu č. 7 - „Řízení přístupu do IS VZP ČR“, která se na PŘ č. 3/2013 odkazuje. Je zde uveden externista, kterým lze chápat i dodavatele. Je třeba sjednotit pojmy.
4. PŘ č. 1/2016 – „Detailní bezpečnostní politika pro koncové uživatele ICT VZP ČR “ odkazuje na dodavatele v čl. 27 odst. 2)
5. Úsekem informačních a komunikačních technologií (ÚICT) byla v době od 8/2018 do 2019 vyvinuta interní aplikace EEX (Evidence externistů), od 11/2019 byl zahájen její pilotní provoz. Aplikace EEX má zajišťovat evidenci všech přístupů a přístupových oprávnění dodavatelů a má v ní probíhat životní cyklus řízení přístupů včetně procesu schvalování přístupů a přístupových oprávnění. Dokument popisující některé činnosti v EEX se nazývá „Pracovní postup pro aplikaci Evidence Externistů (EEX)“. Dle zjištění neobsahuje všechny potřebné informace, dle nichž by osoba, která za VZP odpovídá za vyžádání přístupu pro dodavatele, mohla pracovat tak, aby úspěšně spustila proces zadání nového požadavku na zřízení přístupu dodavateli a jeho schvalování. Nutné dokument revidovat.
6. Nově od 5/2020 byl schválen a je platný dokument „Podmínky pro přístup Dodavatele do vnitřní sítě VZP ČR prostřednictvím VPN VZP ČR“ (dále jen „Podmínky VPN“), který je přikládán jako příloha ke všem nově uzavíraným hlavním smlouvám s dodavateli.
7. V současnosti bylo zjištěno, že dle nových Podmínek VPN nejsou povinnosti VZP jasně dokumentovány a stanovena za ně příslušným útvarům odpovědnost včetně potřebných činností a procesů. Do dodaných dokumentů je nutné toto zapracovat.
8. Dokument „Postupy pro řízení účtů a přístupu do AAUX“ a“ Postupy pro řízení účtů a přístupu do Active Directory“, viz Intranet.
9. Dokument „Politika VPN přístupu“ a dokument „Certifikační politika“.

Bylo zjištěno, že v tuto chvíli nemá ÚICT (Úsek informačních a komunikačních technologií VZP ČR) jasný názor na to, jak by kompletní procesy spojené s řízením přístupu a přístupových oprávnění měly být nastaveny/fungovat. Proto OIKB (Oddělení informační a kybernetické bezpečnosti VZP ČR) zadává toto plnění (vytvoření potřebných dokumentů) dodavateli s tím, že OIKB se bude na plnění podílet za oblast stanovení a kontroly bezpečnostních opatření a navrhovaných procesů a ÚICT bude poskytovat potřebnou součinnost.

Cíl plnění:

Cílem plnění je vytvořit ucelený vnitřní předpis popisující na jednom místě plně pravidla a požadavky kladené na řízení přístupu a přístupových oprávnění dodavatelů, který bude

odkazovat/jehož přílohou budou potřebné dokumenty popisující bezpečnostní opatření, procesní pravidla a postupy pro zajištění řízení životního cyklu přístupů dodavatelů, evidenci přístupů a provádění pravidelné kontroly přístupů, s uvedením dílčích kroků (činností) a stanovením odpovědností konkrétních rolí/útvarů za tyto kroky (činnosti), tak, aby všechny zainteresované útvary VZP ČR/zaměstnanci v daných rolích měly ucelený materiál s jasnými postupy, co v dané věci mají udělat, aby byl proces zřizování přístupů a přístupových oprávnění, vyžádaný na základě oprávněných potřeb dodavatele, zajištěn VZP plynule, s jasně danými kroky a pravidly a bez prodlev a byla zajištěna bezpečnost v řízení přístupů dodavatelů.

Minimální požadavky na plnění dodavatele:

A. VZP ČR požaduje prověřit stávající stav procesů spojených s životním cyklem řízení přístupu a přístupových oprávnění dodavatelů (zajištěním vyžadování/přidělování/změn/zablokování/ mazání účtů) a dle nejlepší praxe dodavatelem navrhnout nový stav řešení odrážejí bezpečnost.
B. VZP ČR požaduje dodat výše zmiňovaný ucelený vnitřní předpis ve formě příkazu ředitele VZP ČR s názvem „Řízení přístupu a přístupových oprávnění dodavatelů“ (dále jen „PŘ“), který nahradí plně PŘ 3/2013 a PN ÚICT č. 05/2015 příp. i další, a který bude popisovat celou problematiku řízení přístupu a přístupových oprávnění dodavatelů a činností nutných provést v tomto procesu danými útvary VZP ČR, tak aby tato oblast již nebyla potřeba řešit v různých jiných stávajících platných vnitřních předpisech.
   Přičemž předpokládáme, že PŘ bude řešit/stanovovat minimálně:
   1. pravidla a postupy řízení přístupů a přístupových oprávnění dodavatelů (autentizaci a autorizaci) ke všem aktivům a komponentám ICT VZP ČR, k nimž může mít dodavatel přístup včetně přístupu dodavatelů prostřednictvím VPN,
   2. stanovovat práva, povinnosti, odpovědnosti a vnitřní procesy k zajištění naplnění výše uvedených Podmínek VPN pro přístup Dodavatele do vnitřní sítě VZP ČR prostřednictvím VPN VZP ČR, pro všechny zúčastněné strany,
   3. uvádět bezpečnostní požadavky na cyklus řízení přístupu a přístupových oprávnění dodavatelů (vyžadování/změny/zablokování/ukončení),
   4. stanovovat pravidla a postupy pro provádění pravidelných revizí a kontrol přístupů a přístupových oprávnění úsekem ICT,
   5. stanovovat bezpečnostní opatření na zajištění řízení přístupu, stanovující bezpečnostní požadavky na technické nástroje k tomu využívané,
   6. začlenění aplikace EEX do procesu řízení přístupů dodavatelů, a odkazovat na uživatelskou příručku práce v EEX, kterou dodavatel reviduje tak, aby proces byl garantovi smlouvy jasný a též stanovoval závazná pravidla a postupy řízení přístupových oprávnění k aplikaci EEX,
   7. co se v rámci řízení přístupu a přístupových oprávnění dodavatelů vždy považuje za bezpečnostní incident, který je nutné hlásit Odboru bezpečnosti VZP ČR.

   Přičemž požadujeme, aby PŘ:
   a) odkazoval na dokument „Uživatelská příručka EEX - pravidla a postupy práce v EEX související s potřebou vyžádat/změnit/ukončit přístup a přístupové oprávnění garantem smlouvy za VZP“, dodavatel může vycházet z dokumentu bod 5 Stávající stav,
   b) odkazoval na dokument “Řízení přístupu a přístupových oprávnění k aplikaci EEX“. Tento dokument není vytvořen, VZP ČR ho požaduje v rámci plnění dodat, v něm požaduje zachovat požadavek na přístup uživatelů EEX jen k informacím, která daná role potřebuje včetně stanovení minimálních požadavků na logování aplikace EEX,
   c) odkazoval na dodavatelem revidovaný dokument „Postupy pro řízení účtů a přístupu do Active Directory“, příp. dodavatel vytvoří nový dokument „Řízení přístupu a přístupových oprávnění v Active Directory – dodavatelé“, který bude popisovat životní cyklus účtů dodavatelů v AD.,

d) odkazoval na dodavatelem revidovaný dokument „Postupy pro řízení účtů a přístupu do AAUX“, příp. dodavatel vytvoří nový dokument „Řízení přístupu a přístupových oprávnění do AAUX – dodavatelé“, který bude popisovat životní cyklus účtů dodavatelů v AAUX.
e) popisoval pravidla a postupy, které musí být zajištěny na straně VZP ČR ke splnění povinností daných VZP ČR v dokumentu Podmínky VPN (možné jako odkaz nebo příloha PŘ), včetně toho, že vytvoří/reviduje návody pro dodavatele, dle nichž si vygenerují žádost o certifikát atd.,
f) odkazoval na certifikační politiku pro vydávání VPN certifikátů dodavatelům a popisoval poskytované služby CA VZP v souvislosti s vydáváním/obnovou/revokací VPN certifikátů ČR dodavatelů a stanovoval náležitosti takových certifikátů vydávaných dodavatelům z hlediska doporučení NÚKIB a bezpečnosti (sha1 by již zřejmě nemělo být používáno). VZP požaduje takový dokument dodat.,
g) odkazoval na formulář pro vyžadování přístupových oprávnění k podpůrným aktivům VZP ČR dodavateli (tj. revidoval stávající existující formulář tak, aby v něm byly uvedeny všechny potřebné informace, které jsou nutné garantem smlouvy zadat, při vyžadování přístupu/přístupových oprávnění v aplikaci EEX (Příloha č. 1 Evidenční list PN ÚICT č. 05/2015 nevyhovuje současným potřebám),
h) odkazoval na závazné Podmínky VPN a uváděl, kdo odpovídá za to, že tyto Podmínky VPN budou součástí každé hlavní smlouvy,
i) bude mít přílohu, která bude popisovat bod 4. písm. B),
j) bude mít ukládací část s uvedenými úkoly, příp. část přechodných ustanovení.

VZP požaduje v návrzích dokumentů uvádět očekávaný stav řízení přístupů a přístupových oprávnění dodavatelů, nikoliv popisovat stávající stav, který nemusí být z pohledu procesního ani bezpečnostního vhodný. Očekávaný stav dodavatel po provedení analýzy konzultuje s ÚICT, příp. ostatními útvary tak, aby bylo zjištěno, že lze očekávaný stav naplnit a v přechodných ustanoveních PŘ uvedeno do kdy.

PŘ musí být koncipován tak, aby byl přehledný a členěný pro jednotlivé útvary VZP, příp. osoby zainteresované v procesu řízení přístupu a přístupových oprávnění dodavatelů, tedy např. aby si úsek zajišťující certifikační služby vzal jen dokument týkající se jeho a dle něho postupoval, aby garant smlouvy vzal pouze část řešící, jak vyžádá různé fáze životního cyklu v aplikaci EEX, aby si odpovědná osoba/útvar za provádění pravidelných kontrol v EEX vzala jen část popisující, jaké pravidelné kontroly má dělat a komu poskytovat výstup z kontroly, aby útvar mající na starost AAUX měl k dispozici jen svou část týkající se přístupů na AAUX dodavatelů.

V rámci vytvoření PŘ požaduje VZP ČR navrhované procesy ověřit/otestovat (na bezpečnost/funkčnost/ srozumitelnost práce) dle PŘ a na splnění zákonných požadavků a průkaznost činností při přidělování přístupů a přístupových oprávnění dodavatelům pro případný audit KB. Toto provede dodavatel spolu s OIKB.

C. VZP ČR v rámci plnění požaduje dodat též návrhy změnových listů k vnitřním předpisům uvedeným v stávajícím stavu, dotčených provedenou změnou tj. návrhy aktualizace částí/zrušení částí týkajících se řízení přístupu a přístupových oprávnění dodavatelů (z důvodu jejich nahrazení/přesunutí do nového PŘ) ve formátu dle vnitřního předpisu pro vydávání vnitřních předpisů. Současně požadujeme doplnit do PŘ č. 1/2016, který je určen pro všechny uživatele VZP informaci o tom, že vyžadování přístupu a přístupových oprávnění pro smluvní dodavatele VZP ČR řeší nový PŘ, dle něhož toto vyžadují oprávněné osoby uvedené v hlavní smlouvě s dodavatelem.

VZP požaduje návrhy dokumentů předem konzultovat a předložit k připomínkám dotčeným stranám (zpracovatelům, příp. předkladatelům) a jejich připomínky vypořádat mimo vnitřní připomínkové řízení.
Po předložení dokumentu a změnových listů do vnitřního připomínkového řízení na Intranetu vypořádat připomínky z připomínkového a schvalovacího řízení.

Přičemž VZP ČR požaduje se na všechny pracovníky dodavatele/dodavatele dívat jako na administrátory ve smyslu ZKB (zákon o kybernetické bezpečnosti), tj. dle vnitřních předpisů, že mají privilegovaná oprávnění s tím, že každý uživatel dodavatele, pokud pracuje v rámci více plnění, tj. různých smluv VZP s dodavatelem, musí mít z hlediska bezpečnosti samostatný účet pro každou takovou smlouvu a účet s parametry dle VKB (vyhláška č. 82/2018 Sb.).

<u>Předpokládaný harmonogram plnění:</u>

- do 4 měsíců od zahájení plnění předložení výstupů z bodům plnění A) – C),
- zbylý čas je na vypořádání připomínek v rámci interního připomínkového a schvalovacího řízení.