Příloha č. 3 – Bezpečnostní pravidla pro dodavatele

Cílem těchto bezpečnostních pravidel je snižování kybernetických rizik a zvyšování účinnosti bezpečnostních opatření chránící Aktiva KÚ JK, ke kterým mají přístup dodavatelé.

1. Základní odpovědnosti dodavatele (poskytovatel ve smyslu této smlouvy)

Dodavatel řešení:

a) Je povinen dodržovat požadavky na bezpečnost informací v souladu s platnými a účinnými právními předpisy České republiky.

b) Odpovídá za své řešení/dodávku/správu tak, aby respektovalo požadavky na bezpečnost KÚ JK, zabránilo bezpečnostním incidentům a stavu kybernetického nebezpečí.

c) Odpovídá za dodávku a implementaci řešení v požadované kvalitě i z pohledu bezpečnosti.

d) Ručí za trvalé zachování mlčenlivosti všech svých pracovníků i po ukončení smluvního vztahu s objednatelem.

Dodavatel je povinen akceptovat použití prostředků bezpečnostního auditu, které mohou být útvarem IT využity k sledování aktivit v prostředí ICT/IS či aktivity procházejících přes toto prostředí.

2. Ochrana Aktiv

Dodavatel se před vlastním přístupem k datům a informacím KÚ JK musí zavázat mlčenlivostí. Tzn., že platí povinnost Dodavatele se zavázat a také povinnost pracovníků KÚ JK (prioritně ve smlouvě, prohlášením dodavatele, formulářem, ...) zavázat dodavatele a nezpřístupnit data a informace dodavateli dříve, než dojde k jeho závazku mlčenlivosti (tj. podpisu NDA – Non Disclosure Agreement či CA – Confidentiality Agreement).

3. Přístup k ICT/IS

Přihlášení dodavatele do sítě KÚ JK musí podléhat kontrole přístupu na základě autorizace po předchozí autentizaci, včetně autentizace přes VPN v případě užití VPN klienta. Přihlašovací proces do VPN a do Windows domény poskytuje základní bezpečnostní funkce – nikdy se nezobrazuje vkládané heslo a heslo není nikde přenášeno a ukládáno v nezašifrované formě. Přístup ke službám ICT/IS je vždy zajištěn přes proces autentizace, autorizace a bezpečnostního auditu.

4. Ochrana před škodlivým softwarem

Dodavatel je povinen:

a) Centrálně organizovat zabezpečení svých koncových stanic v připojeních do své infrastruktury (např. řízení personálních firewallů, antivirového SW atd.) a to minimálně na úrovni standardů KÚ JK. Standardy KÚ JK se řídí zákonem č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen ZoKB), a zejména vyhláškou č. 82/2018 Sb., o kybernetické bezpečnosti, ve znění pozdějších předpisů (dále jen VoKB) a dále bezpečnostními doporučeními NCKB pro administrátory v aktuálně platné verzi. Dodavatel by měl v přiměřené míře splňovat požadavky uvedených dokumentů.

b) Obsahem antivirové ochrany jsou taková opatření technického a administrativního charakteru, která vedou k detekci a následnému odstranění infiltrujícího software u všech prostředků provozovaných v rámci infrastruktury Dodavatele.

c) Dodavatel musí na své straně definovat zásady bezpečného užívání Internetu a s těmito zásadami seznámit veškerý personál užívající ICT prostředky infrastruktury Dodavatele.

d) Dodavatel musí na pracovních stanicích v jeho odpovědnosti zajistit bezpečné nakonfigurování prohlížečů obsahu Internetu (např. www prohlížeče).

5. Řízení bezpečnostních rizik

V oblasti plnění povinností uvedených v § 5 VoKB, se dodavatel zavazuje zejména:

a) Řídit vlastní rizika, která mohou ovlivnit poskytování předmětu plnění.

b) Alespoň 1x ročně vytvořit a předložit Zprávu o řízení kybernetických rizik, která bude minimálně pokrývat:

   I. vyhodnocení stavu kybernetické bezpečnosti za hodnocený rok, včetně vyhodnocení souladu s těmito Bezpečnostními požadavky
   II. identifikaci a hodnocení rizik s vazbou na předmět plnění,
   III. realizovaná bezpečnostní opatření,
   IV. nepokrytá bezpečnostní rizika a návrh opatření,
   V. vyhodnocení bezpečnostních událostí a incidentů.

6. Zvládání kybernetických bezpečnostních událostí a incidentů

V oblasti plnění povinností uvedených v § 14 VoKB, se dodavatel zavazuje zejména:

a) Stanovit a popsat na své straně činnosti, role a jejich odpovědnosti a pravomoci vedoucí k rychlému a účinnému zvládání bezpečnostních incidentů.

b) Bez zbytečného odkladu hlásit objednateli všechny bezpečnostní události a incidenty s potenciálním negativním dopadem na objednatele, a to stanoveným komunikačním kanálem nebo prostřednictvím odpovědné osoby.

c) Vyhodnocovat informace o bezpečnostních incidentech a uchovávat je pro budoucí použití s ohledem na požadavky platné české a evropské legislativy.

d) V případě vzniku bezpečnostní události a následného zvládání a vyhodnocování bezpečnostního incidentu a/nebo v případě podezření na bezpečnostní incident poskytnout objednateli součinnost a relevantní informace o podezřelém zařízení či osobě na straně dodavatele.

e) Bez zbytečného odkladu a po dohodě s objednatelem realizovat opatření požadovaná objednatelem v dohodnutých termínech ke snížení dopadu bezpečnostního incidentu nebo zamezení pokračování incidentu.

f) Spolupracovat při analýze příčin bezpečnostního incidentu a navrhnout opatření s cílem zamezit jeho opakování v případě, že dodavatel bezpečnostní incident zapříčinil nebo se na jeho vzniku podílel.

Dodavatel bere na vědomí, že postup zvládání bezpečnostního incidentu či jiný důsledek porušení těchto Bezpečnostních požadavků, jehož příčina je na straně dodavatele, nebude posuzován jako okolnost vylučující odpovědnost dodavatele za prodlení s řádným a včasným plněním předmětu této smlouvy a nebude důvodem k jakékoli náhradě případné újmy dodavateli či jiné osobě ze strany objednatele. Ostatní ustanovení ohledně odpovědnosti dodavatele za prodlení obsažená v této smlouvě nejsou tímto ustanovením dotčena.

7. Řízení kontinuity činností

V oblasti plnění povinností uvedených v § 15 VoKB, se dodavatel zavazuje zejména:

a) Vyhodnocovat a dokumentovat možné dopady kybernetických incidentů s posouzením možných dopadů do kontinuity činností.

b) Určit minimální úroveň poskytovaných služeb přijatelnou z hlediska zajištění kontinuity poskytovaných činností.

c) Určit dobu obnovení chodu, během které bude po bezpečnostním incidentu obnovena minimální úroveň poskytovaných služeb dle písm. b).

d) Určit časové období, za které musí být zpětně obnovena data po kybernetickém bezpečnostním incidentu nebo po selhání.

e) Vypracovat, aktualizovat a pravidelně testovat plány kontinuity činnosti a havarijní plány související s poskytováním předmětu plnění.

8. Akvizice, vývoj a údržba

V oblasti plnění povinností uvedených v § 13 VoKB, se dodavatel zavazuje zejména:

a) Zajistit bezpečnou implementaci, inovaci, aktualizaci a testování technologií, které jsou předmětem plnění smlouvy.

b) Předat objednateli dokumentaci předmětu plnění minimálně v následujícím rozsahu:

I. dokumentaci skutečného provedení,
II. dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů,
III. dokumentaci obsahující popis autorizačního konceptu a oprávnění,
IV. dokumentaci obsahující zálohovací a archivační postupy,
V. dokumentaci obsahující instalační a konfigurační postupy,
VI. dokumentaci pro zajištění kontinuity provozu a obnovy po havárii.

9. Kontrola a audit Dodavatele

V oblasti plnění povinností uvedených v § 16 VoKB, se dodavatel zavazuje zejména:

a) Umožnit objednateli provést na straně dodavatele minimálně jedenkrát (1x) za rok pravidelné vyhodnocení rizik souvisejících s předmětem plnění a poskytnout potřebnou součinnost.

b) Umožnit objednateli nebo Národnímu úřadu pro kybernetickou a informační bezpečnost (NÚKIB) provést kontrolu souladu zavedených bezpečnostních opatření vyžadovaných na dodavateli těmito Bezpečnostními požadavky a poskytnout potřebnou součinnost. Tento odstavec se neaplikuje, pokud je dodavatel v rozsahu předmětu plnění orgánem nebo osobou uvedenou v § 3 písm. c), d), f) nebo g) ZoKB;

c) Umožnit objednateli provést po vzájemné dohodě v rozsahu předmětu plnění testy dostupnosti, důvěrnosti a integrity dat, informací a jiných zdrojů dodavatele, které jsou využívány k poskytování předmětu plnění, a poskytnout potřebnou součinnost;

d) Zajistit bezodkladné odstranění zjištěných nedostatků a nesouladu s těmito Bezpečnostními požadavky.

10. Ošetření výjimek

Ve výjimečných případech je možno vyhlásit výjimku z dodržování bezpečnostních pravidel. Udělení výjimek ze stanovených pravidel se provádí na základě požadavku zaslaného manažerovi kybernetické bezpečnosti, který má právo výjimku udělit.

Schváleno: Bezpečnostní komise – Výbor pro řízení kybernetické bezpečnosti

HartSOFT
Digitálně podepsal Petra Hartová
Datum: 2025.03.05 09:04:42 +01'00'