Minimální požadavky objednavatele na významné dodavatele

Dodavatel = rovněž také zhotovitel, poskytovatel, účastník apod.

Objednavatel požaduje, aby dodavatel plnil zejména pak níže uvedené minimální požadavky významného dodavatele:

Pokud analýza v souvislosti s řízením rizik určí některé dodavatele ONN jako významné (§2 písm. n) VoKB), musí být celý nákupní proces od zadávacího řízení přes výběr dodavatele po smlouvu v souladu s přílohou č. 7 VoKB.

Cílem je zajištění plnění legislativy a snížení rizika v souvislosti se zajištěním důvěrnosti, dostupnosti a integrity systémů, které zajišťují výkon základní služby. Proto je tento požadavek pro ONN naprosto nezbytný.

Každý významný dodavatel tedy musí splňovat tyto minimální požadavky z hlediska kybernetické bezpečnosti a legislativy:

1. ŘÍZENÍ INFORMAČNÍ A KYBERNETICKÉ BEZPEČNOSTI

1.1 Významný dodavatel má povinnost ve svých interních procesech realizovat tato opatření:

1.1.1 má stanoven plán rozvoje bezpečnostního povědomí, jehož cílem je zajistit odpovídající vzdělávání a zlepšování bezpečnostního povědomí v této minimální formě, obsahu a rozsahu:

a) poučení uživatelů, administrátorů, osob zastávajících bezpečnostní role a dodavatelů o jejich povinnostech a o bezpečnostní politice;
b) potřebná teoretická i praktická školení uživatelů, administrátorů a osob zastávajících bezpečnostní role formou vstupních a pravidelných školení;

1.1.2 pro osoby zastávající bezpečnostní role v souladu s plánem rozvoje bezpečnostního povědomí zajišťuje pravidelná odborná školení, přičemž vychází z aktuálních potřeb v oblasti kybernetické bezpečnosti a provádí a ověřování bezpečnostního povědomí zaměstnanců v souladu s jejich pracovní náplní;

1.1.3 zajišťuje kontrolu dodržování bezpečnostní politiky ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role a má nastaven proces restrikcí pro vynucení dodržování bezpečnostních politik;

1.1.4 vede o provedených školení přehledy, které obsahují předmět školení a seznam osob, které školení absolvovaly.

1.1.5 alespoň jedenkrát ročně předává ONN informace, týkající se osob souvisejících s poskytovaným předmětem plnění smlouvy, o provedených školeních a jejich obsahu.

1.1.6 v případě ukončení smluvního vztahu s administrátory a osobami zastávajícími bezpečnostní role zajišťuje předání odpovědností;

1.1.7 určuje pravidla a postupy pro řešení případů porušení stanovených bezpečnostních pravidel ze strany uživatelů, administrátorů a osob zastávajících bezpečnostní role;

1.2 Využívá-li dodavatel při poskytování předmětu plnění subdodavatele, je povinen zajistit adekvátní dodržování těchto bezpečnostních pravidel rovněž ve smluvních vztazích se svými subdodavateli.

2. PERSONÁLNÍ BEZPEČNOST

2.1 Dodavatel zajistí seznámení všech osob, účastnících se plnění dle této uzavřené smlouvy s ONN a s těmito bezpečnostními pravidly, a to písemně.

2.2 Osoby, účastnící se plnění dle této uzavřené smlouvy s ONN musí mít prokazatelné potřebné kvalifikační předpoklady, zkušenosti a znalosti nutné k zajištění řádného plnění smlouvy.

3. ŘÍZENÍ PROVOZU

3.1 Dodavatel se zavazuje:

3.1.1 zajistit bezpečný provoz informačního systému a infrastruktury využívané pro poskytování předmětu plnění v souladu s požadavky vyhlášky č. 82/2018 Sb., a doporučeními technických norem řady ISO/IEC 27000, zejména pak mezinárodní bezpečnostní standardy, jako jsou ISO/IEC 27001 (pro řízení bezpečnosti informací), IEC 62443 (pro zabezpečení průmyslových řídicích systémů);

3.1.2 kdykoliv v průběhu trvání této platnosti smlouvy na vyžádání poskytnout ONN přehled o bezpečnostních opatřeních zavedených na svém informačním systému a infrastruktuře, kterými plní předmět této smlouvy;

3.1.3 povinen předat certifikáty o plnění výše uvedených standardů již v době probíhajícího výběru dodavatele. V případě, že dodavatel nedisponuje uvedenými certifikáty, neznamená to vyloučení z výběru dodavatele. V tomto případě musí detailně uvést v příloze k nabídce, zda vůbec a jakým způsobem plní tyto podmínky ONN pro významné dodavatele. ONN může v rámci interních procesů rozhodnout, zda je riziko neplnění dílčích částí těchto podmínek akceptovatelným rizikem.

4. ZABEZPEČENÍ KOMUNIKACE

4.1 Komunikace mezi systémy, jež jsou předmětem plnění této smlouvy, a ostatními řídicími systémy musí být šifrována pomocí silných kryptografických metod (např. TLS). Povinností dodavatele je zajistit, aby žádná data nebyla odesílána nebo přijímána bez řádného šifrování.

5. ŘÍZENÍ PŘÍSTUPU

5.1 Identifikace, podmínky identifikace:

a) Každý zaměstnanec dodavatele podílející se na plnění smlouvy výpočetními prostředky dodavatele, musí mít v rámci své ICT infrastruktury evidován a veden svůj vlastní jedinečný uživatelský účet, kterému jsou v jednotlivých systémech, modulech nebo aplikacích přiřazeny specifické role. Každý zaměstnanec dodavatele musí být veden s platnými identifikačními a aktuálními kontaktními údaji.

5.2 Autentizace, podmínky pro autentizaci při využití ICT infrastruktury ONN:

a) k jednoznačné identifikaci privilegovaných uživatelů systémů se využívá více faktorová autentizace;
b) ověření heslem - pokud není možné použít jednoznačnou identifikaci privilegovaných uživatelů více faktory, je použita autentizace pomocí kryptografických klíčů se zaručením obdobné úrovně bezpečnosti nebo použití hesla s definovanými pravidly.

5.3 Autorizace - Zaměstnanci dodavatele jsou povinni v ICT infrastruktuře ONN využívat privilegovaná oprávnění jen v přiměřené míře a jen po dobu nezbytně nutnou pro vykonání činností v souladu s plněním předmětu smlouvy. Uživatelé nesmějí používat účty s privilegovanými oprávněními pro běžnou práci nesouvisející se správou systému.

5.4 Vzdálený přístup - Pracovní stanice dodavatele přistupující k infrastruktuře ONN prostřednictvím VPN (Virtual Private Network) musí mít:

a) pokročilou funkční antivirovou ochranu;
b) funkční personal firewall;
c) funkční nastavené automatické aktualizace antiviru;
d) aktualizované aplikace třetích stran za dodržení autorských práv třetích stran;
e) zajištěno šifrování všech paměťových médií, na kterých jsou uložena data a informace ONN. Přístup k paměťovým médiím a k dešifrování chráněných dat a informací ONN musí být umožněno jen oprávněným osobám dodavatele;
f) nainstalovaného VPN klienta, instalovaného výlučně v odpovědnosti dodavatele;

5.5 Fyzická bezpečnost - Dodavatel musí zajistit fyzickou bezpečnosti objektů, které jsou dotčeny s plněním smlouvy s ONN, zejména pak serveroven, infrastruktury apod.

6 ŘÍZENÍ ZMĚN

6.1 Podmínky - změny na straně dodavatele musí být řízeny s ohledem na kritičnost informací, systémů, procesů a opětovným posuzováním rizik.

6.2 Dodavatel se zavazuje:

a) řídit a evidovat smluvní změny;

b) řídit a evidovat změny v poskytovaných službách v souladu s požadavky VoKB a doporučeními technických norem řady ISO/IEC 27000.

7 AKVIZICE, VÝVOJ A ÚDRŽBA

7.1 Dodavatel se zavazuje:

7.1.1 zajistit bezpečnou implementaci, inovaci, aktualizaci, testování technologií, které jsou předmětem plnění, a to jak nových verzí, tak servisních patchů;

7.1.2 předat ONN dokumentaci předmětu plnění minimálně v následujícím rozsahu:

a) dokumentaci skutečného provedení, je-li to vzhledem k předmětu plnění této smlouvy validní;
b) dokumentaci všech bezpečnostních nastavení, funkcí a mechanismů;
c) dokumentaci obsahující popis autorizačního konceptu a oprávnění;
d) dokumentaci obsahující zálohovací a archivační postupy;
e) dokumentaci obsahující instalační a konfigurační postupy;
f) dokumentaci zahrnující testy zranitelností a soulad s bezpečnostními požadavky ONN;
g) dokumentaci pro zajištění kontinuity provozu a obnovy po kybernetické bezpečnostní události nebo kybernetickém bezpečnostním incidentu.

ONN nebude považovat provedení jakýchkoliv prací za hotové bez předání uvedené dokumentace.

7.2 V případě vývoje se dodavatel zavazuje:

a) dodržovat a implementovat nejlepší praktiky pro bezpečný vývoj softwaru dle doporučení technických norem řady ISO/IEC 27000;
b) pokud jsou softwarové auditní činnosti a předání zdrojového kódu k řešení součástí plnění dle smlouvy, bude umožněn audit prováděného nebo provedeného plnění a na písemnou žádost bude předložen vyvíjený zdrojový kód k řešení na provedení code review (automatizovaně prostřednictvím bezpečnostního nástroje i manuálně), a to zejména za účelem ověření skutečnosti, zda bylo postupováno dle plnění v souladu se smlouvou;
c) zajistit, že plnění bude obsahovat jen ty součásti, které jsou objektivně potřebné pro řádné provozování řešení anebo které jsou specifikovány výslovně ve smlouvě (zejména, že řešení nebude obsahovat žádné nepotřebné komponenty, žádné programové vzorky apod.);
d) zajistit bezpečnost testovacího prostředí u dodavatele a ochranu poskytnutých dat ONN;
e) zajistit, že v rámci poskytovaného plnění bude dodávané řešení v souladu s doporučeními technických norem řady ISO/IEC 27000;
f) nevyvíjet, nekompilovat a nešířit v prostředí ONN programový kód, který má za cíl nelegální ovládnutí, narušení dostupnosti, důvěrnosti nebo integrity nebo neautorizované či nelegální získání dat a informací.

7.3 Bezpečnostní aktualizace a patchování:

a) Dodavatel zaručuje pravidelné aktualizace softwaru a patchování zranitelností, aby se předešlo možným kybernetickým útokům.
b) Musí existovat jasný proces, jakým způsobem a jak rychle jsou zranitelnosti řešeny po jejich identifikaci.

8 MONITORING

8.1 Přístup zaměstnanců dodavatele k interním informacím a k informačním a komunikačním a řídícím systémům související se smlouvou s ONN je nepřetržitě zaznamenáván, monitorován a vyhodnocován.

Události v systémech, jež jsou předmětem plnění této smlouvy, a souvisejících systémech jsou zaznamenávány do logů, minimálně však:

a) úspěšné a neúspěšné přihlášení a odhlášení uživatelů;
b) činnosti provedené administrátory;
c) úspěšné a neúspěšné manipulace s účty, oprávněními a právy;
d) neprovedení činností v důsledku nedostatku přístupových oprávnění;
e) činnosti uživatelů, které mohou mít vliv na bezpečnost informačního, komunikačního a řídícího systému;
f) zahájení a ukončení činností technických aktiv;
g) automatická varovná nebo chybová hlášení technických aktiv;
h) přístupy k logům, pokusy o manipulaci s logy a změny nastavení nástroje pro zaznamenávání činností a použití mechanismů autentizace včetně změny údajů, které slouží k přihlášení.

8.2 Dodavatel je povinen průběžně monitorovat v rámci své ICT infrastruktury zveřejněné a známé bezpečnostní chyby, které mohou ovlivnit hladký a bezpečný provoz systémů souvisejících s jím poskytovanými službami. Jedná se například o zranitelnosti v operačních systémech, software třetích stran, webové komponenty atd.

9 KYBERNETICKÉ BEZPEČNOSTNÍ UDÁLOSTI / INCIDENTY (dále jen „KBI, KBU“)

9.1 Dodavatel má za povinnost hlásit veškerá podezření na kybernetické bezpečnostní události MKB v ONN. Termín hlášení je bezprostředně (ihned, bez prodlení) po zjištění KBI/KBU, a to telefonicky s následným shrnutím informací prostřednictvím e-mailu. Informace musí vždy minimálně obsahovat:

a) data a času zjištění;
b) povahu události;
c) zdroje události;
d) cíle / oběti události;
e) potencionálního dopadu.

9.2 Disaster recovery plán - Dodavatel musí disponovat plány pro obnovení provozu po KBI/KBU tak, aby byl schopen poskytovat plnění této smlouvy.

10 AUDIT DODAVATELE (ZÁKAZNICKÝ AUDIT), ZÁLOHOVÁNÍ A PENETRAČNÍ TESTOVÁNÍ

10.1 Oprávnění k provedení auditu dodavatele - ONN si vyhrazuje právo provádět audity významného dodavatele, a to i prostřednictvím jiné právnické osoby. ONN odešle minimálně 5 pracovních dnů oznámí dodavateli záměr na provedení auditu. Obě strany si dohodnou obsah, potřebnou součinnost a časový plán auditu s tím, že ONN se zavazuje postupovat tak, aby nenarušila provozní potřeby dodavatele.

10.2 Auditovaná strana (dodavatel) obdrží k vyjádření závěrečnou zprávu auditu obsahující případná zjištění, na jejichž základě:

a) dodavatel navrhne opatření a termíny řešení a předá jejich seznam ONN k odsouhlasení.
b) ONN následně potvrdí souhlas s navrženými opatřeními nebo je vrátí s připomínkami dodavateli k přepracování.

10.3 Auditovaná strana (dodavatel) má za povinnost v určeném čase zajistit realizaci dohodnutých nápravných opatření.

10.4 Dodavatel musí provádět v pravidelných intervalech penetrační testování svých systémů, které jsou dotčeny se zajištěním výkonu smlouvy s ONN. Výsledné protokoly poskytne na vyžádání bezodkladně ONN.

10.5 Dodavatel je povinen provádět zálohování dat ONN tak, aby bylo zajištěno jejich obnovení v případě potřeby. Dodavatel je současně pravidelně (kvartálně) provádět testování obnovy dat ze zálohy.

11 OCHRANA AKTIV PROTI NEAUTORIZOVANÝM ČINNOSTEM

11.1 Dodavatel na aktiva ONN neinstaluje a nepoužívá nástroje, které nejsou součástí předmětu plnění.

12 PODMÍNKY PŘI UKONČENÍ SMLOUVY

12.1 V případě ukončení smluvního vztahu musí být ukončeny veškeré přístupy dodavatele a jeho zaměstnanců k aktivům ONN nejpozději k termínu ukončení smluvního vztahu.

12.2 Pokud byla dodavateli poskytnuta informační aktiva (data) ONN, musí být nejpozději k termínu ukončení smluvního vztahu vrácena a beze zbytku smazána způsobem dle standardu, který definuje ONN před touto skutečností ze všech informačních systémů dodavatele a nosičů dodavatele taková aktiva obsahujících.