TECHNICKÁ SPECIFIKACE

1 Předmět plnění

Předmětem plnění veřejné zakázky je provedení analýzy stavu kybernetické bezpečnosti dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti), ve znění pozdějších předpisů (dále jen „ZoKB“) a vyhlášky č. 82/2018 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních, náležitostech podání v oblasti kybernetické bezpečnosti a likvidaci dat (vyhláška o kybernetické bezpečnosti), v platném znění (dále jen „VoKB“), včetně otestování stavu zabezpečení IT infrastruktury.

1.1 Prostředí STC

STÁTNÍ TISKÁRNA CENIN, státní podnik (dále jen „STC“) v současné době není tzv. povinnou osobou ve smyslu § 3 ZoKB, byla však informována o její roli významného dodavatele ze strany povinné osoby. STC má současně zavedený a certifikovaný systém řízení bezpečnosti informací v rozsahu normy ČSN EN ISO/IEC 27001:2013.

1.1.1 Současný stav dokumentace

STC má platnou směrnici Systém řízení bezpečnosti informací (dále jen „SŘBI“), která je závazná pro všechny zaměstnance. Na tuto směrnici navazují metodické pokyny útvaru IT a provozní dokumentace informačních aktiv. Bezpečnostní dokumentace reflektuje požadavky ZoKB a VoKB, přičemž absence klasifikace dle § 3 ZoKB je nahrazena vlastní metodikou, která vychází z analýzy rizik. Přibližný rozsah jednotlivých dokumentů (dále jen „související dokumentace“) je uveden níže.

- Směrnice SŘBI (1 dokument, celkem **100** stran A4);
- Metodické pokyny (12 dokumentů, celkem **60** stran A4);
- Provozní dokumentace (20 dokumentů, celkem **100** stran A4);
- Havarijní plán (11 dokumentů, celkem **60** stran A4);
- Směrnice řízení dokumentace (celkem **30** stran A4);
- Další relevantní dokumentace (do **100** stran A4);
- Registr aktiv (**60** položek, resp. řádků);
- Analýza rizik (**160** položek, resp. řádků).

1.1.2 Současný stav IT infrastruktury

STC provozuje svou IT infrastrukturu ve třech výrobních závodech, přičemž z hlediska síťové topologie je tato infrastruktura dělena na administrativní síť a na několik výrobních sítí. Tyto sítě jsou od sebe vzájemně fyzicky odděleny.

V administrativní síti (dále jen „AS“) jsou připojeni všichni administrativní pracovníci a je určena pro běžnou operativu, jako je například provoz podpůrných informačních systémů nebo elektronické pošty. AS je připojena do sítě internet a je tvořena z níže uvedených prvků.

- **80** aktivních prvků;
- **3** firewallů;
- **15** fyzických serverů;
- **160** virtuálních serverů;
- **250** koncových stanic;
- **50** dalších síťových prvků.

Výrobní sítě (dále jen „VS“) jsou určeny pro provoz výrobních systémů STC, u kterých je nutné zajistit vysokou míru důvěrnosti a integrity. VS nejsou připojeny do sítě internet. Pro účely této analýzy STC určila dvě konkrétní VS, přičemž každá z níže uvedených zastupuje specifickou kategorii.

Výrobní síť 1 (dále jen „VS1“)

- **1** aktivní prvek;
- **2** fyzické servery;
- **6** koncových stanic.

Výrobní síť 2 (dále jen „VS2“)

- **6** aktivních prvků;
- **4** fyzické servery;
- **20** koncových stanic.

1.2 Dokumentační část

Cílem této části analýzy je ověřit současný stav existující související dokumentace vzhledem k požadavkům ZoKB a VoKB. Analýza dokumentační části bude zahrnovat minimálně níže uvedené.

1.2.1 Posouzení stavu SŘBI

Posouzení obsahu, formy a struktury související dokumentace z hlediska požadavků ZoKB, VoKB a zabezpečení kontinuity činností. Předmětem posouzení je AS i VS. Výstup bude obsahovat níže uvedené části.

- Shrnutí stavu SŘBI s uvedenými zjištěními a návrhy opatření;
- Posouzení hierarchie související dokumentace s ohledem na různé řídící dokumenty v případě AS/VS;
- Doporučení na zlepšení bezpečnosti IT z pohledu implementovaných procesů;
- Návrhy úprav související dokumentace včetně přípravy a předání šablon konkrétních dokumentů;
- Případné návrhy nové související dokumentace včetně přípravy a předání šablon dokumentů;
- Stanovení priorit potřebných opatření a návrh harmonogramu jejich realizace.

1.2.2 Posouzení stavu organizačních opatření dle VoKB

Zhodnocení míry implementace organizačních opatření v procesech útvaru IT a koncových uživatelů v rozsahu dle § 3 až § 16 VoKB. Předmětem posouzení je AS. Výstup bude obsahovat níže uvedené části.

- Shrnutí stavu organizačních opatření s uvedenými zjištěními a návrhy opatření;
- Vyhotovení návrhů řešení neúplných či chybějících organizačních opatření;
- Stanovení priorit potřebných opatření a návrh harmonogramu jejich realizace.

1.2.3 Posouzení stavu technických opatření dle VoKB

Zhodnocení míry skutečného stavu implementace technických opatření v rozsahu dle § 17 až § 29 VoKB. Předmětem posouzení je AS. Výstup bude obsahovat níže uvedené části.

- Shrnutí stavu technických opatření s uvedenými zjištěními a návrhy opatření;
- Vyhotovení návrhů řešení neúplných či chybějících technických opatření;
- Případný návrh na doplnění, změnu či optimalizaci používaných bezpečnostních technologií;
- Stanovení priorit potřebných opatření a návrh harmonogramu jejich realizace.

1.3 Technická část

Cílem technické části analýzy je nedestruktivním způsobem prověřit úroveň zabezpečení IT infrastruktury, s cílem zvýšit její odolnosti vůči kybernetickým hrozbám a útokům. Předmětem technické části je AS. Analýza technické části bude zahrnovat minimálně níže uvedené.

1.3.1 Identifikace aktiv v síti STC

- Poskytovatel pomocí skenu sítě identifikuje různé systémy v síti a infrastruktuře STC;
- Identifikace aktiv bude provedena s ohledem na výsledky analýzy dokumentační části.

1.3.2 Zjištění konfiguračních detailů

- U identifikovaných systémů Poskytovatel otestuje různé atributy, jako je např. operační systém, otevřené porty, nainstalovaný software, uživatelské účty nebo souborová struktura systému.

1.3.3 Přiřazení známých zranitelností

- Výsledky předchozích bodů (1.3.1 a 1.3.2) Poskytovatel použije pro k přiřazení známých zranitelností k identifikovaným systémům;

1.3.4 Ohodnocení identifikovaných hrozeb

- U zranitelností s vysokou mírou rizikovosti Poskytovatel manuálně prověří možnost jejich zneužití s cílem dosažení kompromitace systémů;
- Určení míry výsledné závažnosti zranitelností bude provedeno s ohledem na výsledky analýzy dokumentační části.

2 Obecné požadavky

Analýza zahrne v dostatečném detailu předanou související dokumentaci, následná hloubková analýza bude provedena formou řízených rozhovorů.

2.1 Seznámení s prostředím STC

- Předmětem seznámení budou informační a komunikačními systémy a technologie, dále procesy a související dokumentace, které se vztahují k oblasti kybernetické bezpečnosti a řízení rizik.

2.2 Vypracování návrhu aktivit ke zlepšení kybernetické bezpečnosti

- Výstupem bude popis budoucího stavu SŘBI a přehled doporučených technických i organizačních bezpečnostních opatření v provozu chráněných aktiv;
- Jednotlivé oblasti budou posouzeny ve smyslu současné úrovně zralosti i návrhu zralosti cílové včetně odůvodnění.

2.3 Provedení prioritizace aktivit a návrh celkového harmonogramu provedení opatření

- Výstupem bude seznam všech aktivit s určením jejich priorit, vzájemných závislostí, doporučení na čas jejich zahájení a odhad jejich doby trvání;
- Z analýzy bude pro každou oblast patrné, jaká opatření mají nejvyšší účinnost ve smyslu snížení bezpečnostního rizika a měla by být realizována přednostně;
- Zavedení opatření budou naplánována metodou, jež zajistí co nejrychlejší snížení nejvýznamnějších rizik.

2.4 Součinnost STC

- STC umožní Poskytovateli přístup do AS za účelem realizace technické části analýzy;
- Poskytovatel je povinen definovat konkrétní parametry pro vytvoření FW pravidla s cílem zpřístupnit určené segmenty sítě pro účely technické části analýzy.

3 Harmonogram

- T = okamžik nabytí účinnosti smlouvy (předpoklad okamžiku T je 1.7.2022);
- T + 10 pracovních dní = předložení finální verze harmonogramu provedení analýzy KB;
- T + 2 měsíce = předání návrhu dokumentační části zprávy;
- T + 4 měsíce = předání akceptované závěrečné zprávy (dokumentační a technická část);