MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Ministerstvo financí České republiky

NÚKIB

eGC tým Bezpečnost

Hodnocení dopadů a zařazování do bezp. úrovní

Závazná bezpečnostní opatření pro dodavatele

Plk. Ing. Tomáš Hampl, PPČR

Ing. Zdeněk Jiříček, AFCEA / Microsoft s.r.o.

Pracovní tým Bezpečnost

- **Zástupci**
  - Státní organizace
  - „Bezpečnostní složky“
  - NÚKIB / NCKB
  - ÚOOÚ
  - Státní podniky (NAKIT, SPCSS)
  - Odborná veřejnost (společná nominace Hospodářské komory, ICT Unie, AFCEA)
- **Poslání**
  - Pravidla umístění do státní nebo komerční části eGC na základě hodnocení bezpečnostních dopadů (kap. 5.1.2, 5.1.3 SAZ)
  - Stanovení bezpečnostních požadavků na obě části SeGC, KeGC

Bezpečnost v SAZ eGC

- Kap. 5.2 – Hodnocení úrovně bezpečnostních dopadů
  - 5.2.1 Určení úrovně bezpečnostních dopadů IS
  - 5.2.2 Určení požadované bezpečnostní úrovně služeb eGC
  - 5.2.3 Vztah k ZKB a k ZoUI
  - 5.2.4 Zpracování osobních údajů a vazba na GDPR
- Kap. 6.2 - Bezpečnostní standardy a opatření
  - 6.2.1 Místo uložení a zpracování dat
  - 6.2.2 Bezpečnostní úrovně služeb eGC (Tabulka opatření)
  - … dále bezp. opatření na straně uživatelů, bezp. dohled atd.
- SAZ Příloha 4: Metodika stanovení požadavků na bezpečnost IS

Kap. 5.1.3: Využívání služeb KeGC/SeGC

- Dle požadované bezpečnostní úrovně IS nebo jeho části:
  - požadovaná BÚ 4 ⇨ SeGC;
  - požadovaná BÚ 1-3 ⇨ KeGC
- Hybridní eGC: dekompozice IS na části s různými bezp. dopady a požadavky na BÚ.
  - Provozovatel SeGC bude zpravidla v roli integrátora.
- Provozovatelé KeGC a SeGC musí splnit bezpečnostní a provozní požadavky dle kap. 6.2, v jednání vazba na chystanou „Cloudovou vyhlášku" NÚKIB
- BÚ se aplikují primárně na celé IS; kde to je výhodnější pro zadavatele, lze aplikovat samostatně na dekomponované části IS

Kap. 5.2: Hodnocení úrovně bezp. dopadů

- **5.2.1 Krok 1: Určení úrovně bezp. dopadů IS**
  - Závažnost bezp. dopadů (narušení důvěrnosti, integrity, dostupnosti, úplná ztráta dat) převzato z NÚKIB „Metodika k vodítkům pro hodnocení dopadů v1.2" z března 2018
  - 10 oblastí dopadů, odvozených od hodnocení kritické infrastruktury státu
  - Závěr krok 1: jaké maximální úrovně dopadů mohou nastat narušením C-I-A
    - na celý IS nebo jeho dekomponovanou část
- **5.2.2 Krok 2: mapování max. úrovně dopadů na BÚ eGC**
  - Ztrátou důvěrnosti: úroveň dopadu = požadovaná BÚ
  - Ztrátou integrity / úplnou ztrátou dat: pro vyšší dopady zvážit opatření pravidelných replik dat do úložiště on-premise nebo do SeGC a ošetřit RPO (Recovery Point Objective)
  - Ztrátou dostupnosti: zajistit dostatečnou rezervu ve smluvních závazcích dostupnosti v SLA

Kap. 6.2: Opatření pro dodavatele

- Opatření: přístup založený na riziku (BÚ 1 - 4)
- Maximální uplatnění standardů ČSN/ISO/IEC (řada 27000)
- Prokazatelnost zavedení opatření standardními auditními zprávami a podkladovou dokumentací

S.1 – S.8 **Smluvní podmínky**	Bezpečnost jako součást smluvních podmínek: SLA, podpora, závazek opatření, reakce na incidenty, GDPR atd.
N.1 – N.6 **Normy a standardy**	Přiměřeně: Zavést opatření dle ČSN/ISO/IEC 27001, 27017, 27018, 20000, požadavky VKB
C.1 – C.9 **Certifikace a audity**	Přiměřeně: Požadavek certifikace dle výše uvedených norem + audity SSAE 18 - SOC 1 / 2 Type II, penetrační testy
U.1 – U.11 **Upřesnění opatření**	Prokázat dokumentací: zálohy, plán BC/DR, logování, eventy, ochrana DDoS, SOC, šifrování, authN, replikace dat on-prem.
K.1 – K.5 **Komunikační sítě**	Fixní IP adresa, VPN dle CMS, peering v ČR, FENIX, šifrování při přenosech

Shrnutí bezp. norem a certifikací

Nejdůležitější uplatňované normy a certifikace	BÚ 1	BÚ 2	BÚ 3	BÚ 4
SLA – vyhodnocování na měsíční bázi [%] (SAZ Příloha 5)	96,16	99,45	99,90	99,99
ČSN ISO/IEC 27001 (Cert., SoA, auditní zpráva)	Část.	X	X	X
ČSN ISO/IEC 27017 (Cert., SoA, auditní zpráva)		X	X	X
ČSN ISO/IEC 27018 (Cert., SoA, auditní zpráva)		X	X	X
ČSN ISO/IEC 20000				X
Auditní zpráva SSAE18 - ISAE3402 / SOC 1 Type II			X	X
Auditní zpráva SSAE18 - SOC 2 Type II			X	X
Podmínky VKB č. 82/2018 Sb.			X	X
Zpráva o penetračních testech nebo umožnění pen. testů			X	X
Bezpečnostní způsobilost administrátorů §80-87 ZoUI				X

Pozn.: pro dodavatele SaaS vyvářeného na míru pro účely výkonu veřejné správy (§2 ZoISVS) je rozsah ISO omezen na bezp. vývoj a údržbu SW (dle rozsahu odpovědnosti), a zbytek norem a auditů může prokázat na úrovni provozovatele PaaS/IaaS

Priority týmu Bezpečnost v projektu eGC

- Co již bylo dodáno v oblasti bezpečnosti eGC:
  - Pravidla umísťování do (resp. využívání služeb) KeGC vs. SeGC
  - Metodika zařazování ISVS do bezpečnostních úrovní (BÚ)
  - Návrh bezpečnostních opatření, přiměřeně dle BÚ
  - Návrh způsobu ověřování zavedených opatření u dodavatelů
  - Společně s Provozním a Organizačním týmem: minimální požadavky na SLA a podporu služby

- Co ještě zbývá dodat:
  - Jak zahrnout požadavky na opatření jako kvalifikační kritéria v souladu se ZZVZ
  - Úroveň bezpečnosti jako atribut služby v rámci Katalogu služeb eGC
  - Najít přijatelnou variantu ověřování opatření u dodavatelů KeGC
  - Propojit pravidla pro eGC s chystanou cloudovou vyhláškou NÚKIB

Proč využívat služby eGC

- Záměr zvýšení úrovně zabezpečení / reakce na požadovanou BÚ
  - Možnost přenesení některých povinností a bezp. opatření na provozovatele KeGC / SeGC (GDPR, ZKB)
  - Možnost využít externí dohledové služby / virtuální SOC
- Minimální smluvní požadavky (SAZ Příloha 5)
  - SLA podložené kredity za nesplnění
  - Minimální pravidla pro smluvní podporu
  - GDPR: smluvní přenesení části odpovědnosti na zpracovatele
- Jiné organizační výhody
  - Řešení otázky nedostatku vlastních IT odborníků
  - Postupný přechod od komplexnosti veřejných zakázek (HW / SW komponenty) na jednodušší SW jako službu

MINISTERSTVO VNITRA ČESKÉ REPUBLIKY

Ministerstvo financí České republiky

NÚKIB

eGC tým „Bezpečnost“

Děkujeme za pozornost!