TLP: GREEN



Státní cloud bezpečně

Služby KCKB a certifikovaný CSIRT-SPCSS

SPCSS
Státní pokladna
Centrum sdílených služeb

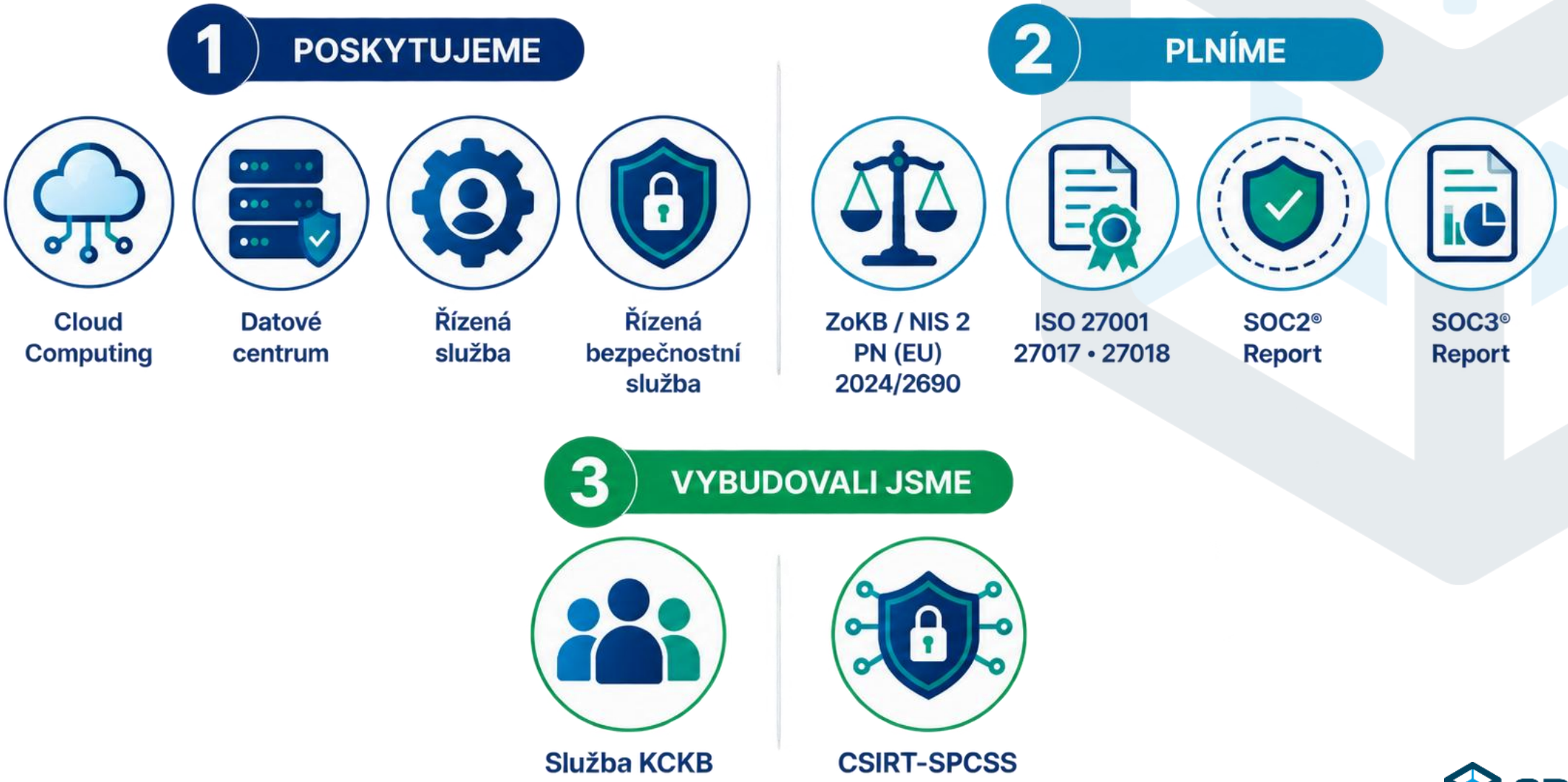


Bc. Jiří Štegl

Manažer kybernetické bezpečnosti

jiri.stegl@spcss.cz

Poskytovatel služeb Státní části eGC



Služby poskytované SPCSS

Cloud computing

IaaS
výpočetní výkon, datové úložiště, zálohování, archivace, firewall, loadbalancing

PaaS
provozní prostředí pro aplikace, správa OS, virtualizace, databází, SAP Base

Cloudové služby eGovernment Cloudu
(poskytovatel státního cloudu - bezpečnostní úroveň 4)

Datové centrum

Prostory a infrastruktura pro bezpečné umístění a provoz IT technologií

Národní datové centrum – infrastruktura pro orgány veřejné moci

Řízené služby

Instalace, správa, provoz či údržba technických aktiv – on-site nebo vzdáleně

Správa provozu IISSP, AISG, aplikačních či infrastrukturních komponent

Řízené bezpečnostní služby

Kybernetický monitoring a detekce hrozeb (SECaaS)na perimetru zákazníka

Analýza incidentů, dokumentace, architektura bezpečnosti



Služba Kompetenční centrum KB

Jak spolupráce probíhá?

1 ZJISTÍME POTŘEBU



GAP analýza, legislativní požadavky

2 VYBEREME DOKUMENTY A AKTIVITY



Katalog dokumentace a povinností

3 SPOČÍTÁME PRACNOST



Formulář pracnosti, cenová kalkulace

4 REALIZUJEME



Analýza rizik, BIA, dokumentace

5 PŘEDÁME VÝSTUPY / PODPORUJEME DÁL



Výstupy, konzultace, podpora při auditech

Dvě cesty ke stejnému cíli

Komplexní řešení

- GAP analýza

	A	B	C	D	E	F	G
1					GAP analýza	Opatření je aplikováno v plném rozsahu	
2						Opatření je aplikováno částečně	
3						Opatření není aplikováno	
4					82/2018 Sb. vs 409/2025 Sb.	Nový bod ve vyhlášce 409/2025 Sb.	
5						Opatření není relevantní	

	A	B	C	D	E	F
1	Bod	Typ opatření	Název	Počet bodů v rámci §	Plněných bodů	Plněno (%)
2	§ 3	Organizační opatření	Systém řízení bezpečnosti informací	19	12	63
3	§ 4		Požadavky na vrcholné vedení	29	3	10
4	§ 5		Stanovení bezpečnostních rolí	9	6	67
5	§ 6		Řízení bezpečnostní politiky a bezpečnostní dokumentace	9	4	44
6	§ 7		Řízení aktiv	13	8	62
7	§ 8		Řízení rizik	23	15	65
8	§ 9		Řízení dodavatelů	15	7	47
9	§ 10		Bezpečnost lidských zdrojů	17	10	59
10	§ 11		Řízení změn	10	9	90
11	§ 12		Akvizice, vývoj a údržba	8	2	25
12	§ 13		Řízení přístupu	12	10	83
13	§ 14		Zvládání kybernetických bezpečnostních událostí a incidentů	16	15	94
14	§ 15		Řízení kontinuity činností	8	7	88
15	§ 16		Provádění auditu kybernetické bezpečnosti	11	6	55
16	§ 17	Technická opatření	Fyzická bezpečnost	9	7	78
17	§ 18		Bezpečnost komunikačních sítí	9	7	78
18	§ 19		Správa a ověřování identit	32	29	91
19	§ 20		Řízení přístupových práv a oprávnění	3	3	100
20	§ 21		Detekce kybernetických bezpečnostních událostí	11	10	91
21	§ 22		Zaznamenávání událostí	26	21	81
22	§ 23		Vyhodnocování kybernetických bezpečnostních událostí	8	3	38
23	§ 24		Aplikační bezpečnost	15	9	60
24	§ 25		Kryptografické algoritmy	9	5	56
25	§ 26		Zajišťování dostupnosti regulované služby	10	5	50
26	§ 27		Zabezpečení průmyslových, řídicích a obdobných specifických technických aktiv	N/A		
27						
28			Celkové plnění v rámci 409/2025 Sb.	331	213	64

Konkrétní potřeby

- Katalog dokumentace a povinností

ID dokumentu	ázev dokumentu / výst	Typ	Vazby na požadavl	Popis / účel dokumentu
D002	Stanovení cílů SŘBI	Dokument	§ 3 a)	Dokument popisuje a upravuje oblast „Stanovení cílů SŘBI“, vymezuje její účel, základní pravidla, odpovědnosti, související
D003	Metodika pro stanovení procesu výjimek z BP	Plán	§ 3 j)	Dokument upravuje proces řízení výjimek z bezpečnostních pravidel, včetně podmínek schválení, evidence, odpovědností, platnosti
D004	Návrh bezpečnostních opatření	Dokument	§ 3 c)	Dokument popisuje a upravuje oblast „Návrh bezpečnostních opatření“, vymezuje její účel, základní pravidla, odpovědnosti, související
D005	Bezpečnostní politika (IS)	Směrnice	§ 3 c), § 3 d), § 4 b), § 6 (1), § 6 (2)	Dokument vymezuje základní pravidla bezpečnostní politiky, zásady řízení kybernetické bezpečnosti, odpovědnosti, povinnosti osob a návaznost na další bezpečnostní dokumentaci. V případě BP pro IS
D030	Analýza rizik - Metodika řízení aktiv a rizik - Nabízí se jako služba Analýza rizik celkově	Metodika / pravidla	c), § 7 g), § 7 h), § 8 (1), § 8 1., § 8 2., § 8 3., § 8 4., § 8 5., § 8 6., § 8 7., § 8 8., § 8 a), §	Dokument se věnuje řízení rizik, jejich identifikaci, hodnocení, evidenci, návrhu opatření, akceptaci rizik a pravidelnému přezkumu ve vztahu k aktivům a službám.
D031	Analýza rizik -Evidence aktiv v rozsahu řízení KB, včetně vyjmutých primárních aktiv a důvodů vyjmutí - Nabízí	Evidence / registr	§ 7 d), § 7 e), § 7 f)	Dokument se věnuje řízení rizik, jejich identifikaci, hodnocení, evidenci, návrhu opatření, akceptaci rizik a pravidelnému přezkumu ve vztahu k aktivům a službám.
D032	Analýza rizik - Zpráva o hodnocení rizik - Nabízí se jako služba Analýza	Zpráva / protokol	§ 16 2.	Dokument se věnuje řízení rizik, jejich identifikaci, hodnocení, evidenci, návrhu opatření, akceptaci rizik a pravidelnému
D033	Analýza rizik - Plán zvládání rizik - Nabízí se jako služba Analýza rizik	Plán	§ 3 2., § 3 b), § 8 1., § 8 (2), § 8 2., § 8 (3), § 8 3., § 8 (4), § 8 4., § 8	Dokument se věnuje řízení rizik, jejich identifikaci, hodnocení, evidenci, návrhu opatření, akceptaci rizik a pravidelnému
D034	Analýza rizik - Prohlášení o aplikovatelnosti - Nabízí se jako služba	Dokument	§ 8 1., § 8 2., § 8 f)	Dokument se věnuje řízení rizik, jejich identifikaci, hodnocení, evidenci, návrhu opatření, akceptaci rizik a pravidelnému

Co následuje po GAP analýze?

Zákazník si volí, s čím chce pomoci

- Bezpečnostní dokumentace k regulované službě
- Nastavení procesů, rolí a odpovědností
- Zpracování analýzy rizik a BIA
- Školení, vzdělávání, konzultace
- Podpora při kontrolách a auditech

„Od vlastní realizace až po řešení na klíč"

KCKB v životním cyklu regulované služby

Před provozem služby

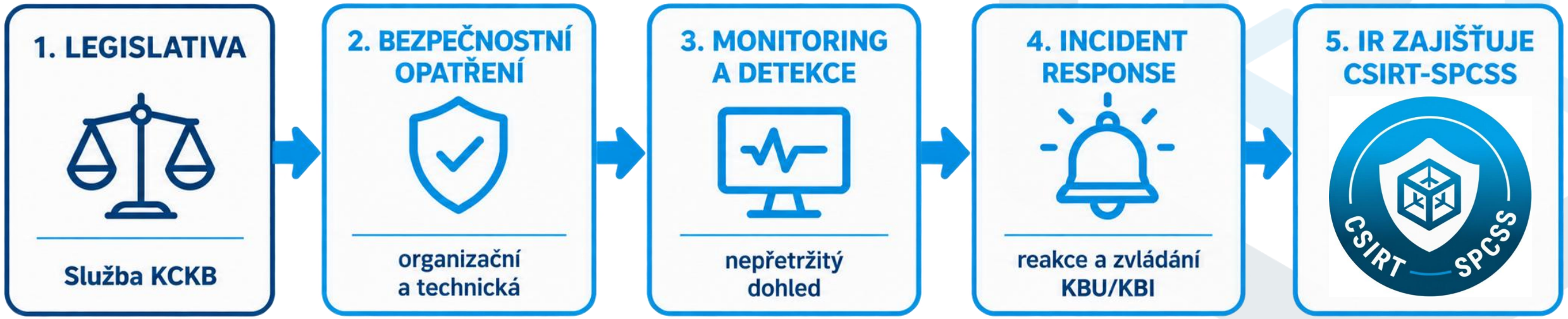
- Identifikace povinností
- Nastavení procesů a rolí
- Zpracování analýzy rizik a BIA
- Zpracování povinné bezpečnostní dokumentace
- Aktualizace / vytvoření vnitřních předpisů
- Nastavení odpovědností a komunikace s dodavateli

Po dobu provozu služby

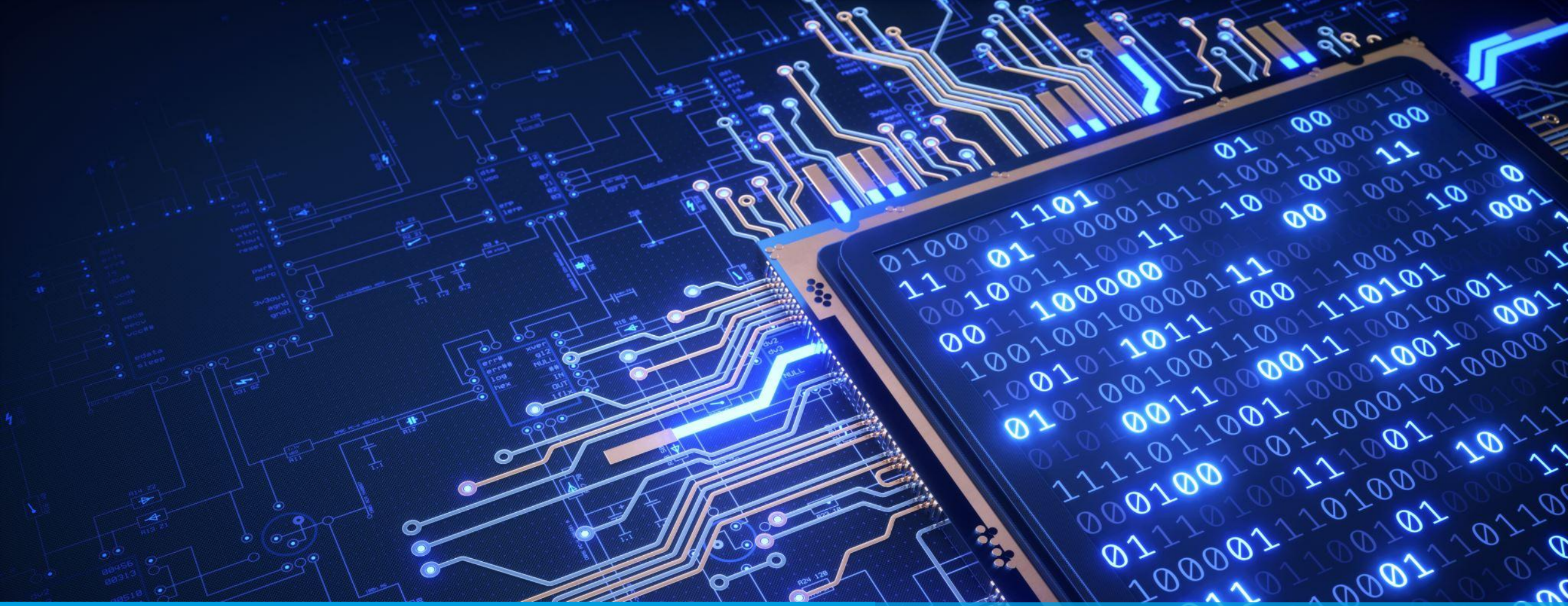
- Dohled nad souladem s legislativou
- Pravidelné revize procesů
- Pravidelné aktualizace AR a BIA
- Aktualizace dokumentace
- Pravidelné konzultace a reporting
- Návrhy nápravných opatření a změn
- Podpora při auditech a kontrolách

„Od přípravy regulované služby k její průběžné bezpečnosti"

Soulad s legislativou je jen začátek …



„Připravenost na papíře nestačí. Musíme umět reagovat v praxi"



CSIRT-SPCSS

CSIRT-SPCSS

Computer Security Incident Response Team

- Řídí a řeší kybernetické bezpečnostní incidenty
- Působí nad systémy a službami provozovanými SPCSS
- Reaguje na incidenty do 15 minut od zjištění
- Analyzuje, komunikuje, ukládá opatření a dokumentuje
- Koordinuje spolupráci (SOC, IT provoz, zákazníci, NÚKIB)
- Plní zákonné povinnosti (ZoKB / NIS2)
- Vzdělává se a dokládá odbornost certifikacemi
- Od 9.5.2025 Trusted Introducer Certified Team
- Organizační, procesní a provozní vyspělost podle SIM3

Role CSIRT-SPCSS: ***centrální autorita pro KBI v SPCSS***

https://www.spcss.cz/csirt/

CSIRT-SPSS

Spolupráce

- Autorita
- Složky
- Policie
- Odborná veřejnost
- Komunity

Bezpečný státní cloud: od prevence po reakci

KCKB

PREVENCE A PŘIPRAVENOST

Řízení rizik, bezpečnostní procesy
a soulad s legislativou

CSIRT-SPCSS

DETEKCE A REAKCE

Monitoring, řešení incidentů
a koordinace spolupráce

„Bezpečnost není jen o splnění povinností.
Je o schopnosti předcházet hrozbám a účinně na ně reagovat.“

Děkuji za pozornost

jiri.stegl@spcss.cz | www.spcss.cz

SPCSS