TLP: GREEN

Státní cloud bezpečně
Služby KCKB a certifikovaný CSIRT-SPCSS

E-government 20:10, 8.9.2026

SPCSS
Státní pokladna
Centrum sdílených služeb

Pavlína Havelková

vedoucí odboru Kompetenční centrum kybernetické bezpečnosti

pavlina.havelkova@spcss.cz

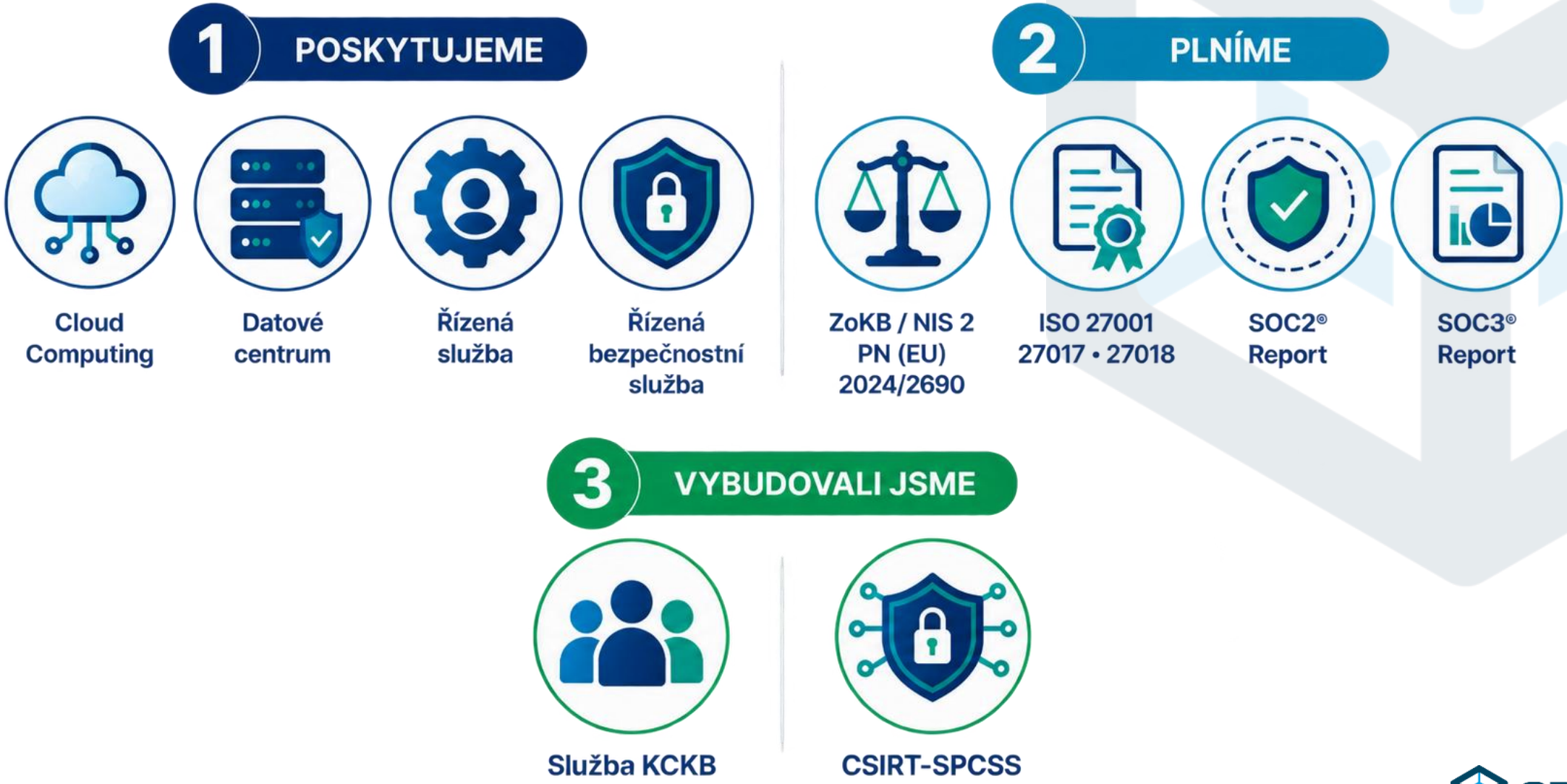
Lenka Gardašová

vedoucí CSIRT-SPCSS

lenka.gardasova@spcss.cz

Úsek bezpečnosti SPCSS

Poskytovatel služeb Státní části eGC



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	Název dokumentu / výst	Typ	Vazby na požadavk	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

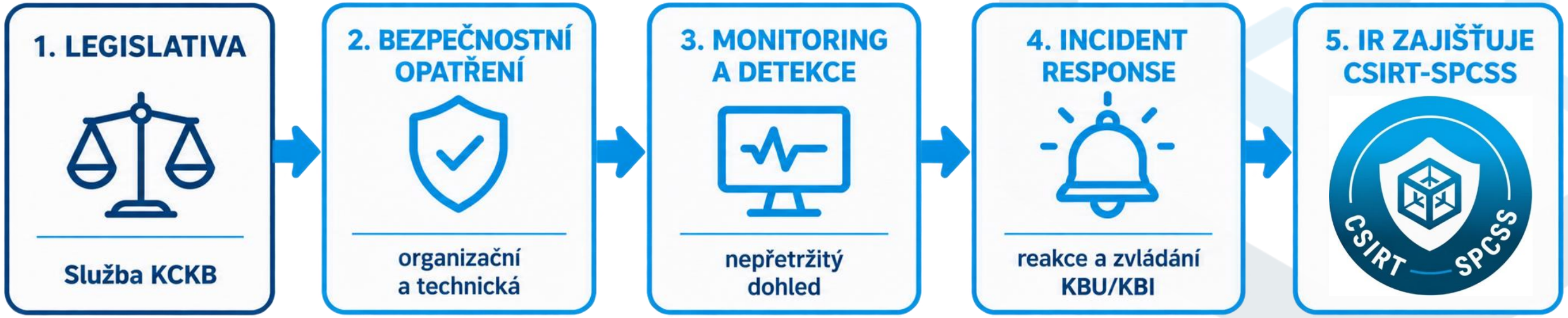
- Identifikace povinností
- Nastavení procesů a rolí
- Zpracování analýzy rizik a BIA
- Zpracování povinné bezpečnostní dokumentace
- Aktualizace / vytvoření vnitřních předpisů
- Nastavení odpovědností a komunikace s dodavateli

Po dobu provozu služby

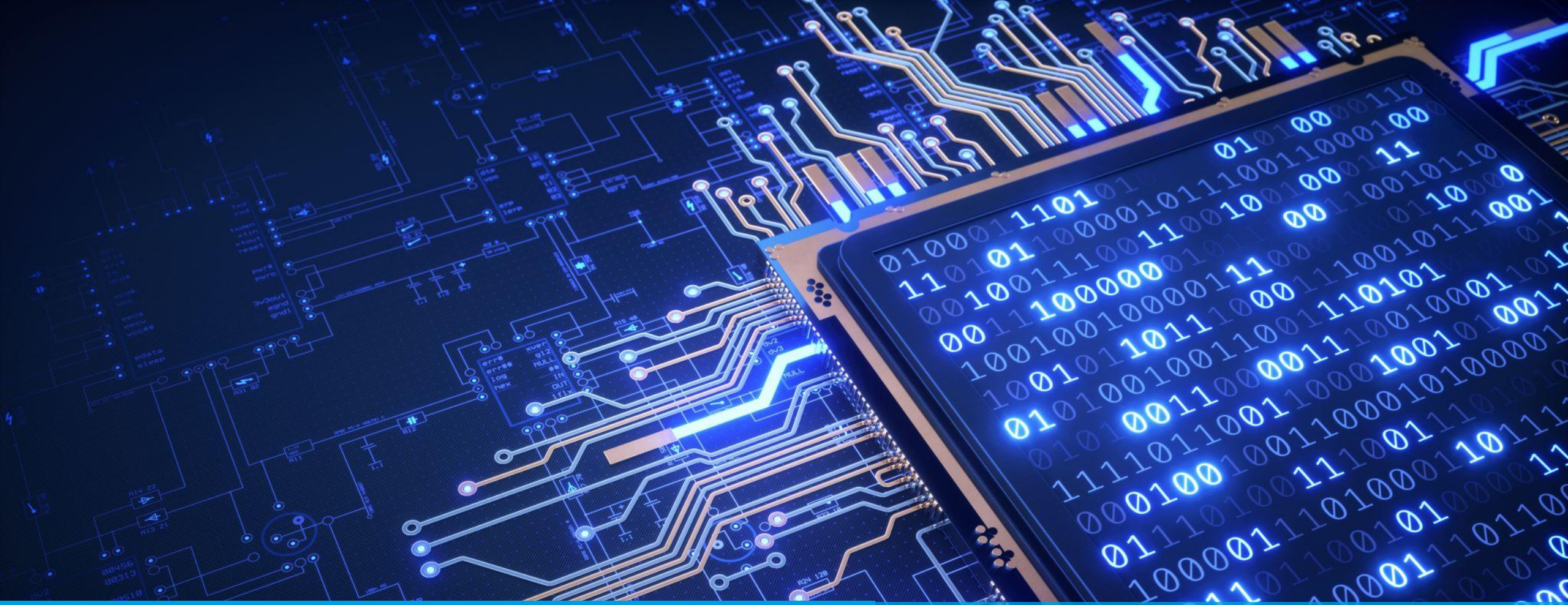
- Dohled nad souladem s legislativou
- Pravidelné revize procesů
- Pravidelné aktualizace AR a BIA
- Aktualizace dokumentace
- Pravidelné konzultace a reporting
- Návrhy nápravných opatření a změn
- Podpora při auditech a kontrolách

„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

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

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

CSIRT-SPCSS

DŮVĚRA

ODBORNOST

PROPOJENÍ

VYSPĚLOST

Ověřená důvěryhodnost

- 9.5.2025 Trusted Introducer Certified Team
- Organizační, procesní a provozní vyspělost podle SIM3

„Certifikace nejsou dekorace. Jsou důkazem vyspělosti.“

FIRST
Člen mezinárodní komunity od 2021

SIM3
2 certifikovaní auditoři v týmu

TRANSITS
Praktický rozvoj Incident Response

Co to znamená pro zákazníka:

- rychlejší navázání důvěry při incidentu
- společný jazyk s evropskou a globální komunitou
- disciplína, která obstojí před externím ověřením

CSIRT-SPCSS

Řízená kvalita v uzavřené smyčce

- Metriky, audity a pravidelné revize převádějí zkušenost týmu do opakovatelného výkonu

01 MĚŘÍME	02 OVĚŘUJEME	03 ZLEPŠUJEME
reakční doby SLA trendy KBU/KBI	SIM3 audit SOC-CMM připravenost	nápravná opatření školení playbooky

Výsledek:

- **nejen** zvládnout incident
- zvládnout ho **standardizovaně**, **konzistentně**, **doložitelně** a pokaždé **lépe**

CSIRT-SPCSS

TI Certifikace

History

Date	Description
09 May 2025	CSIRT-SPCSS (CZ) is now a certified team
21 Sep 2024	CSIRT-SPCSS (CZ) is now a certification candidate team
01 Dec 2023	CSIRT-SPCSS (CZ) is now an accredited team
31 Oct 2023	CSIRT-SPCSS (CZ) is now an accreditation candidate team
22 Oct 2021	CSIRT-SPCSS (CZ) has completed the re-listing process
26 Jun 2018	CSIRT-SPCSS (CZ) is now a listed team

Komunita bezpečnostních týmů v ČR

Země	Počet týmů	Listed	Accredited	Certified	Kandidáti / čekající
Czech Republic	74	38	25	5	6
Spain	53	22	28	1	2
France	45	15	21	1	7
Poland	43	10	21	7	5
Italy	39	11	24	2	2
Germany	34	13	16	4	1
Sweden	18	4	8	2	4
Netherlands	17	4	7	4	2
Slovakia	17	3	10	3	1
Portugal	16	5	7	3	1
Romania	12	1	11	0	0
Switzerland	11	4	5	1	1
Belgium	10	1	7	1	1

CSIRT-SPSS

Spolupráce

- Autorita
- Složky
- Policie
- Odborná veřejnost
- Komunity

Ještě stihnete

15:00 Zámecký sál

OD SERVERU KE SLUŽBĚ:

JAK STAVÍME ZÁKLADY STÁTNÍHO CLOUDU

Radek Kulhánek (SPCSS)

a

Martin Černický (IBM)

Pozn.: Obrázky použité v prezentaci byly vytvořeny s využitím AI


Spolehlivý
Poskytovatel
Cloudových
Služeb
Státu
spcss.cz
SPCSS
Státní pokladna
Centrum sdílených služeb