Zákon o kybernetické bezpečnosti

dle právního stavu ke dni 1. 8. 2017

Povinnosti orgánů a osob podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů

Národní úřad pro kybernetickou a informační bezpečnost

NÚKIB

Službou elektronických komunikací rozumíme službu obvykle poskytovanou za úplatu, která spočívá zcela nebo převážně v přenosu signálů po sítích elektronických komunikací, včetně telekomunikačních služeb a přenosových služeb v sítích používaných pro rozhlasové a televizní vysílání a v sítích kabelové televize, s výjimkou služeb, které nabízejí obsah prostřednictvím sítí a služeb elektronických komunikací nebo vykonávají redakční dohled nad obsahem přenášeným sítěmi a poskytovaným službami elektronických komunikací; nezahrnuje služby informační společnosti, které nespočívají zcela nebo převážně v přenosu signálů po sítích elektronických komunikací.
(§ 2 písm. n) zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích))

Sítí elektronických komunikací rozumíme přenosové systémy, popřípadě spojovací nebo směrovací zařízení a jiné prostředky, včetně prvků sítě, které nejsou aktivní, které umožňují přenos signálů po vedení, rádiovými, optickými nebo jinými elektromagnetickými prostředky, včetně družicových sítí, pevných sítí s komutací okruhů nebo paketů a mobilních zemských sítí, sítí pro rozvod elektrické energie v rozsahu, v jakém jsou používány pro přenos signálů, sítí pro rozhlasové a televizní vysílání a sítí kabelové televize, bez ohledu na druh přenášené informace.
(§ 2 písm. h) zákona č. 127/2005 Sb., o elektronických komunikacích a o změně některých souvisejících zákonů (zákon o elektronických komunikacích))

Významnou sítí rozumíme síť elektronických komunikací, zajišťující přímé zahraniční propojení do veřejných komunikačních sítí nebo zajišťující přímé propojení ke kritické informační infrastruktuře.
(§ 2 písm. h) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti))

Digitální službou je služba informační společnosti podle zákona upravujícího některé služby informační společnosti, která spočívá v provozování on-line tržiště, internetového vyhledávače, cloud computingu.
(§ 2 písm. l) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti))

Kritickou informační infrastrukturou je prvek nebo systém prvků kritické infrastruktury v odvětví komunikační a informační systémy v oblasti kybernetické bezpečnosti.
(§ 2 písm. b) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti))

Významným informačním systémem je informační systém spravovaný orgánem veřejné moci, který není kritickou informační infrastrukturou a u kterého narušení bezpečnosti informací (narušení důvěrnosti, dostupnosti a integrity) může omezit nebo výrazně ohrozit výkon působnosti orgánu veřejné moci.
(§ 2 písm. d) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti))

Informačním systémem základní služby je informační systém, na jehož fungování je závislé poskytování základní služby
(§ 2 písm. f) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti))

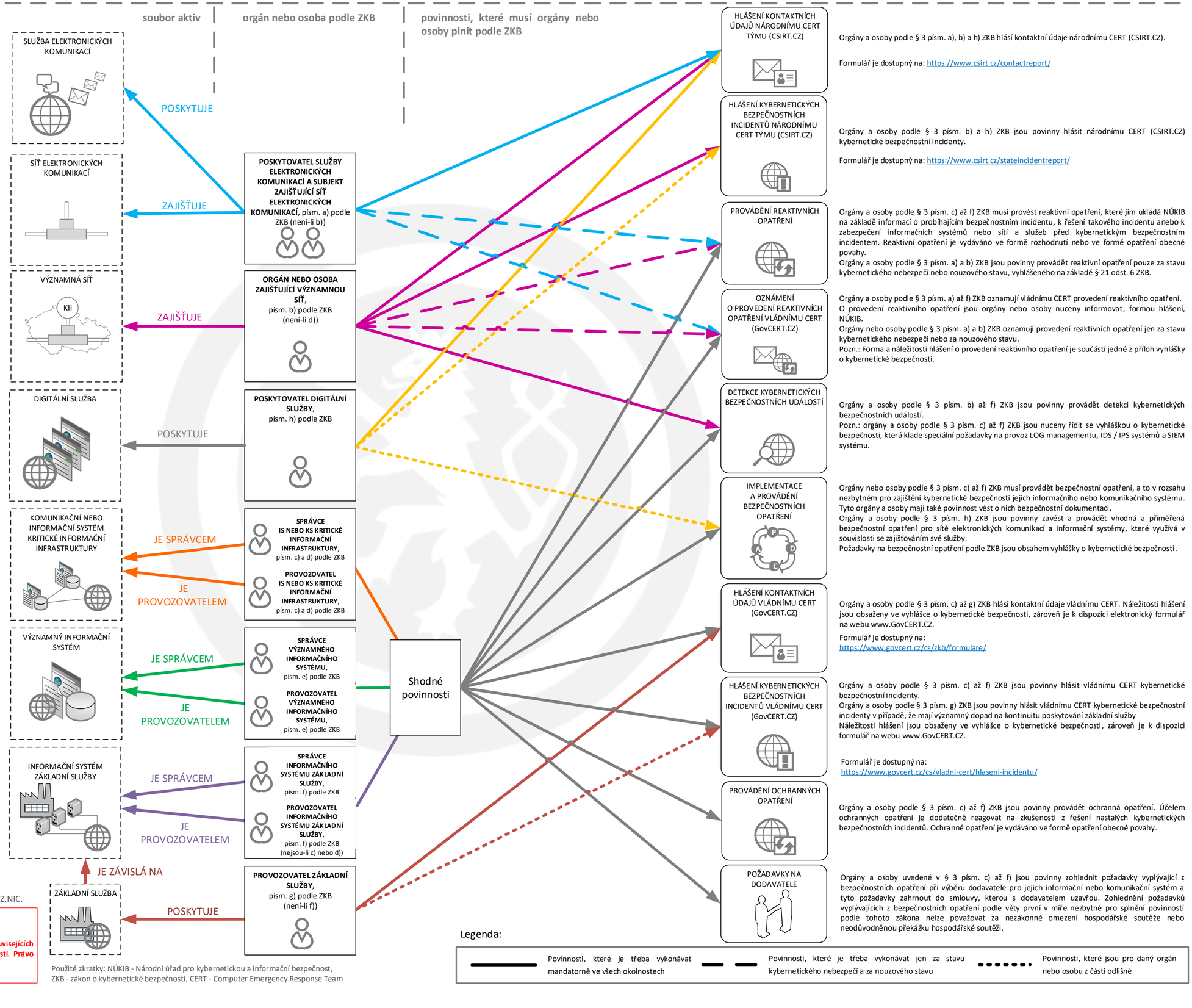
Základní službou je služba, jejíž poskytování je závislé na sítích elektronických komunikací nebo informačních systémech a jejíž narušení by mohlo mít významný dopad na zabezpečení společenských nebo ekonomických činností v některém z těchto odvětví: energetika, doprava, bankovnictví, infrastruktura finančních trhů, zdravotnictví, vodní hospodářství, digitální infrastruktura a chemický průmysl.
(§ 2 písm. i) zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti))

verze 1.0, platná ke dni 20. 3. 2018

Pozn.: Národní CERT zaštiťuje tým CSIRT.CZ, který je provozovaný sdružením CZ.NIC.

Upozornění:

Dokument slouží pouze jako podpůrné vodítko, nenahrazuje žádný ze zákonů a souvisejících prováděcích předpisů. Dokument neobsahuje úplný výčet všech práv a povinností. Právo změny tohoto dokumentu vyhrazeno.



Orgány a osoby podle § 3 písm. a), b) a h) ZKB hlásí kontaktní údaje národnímu CERT (CSIRT.CZ).

Formulář je dostupný na: https://www.csirt.cz/contactreport/

Orgány a osoby podle § 3 písm. b) a h) ZKB jsou povinny hlásit národnímu CERT (CSIRT.CZ) kybernetické bezpečnostní incidenty.

Formulář je dostupný na: https://www.csirt.cz/stateincidentreport/

Orgány a osoby podle § 3 písm. c) až f) ZKB musí provést reaktivní opatření, které jim ukládá NÚKIB na základě informací o probíhajícím bezpečnostním incidentu, k řešení takového incidentu anebo k zabezpečení informačních systémů nebo sítí a služeb před kybernetickým bezpečnostním incidentem. Reaktivní opatření je vydáváno ve formě rozhodnutí nebo ve formě opatření obecné povahy.
Orgány a osoby podle § 3 písm. a) a b) ZKB jsou povinny provádět reaktivní opatření pouze za stavu kybernetického nebezpečí nebo nouzového stavu, vyhlášeného na základě § 21 odst. 6 ZKB.

Orgány a osoby podle § 3 písm. a) až f) ZKB oznamují vládnímu CERT provedení reaktivního opatření. O provedení reaktivního opatření jsou orgány nebo osoby nuceny informovat, formou hlášení, NÚKIB.
Orgány nebo osoby podle § 3 písm. a) a b) ZKB oznamují provedení reaktivních opatření jen za stavu kybernetického nebezpečí nebo za nouzového stavu.
Pozn.: Forma a náležitosti hlášení o provedení reaktivního opatření je součástí jedné z příloh vyhlášky o kybernetické bezpečnosti.

Orgány a osoby podle § 3 písm. b) až f) ZKB jsou povinny provádět detekci kybernetických bezpečnostních událostí.
Pozn.: orgány a osoby podle § 3 písm. c) až f) ZKB jsou nuceny řídit se vyhláškou o kybernetické bezpečnosti, která klade speciální požadavky na provoz LOG managementu, IDS / IPS systémů a SIEM systému.

Orgány nebo osoby podle § 3 písm. c) až f) ZKB musí provádět bezpečnostní opatření, a to v rozsahu nezbytném pro zajištění kybernetické bezpečnosti jejich informačního nebo komunikačního systému. Tyto orgány a osoby mají také povinnost vést o nich bezpečnostní dokumentaci.
Orgány a osoby podle § 3 písm. h) ZKB jsou povinny zavést a provádět vhodná a přiměřená bezpečnostní opatření pro sítě elektronických komunikací a informační systémy, které využívá v souvislosti se zajišťováním své služby.
Požadavky na bezpečnostní opatření podle ZKB jsou obsahem vyhlášky o kybernetické bezpečnosti.

Orgány a osoby podle § 3 písm. c) až g) ZKB hlásí kontaktní údaje vládnímu CERT. Náležitosti hlášení jsou obsaženy ve vyhlášce o kybernetické bezpečnosti, zároveň je k dispozici elektronický formulář na webu www.GovCERT.CZ.

Formulář je dostupný na:
https://www.govcert.cz/cs/zkb/formulare/

Orgány a osoby podle § 3 písm. c) až f) ZKB jsou povinny hlásit vládnímu CERT kybernetické bezpečnostní incidenty.
Orgány a osoby podle § 3 písm. g) ZKB jsou povinny hlásit vládnímu CERT kybernetické bezpečnostní incidenty v případě, že mají významný dopad na kontinuitu poskytování základní služby
Náležitosti hlášení jsou obsaženy ve vyhlášce o kybernetické bezpečnosti, zároveň je k dispozici formulář na webu www.GovCERT.CZ.

Formulář je dostupný na:
https://www.govcert.cz/cs/vladni-cert/hlaseni-incidentu/

Orgány a osoby podle § 3 písm. c) až f) ZKB jsou povinny provádět ochranná opatření. Účelem ochranných opatření je dodatečně reagovat na zkušenosti z řešení nastalých kybernetických bezpečnostních incidentů. Ochranné opatření je vydáváno ve formě opatření obecné povahy.

Orgány a osoby uvedené v § 3 písm. c) až f) jsou povinny zohlednit požadavky vyplývající z bezpečnostních opatření při výběru dodavatele pro jejich informační nebo komunikační systém a tyto požadavky zahrnout do smlouvy, kterou s dodavatelem uzavřou. Zohlednění požadavků vyplývajících z bezpečnostních opatření podle věty první v míře nezbytné pro splnění povinností podle tohoto zákona nelze považovat za nezákonné omezení hospodářské soutěže nebo neodůvodněnou překážku hospodářské soutěži.

Legenda:

Povinnosti, které je třeba vykonávat mandatorně ve všech okolnostech

Povinnosti, které je třeba vykonávat jen za stavu kybernetického nebezpečí a za nouzového stavu

Povinnosti, které jsou pro daný orgán nebo osobu z části odlišné

Použité zkratky: NÚKIB - Národní úřad pro kybernetickou a informační bezpečnost, ZKB - zákon o kybernetické bezpečnosti, CERT - Computer Emergency Response Team