T y p o v ý p l á n

Typ krizové situace: Narušení bezpečnosti informací kritické informační infrastruktury

---

1. Základní část

1.1. Popis krizové situace

Krizové situace („KS“) způsobené narušením bezpečnosti informací kritické informační infrastruktury („KII“) jsou vzhledem k různé povaze informačních nebo komunikačních systémů, které jsou jako KII určeny, a vzhledem ke službám, které systémy zajišťují, různorodé.

KII je z velké části spojená s již určenými prvky kritické infrastruktury („KI“) identifikovanými zejména v oblastech energetiky, veřejné správy, elektronických komunikací a finančního trhu a měny. Nastane-li KS v oblasti kybernetické bezpečnosti, může mít dopad na funkčnost subjektu KI a mít tak dopad na jeho fungování a služby.

KS způsobené narušením bezpečnosti informací v KII jsou z hlediska procesu řešení podobné; řeší je zpravidla zasažený subjekt, NÚKIB a další instituce na centrální úrovni státu. Důsledky způsobené narušením KII však mohou být lokální, podobně jako v případě narušení funkce či činností prvku KI. Proto je nutné v těchto částech odkázat na příslušné typové plány zpracované pro KS, které mohou v odvětví, na které je KII navázáno, nastat.

Povaha KS je přímo závislá i na způsobu narušení bezpečnosti informací KII, kdy různé způsoby narušení mohou způsobit různé efekty a tudíž je nutné k nim přistupovat individuálně.

Možnosti výskytu KS způsobené narušením bezpečnosti informací KII jsou reálné. Současná společnost je na informačních a komunikačních systémech závislá, jelikož přebírají značnou část činností, které byly dříve vykonávány manuálně. Tato závislost však vytváří zejména dva typy rizik.

Prvním z nich je riziko neúmyslného selhání technologií či lidí, které může vést k selhání služby poskytované informačními nebo komunikačními systémy. Druhým je riziko úmyslného napadení informačních nebo komunikačních systémů. Útoky nejsou jednotvárné, naopak jsou prováděny s různými motivacemi a tudíž i různými technikami s následujícími různými dopady na poskytovanou službu.

Proces řešení KS způsobené narušením informací v KII je z podstaty věci nutné vést ve dvou rovinách. Následky ve fyzickém světě (tedy zapojení složek IZS a další procesy dle zákona č. 240/2000 Sb., krizového zákona) bude zpravidla řešeno do jisté míry odděleně od následků v kyberneticko-bezpečnostní rovině (tedy řešení incidentů dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti).

1.1.1. Předpokládaný územní a časový rozsah

Předpokládaný územní a časový rozsah působení KS je závislý na specifikách sektoru, ve kterém informační nebo komunikační systém funguje, a v případě úmyslného narušení pak i na motivaci, schopnostech a síle útočníka.

Příkladem tak nelze určit, zdali KS způsobená narušením bezpečnosti informací v KII, bude trvat pouze v rozmezí hodin nebo v rozmezí dnů.

1.1.2. Výčet možných příčin vzniku

Příčiny lze rozlišit několika způsoby, např.:

- dle povahy (úmyslné / neúmyslné),
- dle typu útoku (DDoS / ransomware / spyware / sociální inženýrství / kinetický / aj.),
- dle motivace útočících subjektů (finanční prospěch / politický důvod / vojenská výhoda / aj.).

a) Narušení bezpečnosti informací dle povahy narušení

Neúmyslné narušení bezpečnosti informací může nastat například:

- selháním technologie (přímé poškození provozních zařízení, disfunkční chování systémů, atd.),
- selháním osob,
- živelnou pohromou,
- dlouhodobým narušením dodávek elektrické energie,
- aj.

Úmyslné narušení bezpečnosti informací je pak kybernetickým útokem, jehož způsoby mohou být různé, přičemž je nutné vyjít z typu útoku a motivace útočníků (uvedených pod písm. b) a c)).

b) Narušení bezpečnosti informací dle typu útoku

V současné době roste jak počet útoků na informační a komunikační systémy, tak se také rozšiřuje množina způsobů jejich provedení.

Lze rozlišit například:

- kinetický zásah – činnost informačního nebo komunikačního systému je narušena kinetickým zásahem ať již destruktivním či nedestruktivním,
- DoS/DDoS – (distribuované) odepření služby, charakterizované zahlcením systému požadavky,
- škodlivý malware – v jeho rámci pak zejména ransomware, tj. útok, jehož cílem je znepřístupnění dat, se kterými systém pracuje, čímž dochází k nefunkčnosti daného systému a v některých případech k nenávratnému ztracení dat,
- sociální inženýrství – útok, při kterém je využito zejména slabin na straně chování uživatelů a mezer v organizačních bezpečnostních opatřeních,
- kombinace výše uvedených – sofistikované útoky jsou často prováděny s využitím kombinace více typů útoků (např. výše zmíněných).

c) Narušení bezpečnosti informací dle motivace útočících subjektů

V současné době roste jak počet útoků na informační a komunikační systémy, tak se také rozšiřuje množina jejích způsobů.

Lze rozlišit například:
- hacktivismus,
- materiální obohacení,
- konkurenční boj,
- vnitřní hrozba ze strany zaměstnance / selhání lidského faktoru,
- špionáž,
- prosazování politických názorů,
- terorismus,
- konflikt s nestátním či státním aktérem.

1.1.3. Popis skutečností indikujících, že může vzniknout krizová situace

Příznaky, které mohou vést ke vzniku KS a mohou narušit funkčnost informačního nebo komunikačního systému:

- kybernetické útoky na obdobné systémy v zahraničí,
- kybernetické útoky na obdobné systémy v ČR,
- eskalace konfliktu mezi ČR nebo organizací, jejichž je ČR členem, a jinými státními či nestátními aktéry s kapacitou provést či jinak obstarat provedení závažných kybernetických útoků,
- další skutečnosti dle specifik sektorů, ve kterých se KII nachází.

1.1.4. Popis skutečností a indikátorů o zvládání krizové situace

Zvládání KS způsobené narušením bezpečnosti informací v KII je nutné rozdělit na dvě roviny. První rovina se věnuje zvládání důsledků, které narušení KII způsobuje (tj. např. výpadek elektřiny, výpadek telekomunikačních služeb, nedostupnost dalších kritických služeb aj.), zatímco druhá rovina se zaměřuje na řešení příčiny a nápravu fungování systému KII (tj. náprava fungování samotného systému). Obě roviny mohou být do jisté míry nezávislé.

Rovina důsledků je řešena skrze zásady uvedené v souvisejících typových plánech

V rovině příčin KS je pro posouzení zvládání KS běžnou činností nutné uvažovat zejména

- časový rozsah narušení bezpečnosti informací v informačních systémech,
- důsledek narušení bezpečnosti informací pro činnost KII,
- postupy a činnosti, které jsou pro zvládnutí situace potřebné,
- v případech způsobených kybernetickým útokem kontext útoků, tj. vyjádření útočníků o možném trvání útoků, jejich zdrojích, jejich požadavcích;

v případě neexistujícího či nedůvěryhodného vyjádření útočníků zejména geopolitický kontext, konkurenční prostředí, či jiné kontextuální informace v závislosti na charakteru a motivaci útočníka.

Popis skutečností indikujících, že vzniklá situace je krizová:

- narušení bezpečnosti informací v informačních a komunikačních systémech KI způsobuje omezení či přímo výpadek služeb poskytovaných prvkem KI,
- správce či provozovatel informačního nebo komunikačního systému není schopen svými silami nastalou situaci zmírnit či odvrátit,
- další dle specifik sektorů, ve kterých se KII nachází (vizte příloha č. 1),
- přetrvávání výpadku dodávek služeb elektronických komunikací,
- rozsah narušení KII neumožňuje dodávky služeb vybraným účastníkům, kterým dodávky služeb musí být zachovány,
- reálné nebezpečí vzniku sekundárních KS, postupný nárůst ohrožení základních funkcí státu a kritické infrastruktury.

Popis skutečností způsobujících, že krizová situace probíhá (trvá), popřípadě se ji nedaří stabilizovat a vyřešit:

- přetrvávající kybernetické útoky na komunikační a informační systémy,
- kumulace působení dalších rizik a ohrožení,
- trvání přerušení dodávky služeb poskytovaných KII,
- nárůst rozsahu sil, prostředků a zdrojů potřebných k likvidaci následků KS,
- celostátní rozsah KS, popřípadě postižení i sousedních států,
- probíhající sekundární KS,
- narušení základních funkcí státu.

Popis skutečností indikujících, že vzniklá situace přestává být krizová:

- slábne (přestává působit) vliv příčin vzniku KS,
- eliminace kybernetických útoků na komunikační a informační systémy,
- přerušené služby jsou postupně obnovovány.

1.1.5. Výčet možných sekundárních událostí

Sekundární události způsobené narušením prvku KII jsou závislé na službě, kterou poskytuje KI, na kterou je KII navázáno.

Příklady sekundárních událostí lze nalézt v Příloze č. 1.

1.2. Následky krizové situace

KS způsobené narušením KII a jejich následky lze, podobně jako v předchozím případě, možné identifikovat ve dvou rovinách.

V rovině dopadů způsobených omezením nebo zastavením služeb, které narušení KII

způsobilo, je nutné odkázat na typové plány pro jednotlivé oblasti, které jsou určenou KII ovlivňovány či ovládány. Obecný a jednotný popis platný pro veškeré KII není možný.

Druhou rovinu následků lze identifikovat jako specifickou kyberneticko-bezpečnostní. Touto rovinou se rozumí zejména dopad na ostatní subjekty využívající kyberprostor či subjekty operující systémy, které by mohly být KS dotčeny.

1.2.1. Dopady na životy a poškození zdraví osob

Dopady na život a poškození zdraví osob v důsledku působení krizových stavů v oblasti kybernetické bezpečnosti jsou určeny funkcí, kterou KII zajišťuje. Vizte typové plány k jednotlivým oblastem, na které je KII navázána.

1.2.2. Zničení nebo poškození majetku

Kybernetický bezpečnostní incident způsobený kybernetickým útokem může způsobit narušení bezpečnosti informací i v jiných informačních a komunikačních systémech.

V případě DoS/DDoS útoků lze uvažovat o sekundárním zahlcení navázaných systémů, které nebyly cílem útoku (příkladem budou při DDoS útoku na poskytovatele služeb elektronických komunikací zasaženy i další informační nebo komunikační systémy, které byly skrze tohoto poskytovatele připojeny).

V případě útoků prostřednictvím malware/worm lze uvažovat i o napadení informačních systémů, které nebyly primárním cílem útoku, nicméně díky podobné povahy systému nebo necílenému rozšíření malware na tyto informační systémy.

Kybernetickým bezpečnostním incidentem může dojít k zničení nebo poškození majetku a to i nevratně.

Ve zbytku vizte typové plány k jednotlivým oblastem, na které je KII navázána.

1.2.3. Poškození životního prostředí

Dopady na životní prostředí v důsledku působení krizových stavů v oblasti kybernetické bezpečnosti jsou určeny funkcí, kterou KII zajišťuje. Vizte typové plány k jednotlivým oblastem, na které je KII navázána.

1.2.4. Mezinárodní dopady

KS způsobené kybernetickým bezpečnostním incidentem mohou mít mezinárodní dopady a to jak v rovině materiální, tak také v rovině politické (diplomatické či mezinárodně-právní). Oproti jiným oblastem, neexistence pevných hranic v kyberprostoru možnost existence těchto dopadů zesiluje.

Škodlivá aktivita může mít přímý dopad na systémy umístěné v cizích státech (např. v případě existence botnet, který je ovládán nebo pouze útočí z teritoria České republiky). Možný rozsah dopadů nelze předem určit, je silně závislý na charakteru a příčině KS.

Schopnost státu zvládat KS může mít mezinárodní dopady i v diplomatické či mezinárodně-právní rovině, kdy schopnosti státu efektivně omezovat dopady

a řešit příčiny kybernetického bezpečnostního incidentu jsou důležitými aspekty určení rozsahu odpovědnosti státu.

V důsledku kybernetického bezpečnostního incidentu může dojít k přerušení služeb nebo dodávek i na území jiných členských států, zejména v rámci síťových odvětví (elektřina, plyn, ropa).

Ve zbytku vizte typové plány k jednotlivým oblastem, na které je KII navázána.

1.2.5. Ekonomické dopady

Dopady na ekonomiku v důsledku působení krizových stavů v oblasti kybernetické bezpečnosti jsou určeny funkcí, kterou KII zajišťuje, stejně jako charakterem samotného informačního nebo komunikačního systému KII. Vizte typové plány k jednotlivým oblastem, na které je KII navázána.

1.2.6. Sociální dopady

Závažná KS způsobená rozsáhlým narušením bezpečnosti informací ve velkém počtu informačních a komunikačních systémů v České republice může způsobit narušení komunikačních kanálů obyvatelstva i dalších služeb a narušit tak běžné společenské procesy.

Ve zbytku vizte typové plány k jednotlivým oblastem, na které je KII navázána.

1.2.7. Dopady na kritickou infrastrukturu

Dopady na KI lze uvažovat právě s ohledem na specifikum KII, které ve většině případů ovlivňuje či ovládá jiný, již určený prvek KI. V tomto ohledu je nutné na dopady KS způsobené narušením bezpečnosti informací v KII pohlížet skrze na dopady na KI, na kterou je daná KII navázána.

2. Operativní část

2.1. Zásady pro řešení krizové situace

2.1.1. Principy zajišťování kybernetické bezpečnosti v ČR

Individuální odpovědnost za bezpečnost

Jednou ze zásad, na kterých je systém zajišťování kybernetické bezpečnosti státu postaven, je individuální odpovědnost za bezpečnost vlastních systémů a sítí, kdy právě vlastník/správce KII je primárně odpovědný za bezpečnost a zvládání případných mimořádných situací, které ve vztahu k fungování daného systému mohou nastat. Z tohoto ohledu je přistupováno i k řešení KS způsobených narušením bezpečnosti informací v KII.

Při zvládání příčin KS má primární odpovědnost právě vlastník/správce KII. Ten má také často i nejefektivnější nástroje pro řešení problému.

Důvěra a spolupráce

Podstatnou zásadou je zásada důvěry a spolupráce subjektů podílejících se na zajišťování kybernetické bezpečnosti České republiky. Při řešení jakékoli KS způsobené kybernetickým bezpečnostním incidentem je zásadní, aby

subjekty KII spolupracovaly s ostatními subjekty čelících stejnému či obdobnému problému a s centrální autoritou pro oblast kybernetické bezpečnosti, Národním úřadem pro kybernetickou a informační bezpečnost. Ten, jako centrální kontaktní místo přijímá informace od ostatních subjektů KII i zahraničních a jiných partnerů a získává informace o dalších hrozbách v kyberprostoru, a je tak určen k poskytnutí asistence subjektům KII při řešení KS, zejména formou poskytnutí expertních kapacit nebo zprostředkováním kontaktů na další subjekty.

2.1.2. Zásady řešení krizové situace

Prevence

Primárním předpokladem řešení KS je fungující a zavedený systém řízení bezpečnosti informací v organizaci, včetně všech relevantních technických a organizačních opatření. Tyto opatření by měli vycházet minimálně z prováděcí vyhlášky k zákonu o kybernetické bezpečnosti, případně z relevantních norem ISO/IEC 27001 jakož i z dalších norem, rámců a standardů. V tomto rámci by měly existovat dané postupy pro řešení KS včetně jasného vymezení rolí a odpovědnosti v rámci organizace. Jedná se o základní předpoklad, bez kterého nelze KS efektivně vyřešit.

Komunikace

Subjekt KII zasažený KS musí být připraven a schopen udržet schopnosti komunikace mezi relevantními aktéry jak uvnitř organizace (zejména mezi odbornými technickými pracovníky, středním managementem a nejvyšším managementem), tak i vně organizace (s Národním úřadem pro kybernetickou a informační bezpečnost (dále jen „NÚKIB“), se sektorovými koordinátory, s Policií ČR, s dalšími složkami IZS a místními samosprávami).

Komunikace by také měla probíhat se zákazníky služby, která je KS dotčena a případně i s dalšími subjekty, které mohou být KS zasaženi.

Včasná a úplná komunikace je pro zvládnutí KS zásadní.

Koordinace

V rámci subjektu KII je nutné mít určenou entitu, která bude KS koordinovat. Tato by měla být určena (popřípadě postup jejího určení) v bezpečnostní politice. Veškeré kroky jednotlivých částí organizace (IT specialisté, management, PR, právní podpora aj.) musí být v souladu pro co nejefektivnější řešení situace.

Koordinace by také měla probíhat vně organizaci, zejména s NÚKIB, se sektorovými koordinátory, s ostatními subjekty zasaženými KS, a v případě nutnosti i se složkami IZS a místními samosprávami.

2.2. Systém řešení krizové situace

2.2.1. Orgány a osoby podílející se na řešení krizové situace

NÚKIB / Vládní CERT

Národní autorita pro oblast kybernetické bezpečnosti a hlavní kontaktní místo pro záležitosti kybernetické bezpečnosti v České republice.

Role NÚKIB a Vládního CERT jsou vymezeny v zákoně č. 181/2014 Sb., o kybernetické bezpečnosti (dále jen „ZKB“).

Základní funkcí je příjem a analýza informací o kybernetických bezpečnostních incidentech a událostech, proaktivní nacházení dalších kybernetických bezpečnostních hrozeb a informování subjektů KII a jiných relevantních subjektů o hrozbách a možnostech zabezpečení. NÚKIB/Vládní CERT také poskytuje expertní kapacity subjektům KII pro řešení problémů či KS. V neposlední řadě komunikuje vedle relevantních národních subjektů i se zahraničními CERT pro odstranění příčin majících původ v zahraničí.

Národní CERT

Národní CERT je orgán zabývající se sběrem informací o kybernetických bezpečnostních incidentech a událostech a dalších hrozbách zejména pro poskytovatele služeb elektronických komunikací, které nejsou subjekty KII.

Aktivity Národní CERT jsou důležitou součástí řešení rozsáhlých kybernetických bezpečnostních incidentů, zejména díky své roli vůči subjektům, pro něž je dle ZKB kontaktním místem, a dále také díky expertním kapacitám a know-how.

Orgány činné v trestním řízení

Zejména Policie ČR má kompetence, které v případě rozsáhlých kybernetických útoků jsou využitelné pro řešení KS. Jedná se zejména o schopnosti aktivně zasáhnout proti infrastruktuře, ze které je veden kybernetický útok aj.

Soukromý sektor a akademický sektor

Základní komunikační a informační infrastruktura ve státě je v rukou soukromého sektoru. Ten má také kapacity pro efektivní řešení většiny druhů KS.

Subjekty, se kterými je nutné či vhodné spolupracovat, je možné určit dle charakteru KS a podle toho, jaké prostředky a schopnosti je nutné využít. Zpravidla se bude jednat o poskytovatele služeb elektronických komunikací, telekomunikační operátory či subjekty s obdobnými informačními či komunikačními systémy.

Regionální složky

Z hlediska regionálních složek (zejména pak krajů) je vhodné vyčlenit osobu,

která v případě krizové situace způsobené narušením kybernetické bezpečnosti KII bude schopna komunikovat s ostatními orgány a osobami podílejícími se na řešení KS zejména s ohledem na vzájemnou výměnu informací o charakteru hrozby a existujících a potenciálních (i sekundárních) dopadech.

2.2.2. Proces řešení krizové situace / specifické instituty

Příčiny KS způsobené narušením bezpečnosti informací v informačním nebo komunikačním systému KII jsou řešeny zejména skrze instituty obsažených v ZKB.

Dopady způsobené KS vně problematiky kybernetické bezpečnosti jsou řešeny zejména v souladu se zákonem č. 240/2000 Sb., o krizovém řízení, a zásadami řešení KS v relevantních oblastech, kde dopad nastal.

Hlášení kontaktních údajů

Povinnost hlásit kontaktní údaje na osobu oprávněnou jednat za správce KII je specifikována v § 16 ZKB. Cílem opaření je ustanovit síť osob, které je možné v případě potřeby kontaktovat a řešit s nimi jak kybernetické bezpečnostní události a incidnety, tak vyměňovat informace. Lze doporučit, aby bylo za jeden prvek KII nahlášeno kontaktních údajů více, tak aby byla zajištěna zastupitelnost a dostupnost.

Hlášení kybernetického bezpečnostního incidentu

Povinnost hlásit kybernetické bezpečnostní incidenty u subjektů KII je stanovena v § 8 ZKB. Tento institut umožňuje, aby se o problému včasně dozvěděl Vládní CERT tak, aby mohl incident sám analyzovat a informovat další subjekty, pro které může být hrozba relevantní. Zároveň hlášení umožňuje

Vládnímu CERT poskytnout zasaženým subjektům podporu či asistenci.

Komunikace krizové situace

V případě rozvoje KS na základě kybernetického bezpečnostního incidentu je podstatné, aby byl aktuální stav nadále komunikován zejména mezi zasaženým subjektem a NÚKIB, popřípadě dalšími institucemi, jejichž asistence je vhodná.

NÚKIB dále situaci komunikuje s dalšími relevantními subjekty pro zajištění kybernetické bezpečnosti státu a koordinuje reakci na úrovni státu.

Metodická podpora

V případě nemožnosti zvládat KS vlastními kapacitami, může subjekt KII požádat o podporu ze strany NÚKIB.

Expertní asistence

V případě neefektivnosti pouhé metodické podpory je možné vyslat experty NÚKIB přímo na místo KS.

Varování

NÚKIB v souladu s § 12 ZKB vydává varování, dozví-li se o hrozbě v oblasti kybernetické bezpečnost. Varování jsou zveřejňovány na webu NÚKIB.CZ a mohou být oznamovány kontaktním osobám z řad správců KII. Jedná se tedy o preventivní činnosti směřující k předcházení negativních událostí a eliminaci hrozeb a rizik.

Reaktivní opatření

Dle ustanovení § 13 ZKB může NÚKIB vydat reaktivní opatření k řešení kybernetického bezpečnostního incidentu anebo k zabezpečení informačních systémů nebo sítí a služeb elektronických komunikací před kybernetickým bezpečnostním incidentem a subjekt KII je povinen je provést. Může se jednat o jakoukoli akci přímo směřující k výše uvedenému.

Reaktivní opatření jsou výjimečným nástrojem zejména s ohledem na princip individuální odpovědnosti správce/vlastníka za bezpečnost.

Ochranné opatření

NÚKIB v souladu s § 14 ZKB může vydat ochranné opatření za účelem zvýšení ochrany informačních systémů nebo služeb a sítí elektronických komunikací. Jde tedy zpravidla o opatření, které reaguje na proběhlý kybernetický bezpečnostní incident a jeho cílem je podobnému incidentu předejít anebo snížit jeho dopad.

Stav kybernetického nebezpečí

V případě, kdy je ve velkém rozsahu ohrožena bezpečnost informací v informačních systémech nebo bezpečnost služeb elektronických komunikací anebo bezpečnost a integrita sítí elektronických komunikací, a tím by mohlo dojít k porušení nebo došlo k ohrožení zájmu České republiky (zachování ústavnosti, svrchovanosti a územní celistvosti, zajištění vnitřního pořádku a bezpečnosti, mezinárodních závazků a obrany, ochrana ekonomiky a ochrana života nebo zdraví fyzických osob), může ředitel NÚKIB vyhlásit dle § 21 ZKB tzv. stav kybernetického nebezpečí.

Za stavu kybernetického nebezpečí může NÚKIB nařizovat provedení reaktivních opatření i poskytovatelům služeb elektronických komunikací a subjektům zajišťujících sítě elektronických komunikací.

O KS je zároveň informována vláda a prostřednictvím veřejnoprávních médií také široká veřejnost.

Řešení sekundárních dopadů vizte typové plány jednotlivých oblastí.

2.2.3. Jiné podmínky

Další podmínky vyplývají zejména z dosažitelnosti lidských, finančních a materiálních zdrojů v potřebném rozsahu a struktuře.

2.3. Okolnosti omezující řešení krizové situace

2.3.1. Právní

Právní překážky, které mohou narušit schopnosti a možnosti odpovědných orgánů řešit KS, jsou okrajové.

V současné době nejsou upraveny kompetence odpovědných orgánů k provádění aktivit kybernetické obrany, které mohou být ve specifických případech nutné pro efektivní řešení situace.

Pro subjekty KII nejsou právní skutečnosti omezující řešení KS v současné době identifikovány.

2.3.2. Politická

Specifickým omezením řešení KS mohou být zásahy neinformovaného vedení do aktivit vyžadujících expertní posouzení a řešení.

2.3.3. Mediální

KS může být prohloubena či prodlužována nesprávným, nedostatečným či nepřiměřeným informováním široké či zasažené veřejnosti o KS, dopadech a nutných opatřeních.

Omezení lze také uvažovat u případné informační kampaně vedené útočníky probíhající paralelně s kybernetickými útoky.

2.3.4. Materiální

Některé subjekty se mohou potýkat s nedostatkem lidských, finančních nebo materiálních zdrojů v potřebném rozsahu a struktuře.

Je možné využít asistenční kapacity NÚKIB nebo jím zprostředkované kapacity odborné veřejnosti.

2.3.5. Mezinárodní

Je-li KS způsobena kybernetickým útokem majícím původ v zahraničí, mohou určitá omezení řešení vyplývat z neexistence kontaktního bodu pro záležitosti kybernetické bezpečnosti v tomto státě, nebo z neochoty či neschopnosti takového státu zabránit takové škodlivé aktivitě vycházet z jeho teritoria.

Omezujícím prvkem mohou být také nedostatečně pevně nastavené diplomatické vztahy s takovým státem.

2.4. Opatření pro řešení krizové situace

Označení opatření	Opatření	Provádí	Spolupracuje
1	Koordinace řešení kybernetického bezpečnostního incidentu (KBI) či jiné hrozby	- NÚKIB - zasažený subjekt	- Provozovatel Národního CERT - další relevantní subjekty
2	Stanovení osoby pro případnou komunikaci s NÚKIB, správcem KII nebo dalšími orgány a osobami podílejícími se na řešení kybernetické KS.	- krajský úřad	

Dopady narušení bezpečnosti informací kritické informační infrastruktury a navazující opatření vizte příloha č. 1.

3. Pomocná část

3.1. Právní předpisy

- zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
- zákon č. 239/2000 Sb., o integrovaném záchranném systému a o změně některých zákonů
- zákon č. 240/2000 Sb., o krizovém řízení a o změně některých zákonů (krizový zákon)
- zákon č. 241/2000 Sb., o hospodářských opatřeních pro krizové stavy a o změně některých souvisejících zákonů
- vyhláška 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)
- nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury

3.2. Podklady, formuláře

Formulář hlášení kybernetického bezpečnostního incidentu
(dle přílohy č. 8 vyhlášky č. 82/2018 Sb., o kybernetické bezpečnosti

https://www.govcert.cz/download/kii-vis/container-nodeid-649/incidentreportnckb.pdf

3.3. Organizační údaje

Kontaktní spojení na rozhodující složky a odborníky schopné poskytnout pomoc při řešení KS

Národní úřad pro kybernetickou a informační bezpečnost

Mučednická 31

616 00 Brno – Žabovřesky

hlášení incidentů: cert.incident@nukib.cz,

Vládní CERT: cert@nukib.cz,

NCKB: nckb@nukib.cz

Hlášení incidentů: cert.incident@nukib.cz, Tel.: +420 541 110 777

Hlášení incidentu mimo pracovní dobu: +420 725 502 878

Národní CERT, CSIRT.CZ

CZ.NIC, zájmové sdružení právnických osob

Milešovská 1136/5

130 00 Praha 3

hlášení incidentů: +420 910 101 010 (v pracovních dnech od 09:00-17:00)

+420 222 745 111 (mimo pracovní dobu)

Hlášení incidentů: abuse@csirt.cz

Hlášení incidentů (webový formulář): https://csirt.cz/stateincidentreport/

7. Identifikační údaje o zpracovateli typového plánu

7.1. Název a adresa zpracovatele typového plánu

Národní úřad pro kybernetickou a informační bezpečnost
Mučednická 31
Brno 616 00
Česká republika

7.2. Názvy a adresy subjektů, které poskytly zpracovateli součinnost

7.3. Kontaktní údaje osob, které se podílely na zpracování typového plánu

Václav Borovička, odbor kybernetických bezpečnostních politik
Tel.: +420 727 929 094
e-mail: v.borovicka@nukib.cz

Adam Kučínský, odbor regulace
Tel.: + 420 725 882 129
e-mail: a.kucinsky@nukib.cz

Michaela Vašková, odbor regulace
Tel.: + 420 606 038 083
e-mail: m.vaskova@nukib.cz

Příloha č. 1: Odvětví podle přílohy č. 1 nařízení vlády č. 432/2010 Sb., ve kterých jsou určeny prvky KII (stav k 1. 1. 2018)

Odvětví	Pododvětví	Určena KII	Dopady kybernetického bezp. incidentu	Vazba na další typové plány
I. Energetika	A. Elektřina	Ano	Blackout	19. Narušení dodávek elektrické energie velkého rozsahu 18. Radiační havárie
	B. Zemní plyn	Ano	Zastavení dodávek zemního plynu,	16. Narušení dodávek plynu velkého rozsahu
	C. Ropa a ropné produkty	Ano	Zastavení dodávek zemního produktů, únik produktů do prostředí	17. Narušení dodávek ropy a ropných produktů velkého rozsahu
II. Vodní hospodářství	-	Ano	Zastavení dodávek vody, unik znečistěné vody do prostředí	15. Narušení dodávek pitné vody velkého rozsahu
III. Potravinářství a zemědělství	A. Rostlinná výroba	Ne	-	-
	B. Živočišná výroba	Ne	-	-
	C. Potravinářská výroba	Ne	-	-
IV. Zdravotnictví	-	Ne	-	-
V. Doprava	A. Silniční doprava	Ne	-	-
	B. Železniční doprava	Ano	Nedostupnost dopravního spojení, závažná havárie v železniční dopravě	
	C. Letecká doprava	Ano	Nedostupnost dopravního spojení, závažná havárie v letecké dopravě	
	D. Vnitrozemská vodní doprava	Ne	-	-
VI. Komunikační a informační systémy		Ano	Nedostupnost komunikačních služeb, internetu, zprostředkovaně další dopady uvedené v této tabulce	11. Narušení funkčnosti významných systémů elektronických komunikací
VII. Finanční trh a měna	-	Ano	Nedostupnost služeb pro občany, firmy a státní instituce, významné ekonomické škody	22. Narušení finančního a devizového hospodářství státu velkého rozsahu
VIII. Nouzové služby	A. Integrovaný záchranný systém	Ano	Nedostupnost služeb pro občany	
	B. Radiační monitorování	Ne	-	-

	C. Předpovědní, varovná a hlásná služba	Ano	Nedostupnost služby pro občany a letecké služby	
IX. Veřejná správa	A. Veřejné finance	Ano	Nedostupnost služby, uniky, citlivých informací, narušení zákonnosti	22. Narušení finančního a devizového hospodářství státu velkého rozsahu
	B. Sociální ochrana a zaměstnanost	Ano	Nedostupnost služby, uniky, citlivých informací, narušení zákonnosti	21. Narušování zákonnosti velkého rozsahu (včetně terorismu)
	C. Ostatní státní správa	Ano	Nedostupnost služby, uniky, citlivých informací, narušení zákonnosti	21. Narušování zákonnosti velkého rozsahu (včetně terorismu)
	D. Zpravodajské služby	Ne	-	-