A-T-21

Č.j.: HSPM-3538-9-13/2020 ÚPP

Výtisk číslo:
Počet listů:

PLZEŇSKÝ KRAJ

ROZPRACOVÁNÍ TYPOVÉHO PLÁNU NA POSTUPY PRO ŘEŠENÍ

krizové situace

NARUŠENÍ BEZPEČNOSTI INFORMACÍ KRITICKÉ INFORMAČNÍ INFRASTRUKTURY

OBSAH **strana**

Zkratky

IS	Informační systém	KS	Krizová situace
IZS	Integrovaný záchranný systém	KÚ PK	Krajský úřad Plzeňského kraje
KBI	kybernetický bezpečnostní incident	NÚKIB	Národní úřad pro kybernetickou a informační bezpečnost
KI	Kritická infrastruktura	ZKB	Zákon o kybernetické bezpečnosti

A. POPIS KRIZOVÉ SITUACE

1. Charakteristika krizové situace

- vzhledem k nárůstu závislosti současné společnosti na informačních a komunikačních systémech je možnost KS reálná,
- spojená s určenými prvky KI – oblast energetiky, veřejné správy, elektronických komunikací a finančního trhu a měny,
- dopad na funkčnost subjektu KI – dopad na jeho fungování a služby,
- řeší zpravidla zasažený subjekt, NÚKIB a další instituce na centrální úrovni státu,
- 2 typy rizik:
  1) riziko neúmyslného selhání technologií či lidského faktoru – může vést k selhání služby poskytované informačními nebo komunikačními systémy,
  2) riziko úmyslného napadení informačních nebo komunikačních systémů – různé motivace a dopady,
- řešení KS:
  1) následky ve fyzické rovině (zapojení složek IZS – dle zákona č. 240/2000 Sb., krizový zákon),
  2) následky v kyberneticko-bezpečnostní rovině (řešení incidentů dle zákona č. 181/2014 Sb., o kybernetické bezpečnosti).

2. Předpokládaný územní a časový rozsah působení

- závislý na specifikách sektoru a nastalé KS, ve které IS funguje,
- při úmyslném narušení i na motivaci, schopnostech a síle útočníka,
- rozdílná doba trvání – rozmezí hodin x dnů.

3. Možné příčiny vzniku, indikátory vzniku a rozvoje

Narušení bezpečnosti informací:

a) dle povahy narušení:

neúmyslné

- selhání technologie (přímé poškození provozních zařízení, disfunkční chování systémů, atd.);
- selhání osob;
- živelní pohroma;
- dlouhodobé narušení dodávek elektrické energie.

úmyslné

- kybernetický útok.

4. Možné příčiny vzniku, indikátory vzniku a rozvoje

Narušení bezpečnosti informací:

b) <u>dle typu útoku:</u>

- kinetický zásah – činnost informačního nebo komunikačního systému je narušena kinetickým zásahem (destruktivním x nedestruktivním);
- DoS/DDoS[1] – odepření služby, charakterizované zahlcením systému požadavky;
- škodlivý malware[2] – v jeho rámci pak zejména ransomware[3], 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.

c) <u>dle motivace útočících subjektů:</u>

- 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] Denial of service (DoS) (česky odepření služby) je typ útoku na internetové služby nebo stránky, jehož cílem je cílovou službu znefunkčnit a znepřístupnit ostatním uživatelům; může k tomu dojít přehlcením požadavky či využitím nějaké chyby, která sice útočníkovi neumožní službu ovládnout, ale umožní ji rozbít. Podtypem útoku DoS je tzv. distributed denial of service (DDoS), při kterém je pro přehlcení cílové služby požadavky využito velké množství rozptýlených počítačů.

[2] Malware (škodlivý software, zákeřný software) je program určený k poškození nebo vniknutí do počítačového systému.

[3] Ransomware (vyděračský software, vyděračský program) je druh škodlivého programu, který blokuje počítačový systém nebo šifruje data v něm zapsaná, a pak požaduje od oběti výkupné za obnovení přístupu.

5. Popis skutečností nasvědčujících, že danou situaci není možné zvládnout běžnou činností

- 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.

6. Předpokládané sekundární události

Závislé na službě, kterou poskytuje KI, na kterou je KII navázáno.

Události způsobené omezením nebo zastavením služeb, které narušení KII způsobilo, viz:
- Rozpracování typového plánu na postupy pro řešení krizové situace NARUŠENÍ DODÁVEK PLYNU VELKÉHO ROZSAHU
- Rozpracování typového plánu na postupy pro řešení krizové situace NARUŠENÍ DODÁVEK ELEKTRICKÉ ENERGIE VELKÉHO ROZSAHU
- Rozpracování typového plánu na postupy pro řešení krizové situace NARUŠENÍ DODÁVEK ROPY A ROPNÝCH PRODUKTŮ VELKÉHO ROZSAHU
- Rozpracování typového plánu na postupy pro řešení krizové situace NARUŠENÍ DODÁVEK PITNÉ VODY VELKÉHO ROZSAHU
- Rozpracování typového plánu na postupy pro řešení krizové situace NARUŠENÍ FUNKČNOSTI VÝZNAMNÝCH SYSTÉMŮ ELEKTRONICKÝCH KOMUNIKACÍ
- Rozpracování typového plánu na postupy pro řešení krizové situace NARUŠENÍ FINANČNÍHO A DEVIZOVÉHO HOSPODÁŘSTVÍ STÁTU VELKÉHO ROZSAHU

Události kyberneticko-bezpečnostní:
- dopad na ostatní subjekty využívající kyberprostor či subjekty operující systémy, které by mohly být KS dotčeny

7. Následky krizové situace

Dopady na životy a zdraví osob
- blackout,
- zastavení dodávek zemního plynu,
- zastavení dodávek ropných produktů,
- zastavení dodávek vody,

7. Následky krizové situace

Dopady společenské

- nedostupnost dopravního spojení,
- nedostupnost komunikačních služeb, internetu,
- nedostupnost služeb pro občany, firmy a státní instituce v oblasti finančního a devizového hospodářství,
- nedostupnost služeb pro občany v oblasti IZS.

Dopady na životy a zdraví osob

- nedostupnost dopravního spojení v železniční dopravě,
- závažná havárie v železniční dopravě,
- závažná havárie v letecké dopravě,
- nedostupnost komunikačních služeb, internetu,
- nedostupnost služeb pro občany, firmy a státní instituce v oblasti finančního a devizového hospodářství,
- nedostupnost služeb pro občany v oblasti IZS,
- nedostupnost služeb ve zdravotnictví.

Dopady na životní prostředí

- únik ropných produktů do prostředí,
- únik znečištěné vody do prostředí.

Dopady ekonomické

- blackout,
- zastavení dodávek zemního plynu,
- zastavení dodávek zemních produktů,
- zastavení dodávek vody.

Dopady na kritickou infrastrukturu

- dle specifikace narušení bezpečnosti informací kritické informační infrastruktury, která ovlivňuje či ovládá určený prvek KI.

B. PLÁNOVANÁ ČINNOST SUBJEKTŮ PODÍLEJÍCÍCH SE NA ŘEŠENÍ KRIZOVÉ SITUACE

P. č.	ÚKOL / ČINNOST OPATŘENÍ	Nařizuje/ zodpovídá/ provádí	Spolupracuje	Dokumentace
PŘI HROZBĚ VZNIKU KRIZOVÉ SITUACE – při zjištění narušení bezpečnosti informací KII				
1.	Ustanovit osoby pro komunikaci.	KÚ PK	NÚKIB	Karta opatření 2
2.	Nahlásit kontaktní údaje osoby pro komunikaci do datové schránky NÚKIB	KÚ PK	NÚKIB	Karta opatření 2
3.	Nahlásit incident – dotčený subjekt nahlásí incident Vládnímu CERTu na pohotovostní telefonní linku nebo emailem	Dotčený subjekt	NÚKIB/Vládní CERT	Formulář hlášení kybernetického bezpečnostního incidentu
4.	NÚKIB vydá rozhodnutí, ve kterém uloží provést reaktivní opatření k řešení KBI anebo k zabezpečení IS nebo sítí a služeb elektronických komunikací před KBI.	NÚKIB/ Dotčený subjekt/ subjekty	NÚKIB/ Dotčený subjekt/ subjekty	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, § 13
5.	NÚKIB za účelem zvýšení ochrany IS nebo služeb a sítí elektronických komunikací a na základě analýzy již vyřešeného KBI jako ochranné opatření vydá opatření obecné povahy, ve kterém: . správci a provozovateli IS KII, . správci a provozovateli KS KII, . správci a provozovateli významného IS, . správci a provozovateli IS základní služby stanoví způsob zvýšení ochrany IS nebo služeb a sítí elektr. komunikací a přiměřenou lhůtu k jeho provedení	NÚKIB/ Dotčený subjekt/ subjekty	NÚKIB/ Dotčený subjekt/ subjekty	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, § 14

P. č.	ÚKOL / ČINNOST OPATŘENÍ	Nařizuje/ zodpovídá/ provádí	Spolupracuje	Dokumentace
	PŘI VZNIKU KRIZOVÉ SITUACE			
1.	**Vyhlášení Stavu kybernetického nebezpečí** NÚKIB vydá rozhodnutí nebo opatření obecné povahy: . orgánu nebo osobě zajišťující významnou síť, . správci a provozovateli IS KII, . správci a provozovateli KS KII, . správci a provozovateli významného IS, . správci a provozovateli IS základní služby	NÚKIB/ orgány krizového řízení/ povinné osoby dle ZKB	NÚKIB/ orgány krizového řízení/ povinné osoby dle ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, § 21
	Vyhlášení krizového stavu – NOUZOVÝ STAV (Vláda ČR) Rozpracovat krizová opatření, zajistit vyhlášení na postiženém území.	NÚKIB/ orgány krizového řízení/ povinné osoby dle ZKB	NÚKIB/ orgány krizového řízení/ povinné osoby dle ZKB	Zákon č. 181/2014 Sb., o kybernetické bezpečnosti, § 21

C. KARTY OPATŘENÍ PRO ŘEŠENÍ KRIZOVÉ SITUACE

KARTA OPATŘENÍ

Opatření	Označení opatření
Koordinace řešení kybernetického bezpečnostního incidentu (KBI) či jiné hrozby	1

Nařizuje (schvaluje)	Statutární orgán zasaženého subjektu	**Provádí**	- zasažený subjekt - NÚKIB	**Spolupracuje**	- Provozovatel Národního CERT - další relevantní subjekty

Související právní předpisy

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB)
Vyhláška č. 316/2014 Sb., o kybernetické bezpečnosti

Věcné zdroje, další mimořádné zdroje, síly a prostředky

různé, dle povahy krizové situace

Další potřebné informace související s plněním opatření

Zasažený subjekt se primárně pokouší příčinu KBI nebo ochranu před hrozbou zajistit sám v souladu s principem individuální odpovědnosti za bezpečnost vlastních systémů a sítí. Zároveň má povinnost hlásit informace o KBI Vládnímu CERT (NÚKIB) a krizovou situaci s ním dále koordinuje.

Popis činností k realizaci opatření

P. č.	Činnosti na ústřední úrovni	Nařizuje	Provádí	Spolupracuje
1.	Přijetí hlášení o KBI či jiné hrozbě		NÚKIB	- zasažený subjekt
2.	Koordinace s ostatními potenciálně ohroženými subjekty		NÚKIB	- zasažený subjekt - Národní CERT - ostatní relevantní subjekty
3.	Vydání doporučení k zabezpečení KII		NÚKIB	- zasažený subjekt - další ohrožené subjekty
4.	Vydání reaktivního opatření	NÚKIB	- zasažený subjekt	
P. č.	**Činnosti na krajské úrovni**	**Nařizuje**	**Provádí**	**Spolupracuje**
P. č.	**Činnosti na úrovni obce s rozšířenou působností**	**Nařizuje**	**Provádí**	**Spolupracuje**

KARTA OPATŘENÍ

Opatření	Označení opatření
Určení osoby pro komunikaci s orgány nebo osobami podílejícími se na řešení kybernetické krizové komunikace	2

Nařizuje (schvaluje)		**Provádí**	- krajský úřad	**Spolupracuje**	

Související právní předpisy

Zákon č. 181/2014 Sb., o kybernetické bezpečnosti (ZKB)
Zákon č. 240/2000 Sb., krizový zákon

Věcné zdroje, další mimořádné zdroje, síly a prostředky

různé, dle povahy krizové situace

Další potřebné informace související s plněním opatření

Příčina kybernetické krizové situace je řešena na centrální úrovni společně se zasaženým subjektem.

V případě potřeby je vhodné mít ustanovenou osobu, která bude schopna komunikovat s ostatními orgány a osobami podílejícími se na řešení krizové situace zejména s ohledem na vzájemnou výměnu informací o charakteru hrozby a existujících a potenciálních (i sekundárních) dopadech.
Kontaktní údaje takto ustanovené osoby zašlete do datové schránky NÚKIB (ID datové schránky: zzfnp3).

V případě, že toho bude třeba je možné NÚKIB jako ústřední správní úřad kontaktovat zde:

V pracovní době (po-pá, 7:45 – 16:30):
Mučednická 1125/31
616 00 Brno – Žabovřesky
Tel.: +420 541 110 777
P.O. Box 17, Brno 16, CZ 616 00

Mimo pracovní dobu:
+420 725 502 878

Popis činností k realizaci opatření

P. č.	Činnosti na ústřední úrovni	Nařizuje	Provádí	Spolupracuje
P. č.	**Činnosti na krajské úrovni**	**Nařizuje**	**Provádí**	**Spolupracuje**
1.	Ustanovení osoby pro komunikaci		- krajský úřad	NÚKIB
2.	Nahlášení kontaktních údajů osoby pro komunikaci do datové schránky NÚKIB		- krajský úřad	NÚKIB
P. č.	**Činnosti na úrovni obce s rozšířenou působností**	**Nařizuje**	**Provádí**	**Spolupracuje**

Formulář hlášení kybernetického bezpečnostního incidentu

Míra ochrany informace*: Neomezeno (veřejné)

Kontaktní údaje

Orgán a osoba uvedená v § 3 písm. c) a e) zákona*:

Identifikátor****:

E-mail*:

Telefon*:

Pokračování*: Iniciační oznámení CERT/CSIRT týmu **ID**:**

Detaily kybernetického bezpečnostního incidentu/kybernetické bezpečnostní události

Jedná se o hlášení: INCIDENTU

Datum a čas zjištění*: **YYYY MM DD hh : mm** **Časová zóna*:** **+- hh**

Datum a čas výskytu incidentu: **YYYY MM DD hh : mm** **Časová zóna*:** **+- hh**

Kategorie incidentu*: Kategorie I – méně závažný kybernetický bezpečnostní incident

Typ incidentu*:

Kybernetický bezpečnostní incident způsobený kybernetickým útokem nebo jinou událostí vedoucí k průniku do systému.

Upřesnění podle standardu ENISA/eCSIRT.net – “Incident Classification“ ***:

Abusive Content (např. spam, kyberšikana, nevhodný obsah)
Malicious Code (např. virus, červ, trojský kůň, dialer, spyware)
Information Gathering (např. skenování, sniffing, sociální inženýrství)
Intrusion Attempts (např. zneužití zranitelnosti, kompromitace aktiva, “0-day“ útok)
Intrusions (např. kompromitace aplikace nebo uživatelského účtu)

Availability (např. narušení dostupnosti způsobené DoS/DDoS útokem nebo sabotáží)

Information Security (např. neautorizovaný přístup nebo neautorizovaná změna informace, ..)
Fraud (např. neoprávněné využití ICT – porušení licenčních práv, krádež identity aj.)
Ostatní

Současný stav zvládání kybernetického bezpečnostního incidentu*:

Probíhá analýza a šetření kybernetického incidentu

Počet zasažených systémů (odhad)*:

Odhad počtu dotčených uživatelů*:

Popis incidentu*:

Rozsah škod:

Jaká opatření již byla přijata?:

Systémové detaily – cíl útoku (kompromitovaný systém)

Host nebo IP*:

Funkce hosta*:

Port:

Protokol:

OS / jiný systém + verze:

Umístění systému v architektuře:

Systémové detaily – zdroj útoku (je-li znám)

Host / IP nebo jiné (zařízení/uživatel):

Port:

Protokol:

[*] Povinné pole
[**] Povinné pole v případě, že je vybrána volba „pokračování dříve oznámeného incidentu“, jedná se o ID dříve oznámeného incidentu / události, na které chcete navázat nové hlášení
[***] zdroj: http//www.ecsirt.net/cec/service/dokuments/wp4-clearinghouse-policy-v12.html
[****] Identifikátor zadávejte jen tehdy, pokud Vám byl sdělen ze strany GovCERTu (jde o jednoznačný identifikátor orgánu nebo osoby)

UPOZORNĚNÍ:
Právo změny dokumentu vyhrazeno.
Orgány a osoby podle § 3 zákona o kybernetické bezpečnosti, písm. b) (orgány nebo osoby zajišťující významnou síť) hlásí kybernetické bezpečnostní incidenty národnímu CERT týmu (NIC.CZ) prostřednictvím formuláře, zveřejněného na: www.csirt.cz/stateincidentreport