



# **Analýza rizik kybernetické bezpečnosti**

-

## **od teorie k praxi**

František Janů

# K čemu nám vlastně je analýza rizik?

- Jakým hrozbám může být organizace vystavena?
- Jsou naše aktiva zranitelná?
- Jaké dopad by to mohlo mít na naši organizaci?
  - Finanční ztráta
  - Poškození pověsti atd...

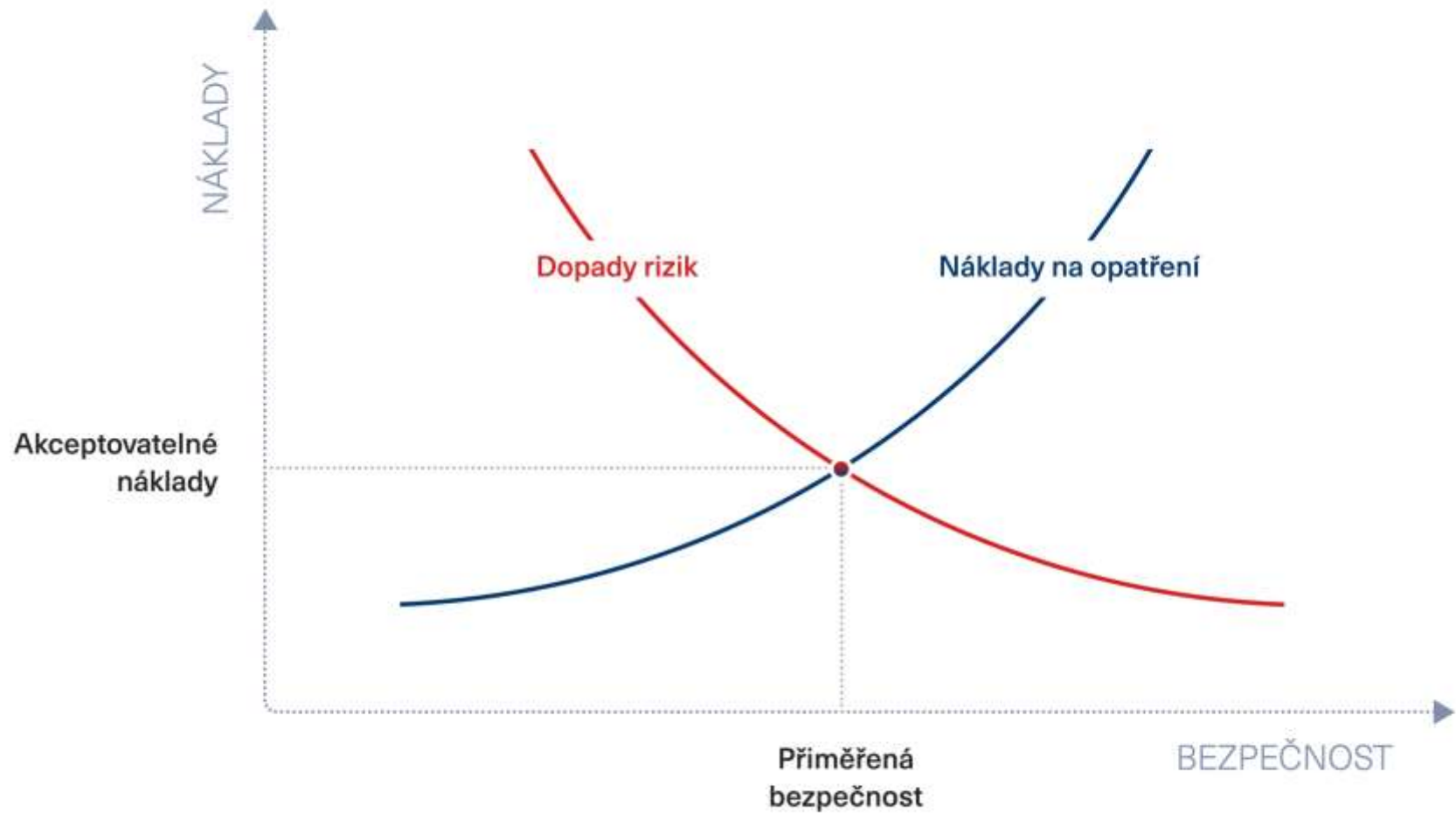
---

---

## Co je cílem analýzy rizik?

- Pomoci najít „přiměřenou bezpečnost“
  - Abychom byli v bezpečí
  - Abychom určili přiměřené náklady

# Jak najít „přiměřenou“ bezpečnost?



CSA

# CSA – online analýza rizik



# Bezpečnostní role

The screenshot displays a user management interface. On the left, a search bar labeled 'hledat osobu' is positioned above a tree view of roles. The selected role is 'AMATO office s.r.o.', which is highlighted in red. Underneath, a list of roles is shown with expandable arrows: 'A) Výbor pro řízení KB' (expanded), 'Architekt KB', 'Auditor KB', 'Manažer KB' (expanded), 'Garant', 'B) Garanti primárních aktiv', 'C) Garanti podpůrných aktiv', and 'D) administrátoři'. The 'Garant' role is expanded to show 'Anna Fraiová' and 'Garant'. On the right, a 'Kompletní seznam osob' (Complete list of persons) is shown. It includes a search bar, a 'Přidat novou osobu' button, and a table of users. The table has columns for 'Jméno', 'Email', 'Kontakt', and 'Systémový uživatel'. Below the table, there is a pagination control showing '10' items per page and a total of 'Celkem 19, záznamů na stranu'.

<input type="checkbox"/>	Jméno	Email	Kontakt	Systémový uživatel		
<input type="checkbox"/>	Beáta Veselá			ne		
<input type="checkbox"/>	Ondřej Chrást			ne		
<input type="checkbox"/>	Petr Šustáček			ne		
<input type="checkbox"/>	Tomáš Dobrovolný			ne		
<input type="checkbox"/>	Jakub Skalický			ne		
<input type="checkbox"/>	František Janů			ne		
<input type="checkbox"/>	Jaroslav Handlíř			ne		
<input type="checkbox"/>	Dan Kresa			ne		
<input type="checkbox"/>	Vojtěch Hvězda			ne		

§ 6 Organizační bezpečnost | § 7 Bezpečnostní role

# Analýza aktiv

## Editace aktiva: Měření spotřeby dodávaných energií

Obecné   Hodnocení aktiva   Hodnocení důležitosti   Identifikace hrozeb/zranitelnosti   Způsoby používání a manipulace   Vlastní atributy

vybrat oblast

Měření spotřeby dodávaných energií

Druh

Primární

Typ

vyberte

podkategorizace:  IS KIS  KS KII  VIS

Způsob likvidace

vyberte

Lokalizace

vyberte

Garant

Tomáš Dobrovolný

Dodavatel

Delay, a.s.

Provozovatel

vyberte

Na kolik procent je provozovatel

0 %

Závislost na aktivech

Serverovna (služby provozu IT)

Aktiva závislá na tomto aktivu

vyberte

Popis

**B** *I*

Zrušit

Uložit

Následující krok >

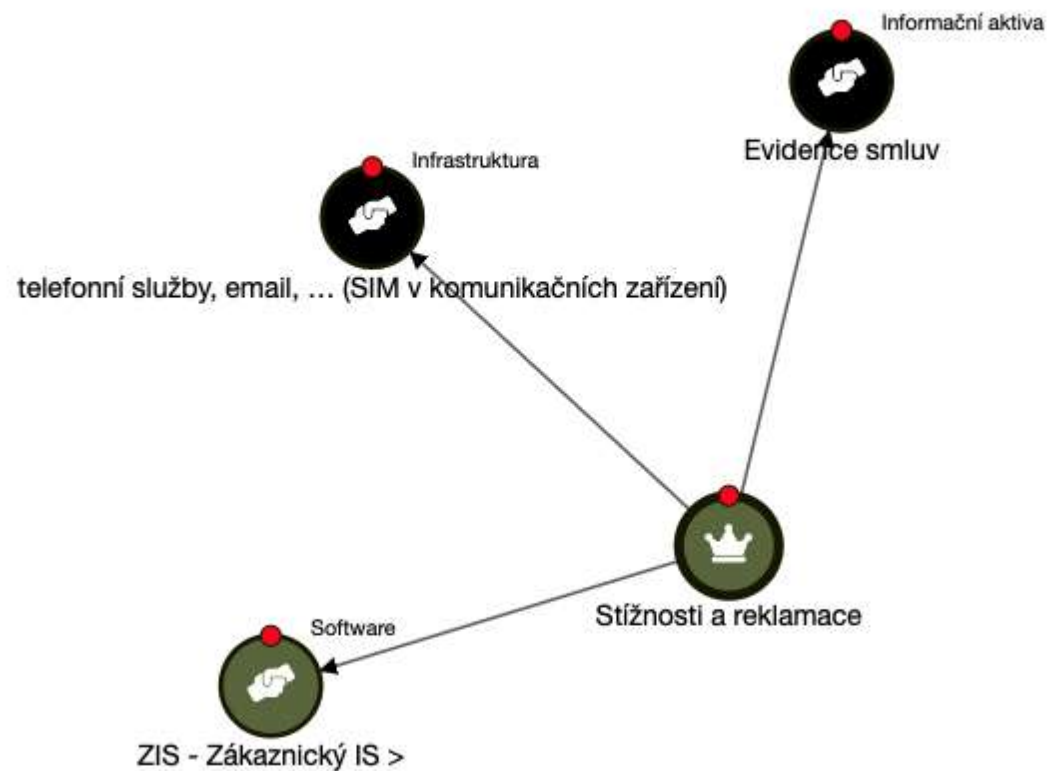
# Určení vazeb mezi aktivy

## Druhy aktiv

	Podpůrné	<input checked="" type="checkbox"/>
	Primární IS KIS / KS KII / VIS	<input checked="" type="checkbox"/>
	Nezařazeno	<input checked="" type="checkbox"/>

## Klasifikace rizik

	Nízké
	Střední
	Vysoké
	Kritické
	Neohodnoceno



§ 4 Řízení aktiv



# Hodnocení aktiv

AKTIVA

Stupnice pro hodnocení **důvěrnosti** 4

Úroveň	Popis	
1 1/Nízká	Aktiva jsou veřejně přístupná nebo byla určena ke zveřejnění. Narušení důvěrnosti aktiv neohrožuje oprávněné zájmy povinné osoby. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle tzv. traffic light protokolu (dále jen „TLP“) je využíváno označení TLP:WHITE.	 
2 2/Střední	Aktiva nejsou veřejně přístupná a tvoří know-how povinné osoby, ochrana aktiv není vyžadována žádným právním předpisem nebo smluvním ujednáním. V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:GREEN nebo TLP:AMBER.	 
3 3/Vysoká	Aktiva nejsou veřejně přístupná a jejich ochrana je vyžadována právními předpisy, jinými předpisy nebo smluvními ujednáními (například obchodní tajemství, osobní údaje). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:AMBER.	 
4 4/Kritická	Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:RED nebo TLP:AMBER.	 
5	<input type="text" value="název úro"/> <input type="text" value="popis úrovně"/>	

Stupnice pro hodnocení **integrity** 4

Stupnice pro hodnocení **dostupnosti** 4

§ 4 Řízení aktiv

# Hodnocení aktiv

## Editace aktiva: Měření spotřeby dodávaných energií

Obecné

Hodnocení aktiva

Hodnocení důležitosti

Identifikace hrozeb/zranitelnosti

Způsoby používání a manipulace

Vlastní atributy

### C - Důvěrnost

4/Kritická

Aktiva nejsou veřejně přístupná a vyžadují nadstandardní míru ochrany nad rámec předchozí kategorie (například strategické obchodní tajemství, zvláštní kategorie osobních údajů). V případě sdílení takového aktiva s třetími stranami a použití klasifikace podle TLP je využíváno zejména označení TLP:RED nebo TLP:AMBER.

### I - Integrita

4/Kritická vysoká

Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity vede k velmi vážnému poškození oprávněných zájmů povinné osoby s přímými a velmi vážnými dopady na primární aktiva.

### A - Dostupnost

3/Vysoká

Narušení dostupnosti aktiva by nemělo překročit dobu několika hodin. Jakýkoli výpadek je nutné řešit neprodleně, protože vede k přímému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za velmi důležitá.

### Stanovte pravidla ochrany

B I ::= ½=

### Výsledné hodnocení

4

4/KRITICKÝ

< Předchozí krok

Zrušit

Uložit

Následující krok >

§ 4 Řízení aktiv

# Analýza aktiv

The screenshot displays the 'Analýza aktiv' (Asset Analysis) interface. At the top, there are buttons for 'Import', 'Exportovat vše', and '+ Vytvořit'. Below this, there are tabs for 'Primární aktiva', 'Aktiva', and 'Katalog aktiv'. A section for 'označené položky:' includes 'exportovat', 'stáhnout karty aktiv', and 'režim'. The main table has columns: 'Název aktiva', 'Oblast', 'Druh', 'Typ', 'Garant', and 'Dopad'. The table lists various assets such as 'Kamerový systém', 'Osobní údaje zákazníků', 'CSA', 'Dodávky nepřerušitelného napájení et. napájení', 'Prostory ICT (Servovna)', 'Měření spotřeby dodávaných energií', 'IT systém', 'Zaměstnanci', 'Zákazníci', and 'UPS'. Each row includes a checkbox, a crown icon, and a status indicator (e.g., '4/Kritický / 4'). At the bottom, there is a pagination control showing '(Položek: 1 - 10 z 81)' and a legend for 'Horní dopad:' with categories 1-1/Nízký, 2-2/Střední, 3-3/Vysoký, and 4-4/Kritický.

	Název aktiva	Oblast	Druh	Typ	Garant	Dopad	
<input type="checkbox"/>	Kamerový systém		Podpůrné	Osobní údaje	Tomáš Dobrovýň	4/Kritický / 4	
<input type="checkbox"/>	Osobní údaje zákazníků		Podpůrné	Osobní údaje	Tomáš Dobrovýň	4/Kritický / 4	
<input type="checkbox"/>	CSA		Primární	Software		4/Kritický / 4	
<input type="checkbox"/>	Dodávky nepřerušitelného napájení et. napájení		Podpůrné	Infrastruktura	Ondřej Chrást	4/Kritický / 4	
<input type="checkbox"/>	Prostory ICT (Servovna)		Podpůrné		František Janů	4/Kritický / 4	
<input type="checkbox"/>	Měření spotřeby dodávaných energií		Primární		Tomáš Dobrovýň	4/Kritický / 4	
<input type="checkbox"/>	IT systém		Podpůrné	Software	Tomáš Dobrovýň	3/Vysoký / 3	
<input type="checkbox"/>	Zaměstnanci		Podpůrné	Personál	Alena Šuhajová	3/Vysoký / 3	
<input type="checkbox"/>	Zákazníci		Primární	Hardware	Jakub Skalický	3/Vysoký / 3	
<input type="checkbox"/>	UPS		Podpůrné	Hardware		3/Vysoký / 3	

§ 4 Řízení aktiv

# Identifikace hrozeb a zranitelností

Editace aktiva: **Měření spotřeby dodávaných energií**

Obecné

Hodnocení aktiva

Hodnocení důležitosti

Identifikace hrozeb/zranitelností

Způsoby používání a manipulace

Vlastní atributy

Přidat

Přidat vše z registru rizik

Hrozba

zranitelnosti



vyberte hrozbu

vyberte zranitelnost

Identifikované

Hrozba

zranitelnosti



Nedodržení smluvního závazku ze strany dodavatele

Nedostatečná míra nezávislé kontroly

< Předchozí krok

Zrušit

Uložit


Následující krok >

# Hodnocení rizik

RIZIKA

Stupnice pro hodnocení **dopadů** 4

Stupnice pro hodnocení **hrozeb** 4

	Úroveň	Popis	
^ v	1 1/Nizká	Hrozba neexistuje nebo je málo pravděpodobná. Předpokládaná realizace hrozby není častější než jednou za 5 let.	 
^ v	2 2/Střední	Hrozba je málo pravděpodobná až pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 roku do 5 let.	 
^ v	3 3/Vysoká	Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.	 
^ v	4 4/Kritická	Hrozba je velmi pravděpodobná až víceméně jistá. Předpokládaná realizace hrozby je častější než jednou za měsíc.	 
	5	<input type="text" value="název úro"/>	<input type="text" value="popis úrovně"/> <span style="float: right; background-color: green; color: white; padding: 2px 5px;">přidat</span>

Stupnice pro hodnocení **zranitelností** 4

§ 5 Řízení rizik

# Hodnocení rizik

## Měření spotřeby dodávaných energií

Ohodnocení

Opatření

### Dopad

4/Kritický

### Dopad ovlivňuje:

C - Důvěrnost  I - Integrita  A - Dostupnost

### Hrozba

3/Vysoká

Hrozba je pravděpodobná až velmi pravděpodobná. Předpokládaná realizace hrozby je v rozpětí od 1 měsíce do 1 roku.

### Zranitelnost

2/Střední

Zneužití zranitelnosti je málo pravděpodobné až pravděpodobné. Jsou zavedena bezpečnostní opatření, jejichž účinnost je pravidelně kontrolována. Schopnost bezpečnostních opatření včas detekovat možné zranitelnosti nebo případné pokusy o překonání opatření je omezena. Nejsou známy žádné úspěšné pokusy o překonání bezpečnostních opatření.

**Hrozba:** [W52d1] Nedodržení smluvního závazku ze strany dodavatele

**Zranitelnost:** [WL8JW] Nedostatečná míra nezávislé kontroly

Riziko

24 (38%)

VYSOKÉ

Riziko je dlouhodobě nepřijatelné a musí být zahájeny systematické kroky k jeho odstranění.

Zavřít

Uložit




# Návrh opatření pro snížení rizik

## Riziko [WL8JW] na aktivu [WYL9o] Měření spotřeby dodávaných energií

Ohodnocení

Opatření

	<b>Dopad</b> 4/Kritický / 4	<b>x</b>	<b>Hrozba</b> 3/Vysoká / 3	<b>x</b>	<b>Zranitelnost</b> 2/Střední / 2	<b>=</b>	<b>Riziko</b> Vysoké / 24 (38%)
<b>Cílené riziko:</b>	<b>4</b>		<b>3</b>		<b>1</b> ↓ 50%		<b>12 (19%)</b> ↓ 50%
<b>Výsledné riziko:</b>	<b>4</b>		<b>3</b>		<b>2</b>		<b>24 (38%)</b>

Aplikované	ID	Název	Štítky	Hodnota snížení hrozby	Hodnota snížení zranitelnosti
		<input type="text" value="vyberte"/>	<a href="#">← vyberte opatření či napište nové</a>		
	a1OG1	Revize smluvních vztahů s dodavatelem IS		<input type="text" value="0"/>	<input type="text" value="2"/>  

Zavřít

Uložit

# Prezentace výsledných rizik

označené položky:

[exportovat](#) [stáhnout karty rizik](#)

Aktivum	Druh	Garant	Druh hrozby	Druh zranitelnosti	Dopad	Hrozba	Zranitelnost	Riziko	Cílené riziko	Výsledné riziko	Akceptováno
	vyberte	vyberte			vyberte	vyberte	vyberte	vyberte	vyberte	vyberte	-
Service desk	Podpůrné		Chybné fungování aplikačního programového vybavení	Nejasné nebo neúplné zadání pro vývojáře	3/Vysoký / 3	4/Kritická / 4	4/Kritická / 4	Vysoké / 48 (75%)	Vysoké / 48 (75%)	Vysoké / 48 (75%)	<input type="checkbox"/> ne
Zaměstnanci	Podpůrné	Alena Šuhajová	Zdravotní stav	Covid-19	3/Vysoký / 3	4/Kritická / 4	4/Kritická / 4	Vysoké / 48 (75%)	Vysoké / 48 (75%)	Vysoké / 48 (75%)	<input type="checkbox"/> ne
Service desk	Podpůrné		Zneužití oprávnění	Znamé chyby v programech	3/Vysoký / 3	4/Kritická / 4	4/Kritická / 4	Vysoké / 48 (75%)	Vysoké / 48 (75%)	Vysoké / 48 (75%)	<input type="checkbox"/> ne
IT systém	Podpůrné	Tomáš Dobrovolný	Falšování práv	Nechráněné tabulky s hesly	3/Vysoký / 3	4/Kritická / 4	3/Vysoká / 3	Vysoké / 36 (56%)	Vysoké / 36 (56%)	Vysoké / 36 (56%)	<input type="checkbox"/> ne
Dodávky nepřerušitelného napájení el. napájení	Podpůrné	Ondřej Chrást	Narušení fyzické bezpečnosti	Nedostatečná ochrana aktiv	4/Kritický / 4	3/Vysoká / 3	3/Vysoká / 3	Vysoké / 36 (56%)	Vysoké / 36 (56%)	Vysoké / 36 (56%)	<input type="checkbox"/> ne IA
Dodávky nepřerušitelného napájení el. napájení	Podpůrné	Ondřej Chrást	Pochybení ze strany zaměstnanců	Nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů	4/Kritický / 4	3/Vysoká / 3	3/Vysoká / 3	Vysoké / 36 (56%)	Vysoké / 36 (56%)	Vysoké / 36 (56%)	<input type="checkbox"/> ne IA

§ 5 Řízení rizik



# Prezentace výsledných rizik

Aktiva s nejvyšší hodnotou rizika      Rizika

Aktivum	Druh	Garant	Nejvyšší riziko	
<input type="text"/>	vyberte	vyberte	vyberte	
Service desk	Podpůrné		Vysoké / 48 (75%)	▼
Zaměstnanci	Podpůrné	Alena Šuhajová	Vysoké / 48 (75%)	▼
Dodávky nepřerušitelného napájení el. napájení	Podpůrné	Ondřej Chrást	Vysoké / 36 (56%)	▼
IT systém	Podpůrné	Tomáš Dobrovolný	Vysoké / 36 (56%)	▼
Interní procesy	Podpůrné	Lucie Juříčková	Vysoké / 32 (50%) ▲	▼
Zákazníci	Primární	Jakub Skalický	Vysoké / 27 (42%) ▲	▼
Žádosti o přípojky	Primární	Jaroslav Handlíř	Vysoké / 27 (42%)	▼
Osobní údaje zákazníků	Podpůrné	Tomáš Dobrovolný	Vysoké / 24 (38%) ▲	▼
Prostory ICT (Servovna)	Podpůrné	František Janů	Vysoké / 24 (38%) ▲	▼
Měření spotřeby dodávaných energií	Primární	Tomáš Dobrovolný	Vysoké / 24 (38%)	▼

( Položek: 1 - 10 z 81 )

« předchozí 1 2 3 4 5 ... 7 ... 9 následující »

10 ▼

§ 5 Řízení rizik

# Plány kontinuity

### Editace plánu kontinuity

Obecné   Aktiva   Analytický tým   Výkonný tým   Řídicí tým   Proces   Přílohy

Výpadek dodávky elektrické energie ID PK001

**Popis**

**B** *I* := :=

Lorem ipsum dolor sit amet, consectetur adipiscing elit. Aenean placerat. Duis pulvinar. Aliquam erat volutpat. Aenean vel massa quis mauris vehicula lacinia. Sed vel lectus. Donec odio tempus molestie, porttitor ut, laculis quis, sem. Praesent id justo in neque elementum ultrices. Integer malesuada. Nunc auctor. Integer in sapien. Nunc tincidunt ante vitae massa.

**Štítky**

vyberte

Zrušit   [Následující krok >](#)   [Uložit](#)

§ 15 Řízení kontinuity činností

# Plnění legislativních povinností

3.2 Řízení aktiv (VoKB §4) 20 / 20

✓ − × ! 100%

**Povinná osoba v rámci řízení aktiv**  
odst. 1

<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	stanoví metodiku pro identifikaci aktiv, <small>písm. a)</small>	KOI, ISZE, VIS, DSP opatření
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	stanoví metodiku pro hodnocení aktiv alespoň v rozsahu uvedeném v příloze č. 1 k této vyhlášce, <small>písm. a)</small>	KOI, ISZE, VIS, DSP opatření
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	identifikuje a eviduje aktiva, <small>písm. c)</small>	KOI, ISZE, VIS, DSP opatření
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	určí a eviduje garanty aktiv, <small>písm. d)</small>	KOI, ISZE, VIS, DSP opatření
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	hodnotí a eviduje primární aktiva z hlediska důvěrnosti, integrity a dostupnosti a zařadí je do jednotlivých úrovní podle písmene b), <small>písm. e)</small>	KOI, ISZE, VIS, DSP opatření
<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>	určí a eviduje vazby mezi primárními a podpůrnými aktivy a hodnotí důsledky závislosti mezi primárními a podpůrnými aktivy, <small>písm. f)</small>	KOI, ISZE, VIS, DSP opatření

# Hodnocení dodavatelů

CECH s.r.o. Hodnocení dodavatele CECH s.r.o.

---

**Město:**

**Ulice a číslo:** Polníčka 309

**IČ:** 27680703

**DIČ:** CZ27680703

**Oznámení o významném dodavateli:**  Ano

**Přílohy** [← Zpět](#) [+ Přidat](#)

(Zatím nemáte vložené žádné přílohy)

---

**Serverovna (služby provozu IT)** Dodavatel aktivní











Hodnocení Kontaktní osoby Přílohy

Otázka	Odpověď
Přistupuje dodavatel ke kritickým aktivům nebo službám?	ano
Má vliv výpadek na potřebu mít zajištěnou službu dodavatele?	ne
Ovlivňuje dodavatel kvalitu a dostupnost klíčových služeb?	ne
Má dodavatel přístup k citlivým informacím?	ne
Má dodavatel vliv na bezpečnost IS?	ano
Nacházejí se citlivé informace v držení dodavatele?	ne
Datum odeslání vyznění	14.4.2020

[Upravit](#)

§ 8 Řízení dodavatelů

# Auditní log

20210505 05/05/21			
Filtr položky		Filtr uživatele	
5. 5. 2021 13:46		Aktualizována <b>Odpověď v auditu KB</b> Orgány a osoby uvedené v § 3 písm. c) až g), které jsou orgány veřejné moci, jsou povinny si ve smlouvě s poskytovatelem služeb cloud computingu zejména zajistit, že budou dodržována bezpečnostní pravidla pro poskytování služeb cloud computingu stanovená Úřadem, a že budou mít na základě své žádosti bez zbytečného odkladu k dispozici informace a data, která pro ně poskytovatel služeb cloud computingu uchovává včetně možnosti kontroly uchovávaných informací a dat v reálném čase. uživatelem <b>František Janů</b>	
5. 5. 2021 13:46		Aktualizována <b>Odpověď v auditu KB</b> Orgány a osoby uvedené v § 3 písm. c) až g), které jsou orgány veřejné moci, jsou povinny si ve smlouvě s poskytovatelem služeb cloud computingu zejména zajistit, že budou dodržována bezpečnostní pravidla pro poskytování služeb cloud computingu stanovená Úřadem, a že budou mít na základě své žádosti bez zbytečného odkladu k dispozici informace a data, která pro ně poskytovatel služeb cloud computingu uchovává včetně možnosti kontroly uchovávaných informací a dat v reálném čase. uživatelem <b>František Janů</b>	
5. 5. 2021 13:38		Vytvořeno <b>Opatření rizika</b> Definice a vypracování popisu interních postupů (IT systém) uživatelem <b>František Janů</b>	
5. 5. 2021 13:38		Aktualizováno <b>Riziko</b> IT systém / Nechráněné komunikační linky / Cílený kybernetický útok pomocí sociálního inženýrství, použití špiónážních technik uživatelem <b>František Janů</b>	
5. 5. 2021 13:38		Aktualizováno <b>Riziko</b> IT systém / Nechráněné komunikační linky / Cílený kybernetický útok pomocí sociálního inženýrství, použití špiónážních technik uživatelem <b>František Janů</b>	



**Děkuji za pozornost.**

František Janů

frantisek\_janu@gordic.cz

+420 773 049 126

[www.gordic.cz](http://www.gordic.cz)