Česká zemědělská univerzita v Praze

Provozně ekonomická fakulta

Katedra informačních technologií

Diplomová práce

Analýza bezpečnostních rizik v rámci ICT

Bc. Matěj Král

ČESKÁ ZEMĚDĚLSKÁ UNIVERZITA V PRAZE

Provozně ekonomická fakulta

ZADÁNÍ DIPLOMOVÉ PRÁCE

Bc. Matěj Král

Informatika

Název práce

Analýza bezpečnostních rizik v rámci ICT

Název anglicky

Security risk analysis within ICT

Cíle práce

Cílem diplomové práce je na základě analýzy zhodnotit techniky a účinnosti bezpečnostních procedur v ICT a navržení vhodných řešení k implementaci.
Dílčím cílem je analýza současného stavu bezpečnosti ICT, dále klasifikace trendů v analýze bezpečnostních rizik a řešení incidentů, a také zhodnocení významu bezpečnosti ICT v rámci celkové strategie podniků.

Metodika

Teoretická východiska jsou založena na studiu odborných článků a vědecké literatury z oblasti ICT. Na základě těchto východisek bude zpracována analytická část práce včetně komparace vhodných bezpečnostních strategií.

Doporučený rozsah práce

Bezpečnost ICT – zaměření na risc management a incident management

Klíčová slova

ICT, bezpečnost IS, risk management, incident management, information security management, ISM, ochrana dat

---

Doporučené zdroje informací

BERNARD, Ray. Security technology convergence insights. Waltham, MA: Elsevier, 2015. ISBN 978-012-8028-421.

EDITED BY JOHN R. VACCA. Managing information security. 2nd ed. Burlington: Elsevier Science, 2014. ISBN 978-012-4166-943.

KOHNKE, Anne, Kenneth SIGLER a Dan SHOEMAKER. Implementing cybersecurity: a guide to the National Institute of Standards and Technology Risk Management Framework. Boca Raton, FL: CRC Press, 2017. ISBN 978-149-8785-143.

KUROSE, J F. – ROSS, K W. *Počítačové sítě.* Brno: Computer Press, 2014. ISBN 978-80-251-3825-0.

Předběžný termín obhajoby

2018/19 LS – PEF

Vedoucí práce

Ing. Alexandr Vasilenko, Ph.D.

Garantující pracoviště

Katedra informačních technologií

Elektronicky schváleno dne 11. 9. 2018

Ing. Jiří Vaněk, Ph.D.

Vedoucí katedry

Elektronicky schváleno dne 19. 10. 2018

Ing. Martin Pelikán, Ph.D.

Děkan

V Praze dne 28. 03. 2019

Čestné prohlášení

Prohlašuji, že svou diplomovou práci „Analýza bezpečnostních rizik v rámci ICT“ jsem vypracoval samostatně pod vedením vedoucího diplomové práce a s použitím odborné literatury a dalších informačních zdrojů, které jsou citovány v práci a uvedeny v seznamu literatury na konci práce. Jako autor uvedené diplomové práce dále prohlašuji, že jsem v souvislosti s jejím vytvořením neporušil autorská práva třetích osob.

V Praze dne 28. března 2019 _____

Poděkování

Rád bych poděkoval vedoucímu své práce panu Ing. Alexandru Vasilenkovi, PhD, za vedení diplomové práce a podnětné rady během konzultací.

Analýza bezpečnostních rizik v rámci ICT

Security risk analysis within ICT

Souhrn

Diplomová práce pojednává o bezpečnostních rizicích v rámci ICT s důrazem na aktuální trendy v oblasti cloud computingu. Cílem diplomové práce je analýza stávajících norem, metodik a standardů v oblasti IT bezpečnosti s důrazem na abstrakci aktuálních trendů týkajících se cloud computingu a následný návrh vhodných pokynů a postupů pro jejich řešení v rámci IT bezpečnosti organizace.

Výsledné doporučené postupy pro řízení daných trendů kombinují silné stránky jednotlivých analyzovaných metodik a jsou využitelné při řízení rizik v rámci implementace cloud computingu v organizaci.

Klíčová slova: ICT, bezpečnost IS, risk management, incident management, information security management, ISM, ochrana dat, cloud computing, rizika cloud computingu

Summary

The diploma thesis deals security risks within ICT with emphasis on current trends in cloud computing. The aim of this thesis is to analyze existing standards and methodologies in the field of IT security with emphasis on abstraction of current trends related to cloud computing and the subsequent design of appropriate guidelines and procedures for their solution within the organization's IT security.

The resulting best practices guidelines for management of the trends combine the strengths of individual analyzed methodologies and are useful in risk management within cloud computing implementation in organization.

Keywords: ICT, IS security, risk management, incident management, information security management, ISM, data protection, cloud computing, cloud computing risks

Obsah

Seznam obrázků

Seznam tabulek

1 Úvod

Bezpečnostní rizika jsou přirozenou součástí každého aspektu informačních a komunikačních technologií a jejich identifikace, analýza a řízení je podstatným prvkem procesu řízení IT bezpečnosti v organizaci. Vhodně zvolené postupy pro řízení rizik mohou předcházet bezpečnostním incidentům a ušetřit organizacím nemalé náklady související s nápravou jejich dopadů.

Organizace hledají inovativní způsoby, jak ušetřit finanční prostředky a zároveň zvýšit hodnotu a užitečnost svých informačních systémů, a jedním z velkých trendů v oblasti informačních a komunikačních technologií je cloud computing. Využití služeb cloud computingu může představovat vhodnou platformu, která nabízí organizacím potenciálně méně nákladný model pro řešení jejich výpočetních potřeb a plnění obchodních cílů. I přes nesporné výhody cloud computingu spočívající ve zjednodušení IT procesů v organizaci však cloud computing představuje také zdroj nových rizik, se kterými se musí organizace potýkat. Vzhledem k tomu, že obliba a využití služeb cloud computing stále roste, je důležité, aby organizace správně chápaly výhody, nevýhody i rizika cloud computingu a dokázali jim správně porozumět.

V rámci této práce jsou představeny základní principy IT bezpečnosti a řízení rizik, které se uplatňují i v případě cloud computingu. Na tyto principy navazuje vymezení aktuálních trendů týkajících se bezpečnostních rizik plynoucích z implementace a využívání cloudových služeb a následně jsou analyzovány aktuální normy a metodiky z oblasti IT managementu, jejichž principy lze uplatnit i při řízení rizik cloud computingu. V závěru práce jsou navrženy doporučené postupy kombinující analyzované normy a metodiky pro řízení rizik daných trendů v rámci implementace služeb cloud computingu v organizaci.

2 Cíl a metodika

Cílem diplomové práce je analýza stávajících norem, metodik a standardů v oblasti IT bezpečnosti s důrazem na abstrakci aktuálních trendů týkajících se cloud computingu. Na základě analýzy současného stavu metodik jsou navržena zlepšující opatření, která pokrývají dané trendy z pohledu zaměření jednotlivých metodik. Dílčími cíli práce jsou:

- Vymezení IT bezpečnosti a kybernetické bezpečnosti v rámci organizace,
- určení principů IT bezpečnosti,
- shrnutí metod a postupů týkajících se řízení IT rizik,
- vymezení aktuálních trendů cloud computingu.

Diplomová práce je rozdělena do tří částí – teoretická východiska, analytická část a zhodnocení výsledků, které se dále dělí na jednotlivé kapitoly a podkapitoly.

Úvodní část *teoretická východiska* se zabývá vymezením IT bezpečnosti a kybernetické bezpečnosti z pohledu řízení organizace, dále jsou určeny principy IT bezpečnosti a vymezeny základní pojmy z oblasti řízení IT rizik a také shrnuty metody pro řízení rizik.

V analytické části je stručně představen cloud computing a jsou vymezeny jeho aktuální trendy týkající se řízení rizik v rámci organizace. Dále jsou analyzovány stávající normy a metodiky upravující IT bezpečnost s ohledem na vymezené trendy a je zhodnoceno jejich pokrytí daných trendů.

V závěrečné části jsou na základě syntézy norem a metodik z pohledu jejich zaměření vůči daným trendům uvedeny konkrétní pokyny pro řízení rizik těchto trendů cloud computingu v rámci IT bezpečnosti organizace.

3 Teoretická východiska

Teoretická část práce se zabývá bezpečností podniku z pohledu ICT a definicí a řízení rizik souvisejících s ICT. Dále se zabývá problematikou konkrétních oblastí ICT rizik v souvislosti se stávajícími normami a mezinárodními standardy.

3.1 Podniková bezpečnost

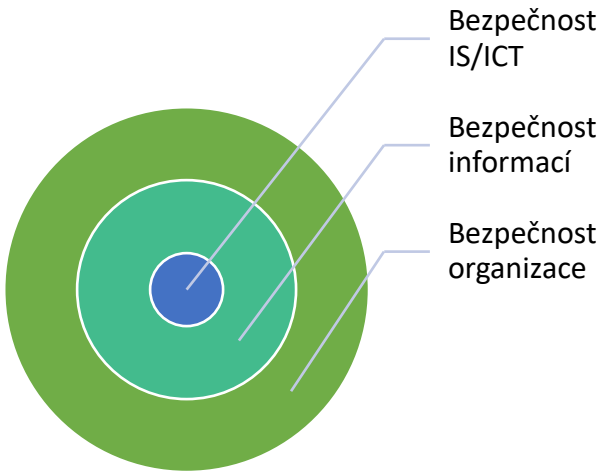
Oblasti bezpečnosti týkající se IT prostředí spolu vzájemně souvisejí a překrývají se spolu s dalšími oblastmi bezpečnosti podniku.

Nejvyšší oblastí je bezpečnost organizace. Její součástí je zajištění bezpečnosti objektů a majetku pomocí ostrahy přístupů do objektu, strážní služby apod, přičemž některé její činnosti napomáhají zároveň i zajištění bezpečnosti IT (např. kontrola oprávnění fyzického přístupu do objektu).

Další oblastí je bezpečnost informací, jejímž cílem a úkolem je shrnout v sobě zásady bezpečné práce s informacemi všeho druhu a všech typů – tedy nejen s informacemi v digitální formě. Bezpečnost informací zahrnuje navíc oproti bezpečnosti IT např. i způsob zpracování dat, jejich uložení a správy archivu nedigitálních dat, zásady poskytování informacím veřejnosti a novinářům a také zásady vystupování pracovníků v médiích apod.

Bezpečnost IS/ICT má za úkol chránit prostředky, která jsou součástí informačního systému podniku, podporovaného informačními a komunikačními technologiemi. (Doucek, 2011, str. 55)

Obrázek 1: Vztah úrovní bezpečnosti v organizaci



Zdroj: vlastní zpracování dle Doucka (2011, str. 56)

Obecně má podniková bezpečnost za úkol chránit hodnotné části podniku, tj. aktiva. Svatá (2016, str. 103) definuje aktivum jako něco, co má hodnotu (měřitelnou nebo neměřitelnou), kterou je potřeba chránit, včetně lidí, infrastruktury, informací, financí a pověsti. Zjednodušeně lze jako aktiva označit cokoli, co má nějakou cenu pro osobu, organizaci či stát. Aktiva lze rozdělit následovně (Kolouch, Bašta, 2019, str. 72):

- Primární – informace nebo služba, kterou zpracovává či poskytuje informační systém.
- Podpůrná – technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému.

V oblasti IT a informačních systémů lze na aktiva nahlížet také z pohledu jejich povahy a vlastností (Doucek, 2011, str. 57):

- Hmotná aktiva – především technické prostředky IT, tj. počítače, síťové prvky, kabelové rozvody a ostatní technická zařízení.
- Nehmotná aktiva.
    - Pracovní postupy využívané v podniku v oblasti ICT.
    - Data – podnikem vytvořené nebo převzaté datové soubory.
    - Programové vybavení – operační systémy počítačů, programové vybavení, kryptografické systémy aj.
    - Služby – počítačové a komunikační služby, základní služby (zajištění provozu např. světlem, topením, klimatizací aj.).

3.2 Kybernetická bezpečnost

Kybernetická bezpečnost představuje podmnožinu samotné bezpečnosti. Její definice však není vzhledem k aktuálnímu vývoji této problematiky ustálená, proto lze nalézt různé definice vztahující se ke konkrétním zájmovým skupinám nebo oblastem. Souhrnné definice kybernetické bezpečnosti jsou také uváděny v právních normách jí se zabývajících, např. směrnice Evropského parlamentu a Rady (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii v čl.4 odst. 2 uvádí definici kybernetické bezpečnosti následovně:

„bezpečností sítí a informačních systémů se rozumí jako schopnost sítí a informačních systémů odolávat s určitou spolehlivostí veškerým zásahům, které narušují dostupnost, autenticitu, integritu nebo důvěrnost uchovávaných, předávaných nebo zpracovávaných dat nebo souvisejících služeb, které tyto sítě a informační systémy nabízejí nebo které jsou jejich prostřednictvím přístupné“.

Kolouch a Bašta (2019, s. 44) na základě těchto i dalších právních norem a jiných definic vymezují kybernetickou bezpečnost následovně:

„Souhrn právních, organizačních, technických a vzdělávacích prostředků, které směřují k zajištění ochrany počítačových systémů a dalších prvků ICT, aplikací, dat a uživatelů“

„Schopnost počítačových systémů a využívaných služeb reagovat na kybernetické hrozby či útoky a jejich následky, jakož i plánování obnovy funkčnosti počítačových systémů a služeb s nimi spojených.“

Dále uvádí, že kybernetická bezpečnost je realizována jak v rámci kyberprostoru, tak mimo něj, a proto není vhodné aplikaci výše uvedených prostředků a principů jakkoliv geolokačně omezovat.

3.2.1 Principy kybernetické bezpečnosti

Smyslem kybernetické bezpečnosti je nejen zajištění bezpečnosti ICT, ale také zajištění bezpečnosti dat a informací, které jsou těmito prvky zpracovávány, přenášeny a uchovávány. Bezpečností informací se tedy rozumí ochrana důvěrnosti, integrity a dostupnosti informací (Doucek, 2011, s. 55).

Při uplatňování kybernetické bezpečnosti se implementují principy zvané triády, z nichž nejpoužívanější je triáda CIA (Kolouch a Bašta, 2019, s. 45):

1. confidentiality („důvěrnost“),
2. integrity („celistvost“),
3. availability („dostupnost“).

Důvěrností se rozumí skutečnost, že k informacím, datům, či k ICT mají přístup pouze subjekty, které jsou k tomu oprávněné. Pro snazší orientaci v množství dat a informací

je vhodné v praxi aplikovat klasifikaci dat. Bezpečnostní standardy ISO/IEC 27000 definují klasifikaci následovně (2013, str. 15):

„Informace mají být klasifikovány v souladu s jejich právními požadavky, hodnotou, kritičností a citlivosti neoprávněnému zneužití nebo modifikaci.“

„Pro značení informací a zacházení s nimi by měly být vytvořeny a do praxe zavedeny postupy, které jsou v souladu s klasifikačním schématem přijatým organizací.“

Na základě těchto norem je tedy vhodné zavést pro klasifikaci dat a informací standardizované schéma, příkladem může být např. Klasifikace informací dle zákona 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti:

a) přísně tajné,
b) tajné,
c) důvěrné,
d) vyhrazené.

Kolouch a Bašta (2019, s. 49) na základě tohoto schématu uvádějí klasifikaci užívanou v komerční sféře:

- Chráněné – neoprávněné nakládání s informacemi by mohlo způsobit závažné poškození či zničení organizace (např. únik strategických informací, zdrojových kódů, schémat zabezpečení, hesel aj.).
- Interní – neoprávněné nakládání s informacemi by mohlo způsobit poškození organizace (např. únik osobních údajů, smluv aj.).
- Citlivé – neoprávněné nakládání s informacemi by mohlo mít negativní dopad na společnost (např. dosud nezveřejněné informace o projektech, plánovaných akcích aj.).
- Veřejné – neoprávněné nakládání s informacemi by nemělo nikoho poškodit a nemělo by mít jakýkoliv dopad na společnost (např. veřejně dostupné kontakty, prezentace projektů aj.).

Integrita představuje znemožnění zásahu do informací, dat, počítačových systémů, jejich nastavení apod. jinou osobou, než tou, která je k takovému úkonu oprávněna. Zároveň integrita představuje jakousi záruku neporušenosti systému, informací či dat (Kolouch a Bašta. 2019, s. 53).

Vyhláška o kybernetické bezpečnosti v příloze č. 1 uvádí stupnici pro hodnocení integrity aktiv:

Tabulka 1: Hodnocení integrity aktiv

Úroveň	**Popis**	**Příklady požadavků na ochranu aktiva**
Nízká	Aktivum nevyžaduje ochranu z hlediska integrity. Narušení integrity aktiva neohrožuje oprávněné zájmy povinné osoby.	Není vyžadována žádná ochrana.
Střední	Aktivum může vyžadovat ochranu z hlediska integrity. Narušení integrity aktiva může vést k poškození oprávněných zájmů povinné osoby a může se projevit méně závažnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány standardní nástroje (například omezení přístupových práv pro zápis).
Vysoká	Aktivum vyžaduje ochranu z hlediska integrity. Narušení integrity aktiva vede k poškození oprávněných zájmů povinné osoby s podstatnými dopady na primární aktiva.	Pro ochranu integrity jsou využívány speciální prostředky, které dovolují sledovat historii provedených změn a zaznamenat identitu osoby provádějící změnu. Ochrana integrity informací přenášených komunikačními sítěmi je zajištěna pomocí kryptografických prostředků.
Kritická	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.	Pro ochranu integrity jsou využívány speciální prostředky jednoznačné identifikace osoby provádějící změnu (například pomocí technologie digitálního podpisu).

Zdroj: Vyhláška č. 82/2018 Sb., příloha 1

Dostupnost je definována jako garance možnosti přístupu k informacím, datům, nebo k počítačovému systému v okamžiku potřeby (Kolouch a Bašta. 2019, s. 53).

Vyhláška o kybernetické bezpečnosti v příloze č. 1 uvádí stupnici pro hodnocení dostupnosti aktiv:

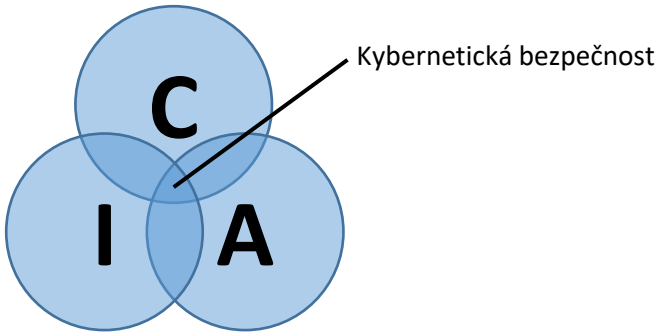
Tabulka 2: Hodnocení dostupnosti aktiv

Úroveň	Popis	Příklady požadavků na ochranu aktiva
Nízká	Narušení dostupnosti aktiva není důležité a v případě výpadku je běžně tolerováno delší časové období pro nápravu (cca do 1 týdne).	Pro ochranu dostupnosti je postačující pravidelné zálohování.
Střední	Narušení dostupnosti aktiva by nemělo překročit dobu pracovního dne, dlouhodobější výpadek vede k možnému ohrožení oprávněných zájmů povinné osoby.	Pro ochranu dostupnosti jsou využívány běžné metody zálohování a obnovy.
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.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb může být podmíněna zásahy obsluhy nebo výměnou technických aktiv.
Kritická	Narušení dostupnosti aktiva není přípustné a i krátkodobá nedostupnost (v řádu několika minut) vede k vážnému ohrožení oprávněných zájmů povinné osoby. Aktiva jsou považována za kritická.	Pro ochranu dostupnosti jsou využívány záložní systémy a obnova poskytování služeb je krátkodobá a automatizovaná.

Zdroj: Vyhláška č. 82/2018 Sb., příloha 1

Kolouch a Bašta (2019, str. 55) v grafickém znázornění triády zobrazují kybernetickou bezpečnost jako průnik jednotlivých oblastí této triády:

Obrázek 2: Triáda CIA



Zdroj: vlastní zpracování dle Koloucha a Bašty (2019, str. 56)

Kolouch a Bašta (2019, s. 45) dále uvádí, že tato základní triáda je již nedostačující k udržení adekvátní úrovně kybernetické bezpečnosti, a proto poukazují na uplatňování Parkerian hexad, což je triáda CIA doplněná o další tři prvky:

4. possesion/Control („držení či kontrola“),
5. authenticity („autentičnost“),
6. utility („užitečnost“).

Obrázek 3: Zobrazení Parkerian hexad

Zdroj: vlastní zpracování dle Koloucha a Bašty (2019, str. 56)

3.3 Řízení rizik v oblasti IT

Řízení rizik je klíčovým nástrojem pro systematické řízení kybernetické bezpečnosti a bezpečnosti informací. Přesná znalost skutečných rizik rozhoduje o výběru a prosazení vhodných bezpečnostních opatření schopných snížit negativní dopady těchto rizik (Doucek, 2011, s. 90).

3.3.1 Základní pojmy řízení rizik

V oblasti řízení rizik jsou definovány základní pojmy, které se vyskytují v normách, vyhláškách i odborné literatuře.

Riziko

Původ slova „riziko“ pochází z terminologie obchodních lodních plaveb ze 17. století, kdy slovo „ris(i)co“ znamenalo „úskalí, které má být obepluto“. Později se toto označení uplatnilo v pojišťovací branži a následně rozšířilo i do dalších oblastí a činností (Svatá, 2016, s. 103).

Norma ISO/IEC 27000 (2018, str. 8) definuje riziko v kontextu s informačními systémy následovně:

„Rizika informační bezpečnosti souvisí s potenciálem, že hrozby využijí zranitelnost informačních aktiv nebo skupiny informačních prostředků a tím poškodí organizaci.“

Obecně lze riziko označit za pojem, který vyjadřuje pravděpodobnost, s jakou může nastat nechtěná událost (Kolouch a Bašta, 2019, s. 68).

Hrozba

Hrozbou je chápána potenciální příčina nechtěného incidentu, jehož výsledkem může být poškození systému nebo organizace. Hrozby týkající se kybernetické bezpečnosti lze rozdělit následovně (Doucek, 2011, s. 57):

- Přírodní a fyzické – živelné pohromy a nehody (poruchy v dodávce elektrického proudu, požáry, povodně aj.),
- technické a technologické – poruchy počítačů, sítí, komponent ICT, poruchy programů aj.,
- lidské,

- neúmyslné – hrozby vyplývající z nedbalosti či neznalosti uživatelů,
- úmyslné,
  - vnější – hackeři, průmyslová špionáž aj.,
  - vnitřní – zaměstnanci, hosté aj.

Hrozby týkající se přímo informačních aktiv lze vymezit následovně (Kolouch a Bašta, 2019, s. 75):

- Únik informace – vyzrazení chráněné informace neautorizovanému subjektu.
- Narušení integrity – poškození, změna, či vymazání dat.
- Potlačení služby – úmyslné bránění v přístupu k informacím, aplikacím, či systému.
- Nelegitimní použití – užití informací neautorizovaným subjektem či neoprávněným způsobem.

Vyhláška o kybernetické bezpečnosti v příloze č. 3 uvádí konkrétní příklady hrozeb:

1) porušení bezpečnostní politiky, provedení neoprávněných činností, zneužití oprávnění ze strany uživatelů a administrátorů,
2) poškození nebo selhání technického anebo programového vybavení,
3) zneužití identity,
4) užívání programového vybavení v rozporu s licenčními podmínkami,
5) škodlivý kód (například viry, spyware, trojské koně),
6) narušení fyzické bezpečnosti,
7) přerušení poskytování služeb elektronických komunikací nebo dodávek elektrické energie,
8) zneužití nebo neoprávněná modifikace údajů,
9) ztráta, odcizení nebo poškození aktiva,
10) nedodržení smluvního závazku ze strany dodavatele,
11) pochybení ze strany zaměstnanců,
12) zneužití vnitřních prostředků, sabotáž,
13) dlouhodobé přerušení poskytování služeb elektronických komunikací, dodávky elektrické energie nebo jiných důležitých služeb,
14) nedostatek zaměstnanců s potřebnou odbornou úrovní,

15) cílený kybernetický útok pomocí sociálního inženýrství, použití špionážních technik,
16) zneužití vyměnitelných technických nosičů dat,
17) napadení elektronické komunikace (odposlech, modifikace).

Událost

V oblasti ICT bezpečnosti představuje událost identifikovatelný stav, který může způsobit narušení bezpečnosti informací nebo narušení bezpečnosti služeb.

Jedná se o událost bez zatím reálného negativního následku pro daný komunikační nebo informační systém, tj. jedná se o hrozbu, která však nemusí být reálná (Kolouch a Bašta, 2019, s. 80).

Incident

Za incident je považována jedna nebo série nechtěných nebo nečekaných událostí, u kterých je významná pravděpodobnost, že ohrozí činnost organizace nebo bezpečnost informací (Svatá, 2016, s. 104).

Incident může být způsoben jak úmyslným, tak nedbalostním jednáním člověka, ale i vyšší moci. Za určitou část kybernetických bezpečnostních incidentů jsou zodpovědné i náhodné jevy, chyby hardwaru, softwaru, chyby učiněné při konfiguraci administrátory, chyby uživatelů aj. (Kolouch a Bašta, 2019, s. 82).

Zranitelnost

Zranitelnost představuje slabé místo aktiva nebo bezpečnostního opatření, které může být zneužito jednou nebo více hrozbami.

V oblasti kybernetické bezpečnosti rozdělují Kolouch a Bašta (2019, s. 72) zranitelnosti následovně:

- Zranitelnosti známé (publikované),
    - opravené (ošetřené),
    - neopravené (neošetřené),
- zranitelnosti neznámé,
    - skryté,
    - neobjevené.

V případě neznámých zranitelností je významné, zda jsou objeveny útočníkem, výrobcem, bezpečnostním analytikem, osobou zabývající se penetračním testováním či uživatelem. Stejně tak je významná motivace osoby, která danou zranitelnost objeví.

Vyhláška o kybernetické bezpečnosti v příloze č. 3 uvádí konkrétní příklady zranitelností:

1) nedostatečná údržba informačního a komunikačního systému,
2) zastaralost informačního a komunikačního systému,
3) nedostatečná ochrana vnějšího perimetru,
4) nedostatečné bezpečnostní povědomí uživatelů a administrátorů,
5) nedostatečná údržba informačního a komunikačního systému,
6) nevhodné nastavení přístupových oprávnění,
7) nedostatečné postupy při identifikování a odhalení negativních bezpečnostních jevů, kybernetických bezpečnostních událostí a kybernetických bezpečnostních incidentů,
8) nedostatečné monitorování činnosti uživatelů a administrátorů a neschopnost odhalit jejich nevhodné nebo závadné způsoby chování,
9) nedostatečné stanovení bezpečnostních pravidel, nepřesné nebo nejednoznačné vymezení práv a povinností uživatelů, administrátorů a bezpečnostních rolí,
10) nedostatečná ochrana aktiv,
11) nevhodná bezpečnostní architektura,
12) nedostatečná míra nezávislé kontroly,
13) neschopnost včasného odhalení pochybení ze strany zaměstnanců.

Útok

Jirásek a kol. (2013, s. 59) definují kybernetický útok jako:

„Útok na IT infrastrukturu za účelem způsobit poškození a získat citlivé či strategicky důležité informace. Používá se nejčastěji v kontextu politicky či vojensky motivovaných útoků.“

Kolouch a Bašta (2019, s. 82) dále uvádějí, že rozdíl mezi kybernetickým bezpečnostním incidentem a kybernetickým útokem primárně spočívá v zavinění.

Bezpečnostní incident může být způsoben jak úmyslným, tak nedbalostním jednáním člověka, případně vyšší mocí, u kybernetického útoku jde však o úmyslné jednání člověka.

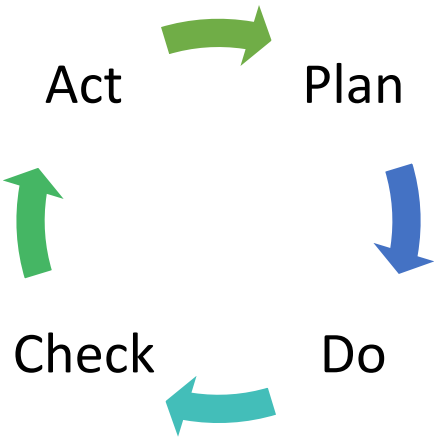
Kybernetický útok lze také definovat jako jednání útočníka či skupiny útočníků, které využívá informační a komunikační technologie k útoku na jinou informační a komunikační infrastrukturu, ať už s cílem narušit dostupnost, důvěrnost nebo integritu dat.

3.3.2 Systém řízení bezpečnosti informací

Systém řízení bezpečnosti informací neboli ISMS z anglického výrazu Information Security Management System, je soubor pravidel, jejichž cílem je zachovat důvěrnost, integritu a dostupnost informací aplikováním procesu řízení rizik (Kolouch a Bašta, 2019, s. 253). Jedná se o efektivní a dokumentovaný systém řízení a správy informačních aktiv s cílem eliminovat jejich možnou ztrátu nebo poškození tím, že jsou určena aktiva, která se mají chránit, jsou zvolena a řízena možná rizika bezpečnosti informací, jsou zavedena opatření s požadovanou úrovní záruk a ta jsou kontrolována (Svatá, 2016, s. 40).

ISMS je součástí procesů a celkového systému řízení organizace a je do těchto systémů integrován, proto je podobně jako ostatní systémy řízení založen na modelu PDCA, tedy Plan – Do – Check – Act (Plánuj – Dělej – Kontroluj – Jednej). PDCA cyklus je jedním ze základních manažerských principů spočívající v postupném zlepšování kvality procesů, služeb, dat, výrobků aj. díky neustálému opakování jeho čtyř základních činností (Kolouch a Bašta, 2019, s. 255):

Obrázek 4: Model PDCA

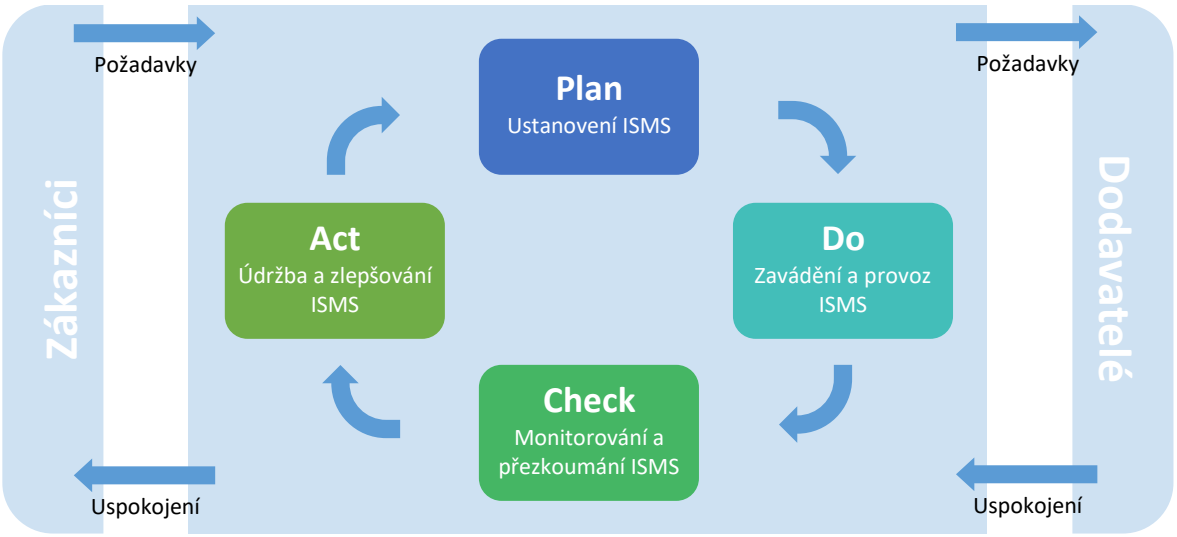


Zdroj: vlastní zpracování dle Koloucha a Bašty (2019, str. 256)

V případě aplikování modelu PDCA na ISMS jsou definovány čtyři etapy procesu následovně (Doucek, 2011, s. 85):

- P – Ustanovení ISMS,
- D – Zavádění a provoz ISMS,
- C – Monitorování a přezkoumání ISMS,
- A – Údržba a zlepšování ISMS.

Obrázek 5: Model PDCA aplikovaný na procesy ISMS



Zdroj: vlastní zpracování dle Doucka (2011, str. 86)

Ustanovení ISMS je snahou o správné naplánování. Počátkem je určení rozsahu řízení a stanovení základního rámce řízení bezpečnosti informací pomocí politiky ISMS. Plánování pokračuje identifikací a ohodnocením rizikových scénářů, které vede k výběru vhodných bezpečnostních opatření.

Při **zavádění a provozu ISMS** se stanovují dílčí, roční plány na zvládání rizik, definují se dlouhodobě platná bezpečnostní pravidla včetně vysvětlení těchto pravidel všem účastníkům a sleduje se účinnost, s jakou je bezpečnost prosazována.

Monitorování a přezkoumání ISMS spočívá ve zpětné vazbě, která má základ v pravidelné kontrole pověřených osob. Součástí této etapy jsou také interní audity ISMS a další kontrolní testy. Všechny získané poznatky o ISMS jsou následně vedením organizace vyhodnoceny a vedou ke zpřesnění cílů pro další období.

Údržba a zlepšování ISMS se věnuje soustavnému zdokonalování a odstraňování nedostatků. Snahou je využití všech nápadů, které dovolí zjednodušit a zkvalitnit systém řízení (Doucek, 2011, s 124).

Na základě těchto procesních etap definují Kolouch a Bašta (2019, s. 258) standardní cíle ISMS v rámci organizace následovně:

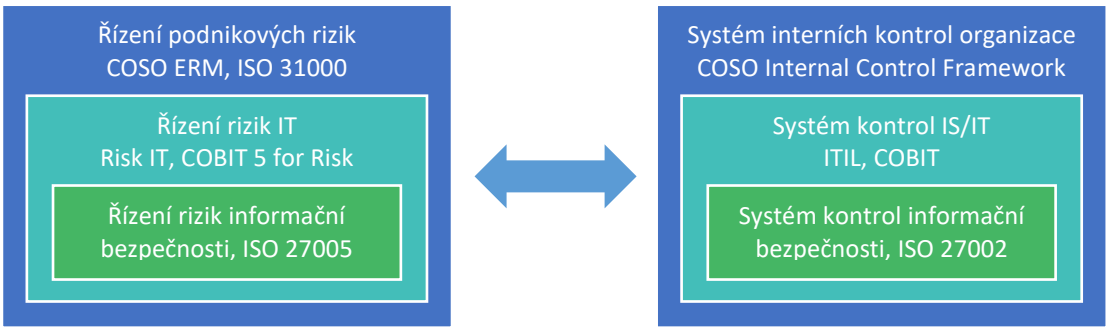
- zajištění bezpečnosti informačních a komunikačních systémů a služeb,
- zajištění kontinuity provozu informačních a komunikačních systémů a služeb,
- ochrana dat a informací,
- ochrana dalších aktiv,
- řešení hrozeb, událostí a incidentů včetně prevence,
- zvyšování bezpečnosti informačních a komunikačních systémů a služeb,
- zvyšování obecného podvědomí uživatelů o bezpečnosti a bezpečnostních hrozbách (edukace),
- sdílení zkušeností s dalšími subjekty.

3.3.3 Proces řízení rizik

Řízení rizik je tedy základem pro každý systém řízení bezpečnosti informací, a navíc podstatným způsobem ovlivňuje efektivitu a fungování celého ISMS (Doucek, 2011, s. 90).

Rizika IT je třeba chápat v kontextu řízení celé organizace. Svatá (2016, s. 101) v rámci organizace zjednodušeně rozeznává tři úrovně rizik, kterým odpovídají i tři úrovně systémů kontrol a s nimi spojených regulací:

Obrázek 6: Vazba mezi úrovněmi rizik a kontrol

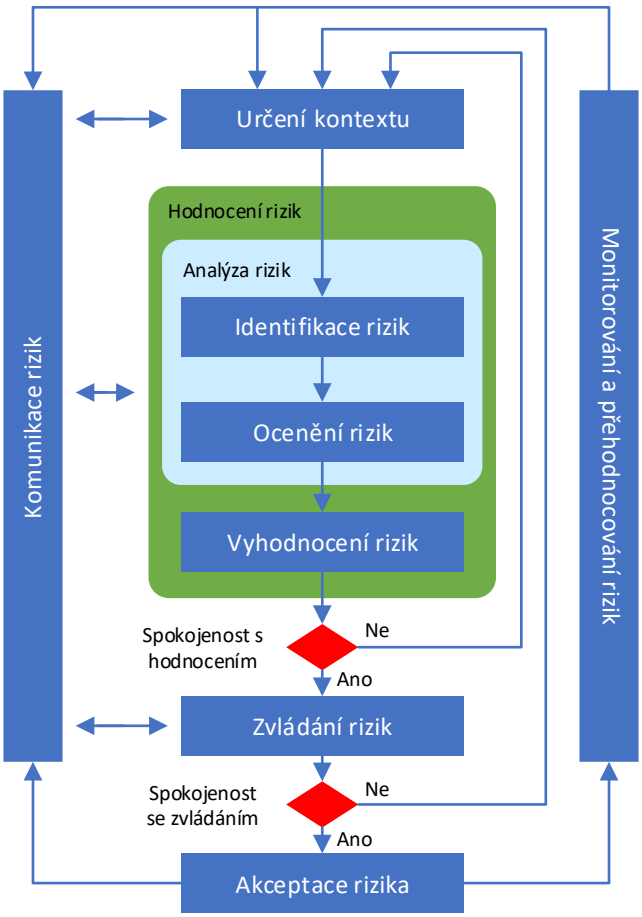


Zdroj: Svatá (2016, str. 101)

Svatá (2016, s. 107) rozděluje proces řízení rizik do čtyř základních etap, které vychází ze standardního konceptu řízení rizik (Obrázek 7):

1. Určení základních východisek – identifikace celkového kontextu pro proces řízení rizik v dané organizaci, tj. požadavků a kritérií hodnocení rizik významných aktiv.
2. Hodnocení rizik – proces, při němž je určována významnost rizik a jejich přijatelná úroveň. Jde o stanovení pravděpodobností, že určité hrozby využijí existujících slabin aktiv a způsobí škodu.
3. Zvládání rizik – stanovení kontrol snižující rizika na akceptovatelnou úroveň.
4. Komunikace a monitorování rizik – řeší vazby procesu na další procesy a oblasti řízení organizace a dále řeší potřebu průběžného monitoringu nastavených kontrol a jejich adekvátnosti vzhledem k měnícímu se prostředí.

Obrázek 7: Koncept řízení rizik



Zdroj: vlastní zpracování dle Doucka (2011, str. 91)

Z pohledu samotného procesu jsou klíčovými etapami hodnocení a ošetření (zvládání) rizik.

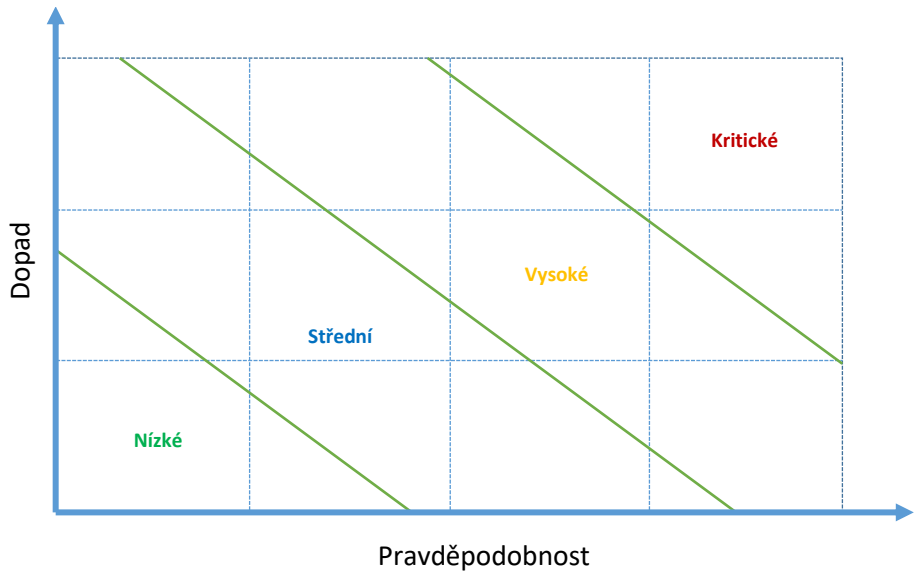
Hodnocení rizik

Základním cílem této etapy je analyzovat identifikovaná potenciální rizika a na základě této analýzy provést vyhodnocení rizik podle jejich priorit. Úroveň rizika je dána pravděpodobností, s jakou může k nežádoucí události dojít, a dále následkem (dopadem), které z takové události mohou vzniknout. Riziko je definováno obecným vzorcem následovně (Svatá, 2016, s. 106):

$$Riziko = pravděpodobnost \times dopad$$

Obecný vzorec má v praxi některá omezení a nedostatky, např. nebere v úvahu různé úrovně slabin aktiv, důležitost aktiv a případně také dostupnost opatření pro snížení rizika. Na jeho základě je však možné aplikovat mapu rizik, což je grafický nástroj usnadňující hodnocení rizik:

Obrázek 8: Mapa rizik



Zdroj: vlastní zpracování dle Svaté (2016, str. 107)

Šikmé čáry na obrázku 8 znázorňují hranice mezi různými kategoriemi rizik:

- Kritické riziko – rizika vyžadující okamžitou reakci (určení opatření pro jejich snížení).

- Vysoké riziko – rizika, která je možné řešit ve vymezeném časovém prostoru.
- Střední riziko – přijatelná rizika, která nevyžadují zavádění nových opatření kromě průběžného monitorování existujících kontrol.
- Nízké riziko – kategorie označující rizika, u kterých je možné ignorovat kontroly a vytvořit příležitost pro snížení nákladů kontrolního systému.

Jednotlivé kategorie (stejně tak hranice je oddělující) jsou pro různé organizace jiné a měly by být předmětem diskuzí v rámci samotného určení základních východisek řízení rizik (Svatá, 2016, s. 107).

Kolouch a Bašta (2019, s. 69) uvádějí, že při hodnocení rizik se obvykle vychází ze tří základních otázek:

- Co špatného (nežádoucího) se může stát? Co může selhat?
- Jaká je možnost / pravděpodobnost, že se to stane?
- Jak závažné (intenzita, velikost apod.) mohou být účinky (dopady, následky)?

Tyto otázky však představují pouze základní rámec, který je schopen definovat vlastní riziko, proto by měly být při určení rizik pokládány ještě doplňující otázky, které se vztahují k významným faktorům ovlivňující charakteristiku rizika:

- Jak dlouho budeme riziku vystaveni? (faktor času)
- Jak se blíží odhady dopadů rizikové události skutečnosti? (faktor nestálosti)
- Je obtížné riziku porozumět? (faktor složitosti)
- Jak dalece spolu souvisí různá rizika nebo rizikové faktory? (faktor vzájemných vztahů)
- Je možné riziko ovládat? (faktor ovlivnění)
- Jak se riziko mění v čase? (faktor životního cyklu)
- Jak nákladná jsou opatření vůči riziku? (faktor nákladové efektivnosti)

K vlastnímu hodnocení pravděpodobnosti a dopadu lze typicky využít kvalitativních a kvantitativních metod, případně jejich kombinace.

Při **kvalitativní analýze** se dopad a pravděpodobnost podrobně popisují pomocí škál hodnot, které se mohou přizpůsobit danému prostředí a druhům rizika. Kvalitativní metoda není náročná na zdroje, avšak kvůli tomu není dostatečně přesná kvůli velké míře subjektivity. Její aplikace se proto doporučuje jako počáteční krok při identifikaci rizik

s následnou podrobnou analýzou, či v případě nedostupnosti statistických numerických údajů potřebných pro kvantitativní přístup. Při hodnocení jsou typicky využívány škály se slovním ohodnocením rizik (Svatá, 2016, s. 108):

- Pravděpodobnost: Vzácná – malá – střední – velká – častá.
- Dopad: Nevýznamný – menší – větší – významný – katastrofální.

Kvantitativní metody se opírají o kvantifikované a číselně vyjádřené údaje. Škály mohou využívat číselně nebo i slovně vyjádřené hranice či limity orientačních hodnot, protože oba atributy rizika se mohou pohybovat v určitých rozpětích a není potřeba je přesně vyčíslit. Kolouch a Bašta (2019, s. 70) uvádějí příklad kvantitativního škálování pravděpodobnosti a dopadu s bodovým ohodnocením:

Tabulka 3: Kvantitativní hodnocení pravděpodobnosti rizika

Body	Pravděpodobnost výskytu rizika	Popis výskytu
5	Jisté	Opakovaný či pravidelný výskyt rizika
4	Pravděpodobné	Výskyt rizika v posledním roce
3	Možné	Výskyt rizika v posledních 3 letech, ale nikoliv v posledním roce
2	Nepravděpodobné	Výskyt rizika v posledních 5 letech
1	Vyloučené	Nezaznamenán žádný výskyt rizika

Zdroj: volně dle Svaté (2016, s. 109) a Koloucha a Bašty (2019, s. 70)

Tabulka 4: Kvantitativní hodnocení dopadu rizika

Body	Dopad rizika	Popis dopadu
5	Krizové	Selhání nebo významné snížení funkcionality organizace
4	Významné	Vyšší než 4 mld. Kč a vyžadující reporting
3	Střední	Dopad na značku organizace, nebo vyšší než 20 mil. Kč
2	Nevýznamné	Dopad jen na omezenou část businessu, nebo dopad menší než 20 mil. Kč
1	Zanedbatelné	Zanedbatelný dopad

Zdroj: volně dle Svaté (2016, s. 109) a Koloucha a Bašty (2019, s. 70)

Přesnějším kvantitativním ukazatelem může být finanční vyjádření. Typickým představitelem tohoto vyjádření je metoda očekávaných ztrát ALE (Annual Loss Expectancy), která je dána vzorcem:

$$ALE = SLE \times ARO$$

kde

- SLE (Single Loss Exposure) je ztráta při jednom výskytu hrozby,
- ARO (Annualized Rate of Occurency) je vyjádření pravděpodobnosti výskytu hrozby za rok.

Cílem této metody je vyjádření korelace mezi hodnotou chráněných aktiv, hodnotou hrozby a hodnotou ochrany. Při aplikaci této metody v oblasti rizik IT se však hodnoty obtížně finančně oceňují, a proto se získávají z různých zdrojů (Svatá, 2016, s. 109).

Výstupem hodnocení rizik by měla být matice rizik sestavené pomocí kombinací kvalitativních a kvantitativních metod. Svatá (2016, s. 109) uvádí postup ohodnocení rizik následovně:

1) Sestavení týmu hodnotitelů výběrem zástupců různých zainteresovaných skupin,
2) určení obecných rizikových faktorů, majících vliv na dodržení stanovených parametrů,
3) stanovení stupně významnosti rizika, tj. váhy a míry rizikových faktorů,
4) ohodnocení jednotlivých rizikových faktorů jednotlivými hodnotiteli,
5) stanovení objektivních měr jednotlivých rizikových faktorů
6) Sestavení matice a seřazení dle ohodnocení rizika

Zvládání rizik

Proces zvládání rizika zahrnuje výběr a přijímání opatření pro změnu rizika. Definování reakcí na rizika a určování jejich priorit je důležité pro to, aby se pokud možno všechna identifikovaná rizika dostala do oblasti přijatelných rizik (Svatá, 2016, s. 112). Svatá (2016, s. 112) dále uvádí čtyři různé reakce na rizika:

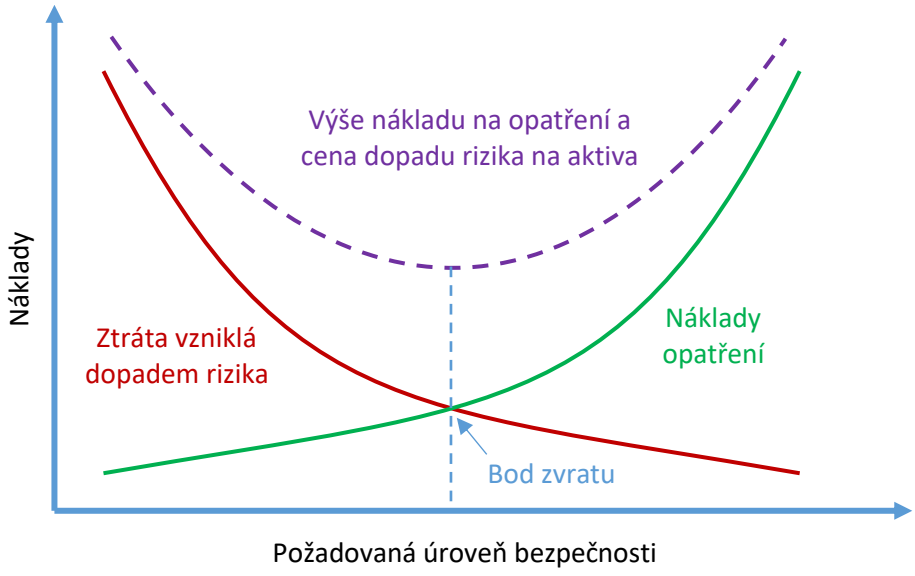
- Vyloučení rizika – používá se tehdy, pokud není možné použít jiné reakce,
- snížení rizika – nastavení takových kontrol, které detekují a snižují buď pravděpodobnost výskytu, nebo dopad škody, nebo obojí,
- sdílení nebo přesunutí rizika – část rizika se přesune nebo sdílí s dalším subjektem, typicky pojištění nebo outsourcing (fakticky se nejedná o přesun rizika, spíše o využívání znalostí poskytovatelů těchto služeb),

- přijetí rizika – organizace nebude přijímat žádná opatření na jeho zmírnění a v případě uskutečnění tohoto rizika budou akceptovány ztráty z něj plynoucí. V případě IT rizik nelze odsouhlasit akceptaci rizik pouze na straně řízení IT, akceptace musí být potvrzena především vlastníky business procesů, vedením organizace a dalšími zájmovými skupinami (např. akcionáři).

Pro řešení rizik obvykle existují různé varianty, které se liší cenou a účinností řešení. Organizace přitom disponují omezenými finančními prostředky, takže je nutná pečlivá analýza efektivnosti jednotlivých řešení a stanovení jejich priorit (Svatá, 2016, s. 112).

Ocenění aktiv bývá v praxi východiskem pro stanovení maximálních nákladů na realizaci opatření na jejich ochranu. Vztahy mezi hodnotou aktiva (resp. Vzniklou ztrátou v případě jeho zničení nebo poškození) a náklady na realizaci ochrany aktiva formou opatření jsou uvedeny na obrázku Obrázek 9 (Doucek, 2011, s. 93).

Obrázek 9: Nákladový model pro realizace bezpečnostních opatření



Zdroj: vlastní zpracování dle Doucka (2011, str. 93)

4 Analytická část

V analytické části je představen cloud computing a jeho trendy v oblasti bezpečnostních rizik. Dále jsou analyzovány konkrétní normy a metodiky a zhodnoceno jejich pokrytí současných trendů.

4.1 Cloud computing

Cloud computing je definován americkým národním institutem standardů a technologií (NIST) jako model umožňující na vyžádání přístup ke sdílenému souboru konfigurovatelných výpočetních prostředků (např. sítí, serverů, úložiště, aplikací a služeb), které lze rychle poskytnout a uvolnit s minimálním úsilím vedení nebo interakcí s poskytovatelem služeb.

Microsoft (2019) popisuje cloud computing jako doručování výpočetních služeb, jako jsou servery, úložiště, databáze, sítě, software, analytické nástroje, inteligentní funkce a další, přes internet a nabízí rychlejší inovace, flexibilitu prostředků a úspory z rozsahu. Obvykle je placeno jen za cloudové služby, které jsou skutečně využívané, což pomáhá organizacím snižovat provozní náklady, efektivněji provozovat infrastrukturu a škálovat s ohledem na obchodní potřeby.

4.1.1 Typy cloudových služeb a jejich nasazení

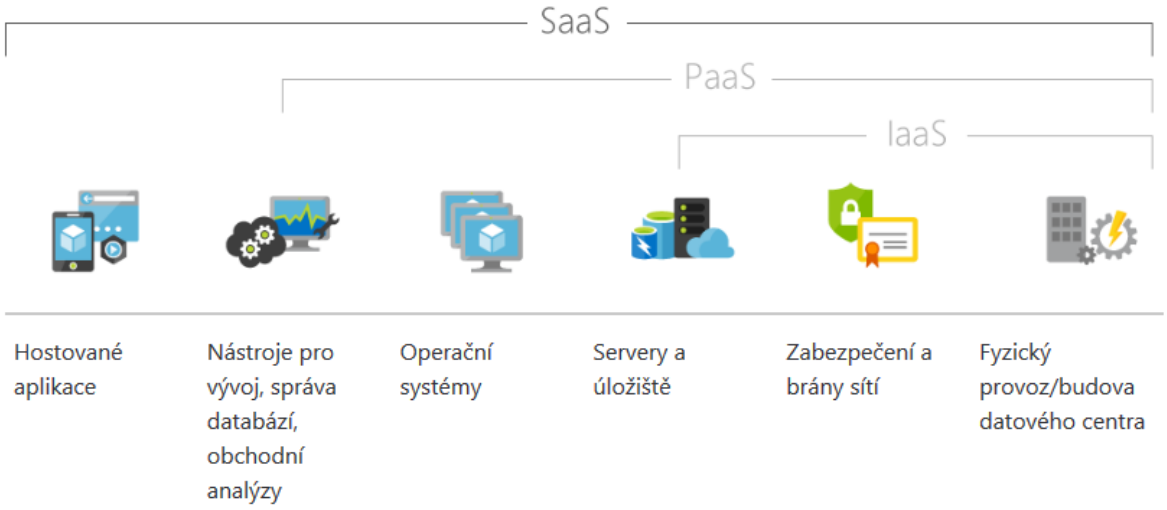
Cloud computing nabízí výpočetní výkon v mnoha různých implementacích, které se rozdělují do kategorií dle typu cloudových služeb a typu cloudových nasazení. Dle typu cloudových služeb se rozlišují (Microsoft, 2019):

- IaaS – „Infrastucture as a service“ – nejzákladnější kategorie služeb cloud computingu, kdy si uživatel pronajímá od poskytovatele cloud computingu samotnou IT infrastrukturu, jako jsou servery, virtuální počítače, úložiště, sítě a operační systémy.
- PaaS – „Platform as a service“ - Platforma jako služba odkazuje na služby cloud computingu, které doručují na vyžádání prostředí pro vývoj, testování, doručování a správu softwarových aplikací. Model PaaS je navržený tak, aby usnadňoval vývojářům vývoj a provoz bez starostí o nastavování a správu podkladové infrastruktury serverů, úložiště, sítě a databází potřebných pro vývoj.

- SaaS – „Software as a Service“ – Software jako služba je metoda doručování softwarových aplikací přes internet, na vyžádání a obvykle na základě předplatného. Pomocí SaaS poskytovatelé cloudu hostují a spravují softwarovou aplikaci a její podkladovou infrastrukturu a obsluhují veškerou údržbu, jako jsou softwarové upgrady a opravy zabezpečení. Uživatelé se k aplikaci připojují přes internet, obvykle pomocí tenkého klienta, tj. webového prohlížeče v telefonu, tabletu nebo počítači.

Jednotlivé funkcionality cloudových služeb a jejich vzájemné vazby jsou zřejmé z obrázku Obrázek 10:

Obrázek 10: Typy cloudových služeb



Zdroj: Microsoft (2019)

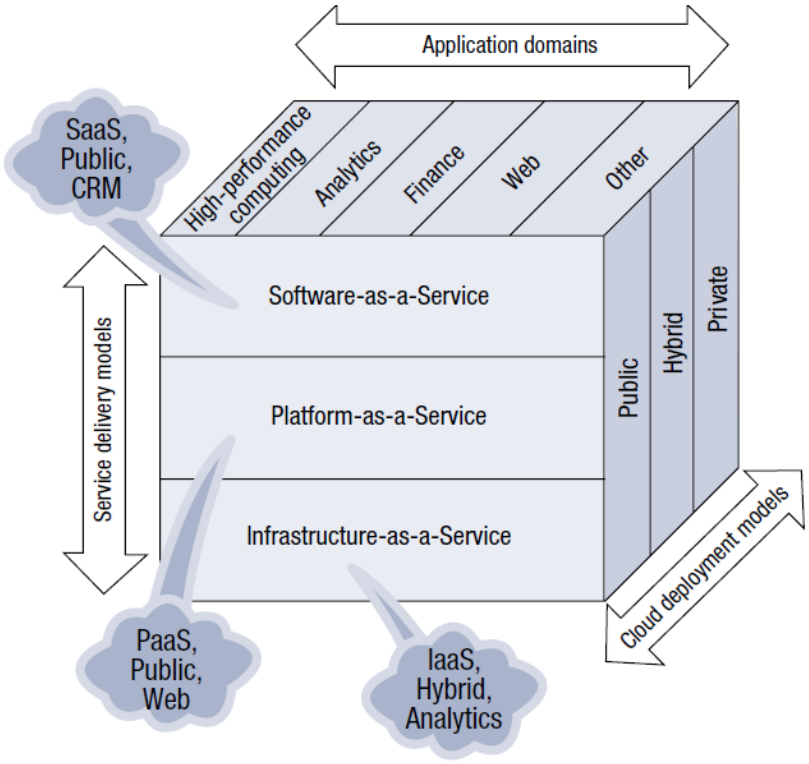
Dále se cloud computing rozlišuje dle typu nasazení, neboli architektury cloud computingu, ve kterém se cloudové služby implementují:

- Veřejný cloud – veřejné cloudy jsou vlastněné a provozované poskytovateli cloudových služeb, kteří dodávají své výpočetní prostředky jako jsou servery a úložiště přes internet. Provozovatelé při tomto typu nasazení vlastní a spravují veškerý hardware, software a další podpůrnou infrastrukturu a uživatel k těmto službám přistupuje vzdáleně, typicky pomocí tenkého klienta.

- Privátní cloud – v případě privátního cloud computingu jsou využívány prostředky jedinou organizací a tyto prostředky jsou typicky fyzicky umístěny v místním datovém centru organizace. V privátním cloud computingu se služby a infrastruktura spravují v privátní síti.
- Hybridní cloud – hybridní cloud computing kombinuje veřejný a privátní cloud, které jsou technologicky propojené, aby mezi nimi šlo sdílet data a aplikace. Možnost hybridního cloudu přesouvat data a aplikace mezi privátním a veřejným cloudem dává organizaci větší flexibilitu a další možnosti nasazení a pomáhá optimalizovat stávající infrastrukturu, zabezpečení a dodržování požadovaných předpisů.

Kombinace typu cloudových služeb, jejich nasazení a způsob využití jsou zřejmé z obrázku Obrázek 11.

Obrázek 11: Implementace cloudu



Zdroj: ISACA (2011, str. 10)

4.2 Trendy cloud computingu

Cloud computing může nabídnout organizacím příležitosti i rizika vyplývající z bezpečnostních faktorů, tj. hrozby s příležitostí na využití známé zranitelnosti s možným dopadem na aktiva.

Mnohé z těchto hrozeb nejsou pro cloud computing jedinečné. Hrozby plynoucí z potenciální ztráty dat, špatné správy ze strany poskytovatele služeb či neoprávněný přístup k citlivým údajům jsou platné i v případě stávajících zapojení třetích stran. Zároveň však cloud computing přináší nové bezpečností aspekty a nové možnosti zranitelností, které vyžadují důkladnou analýzu a řízení rizik.

4.2.1 Řízení rizik dle typu cloud computingu

Rizika cloud computingu se liší dle typu poskytovaných služeb (IaaS, PaaS, SaaS) a také dle typu nasazení cloudu (veřejný, privátní, hybridní). Např. v případě privátního modelu, kdy je využíváno virtualizovaných aplikací v rámci datových center organizace, je riziko takového cloudového řešení velmi podobné stávajícím rizikům podnikové IT bezpečnosti. Naopak v případě veřejného cloudu, kdy poskytované zdroje využívá mnoho klientů, můžou být aktiva vystavena rizikům, která dosavadní podniková IT bezpečnost neřešila.

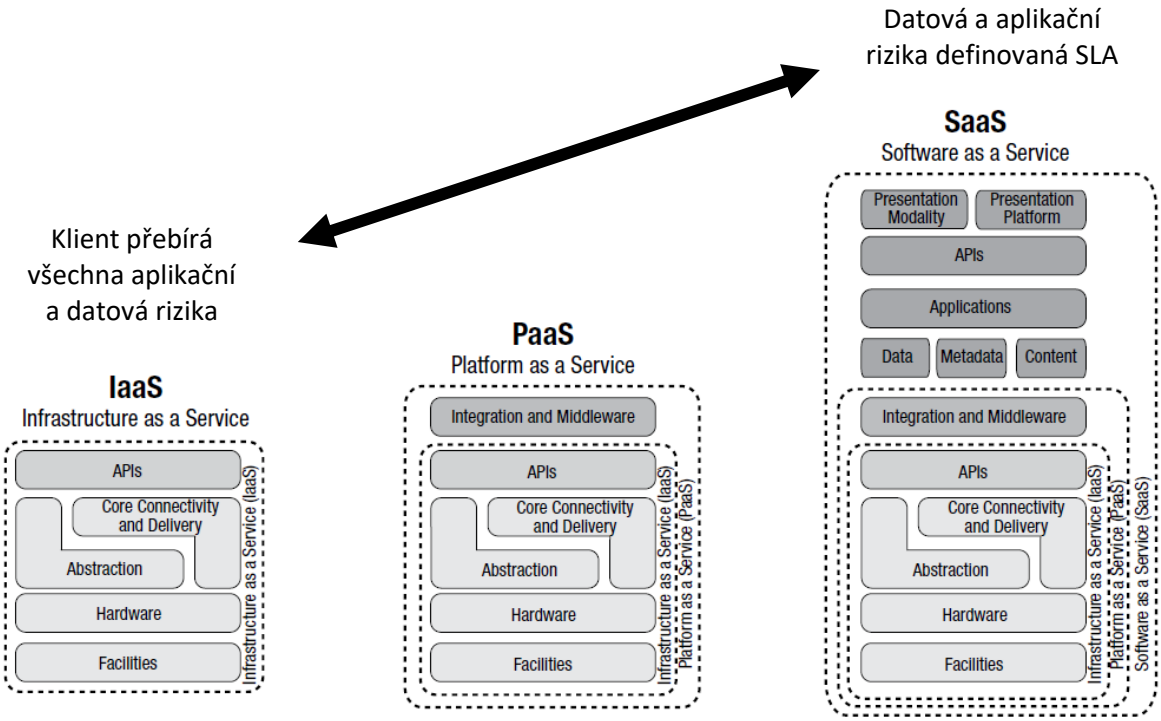
Konečnou odpovědnost za rizika svých aktiv nese klient, poskytovatelé cloudových řešení však mohou částečně přebírat zodpovědnost v oblasti bezpečností rizik dle úrovně a typu poskytovaných služeb cloud computingu. V mnoha případech jsou jednotlivá bezprostřední rizika sdílena mezi poskytovatelem a uživatelem cloud computingu. Rozlišení odpovědnosti za tato sdílená rizika se liší (viz příklad rozlišení datových a aplikačních rizik na Obrázek 12) a může záviset na mnoha faktorech, typicky na poskytovateli cloud computingu a na typu služeb a nasazení, požadavcích klienta a jeho klasifikaci dat.

ISACA (2011, s. 47) uvádí, že v případě veřejného cloud computingu na úrovni IaaS nabízejí poskytovatelé v oblasti řízení rizik základní fyzické a administrativní bezpečnostní procedury a předpisy týkající se samotného datového centra, tj. jeho fyzickou bezpečnost a jeho zabezpečení pomocí systémů detekce narušení, vloupání aj.

V případě veřejného cloud computingu na úrovni PaaS se mohou poskytovatele týkat také rizika nad rámec datové centra, konkrétně např. v oblasti přístupových práv a správy konfigurace.

Na úrovni SaaS mohou poskytovatelé navíc nabízet možnosti řízení rizik v oblasti sledování výkonu, šifrování či zabezpečené komunikace prostřednictvím VPN.

Obrázek 12: Datová a aplikační rizika dle typu CC



Zdroj: ISACA (2011, str. 48)

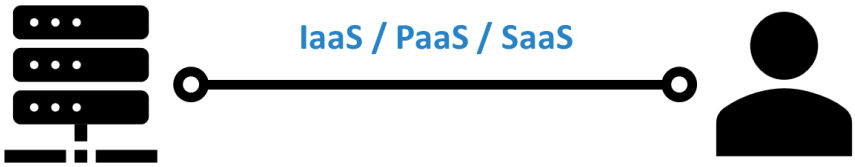
Vzhledem k nezralosti odvětví cloud computingu a také rozdílným metodám a standardům poskytování cloudových služeb existují značné rozdíly v kvalitě a úrovni řízení rizik na straně poskytovatele. Uživatelé proto musí podrobně porozumět možným rizikům a jejich případným kontrolám, které vyplývají z typu služeb a typu nasazení cloud computingu.

Dosavadní metody a postupy, které organizace využívá pro IT bezpečnost a řízení rizik (např. správa uživatelských oprávnění, fyzická bezpečnost, změnové řízení, systémový a softwarový vývoj a také DRP a BCP plány), mohou být zaváděním cloud computingu ovlivněny. Stejně tak také nemusí již být relevantní všechny používané nástroje pro řízení rizik (např. firewallová ochrana, SIEM systémy aj.), jelikož data, která mají tyto systémy vnitřně monitorovat a kontrolovat, jsou záměrně přesunuta mimo dosah kontroly (ISACA, 2011, s. 47).

4.2.2 Řetězec dodavatelů cloud computingu

Při poskytování cloudových služeb je typicky definován vztah *poskytovatel – uživatel*, kdy je na straně poskytovatele organizace, která je fyzickým vlastníkem cloudových služeb (datová centra, infrastruktura, aplikační vrstva, případně samotný software aj.), a na straně uživatele je organizace, která přímo využívá služby poskytovatele. Tento vztah je znázorněn na obrázku Obrázek 13.

Obrázek 13: Vztah poskytovatele a uživatele



Zdroj: vlastní zpracování

V případě využívání některých cloudových služeb (typicky v případě modelu SaaS), však může být poskytovatelem cloudové služby organizace, která pro svou cloudovou službu využívá jinou cloudovou službu další organizace. Z pohledu informační bezpečnosti a řetězce dodavatelů je tak ve vztahu mezi samotným poskytovatelem a uživatelem další subjekt – *zprostředkovatel* – který je tak součástí řetězce poskytované služby, viz Obrázek 14.

Obrázek 14: Vztah poskytovatele, zprostředkovatele a uživatele

Zdroj: vlastní zpracování

Koncový uživatel cloudových služeb tak z hlediska identifikace a řízení rizik musí počítat s dalším subjektem a rozlišovat rizika, která vyplývají ze vztahu *zprostředkovatel – uživatel*, a rizika ze vztahu *poskytovatel – zprostředkovatel – uživatel*. Zatímco ze vztahu *zprostředkoval – uživatel* mohou plynout rizika týkající se spíše samotného softwaru a tedy cloudového typu SaaS (např. přístup třetí strany k datům, změnové řízení či různé auditní

logy aj.), ze vztahu *poskytoval – zprostředkovatel – uživatel* mohou plynou rizika týkající se hardwaru a samotné fyzické bezpečnosti cloudových služeb.

ENISA (2009, s. 12) dále uvádí, že bezpečností rizika třetích stran se nemusí týkat pouze poskytované služby, může se také jednat např. o outsourcing informační bezpečnosti u poskytovatele, případně outsourcovaná podpora týkající se samotné infrastruktury poskytovatele.

Určení celkového řetězce dodavatelů u cloudových služeb může být vhodným předpokladem pro správné určení rizik a pokrytí možných hrozeb.

4.3 Metodiky a standardy cloud computingu

Pro obecné řízení IT bezpečnosti existuje několik metodik a standardů, které mohou organizacím implementující cloud computing pomoci při dosahovaní požadované IT bezpečnosti. Někteří autoři ve svých studiích považují problematiku cloud computingu za natolik komplexní, že současné metodiky a standardy nemohou plně pokrýt rizika plynoucí z implementace cloud computingu a vyžadují nové modely a metodiky pro řízení cloud computingu. Oproti tomu existují také studie, které navrhují vhodné postupy pro zajištění IT bezpečnosti při implementaci cloud computingu dle platných a norem a uznávaných metodik a standardů (Bounagui, Mezrioui a Hafiddi, 2019, s. 101).

Ze stávajících metodik a postupů pro řízení IT bezpečnosti cloud computingu jsou pro účely této práce a analýzu současného pokrytí trendů vybrány tři metodiky/normy:

1) ISO/IEC 270xx
2) COBIT/ISACA
3) ITIL v3

Dle Bounagui, Mezrioui a Hafiddi (2019, s. 101) jsou tyto tři metodiky široce přijaté postupy pro řízení IT bezpečnosti jak v praxi, tak v akademické sféře, a využívání jejich principů poskytuje komplexní pohled na řízení IT v organizaci, proto jsou vhodné pro analýzu jejich aplikovatelnosti na implementaci cloud computingu v organizaci.

4.3.1 ITIL

ITIL je široce adaptovaná metodika pro správu a řízení IT služeb. Poslední verze metodiky (v3) z roku 2007 je založena na procesním řízení organizace a zaměřuje se na

sladění IT služeb s požadavky businessu, zlepšení kvality poskytování IT služeb a snížení nákladů na IT.

Ačkoliv metodika ITIL není koncipována pro podporu cloud computingu, její principy řízení IT v organizaci jsou využitelné i pro řízení IT s využitím cloud computingu.

4.3.2 COBIT/ISACA

ISACA (The Information Systems Audit and Control Association) publikuje metodiku COBIT pro řízení a správu IT. Tato metodika napomáhá organizacím s řízením IT rizik, sladěním IT strategie se stanovenými cíli businessu a se zajištěním právní a regulatorní shody. COBIT poskytuje soubor obecně přijatých opatření, ukazatelů a procesů jak pro maximalizaci hodnoty IT, tak pro rozvoj vhodných postupů v řízení IT organizace (Bounagui, Mezrioui a Hafiddi, 2019, s. 101).

Společnost ISACA vydala v roce 2011 metodiku „IT Control Objectives for Cloud Computing“, která může pomáhat organizacím čelit výzvám v oblasti implementace cloud computingu a rozvíjet komplexní strategii správy infrastruktury a služeb cloud computingu. Tato metodika shrnuje teoretický základ cloud computingu, jeho hlavní přínosy i rizika plynoucí z jeho implementace. Dále tato metodika popisuje konkrétní oblasti řízení rizik dle metodiky COBIT a jejich specifika pro cloud computing, a to jak z pohledu organizace implementující cloud computing, tak z pohledu auditora/kontrolora cloud computingu v organizaci.

4.3.3 Normy ISO/IEC

Série norem ISO/IEC 270xx byla publikována mezinárodní organizací pro standardizaci (ISO) a mezinárodní elektro-technickou komisí (IEC). Tyto normy poskytují bezpečnostní kontroly a osvědčené postupy při vytváření, implementaci, udržování a průběžném zlepšování systému řízení bezpečnosti informací (ISMS) organizace. Hlavní součástí série 27000 jsou normy ISO/IEC 27001 a ISO/IEC 27002, které poskytují komplexní přehled informační bezpečnosti a navrhují konkrétní opatření pro řízení IT bezpečnosti v organizaci.

Na rozdíl od obecné použitelnosti postupů pro řízení rizik bezpečnosti informací má cloud computing své vlastní typy zdrojů rizik, včetně hrozeb a zranitelností, které jsou odvozeny z vlastností cloud computingu, např. využití sítí, škálovatelnost a pružnost systému, sdílení zdrojů, poskytování samoobslužných služeb, správa na vyžádání, poskytování služeb napříč jurisdikcemi a omezenou viditelností implementovaných

kontrolních opatření, proto byla v roce 2017 vydána norma ISO/IEC 27017, která rozšiřuje stávající normu ISO 27002 o specifika cloud computingu a jejich využívání a implementaci. Pokyny rozlišuje pro zákazníka a pro poskytovatele cloudových služeb, případně uvádí shodné pokyny pro oba subjekty.

4.3.4 Analýza atributů metodik

Jednotlivé metodiky přistupují k řízení IT různými způsoby, viz Tabulka 5: Komparativní analýza atributů metodikTabulka 5. Volba určité metodiky, standardu nebo jejich kombinace závisí na organizaci, řídících pracovnících a zralosti a účinnosti procesních prvků.

Tabulka 5: Komparativní analýza atributů metodik

Atribut	**ITIL**	**COBIT/ISACA**	**ISO/IEC 270xx**
Název metodiky	ITIL v3 Service Design ITIL v3 Service Operation ITIL v3 Service Strategy ITIL v3 Service Transition	IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud	ČSN ISO/IEC 27017: Informační technologie – Bezpečnostní techniky – Soubor postupů pro opatření bezpečnosti informací pro cloudové služby založený na ISO/IEC 27002
Vydavatel	OGC, UK	ISACA	ISO/IEC
Verze (rok vydání)	v3 (2007)	2011	1. (2017)
Zaměření	IT management	Řízení IT rizik	Informační bezpečnost
Funkce	Řízení dodávek služeb a podpora	Kontrolní cíle	Systém informační bezpečnosti
Užití	Pokyny a postupy	Metodologie	Pokyny a postupy
Oblast aplikace	Servisní část IT	Všechny oblasti IT řízení	Oblast informační bezpečnosti
Implementační pokyny	Konkrétní pokyny k implementaci	Obecné pokyny určené pro přizpůsobení	Obecné pokyny určené pro přizpůsobení

Zdroj: volně dle Bounagui, Mezrioui a Hafiddi, 2019, s. 102

Sjednocením různých modelů může organizace lépe překonat výzvy a rizika spojená s implementací cloud computingu a využít silných stránek jednotlivých modelů.

4.4 Analýza metod dle současných trendů

V této části práce jsou vybrané metodiky a standardy analyzovány dle daných trendů v oblasti řízení rizik cloud computingu. Z těchto metodik jsou vybrány konkrétní relevantní doporučení a postupy, které upravují nebo jinak řeší problematiku daných trendů.

4.4.1 Řízení rizik dle typu cloud computingu

Rozdělení rizik dle typu využívaného cloud computingu přímo souvisí s identifikací těchto rizik. Jednotlivé typy cloud computingu zasahují do různých úrovní řízení IT a stejně tak i do různých úrovní řízení rizik.

ITIL

Problematika cloud computingu není v metodice ITIL explicitně řešena, přesto se však v dokumentu *ITIL v3 Service Strategy* věnuje problematice řízení rizik v rámci organizace a celkového řízení IT. Metodika se věnuje řízení rizik v několika oblastech:

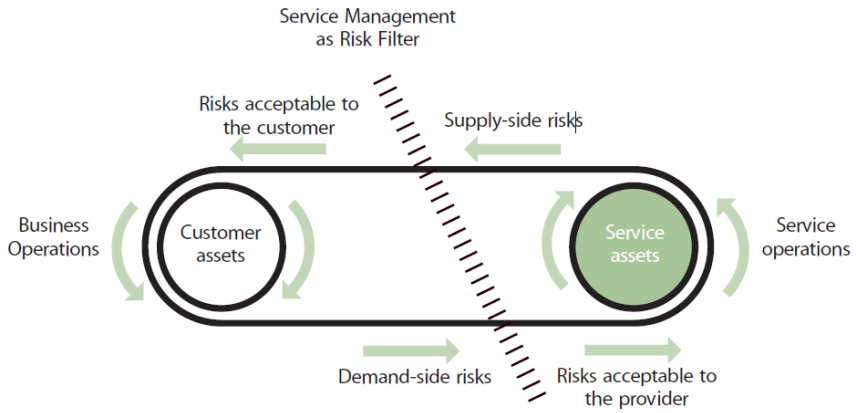
- Transfer rizik,
- rizika poskytovatele služby,
- smluvní rizika,
- rizika návrhu,
- operační rizika,
- tržní rizika.

Metodika ITIL Service Strategy (2007, s. 200) uvádí, že využitím služeb poskytovatelů v IT lze snížit rizika organizace přenesením těchto rizik na poskytovatele. Snížení rizik formou přenesení na poskytovatele služby však zároveň znamená vznik nových z dodavatelského vztahu – přenos rizik je tedy oboustranný.

Poskytovaná služba by měla být jasně definovaná a mělo by jí předcházet adekvátní vyhodnocení rizik, které je poskytovatel služby ochoten převzít. Zároveň by se měl zákazník aktivně zajímat o rizika vyplývající z dodavatelského vztahu a snažit je „filtrovat“ na přijatelnou úroveň. Tento vztah je znázorněn na Obrázek 15. Analýza rizik a vhodné řízení rizik by mělo být aplikováno v rámci servisního katalogu služby pro identifikaci, obsažení a případně snížení rizik v rámci životního cyklu služby.

Podstatnou součástí řízení rizik je také smluvní rámec mezi zákazníkem a poskytovatelem, jelikož pro zákazníka slouží jako prostředek realizace vlastní obchodní strategie a dosahování cílů, a také jako prostředek alokace a řízení většiny operačních rizik spojených s obchodními výsledky. Pojem „smlouva“ v tomto případě zahrnuje formálně, právně závazné smlouvy i méně formální dohody mezi interními skupinami a funkcemi.

Obrázek 15: Vztah rizik mezi poskytovatelem a zákazníkem



Zdroj: ITIL Service Strategy, 2007, s. 201

Rizika ohrožující schopnost poskytovatele služeb plnit své smluvní závazky jsou strategická rizika. Např. infrastruktura má dopad na širokou škálu smluvních závazků a je tedy strategickým aktivem a rizika, kterým jsou tato aktiva vystavena, jsou strategická rizika.

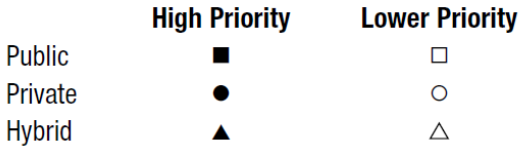
Dopad rizik, hrozeb a slabých míst nemusí být omezen na žádnou konkrétní funkci procesu, a jelikož zákazník nerozlišuje mezi původem rizik, je k jejich řízení nezbytná vzájemná koordinace v rámci životního cyklu.

COBIT/ISACA

Metodika ISACA pro cloud computing je v kategorizaci rizik pro jednotlivé typy cloud computingu nejpodrobnější, jelikož aplikuje jednotlivé oblasti řízení rizik dle metodiky COBIT na prostředí cloud computingu a určuje kontrolní cíle, které jsou pro něj relevantní.

Dle metodiky ISACA (2011, s. 69) mají všechny oblasti řízení rizik (COBIT) určitou aplikovatelnost pro cloud computing, některé však mají vyšší prioritu než jiné. Proto jsou v této metodice zvoleny názorné piktogramy rozlišující priority oblasti pro typ nasazení cloud computingu (privátní, veřejný, hybridní) a vůči konkrétnímu typu cloud computingu (IaaS, PaaS a SaaS), viz Obrázek 16.

Obrázek 16: Legenda metodiky ISACA for Cloud Computing



Zdroj: ISACA, 2011, s. 70

Výsledné určení aplikovatelnosti metodiky COBIT pro konkrétní oblasti řízení rizik cloud computingu je zřejmé z příkladu na Obrázek 17:

Obrázek 17: Hodnocení aplikovatelnosti metodiky ISACA for Cloud Computing

Cloud Computing COBIT Control Objectives	IaaS	PaaS	SaaS
COBIT Domain: Acquire and Implement (AI) ***(cont.)***			
AI3.1 Technological Infrastructure Acquisition Plan Produce a plan for the acquisition, implementation and maintenance of the technological infrastructure that meets established business functional and technical requirements and is in accord with the organisation's technology direction. ***Comment:*** *IaaS is the primary focus, but PaaS may require supporting technology during development and as a precondition of implementation.*	■ ● ▲	■ ● ▲	□ ○ △

Zdroj: ISACA, 2011, s. 87

Pro zhodnocení aplikovatelnosti konkrétních cílů metodiky na trend řízení rizik dle typu cloud computingu lze využít daného rozlišení a zhodnotit jejich významnost pro dané typy služeb cloud computingu dle legendy prioritizace. Pro zhodnocení významnosti jednotlivých cílů metodiky dle typu cloud computingu byla použita následující stupnice:

Tabulka 6: Hodnotící stupnice aplikovatelnosti metodiky ISACA

Počet prioritizací	**Počet bodů**
Žádná vysoká priorita nasazení cloud computingu	0
Jedna vysoká priorita nasazení cloud computingu	1
Dvě vysoké priority nasazení cloud computingu	2
Tři vysoké priority nasazení cloud computingu	3

Zdroj: vlastní zpracování

Zhodnocením metodiky dle uvedené stupnice byla získána Tabulka 7, která znázorňuje významnost jednotlivých oblastí a konkrétních cílů řízení rizik metodiky COBIT dle daného typu cloud computingu. Na základě této sumarizační tabulky lze identifikovat klíčové oblasti řízení rizik za jednotlivé typy cloud computingu.

Tabulka 7: Významnost cílů řízení rizik dle typu cloud computingu

Cíle řízení rizik z oblastí metodiky COBIT	Součet bodů za IaaS	Součet bodů za PaaS	Součet bodů za SaaS
A: Plánování a organizace	**108**	**99**	**120**
Definice a strategie IT plánů	12	12	12
Definice informační architektury	3	3	6
Projektové řízení	36	39	39
Řízení cílů a komunikace	6	6	6
Řízení IT investic	0	0	0
Řízení kvality	0	3	3
Řízení lidských zdrojů	15	12	15
Určení IT procesů, organizace a vztahů	21	9	24
Určení technologického směru	6	6	6
Vyhodnocení a řízení IT rizik	9	9	9
B: Nabytí a implementace	**102**	**102**	**104**
Identifikace automatizovaných řešení	12	12	12
Instalace a pověření a změn	21	27	26
Nabytí a údržba aplikačního software	21	24	30
Nabytí a údržba technologické infrastruktury	9	9	0
Opatření IT zdrojů	12	12	12
Řízení změn	15	15	15
Zavedení provozu a užití	12	3	9
C: Dodání a podpora	**147**	**150**	**165**
Definice a správa servisních stupňů	18	18	18
Identifikace a rozdělení nákladů	12	12	12
Řízení problémů	12	12	12
Řízení služeb třetích stran	12	12	12
Správa dat	9	9	12
Správa fyzického prostředí	0	0	6
Správa operací	0	0	3
Správa požadavků a incidentů	12	12	12
Správa výkonu a kapacity	9	9	12
Vzdělání a školení uživatelů	9	9	9
Zajištění nepřerušitelnosti služby	27	30	30
Zajištění systémové bezpečnosti	27	27	27
D: Monitoring a vyhodnocení	**57**	**33**	**60**
Monitoring a vyhodnocení vnitřních kontrol	18	18	21
Monitoring a vyhodnocení výkonu IT	18	9	18
Poskytnutí IT správy	9	6	9
Zajištění shody s externími požadavky	12	0	12
Celkový součet bodů	**414**	**384**	**449**

Zdroj: vlastní zpracování

ISO/IEC 27017

Norma ISO/IEC 27017 upravuje pokyny pro cloud computing ve vybraných oblastech řízení informační bezpečnosti. Přestože norma možnou rozdílnost pokynů pro jednotlivé typy cloud computingu pouze okrajově zmiňuje u vybraných oblastí, z obecných pokynů pro zákazníka a poskytovatele lze čerpat i při rozlišení řízení rizik dle typu cloud computingu.

Pro kategorizaci rizik bezpečnosti informací dle typu cloud computingu lze čerpat z pokynů pro politiku bezpečnosti informací, a to jak z pokynů pro zákazníka, tak z pokynů pro poskytovatele cloud computingu (ČSN ISO/IEC 27017, 2017, s. 11):

1) Zákazník cloudových služeb

Politika bezpečnosti informací pro cloud computing by měla být definována jako tematicky specifická politika zákazníka cloudových služeb. Politika bezpečnosti informací zákazníka cloudových služeb by měla být v souladu s přijatelnou úrovní rizik bezpečnosti informací organizace pro informace a jiná aktiva organizace.

Při definování politiky bezpečnosti informací pro cloud computing by měl zákazník cloudových služeb vzít v úvahu následující:

- Informace uložené v prostředí cloud computingu mohou být předmětem přístupu a správy ze strany poskytovatele cloudových služeb
- Aktiva mohou být udržována v prostředí cloud computingu, například aplikační programy
- Procesy mohou běžet na virtualizované cloudové službě s vícenásobným pronájmem
- Uživatele cloudových služeb a kontext, ve kterém se používají cloudové služby
- Administrátory cloudových služeb zákazníka cloudových služeb, kteří mají privilegovaný přístup
- Geografickou polohu organizace poskytovatele cloudových služeb a země, ve kterých může poskytovatel cloudových služeb ukládat data zákazníka cloudových služeb (i dočasně).

2) Poskytovatel cloudových služeb

Poskytovatel cloudových služeb by měl rozšířit svou politiku bezpečnosti informací, aby řešila poskytování a používání jeho cloudových služeb, berouce v úvahu následující:

- Základní požadavky bezpečnosti informací použitelné na návrh a implementaci cloudových služeb
- Rizika ze strany autorizovaných interních pracovníků
- Izolace vícenásobného pronájmu a zákazníka cloudových služeb (včetně virtualizace)
- Přístup pracovníků poskytovatele cloudových služeb k aktivům zákazníka cloudových služeb
- Postupy řízení přístupu, například silná autentizace pro administrátorský přístup ke cloudovým službám
- Komunikace se zákazníky cloudových služeb v rámci řízení změn
- Bezpečnost virtualizace
- Přístup k datům zákazníka cloudových služeb a jejich ochrana
- Řízení a správa životního cyklu účtů zákazníka cloudových služeb
- Směrnice pro hlášení narušení a sdílení informací na podporu vyšetřování a forenzního šetření

4.4.2 Řetězec dodavatelů cloud computingu

Řízení dodavatelů je důležitou součástí všech vybraných metodik. Obecně platné pokyny a doporučení jsou v různé míře využitelné a aplikovatelné i na problematiku řízení IT s využitím služeb cloud computingu.

ITIL

Metodika ITIL řeší vztahy s dodavateli v dokumentu *ITIL v3 Service Design*, kde popisuje podrobné procesní metody při řízení dodavatelských vztahů. Ačkoliv metodika ITIL nezohledňuje specifické parametry cloud computingu, z obecně platných pokynů pro řízení dodavatelských vztahu lze čerpat i v případě implementace cloud computingu.

Proces řízení dodavatelů dle metodiky ITIL Service Design (2007, s. 150) by měl zahrnovat:

- Implementace a prosazování dodavatelských zásad a směrnic,

- údržba dodavatelské a smluvní databáze,
- kategorizace dodavatelů a hodnocení rizik,
- posouzení a výběr dodavatelů a jejich smluv,
- vytváření, vyjednávání a uzavírání smluv,
- kontrola, obnovení a ukončení smluv,
- řízení výkonnosti dodavatelů,
- dohody o implementaci služby a plány zlepšení,
- údržba standardních smluv a podmínek,
- řízení smluvního řešení sporů,
- řízení subdodavatelských vztahů.

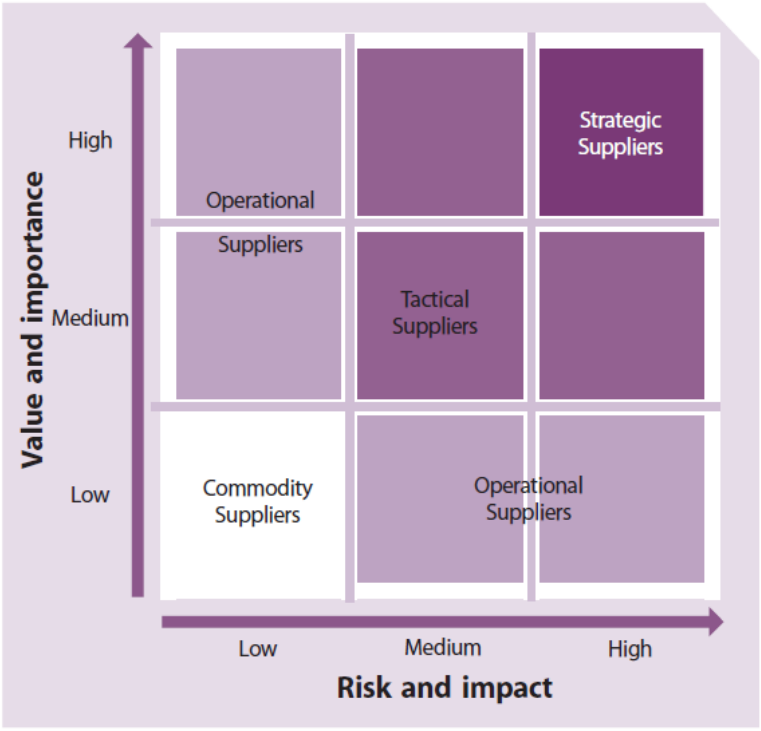
Při aplikování metodiky ITIL na proces řízení řetězce dodavatelů cloudových služeb jsou stěžejní především body *kategorizace dodavatelů a hodnocení rizik* a *řízení subdodavatelských vztahů*, jelikož reflektují jejich požadavky na řízení rizik.

Kategorizace dodavatelů a hodnocení rizik jsou metodikou ITIL Service Design (2007, s. 156) dále definovány a doporučeny konkrétní způsoby, jak k definici přistupovat. Kategorizace by měla být založena na posouzení rizika a dopadu spojeného s užíváním služby dodavatele a na významu dodavatelské služby pro organizaci. Metodika ITIL uvádí čtyři kategorie dodavatelů:

1. Strategický
2. Taktický
3. Operační
4. Komoditní

Jejich význam a rizika jsou zřejmá z Obrázek 18:

Obrázek 18: Kategorizace dodavatelů dle metodiky ITIL



Zdroj: ITIL Service Design, 2007, s. 156

Z definice jednotlivých kategorií vyplývá, že dodavatelé cloud computingu se řadí mezi strategické dodavatele. Na dodavatele této kategorie by měla být zaměřena maximální pozornost a na úrovni strategie by měly být zváženy dostupné možnosti, aby byly z dodavatelského vztahu vytěženy benefity v souladu s obchodní strategií.

COBIT/ISACA

Metodika ISACA pro cloud computing (2011, s. 92) uvádí obecné pokyny z oblasti řízení a správy služeb třetích stran. Řízení služeb třetích stran definuje ISACA jako zajištění souladu požadavků obchodních strategií a služeb poskytovaných třetí stranou (dodavateli, poskytovali a partnery). Efektivní správou služeb dodávaných třetí stranou se minimalizuje riziko spojené s neefektivními dodavateli.

Samotné pokyny a cíle řízení dodavatelských vztahů jsou dle metodiky ISACA rozděleny následovně:

- Identifikace dodavatelských vztahů – identifikace všech dodavatelských služeb a jejich kategorizace dle typu dodavatele, významu a kritičnosti služby.
- Řízení vztahů s dodavateli – formalizování procesu řízení vztahů s dodavateli s důrazem na zajištění kvality založené na důvěře a transparentnosti (např. prostřednictvím SLA a nezávislých auditů).
- Řízení dodavatelských rizik – identifikace a zmírnění rizik spojených s možností dodavatelů pokračovat v efektivním poskytování služeb nepřerušitelným způsobem a zajištění souladu dodávané služby s právními a regulatorními požadavky se všemi náležitostmi řízení rizik (dohoda o mlčenlivosti – NDA, dodržování bezpečnostních požadavků, alternativních dodavatelů aj.).
- Monitoring dodávaných služeb – zavedení procesu monitorování dodávaných služeb pro zajištění plnění požadavků dodavatelem v rámci smluv a ujištění, že dodávaná služba je konkurenceschopná v porovnání s ostatními dodavateli obdobné služby.

Všechny tyto body jsou dle metodiky platné pro typy služeb IaaS, PaaS i SaaS, a stejně tak pro všechny typy nasazení, tedy pro privátní, veřejný i hybridní cloud computing a to s vysokou prioritou užití.

ISO/IEC 27017

Norma ISO/IEC 27017 (2017, s. 26) věnuje řízení dodavatelských vztahů obsáhlé pokyny pro zajištění bezpečnosti informací a ochranu aktiv, která jsou přístupná dodavatelům. Norma uvádí, že organizace by měla v politice určit opatření v oblasti bezpečnosti informací a nařídit, aby se jimi specificky řídil přístup dodavatele k informacím organizace. Tato opatření by se měla zabývat procesy a postupy, které mají být organizací implementovány, stejně jako těmi procesy a postupy, jejichž implementaci by měla organizace požadovat po dodavateli, včetně:

a) identifikace a zdokumentování typů dodavatelů, kterým organizace umožní přístup ke svým informacím, například služby IT, logistické podniky, finanční služby, komponenty infrastruktury IT;
b) normalizovaného procesu a životního cyklu pro řízení vztahů s dodavateli;

c) definování typů přístupu k informacím, které budou povoleny různým typům dodavatelů, a monitorování a řízení přístupu;
d) minimálních požadavků na bezpečnost informací pro každý typ informací a typ přístupu, které budou sloužit jako základ pro smlouvy s jednotlivými dodavateli na základě potřeb a požadavků organizace a jejího profilu rizik;
e) procesů a postupů pro monitorování dodržování stanovených požadavků na bezpečnost informací pro každý typ dodavatele a typ přístupu, včetně přezkoumání třetí stranou a validace výrobků
f) opatření v oblasti přesnosti a úplnosti pro zajištění integrity informací nebo zpracování informací poskytovaných jednou ze smluvních stran;
g) typů povinností pro ochranu informací organizace vztahující se na dodavatele
h) řešení incidentů a nepředvídatelných událostí souvisejících s přístupem dodavatelů, včetně odpovědnosti jak organizace, tak dodavatelů;
i) odolnosti a, pokud je to nutné, opatření pro obnovu a pro nepředvídatelné události k zajištění dostupnosti informací nebo zpracování informací poskytovaných jednou ze smluvních stran;
j) školení týkající se povědomí pro pracovníky organizace zapojené do akvizic, vztahující se k příslušným politikám, procesům a postupům;
k) školení týkajícího se povědomí pro pracovníky organizace spolupracující se zaměstnanci dodavatele, vztahující se k příslušným pravidlům zapojení a chování na základě typu dodavatele a úrovni přístupu dodavatele k systémům a informacím organizace;
l) podmínek, na základě kterých budou požadavky informační bezpečnosti a opatření zdokumentovány ve smlouvě podepsané oběma stranami;
m) řízení nezbytných přechodů informací, vybavení pro zpracování informací a čehokoli jiného, co je třeba přesunout, a zajištění udržování bezpečnosti informací po celou dobu přechodného období.

Tyto pokyny by měly být s dodavateli smluvně ustanoveny, aby se zajistilo, že neexistuje žádné nedorozumění mezi organizací a dodavatelem, pokud jde o povinnost obou stran splňovat relevantní požadavky na bezpečnost informací.

Norma ISO/IEC 27017 (2017, s. 27) dále zmiňuje řetězec dodavatelů informačních a komunikačních technologií a uvádí stručné pokyny pro jejich řízení. Organizacím

doporučuje spolupracovat s dodavateli na porozumění řetězce dodavatelů informačních a komunikačních technologií a všech záležitostí, které mají významný dopad na poskytované produkty a služby. Organizace mohou ovlivnit praktiky v oblasti bezpečnosti informací řetězce dodavatelů informačních a komunikačních technologií tím, že ve smlouvách se svými dodavateli vyjasní záležitosti, které by měly být řešeny jinými dodavateli v rámci řetězce dodavatelů informačních a komunikačních technologií.

Norma dále explicitně uvádí, že řetězce dodavatelů informačních a komunikačních technologií popisované ve směrnici zahrnují také služby cloud computingu.

Specifické pokyny pro poskytovatele cloudových služeb dále uvádí, že pokud poskytoval cloudových služeb využívá dalších peer poskytovatelů cloudových služeb, měl by tento poskytovatel zajistit svým zákazníkům zachování nebo překročení úrovně bezpečnosti informací. Pokud poskytovatel cloudových služeb poskytuje cloudové služby založené na řetězci dodavatelů, mě by poskytovatel cloudových služeb poskytnout cíle v oblasti bezpečnosti informací, a vyžadovat od každého dodavatele provádění činností v oblasti řízení rizik za účelem dosažení těchto cílů.

Norma ISO/IEC 27017 (2017, s. 31) dále uvádí pokyny pro nezávislé přezkoumání bezpečnosti informací.

1) Zákazník cloudových služeb

Zákazník cloudových služeb by si měl vyžádat doložené důkazy, že implementace kontrolních opatření bezpečnosti informací a směrnic pro cloudové služby je v souladu s jakýmkoliv tvrzením ze strany poskytovatele cloudových služeb. Takový důkaz může zahrnovat certifikáty podle příslušných norem.

2) Poskytovatel cloudových služeb

Poskytovatel cloudových služeb by měl zákazníkovi cloudových služeb poskytnout doložené důkazy, aby dokázal svá tvrzení o implementaci kontrolních opatření bezpečnosti informací.

Tam, kde jsou audity individuálních zákazníků cloudových služeb nepraktické nebo mohou zvýšit riziko pro bezpečnost informací, poskytovatel cloudových služeb by měl poskytnout nezávislé důkazy, že bezpečnost informací je implementována a provozována v souladu s politikami a postupy poskytovatele cloudových služeb. Ty by měly být potenciálním zákazníkům cloudových služeb k dispozici před uzavřením smlouvy.

Relevantní nezávislý audit dle výběru poskytovatele cloudových služeb by běžně měl být přijatelnou metodou pro naplnění zájmu zákazníka cloudových služeb o přezkoumání činností poskytovatele cloudových služeb, za předpokladu, že je zajištěna dostatečná transparentnost. Je-li provedení nezávislého auditu nepraktické, poskytovatel cloudových služeb by měl provést sebehodnocení a zákazníkovi cloudových služeb oznámit jeho průběh a výsledky.

5 Zhodnocení výsledků

Současné normy a metody pro řízení IT v organizaci v různé míře upravují taktéž postupy pro řízení cloud computingu v rámci organizace, případně uvádějí obecná doporučení a principy, které lze aplikovat i pro řízení IT s využitím cloud computingu. Na základě analyzovaných norem a metodik jsou navrženy konkrétní postupy a doporučení pro řízení rizik týkající se daných trendů cloud computingu.

Tyto doporučené postupy pro řízení daných trendů kombinují silné stránky jednotlivých analyzovaných metodik, a to z pohledu několika oblastí IT:

- IT managementu (metodika ITIL),
- řízení IT rizik (metodika COBIT/ISACA),
- informační bezpečnost (norma ISO/IEC 27017).

5.1 Řízení rizik dle typu cloud computingu

Různé typy cloud computingu představují pro organizaci rozlišná rizika, kterým v rámci implementace cloud computingu musí čelit. Správná identifikace rizik pro využívaný typ služby cloud computingu představuje také výchozí bod pro další strategické plánování a řízení rizik v rámci celé IT bezpečnosti.

V následujícím přehledu jsou uvedeny klíčové oblasti a procesy pro konkrétní typ cloud computingu, kterým by při identifikaci rizik měla být věnována zvláštní pozornost a nejvyšší priorita.

IaaS

Pro typ služby IaaS jsou klíčové procesy související především se samotným hardwarem a jeho konfigurací, tj.:

- fyzická bezpečnost a správa fyzického prostředí,
- zaškolení personálu pro administraci služby,
- monitoring výkonu a kapacit služby.

PaaS

Při využití typu služby PaaS by měla maximální pozornost věnována především oblastem a procesům, které souvisí s implementačními riziky služeb cloud computingu:

- kompatibilita se stávajícím IT prostředím a využívanými aplikacemi a systémy,
- konfigurační správa a údržba,
- kompatibilita patchů a bezpečnostních záplat.

SaaS

Typ služby SaaS je z pohledu řízení rizik kritický zejména v oblastech a procesech souvisejících s přístupem k informacím a informační bezpečností. Při implementaci tohoto typu služby by měl IT management brát v úvahu především následující:

- přístup třetích stran k aktivům organizace (administrátoři aplikace, správci platformy aj.),
- zajištění dostupnosti služby a přístupu k informacím.

Ačkoliv jsou uvedené doporučení a postupy obecně platné pro všechny typy cloud computingu, je vhodné zaměřit pozornost primárně na výše uvedené oblasti dle typu služby cloud computingu pro neopomenutí klíčových rizik.

5.2 Řetězec dodavatelů cloud computingu

Řízení dodavatelů a řetězce dodavatelů cloud computingu by mělo být řešeno v několika oblastech:

1) Identifikace a analýza dodavatelského vztahu,
2) Implementace a provoz,
3) Monitoring a vyhodnocování služby.

Z pohledu řízení rizik je klíčová samotná oblast identifikace a analýzy dodavatelského vztahu. V této úvodní fázi by měla být podrobně definována podoba služby a její vazby na interní procesy, obchodní cíle a strategie. Mezi konkrétní cíle analýzy by měly patřit následující body:

- zdokumentování dodávané služby a jejich dodavatelů včetně jejich subdodavatelů, kteří se přímo i nepřímo podílí na dodávané službě,
- vymezení typu poskytované cloudové služby (IaaS, PaaS, SaaS) a typu provozu služby či služeb a jejich návaznosti na klíčové procesy organizace,
- kategorizace všech dodavatelů, kterých se týká dodávaná cloudová služba, a jejich vymezení v rámci interního řízení rizik,
- zhodnocení úrovně IT bezpečnosti dodavatele a jeho subdodavatelů formou nezávislých auditů či revizí dostupných auditních reportů, a její srovnání se stávající bezpečnostní strategií organizace,

V oblasti samotné implementace a provozu by se pohledu řízení rizik řetězce dodavatelů měla v rámci řízení IT věnovat pozornost těmto bodům:

- identifikace všech dodavatelů a jejich subdodavatelů, kteří mají umožněn přístup k informacím organizace,
- rozlišení odpovědnosti za jednotlivé parametry služby cloud computingu,
- smluvní vymezení služby cloud computingu v souladu s legislativními a regulatorními požadavky (SLA, OLA, NDA apod.),

V oblasti monitoringu a vyhodnocování služby cloud computingu by se organizace měla zaměřit především na tato témata:

- monitorování a řízení přístupu třetích stran k informacím organizace,
- monitoring a vyhodnocování dostupnosti služby a pravidelné hodnocení jejích technických aspektů,
- pravidelné vyhodnocování služby cloud computingu a zhodnocení její konkurenceschopnosti.

6 Závěr

V úvodní teoretické části práce byl vymezen význam IT bezpečnosti v rámci podnikové bezpečnosti a uvedeny základní pojmy a principy z oblasti IT bezpečnosti. Dále byly uvedeny obecné principy informační bezpečnosti a systému řízení bezpečnosti informací a také základní postupy v oblasti řízení rizik, které jsou aplikovatelné i v případě řízení rizik cloud computingu.

V analytické části byl uveden cloud computing a jeho standardní rozlišení služeb a možností jeho využití. Dále byly definovány aktuální trendy z oblasti cloud computingu a jejich význam pro řízení rizik organizace. Na základě těchto trendů byly zanalyzovány vybrané normy a metodiky z oblasti IT managementu (metodika ITIL, z oblasti řízení IT rizik (metodika COBIT/ISACA) a z oblasti informační bezpečnosti (norma ISO/IEC 27017). Při analýze bylo hodnoceno pokrytí daných trendů normami a metodikami a byly vybrány konkrétní pokyny aplikovatelné pro řízení rizik daných trendů. V závěru práce byly na základě analýzy definovány konkrétní pokyny a postupy pro řízení rizik těchto trendů, které kombinují silné stránky jednotlivých analyzovaných norem a metodik.

Navržené postupy a doporučení pro řízení rizik daných trendů z oblasti cloud computingu mohou být využity při implementaci cloudových služeb a řízení jejich rizik a lze z nich čerpat i při hodnocení výhod a nevýhod cloud computingu v organizaci.

7 Seznam použitých zdrojů

BOUNAGUI, Yassine, Abdellatif MEZRIOUI a Hatim HAFIDDI. Toward a unified framework for Cloud Computing governance: An approach for evaluating and integrating IT management and governance models. In: *Computer Standards & Interfaces*. Volume 62. Amsterdam, Nizozemsko: Elsevier B.V., 2019, 98 - 118. ISSN 0920-5489.

DOUCEK, Petr. *Řízení bezpečnosti informací: 2. rozšířené vydání o BCM.* 2., přeprac. vyd. Praha: Professional Publishing, 2011. ISBN 978-807-4310-508.

Co je cloud computing?: Průvodce pro začátečníky. MICROSOFT. *Microsoft Azure* [online]. Seattle: Microsoft, 2019 [cit. 2019-03-03]. Dostupné z: https://azure.microsoft.com/cs-cz/overview/what-is-cloud-computing/

ČSN ISO/IEC 27017. Informační technologie – Bezpečnostní techniky - *Soubor postupů pro opatření bezpečnosti informací pro cloudové služby založený na ISO/IEC 27002*. Praha: Úřad pro technickou normalizaci, metrologii a státní zkušebnictví, 2017.

ENISA. *Cloud Computing: Information Assurance Framework*. Attiki, Greece: European Network and Information Security Agency (ENISA), 2009. Dostupné také z: https://www.enisa.europa.eu/publications/cloud-computing-information-assurance-framework/

ISACA. *IT Control Objectives for Cloud Computing: Controls and Assurance in the Cloud*. United States of America: ISACA, 2011. ISBN 978-1-60420-185-7.

ISO/IEC 27000:2018(E). *Information technology — Security techniques — Information security management systems — Overview and vocabulary*. Fifth edition. Switzerland: ISO copyright office, 2018.

ISO/IEC 27002:2013(E). *Information technology — Security techniques — Code of practice for information security controls.* Second edition 2013-10-01. Switzerland: ISO copyright office, 2013.

ITIL: Service Design. London: Stationery Office, 2007. ISBN 978-011-3310-470.

ITIL: Service Strategy. London: Stationery Office, 2007. ISBN 978-011-3310-456.

JIRÁSEK, Petr, Luděk NOVÁK a Josef POŽÁR. *Výkladový slovník kybernetické bezpečnosti: Cyber security glossary.* 2., aktualiz. vyd. Praha: Policejní akademie ČR v Praze, 2013. ISBN 978-80-7251-397-0. Dostupné také z: https://www.govcert.cz/cs/informacni-servis/akce-udalosti/2193-vykladovy-slovnik-kyberneticke-bezpecnosti-druhe-vydani/

KOLOUCH, Jan a Pavel BAŠTA. *CyberSecurity*. Praha: CZ.NIC, z.s.p.o., 2019. CZ.NIC. ISBN 978-80-88168-34-8.

SMĚRNICE EVROPSKÉHO PARLAMENTU A RADY (EU) 2016/1148 ze dne 6. července 2016 o opatřeních k zajištění vysoké společné úrovně bezpečnosti sítí a informačních systémů v Unii. In: . Štrasburk: Úřední věštník Evropské unie, 2016, ročník 1., L 194/1. Dostupné také z: https://eur-lex.europa.eu/legal-content/CS/TXT/HTML/?uri=CELEX:32016L1148&from=EN

Zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti, ve znění pozdějších předpisů. In: . Sbírka zákonů, 2015. Dostupné také z: https://www.nbu.cz/cs/pravni-predpisy/zakon-c-412-2005/1122-uplne-zneni-zakona-c-412-2005/

SVATÁ, Vlasta. *Audit informačního systému*. V Praze: Oeconomica, nakladatelství VŠE, 2016. ISBN 978-802-4521-688.

Vyhláška č. 82/2018 Sb., o kybernetické bezpečnosti. In: Sbírka zákonů. 2018, 43/2018. Dostupné také z: https://www.zakonyprolidi.cz/cs/2018-82