NÚKIB

METODIKA K VODÍTKŮM PRO HODNOCENÍ DOPADŮ

Verze 1.2, platná ke dni 20.03.2018

Obsah

Úvod

Tento dokument obsahuje komentář k materiálu „Vodítka pro hodnocení dopadu narušení bezpečnosti informací“, který slouží k hodnocení dopadu narušení bezpečnosti informací u aktiv, informačních a komunikačních systémů, ICT služeb a k následnému řízení rizik. Dokument lze použít i pro vlastní posouzení, zda by daný systém mohl být zařazen pod působnost zákona o kybernetické bezpečnosti.

Vodítka pro hodnocení dopadu narušení bezpečnosti informací naleznete v Příloze č. 1.

Tento dokument a dokument „Vodítka pro hodnocení dopadu narušení bezpečnosti informací“ byl vytvořen ve spolupráci s panem Ing. Liborem Širokým, CISM, CRISC, AMBCI ze společnosti RISK ANALYSIS CONSULTANTS s.r.o. Spolupráce byla bezplatná.

V případě dotazů se prosím obracejte na sekretariát Národního úřadu pro kybernetickou a informační bezpečnost:

Národní úřad pro kybernetickou a informační bezpečnost

Mučednická 1125/31
616 00 Brno – Žabovřesky

Tel.: +420 541 110 777

E-mail: nckb@nukib.cz

Upozornění:

Tento dokument slouží jako podpůrné vodítko, nenahrazuje žádný ze zákonů ani prováděcích právních předpisů. Právo změny tohoto dokumentu vyhrazeno.

1 Účel

Účelem tohoto podpůrného materiálu je nabídnout:

- Hodnocení důležitosti informačních a komunikačních systémů.
- Hodnocení důležitost aktiv a s tím související řízení rizik.
- Odvození požadavků na bezpečnost zpracovávaných informací a informačních systémů.
- Nastavení jednotících kritérií dopadu narušení bezpečnosti informací (dostupnost, důvěrnost, integrita).
- Pomoc správcům informačních a komunikačních systémů se zařazením jejich systémů do správné kategorie podle zákona č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákona o kybernetické bezpečnosti) – tedy zařazení mezi významné informační systémy, informační či komunikační systémy kritické informační infrastruktury či informační systémy základní služby.

Hodnocení důležitosti informačních či komunikačních systémů dané organizace se v souladu s touto metodikou hodnotí pomocí určení kritických dopadů narušení dostupnosti, důvěrnosti a integrity dat a informací nebo ICT služeb (aktiv), na kterých je funkčnost hodnoceného systému závislá.

Primárně se hodnotí celý informační nebo komunikační systém, avšak podle metodiky je možné hodnotit i jednotlivá aktiva (primární i podpůrná).

Pro určení dopadů narušení bezpečnosti je vytvořena hodnotící škála neboli vodítka hodnocení, která obsahují 9 oblastí (obecné scénáře) a 4 úrovně závažnosti dopadů (podrobněji viz samotný materiál v Příloze č. 1).

Použití jednotné škály (vodítek hodnocení) pro hodnocení různých informačních systémů, by mělo zajistit jednotný způsob posouzení závažnosti dopadů narušení bezpečnosti a zároveň umožnit srovnání výsledků mezi jednotlivými organizacemi.

2 Vodítka pro hodnocení dopadů

Pro posouzení závažnosti dopadů způsobených narušením bezpečnosti informací (důvěrnosti, dostupnosti, integrity) jsou navrženy následující oblasti dopadů.

A. **Bezpečnost a zdraví osob**
B. **Ochrana osobních údajů**
C. **Zákonné a smluvní povinnosti**
D. **Trestně-právní řízení**
E. **Veřejný pořádek**
F. **Mezinárodní vztahy**
G. **Řízení a provoz organizace**
H. **Ztráta důvěryhodnosti**
I. **Finanční ztráty**
J. **Zajišťování nezbytných služeb**

Oblasti dopadů A. až J. obsahují obecné scénáře, které by mohly nastat v případě narušení bezpečnosti zpracovávaných dat a informací (narušení důvěrnosti, dostupnosti nebo integrity).

Závažnost dopadů je v každé z oblastí rozdělena do 4 úrovní dopadů (nízký, střední, vysoký a kritický). Matice dopadů je vytvořena tak, aby si úrovně (závažnosti) dopadů v jednotlivých oblastech navzájem odpovídaly (byla mezi nimi přiměřená korelace). V případě, že je pro konkrétní případ hodnocení bezpečnosti dat poplatných více oblastí dopadů (např. je relevantní „A. Bezpečnosti a zdraví osob“ a „B. Ochrana osobních údajů“), použije se pro výsledné stanovení závažnosti dopadu nejvyšší dosažená hodnota v rámci hodnocených oblastí dopadů. Tento přístup ilustruje následující příklad.

Příklad: použití vodítek dopadu

		1	nízká	…	Může způsobit porušení etických, nikoli však právních předpisů vedoucí k negativním osobním dopadům na jednotlivce nebo skupinu osob.	Může zapříčinit porušení interních předpisů a postupů, nikoli však porušení zákonných a smluvních povinností.	…	Může narušit řádné řízení nebo fungování části nebo celé organizace.	Může negativně ovlivnit vztahy s jinými částmi organizace, jinými organizacemi nebo vztahy s veřejností, negativní publicita bude ale omezena na bezprostřední okolí a nebude mít dlouhé trvání.	Může přímo nebo nepřímo vést ke ztrátám menším než 0,05% ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	…
		2	střední	…	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na jednotlivce (pokuta až 10 mil. EUR nebo 2 % celkového ročního obratu - viz čl. 83/4 GDPR).	**Může zapříčinit správní nebo občanskoprávní řízení vedoucí k pokutě nebo k náhradě škody.**	…	Může omezit provádění důležitých činností organizace.	Může negativně ovlivnit vztahy s jinými organizacemi nebo veřejností, negativní publicita se ale bude týkat omezené zájmové skupiny nebo bude široká, avšak krátkodobá.	Může přímo nebo nepřímo vést ke ztrátám mezi 0,05% a 2 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	…
		3	vysoká *	…	**Může způsobit porušení právních předpisů vedoucí k negativním dopadům na velkou skupinu osob (pokuta až 20 mil. EUR nebo 4 % celkového ročního obratu - viz čl. 83/5 GDPR).**	Může zapříčinit porušení právních předpisů vedoucí k zahájení trestního stíhání.	…	**Může způsobit dočasné zastavení nebo podstatné narušení důležitých činností organizace nebo poškodit rozvoj nebo prosazování cílů a zájmů organizace.**	**Může závažně ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní negativní publicity.**	**Může přímo nebo nepřímo vést ke ztrátám vyšším než 2 % a nižším či rovným 10% ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace). *Pozn. v případě PZS je hranice ztráty stanovena na 0,25 % HDP.***	…
ZKB - KII, ISZS		4	kritická **	…	*žádné vodítko*	*žádné vodítko*	…	Závažným způsobem může zasáhnout do fungování celé organizace a může vést až k ukončení činnosti.	Může závažně a dlouhodobě ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní či nadnárodní negativní publicity, s dlouhodobými účinky a požadavky přijetí politické odpovědnosti.	Může přímo nebo nepřímo vést ke ztrátám přesahujícím 10% ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace). *Pozn. v případě KII je hranice ztráty stanovena na 0,5 % HDP.*	…
	ZUI	Narušení bezpečnosti informací v oblasti "důvěrnosti" může způsobit újmu zájmům České republiky anebo nevýhodnost pro zájmy České republiky a zároveň je informace typově uvedena v seznamu utajovaných informací (§ 2 písm. a) zákona č. 412/2005 Sb.). Na základě tohoto dopadu by se za splnění dalších legislativně stanovených podmínek mělo jednat o utajované informace. Pro určení odpovídajícího stupně utajení je třeba postupovat v souladu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. A to za splnění dalších stanovených podmínek, např. uvedených v nařízení vlády č. 522/2005 Sb.									

Obrázek 1 Příklad hodnocení dopadu narušení bezpečnosti informací v informačním systému

V rámci tohoto zjednodušeného příkladu je hodnocen určitý informační systém. Při hodnocení dopadu procházíme tabulku v příloze 1 a hodnotíme nejhorší možné dopady narušení bezpečnosti informací (důvěrnosti, dostupnosti, integrity) v tomto systému. Některé oblasti dopadu (slupce A. – J.) nemusejí být pro všechny systémy relevantní. Pro účely příkladu spisové služby to jsou oblasti (sloupce) A., D. – F. a J. Narušení bezpečnosti informací v tomto hodnoceném systému tedy nebude mít dopad například v oblasti A. Bezpečnost a zdraví osob. Tyto nerelevantní sloupce jsou pro účely tohoto příkladu vypuštěny. V rámci zbývající oblasti dopadu (sloupců) je rozhodný ten nejhorší možný dopad narušení alespoň jednoho z aspektů bezpečnosti informací (důvěrnost, dostupnost, integrita) v rámci jednotlivých oblastí. Podle toho nejhoršího dopadu narušení bezpečnosti informací tedy stanovíme celkovou úroveň dopadu hodnoceného systému.

V rámci příkladu je nejhorší dopad narušení bezpečnosti informací v oblasti B., G., H. Tedy systém je ohodnocen na úrovni 3 – vysoká. Za splnění dalších podmínek (například odvětvových kritérií podle vyhlášky č. 437/2017 Sb.) by měl být takový systém zařazen do kategorie významných informačních systémů nebo informačních systémů základní služby.

2.1 Základní východiska pro hodnocení dopadů narušení bezpečnosti informací

V rámci hodnocení jsou důležité tyto principy:

- Nezkoumají se příčiny (hrozby) narušení bezpečnosti.
- Neurčuje se pravděpodobnost výskytu jednotlivých scénářů.
- Posuzují se nejhorší možné „kritické“ scénáře.
- Neuvažují se existující bezpečnostní opatření.

Je nutné hodnotit narušení všech aspektů bezpečnosti informací, tedy narušení:

- důvěrnosti,
- dostupnosti,
- integrity.

2.2 Postup hodnocení dopadů

Vhodnou metodou hodnocení dopadů je řízené interview s věcným správcem (garantem) daného informačního systému, garantem procesu či služby, kterou systém podporuje a případně lze k rozhovoru přizvat i další specialisty (ICT oddělení, technická správa, bezpečnostní oddělení apod.). Interview by mělo být vedeno analytikem, který je znalý metodiky a postupů kvalitativního a kvantitativního hodnocení dopadů. Obvyklá délka interview na jeden systém či službu je 90 až 120 minut. Tento proces je nutné dokumentovat a tyto dokumenty uschovat pro další využití.

2.3 Průběh hodnocení

V rámci interview jsou garanti dotazováni na nastínění realistického scénáře nejhoršího případu, který by mohl vyplývat z následujících dopadů:

- Narušení **dostupnosti**
  - **nedostupnost** informačního systému (nedostupnost zpracovávaných informací),
  - **ztráta** dat od poslední zálohy, úplná ztráta dat a informací.
- Narušení **důvěrnosti** dat a informací (neoprávněné prozrazení a únik informací).
- Narušení **integrity** dat a informací (vlivem neúmyslné modifikace (chyby), úmyslné modifikace dat a systémové chyby).

Interview zpravidla probíhají podle následujícího scénáře:

- Získání základních informací o hodnoceném informačním systému: účel a rozsah zpracovávaných informací, relevantní legislativa a regulatorní požadavky, kritické termíny, úřední hodiny, lhůty apod.
- Vysvětlení způsobu a postupu hodnocení dopadů. Zejména je potřeba zdůraznit výše uvedené principy.
- Kritické scénáře (scénáře nejhoršího možného dopadu) popsané garantem se porovnají s obecnými vodítky pro hodnocení dopadů (viz příloha tohoto dokumentu). Pro určení závažnosti dopadů je použita stupnice o čtyřech úrovních dopadu (1 – nízký, 2 – střední, 3 – vysoký, 4 – kritický).

Poznámka: V případě, že se na danou situaci dá uplatnit více než jeden scénář současně (např. ohrožení bezpečnosti osob, ztráta důvěryhodnosti, finanční ztráta) se dopady nesčítají. Vždy se bere v rámci vyhodnocení v potaz nejvyšší dosažená úroveň dopadu pro každý z parametrů bezpečnosti.

Po zpracování výsledků interview je vhodné zaslat výstup z hodnocení garantovi k revizi a odsouhlasení provedeného hodnocení.

I. Hodnocení následků nedostupnosti

Hodnocení následků nedostupnosti vychází z předpokladu, že nedochází ke ztrátě dat, jen k jejich dočasné nedostupnosti způsobené výpadkem informačního systému. Následky vyplývající z nedostupnosti dat se mohou lišit v závislosti na délce nedostupnosti systému nebo dané ICT služby. Pro stanovení okamžiku, kdy se poprvé projeví dopady z nedostupnosti a toho jak se v čase tyto dopady vyvíjí, se hodnocení provádí v časových intervalech (tzv. časové řezy).

II. Hodnocení následků ztráty dat

Tento dopad zkoumá následky, které by mohly vzniknout v případě ztráty dat. Pro určení optimálního požadavku na frekvenci zálohování dat se hodnocení provádí pro následující časové intervaly.

Výsledek hodnocení úplné a trvalé ztráty dat ze systému může vyústit například v požadavek na umístění záloh v geograficky oddělené lokalitě.

III. Hodnocení následků narušení důvěrnosti dat

Tento dopad je možné zkoumat zejména z hlediska:

- Prozrazení v rámci organizace – prozrazení zaměstnancům, kteří však nemají oprávnění pro přístup k datům.
- Prozrazení smluvním partnerům – prozrazení smluvním poskytovatelům služeb (zaměstnancům třetí strany, kteří mohou mít oprávněný přístup k systému nebo síti, ale nikoli k datům – například organizace provozující outsourcované informační služby).
- Prozrazení vně organizace – únik informací na veřejnost.

IV. Hodnocení následků narušení integrity dat

Otázky zkoumané při vyšetřování tohoto dopadu se liší podle účelu hodnoceného informačního systému. Neodhalená změna nebo chyba v datech může způsobit zásadní dopady, neboť organizace pak funguje na základě špatných dat. Dopad je možné zkoumat z hlediska:

- Chyby malého rozsahu – neúmyslné modifikace dat, např. chyby při vkládání dat uživatelem, duplikace vstupu.
- Chyby velké rozsahu – narušení správnosti a úplnosti informací velkého rozsahu, např. chyby v kódu informačního systému, porušení integrity dat vlivem technického selhání.
- Úmyslné modifikace – úmyslná změna provedená uživatelem nebo správcem systému nebo útočníkem.

3 Popis a příklady použití jednotlivých oblastí dopadů

A. Bezpečnost a zdraví osob

Neoprávněné prozrazení, modifikace nebo nedostupnost informací mohou vést k ohrožení bezpečnosti a zdraví osob.

Například:

- Prozrazení údajů určitých osob (např. adresa, identita agentů či chráněné osoby dle zákona č. 137/2001 Sb.) může způsobit, že se tyto osoby stanou cílem někoho, kdo jim chce způsobit újmu.
- Neoprávněná modifikace informací (např. informací v rámci komunikace složek integrovaného záchranného systému, informací spojených s výrobními procesy, výrobou energií, léčebnými postupy apod.) může způsobit chybnou funkčnost zařízení nebo může vést k nesprávným rozhodnutím, v jejichž důsledku dojde k ohrožení bezpečnosti nebo zdraví osob.
- Nedostupnost informací z některých systémů (např. komunikační systémy IZS, informace v letecké dopravě, zdravotní záznamy apod.), může vést k nesprávným nebo pozdním rozhodnutím, v jejichž důsledku mohou vzniknout negativní dopady na bezpečnost nebo zdraví určité osoby nebo skupiny osob.

Poznámka: V některých případech je pro určení maximálního dopadu doporučeno také zvážit dopady v oblastech *Ochrana osobních údajů* a *Trestně-právní řízení*.

B. Ochrana osobních údajů

Povinnosti správců a zpracovatelů osobních údajů a práva subjektů údajů nově upravuje nařízení Evropského parlamentu a Rady (EU) 2016/679 ze dne 27. dubna 2016 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (GDPR). Nařízení se použije od 25. května 2018, a to plošně ve všech státech EU.

Některé informační systémy uchovávají a zpracovávají údaje o zaměstnancích, externistech, smluvních partnerech (např. jejich osobní údaje, informace o jejich platu nebo osobním hodnocení). Jiné systémy byly určeny pro zpracování údajů o občanech, a obsahují například informace o jejich finančním či zdravotním stavu. Tyto informace umožňují identifikovat osobu, jíž se týkají.

Například:

- Prozrazení osobních nebo citlivých osobních údajů může způsobit danému jednotlivci psychické problémy, snížit možnost jeho společenského a pracovního uplatnění a

může pak vést k občanskoprávnímu, správněprávnímu nebo trestněprávnímu řízení proti organizaci, která osobní údaje spravuje nebo zpracovává. Maximální výše ukládaných pokut je 20 000 000 €, resp. 4 % z globálního celoročního obratu podniku a to podle toho, která částka je vyšší (viz článek 83 GDPR).

- Neoprávněná modifikace dat v databázi (např. pozměnění pracovního hodnocení na negativní).
- Je důležité, aby nebyly údaje o osobách znepřístupněny nebo zničeny, což by mohlo vést k nesprávným rozhodnutím nebo k nečinnosti v době, kdy by bylo zapotřebí na základě těchto údajů konat (např. lustrace osob). Tato situace může mít podobné důsledky jako neoprávněné prozrazení nebo modifikace.

Poznámka: Pokud dopad spočívá v porušení zákona či smlouvy (např. zákona o ochraně osobních údajů, GDPR), je vhodné vzít při stanovení hodnot dopadů také v úvahu vodítko *Zákonné a smluvní povinnosti, Trestně-právní řízení či Finanční ztráty.* V některých případech, kdy dopad narušení bezpečnosti informací může mít vliv na bezpečnost osob, je třeba přihlédnout k vodítku *Bezpečnost a zdraví osob.*

C. Zákonné a smluvní povinnosti

Zpracovaní a správa dat organizací mohou podléhat požadavkům celé řady smluv a právních předpisů a z nich vyplývajících zákonných a smluvních povinností. Data mohou být také uchovávána a zpracovávána proto, aby organizace byla schopna tyto požadavky naplnit. Neplnění těchto požadavků, ať už úmyslné nebo neúmyslné, může vest k občanskoprávnímu, správněprávnímu nebo trestněprávnímu řízení proti osobám nebo celé organizaci. Toto řízení může vést k pokutám nebo případně až k trestům odnětí svobody. Za relevantní lze považovat všechny předpisy a smlouvy, jimiž se řídí provoz ICT.

Například:

- Může být zákonnou povinností organizace určité informace chránit (např. informace podle zákon č. 101/2000 Sb., GDPR či obchodní tajemství). Jejich prozrazení může být úmyslné, nebo může být důsledkem neodpovídajících organizačních a technických opatření, která organizace k ochraně zákonem stanovených informací realizuje.
- Neoprávněná modifikace informací může vést k porušení zákonem stanovených povinností.
- Nedostupnost informací může vést k porušení zákonem stanovených povinností vztahujících se ke zpřístupňování informací (např. podle zákonů č. 106/1999 Sb. a č. 101/2000 Sb.).
- Porušení smluvní povinnosti může vést k občanskému soudnímu sporu, v němž může být uložena náhrada škody způsobené porušením povinnosti plynoucí organizaci ze smlouvy.

Poznámka: Hodnocení podle této oblasti vodítek je vhodné založit na předběžné právní analýze vymezující právní předpisy a smlouvy, které mají bezprostřední vliv na zpracování informací v rámci organizace.

D. Trestně-právní řízení

Prozrazení nebo modifikace některých údajů může usnadnit spáchání trestného činu. Prozrazení, modifikace nebo nedostupnost některých údajů mohou také mít nepříznivý dopad na vyšetření nebo potrestání trestného činu. Nedostupnost informací může být způsobena i v důsledku úmyslného jednání zaměstnanců, snažících se získat neoprávněnou výhodu sobě nebo třetí osobě.

Například:

- Prozrazení osobních údajů může vést k vydírání, fyzickému násilí nebo ublížení na zdraví.
- Únik informací o zabezpečení systémů nebo havarijních plánů může napomoci ohrožení bezpečnosti a také ke spáchání závažných trestných nebo v některých případech i teroristických činů.
- Prozrazení, modifikace nebo ztráta některých informací v průběhu vyšetřování trestného činu může mít negativní vliv na úspěšnost tohoto vyšetřování (např. prozrazení adres nebo únik informací o klíčových svědcích, znehodnocení důkazů).

E. Veřejný pořádek

Některé organizace mohou zpracovávat data, u kterých by narušení bezpečnosti mohlo ohrozit veřejný pořádek. Mohou to být například informace o místních rozvojových projektech (např. o stavbě nové silnice) nebo životním prostředí, jejichž narušení by mohlo způsobit protesty, demonstrace či stávky.

Například:

- Nespolehlivé poskytování informací nebo dokonce jejich nedostupnost v období rozsáhlých povodní nebo jiných živelních pohrom může způsobit dopravní kolaps, komplikace v zásobování postižených oblastí nebo dokonce vážné problémy při záchranných akcích.
- Prozrazení (předčasný únik) informací o plánu uzavřít místní poštovní úřad, prozrazení návrhu na zmrazení mezd nebo propouštění ve státních podnicích může vyvolat místní nespokojenost, protesty nebo demonstrace.
- Modifikace informací o rozšíření systému dálnic s ekonomickými dopady (např. povinný odprodej pozemků nebo změny plánů územního rozvoje) mohou způsobit nespokojenost určité skupiny obyvatel.

F. Mezinárodní vztahy

Některé organizace vytváří informace, které ovlivňují vztahy mezi ČR a ostatními zeměmi či nadnárodními organizacemi (EU, NATO). Prozrazení nebo neoprávněná modifikace některých druhů informací by mohla ovlivnit vztahy s těmito partnery. Stejně tak by mohla negativně ovlivnit pozici ČR nedostupnost některých typů informací např. v kritických fázích vyjednávání.

Například:

- Únik nebo modifikace informací, které by vedly k podání oficiálního protestu, uvalení sankcí, odvolání velvyslance apod.
- Nedostupnost informací o připravenosti splnit vyjednávané podmínky (např. že byl vydán rozkaz k určitým akcím).

G. Řízení a provoz organizace

Informace mohou být takového charakteru, že jejich ohrožení může narušit efektivní provoz organizace. Pokud má organizace celonárodní význam, nebo poskytuje některé nezbytné služby (např. bankovnictví či energetika) může dojít k dopadům na velké množství osob, ekonomickým ztrátám apod.

Například:

- Informace týkající se změny politiky organizace vůči veřejnosti mohou v případě předčasného prozrazení vyvolat veřejné reakce v rozsahu, který realizaci takové politiky znemožňuje.
- Podobně také informace týkající se personálu organizace, jako jsou změny v pracovních podmínkách, mohou v případě předčasného prozrazení vést k negativním vztahům zaměstnanců s vedením a oslabit tak řízení celé organizace.
- Také modifikace nebo nedostupnost informací v souvislosti s finančními aspekty nebo počítačovým programovým vybavením mohou mít závažné důsledky z hlediska chodu organizace.

H. Ztráta důvěryhodnosti

Neoprávněné prozrazení, modifikace nebo nedostupnost informací může vést ke ztrátě dobrého jména organizace s následným poškozením pověsti, ztrátou důvěryhodnosti a dalšími nepříznivými důsledky. Bezpečnostní incidenty snižují důvěryhodnost organizace a tím i její vážnost v očích veřejnosti či obchodních partnerů. Od toho se odvíjí i vztah veřejnosti a dalších aktérů k těmto organizacím a komplikuje to jejich postavení při prosazování a plnění úkolů, které vyplývají z jejich účelu.

I. Finanční ztráta

V některých informačních systémech se uchovávají a zpracovávají informace, které se přímo týkají finančních transakcí nebo se vztahují k finančnímu fungování organizace nebo organizací jí spravovaných. V důsledku neoprávněného prozrazení a modifikace či nedostupnosti a zničení takových informací může vzniknout finanční ztráta. Tato oblast pokrývá také finanční ztráty způsobené narušením činnosti systému, při němž nedostupnost či zničení informací může způsobit újmu uživatelům, organizaci nebo i dalším stranám. Obnova po výskytu mimořádné události i sanace škod vyžaduje často vynaložení značného času, úsilí a financí, které je také třeba brát v úvahu. U tohoto faktoru je třeba finanční náklady odvodit od času stráveného pracovníky na obnově, ztrát způsobených zastavením činnost, kompenzací dotčených, pokut a plateb za sanaci škod.

Poznámka: Protože reálné dopady se mohou u různých organizací lišit, při použití vodítek v této oblasti je nutné přihlížet k reálnému objemu finančních prostředků spravovaných danou organizací a podle něho modifikovat hodnoty uvedené v tabulce tak, aby vyjadřovaly reálné dopady na organizaci. Vodítko „finanční ztráty“ je z těchto důvodů nastaveno na procento ztráty z ročního rozpočtu či obratu.

J. Zajišťování nezbytných služeb

Některé ICT zpracovávají informace, jejichž narušení může přímo ovlivnit poskytování nezbytných služeb osobám či jiný významný zásah do každodenního života.

Například:

- Modifikací informací v informačním systému (např. doručení zprávy o reálně neexistujícím přepětí či jiné vadě na elektrickém vedení) může dojít k výpadku elektřiny pro určitý počet osob.
- Narušení informací v systému inteligentního řízení dopravy může vést k vytvoření falešné uzavírky na exponovaném dopravním uzlu.

4 Seznam použitých zdrojů

1. Strategický rámec Národního cloud computingu – eGovernment cloud ČR
2. Vodítka metodiky RAMSES, Risk Analysis Consultants, s.r.o.
3. ISO/IEC 27035:2016, Information technology – Security techniques – Information security incident management – Part 2: Guidelines to plan and prepare for incident response
4. Business Impact Level Tables, Extract from HMG IA Standard No. 1, Issue No: 3.5, October 2009, UK Cabinet Office
5. Zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
6. Zákon č. č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti
7. Zákon č. 137/2001 Sb. o zvláštní ochraně svědka a dalších osob v souvislosti s trestním řízením a o změně zákona č. 99/1963 Sb., občanský soudní řád, ve znění pozdějších předpisů
8. Zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů
9. Vyhláška č. 316/2014 Sb., o bezpečnostních opatřeních, kybernetických bezpečnostních incidentech, reaktivních opatřeních a o stanovení náležitostí podání v oblasti kybernetické bezpečnosti (vyhláška o kybernetické bezpečnosti)
10. Vyhláška č. 437/2017 Sb., o kritériích pro určení provozovatele základní služby
11. Vyhláška č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích
12. Nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury
13. ISO 22317 – Societal Security – Business Continuity Management Systems – Business Impact Analysis

Verze dokumentu

Datum	Verze	Změněno (jméno)	Změna
23. 2. 2018	1.0	Široký, Kučínský	Vytvoření dokumentu
15. 3. 2018	1.1	Odd. RAP	Jazyková korektura
20. 3. 2018	1.2	Odd. RAP	Grafická úprava bez úprav textu

Příloha 1

Regulace odpovídající úrovni dopadu	Úroveň dopadu	Vodítka (kategorie) pro určení závažnosti dopadů narušení bezpečnosti informací (dostupnost, důvěrnost, integrita) - NUKIB v1.0 / 23.02.2018									
		A. Bezpečnost a zdraví osob	B. Ochrana osobních údajů	C. Zákonné a smluvní povinnosti	D. Trestně-právní řízení	E. Veřejný pořádek	F. Mezinárodní vztahy	G. Řízení a provoz organizace	H. Ztráta důvěryhodnosti	I. Finanční ztráty	J. Zajišťování nezbytných služeb
Ostatní, ISVS, GDPR, ZKB - VIS, ISZS, ZKB - KII, ISZS, ZUI	1 nízká	*žádné vodítko*	Může způsobit porušení etických, nikoli však právních předpisů vedoucí k negativním osobním dopadům na jednotlivce nebo skupinu osob.	Může zapříčinit porušení interních předpisů a postupů, nikoli však porušení zákonných a smluvních povinností.	*žádné vodítko*	*žádné vodítko*	*žádné vodítko*	Může narušit řádné řízení nebo fungování části nebo celé organizace.	Může negativně ovlivnit vztahy s jinými částmi organizace, jinými organizacemi nebo vztahy s veřejností, negativní publicita bude ale omezena na bezprostřední okolí a nebude mít dlouhé trvání.	Může přímo nebo nepřímo vést ke ztrátám menším než 0,05 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	*žádné vodítko*
Ostatní, ISVS, GDPR, ZKB - VIS, ISZS, ZKB - KII, ISZS, ZUI	2 střední	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) jedné nebo několika osob.	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na jednotlivce (pokuta až 10 mil. EUR nebo 2 % celkového ročního obratu - viz čl. 83/4 GDPR).	Může zapříčinit správní nebo občanskoprávní řízení vedoucí k pokutě nebo k náhradě škody.	Může vytvořit podmínky pro páchání trestné činnosti nebo může ztížit její vyšetřování.	Může zapříčinit rozsahem, formou nebo místem omezené protesty (lokální nepokoje).	Může vytvářet negativní obraz ČR v jednom teritoriu, popř. v jednom státě.	Může omezit provádění důležitých činností organizace.	Může negativně ovlivnit vztahy s jinými organizacemi nebo veřejností, negativní publicita se ale bude týkat omezené zájmové skupiny nebo bude široká, avšak krátkodobá.	Může přímo nebo nepřímo vést ke ztrátám mezi 0,05 % a 2 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace).	Může způsobit závažné omezení či narušení nezbytných služeb pro malé množství osob.
Ostatní, ISVS, GDPR, ZKB - VIS, ISZS, ZKB - KII, ISZS, ZUI	3 vysoká *	Může vést k újmě (ohrožení osobní bezpečnosti, svobody nebo zranění) větší skupiny osob, nebo ohrožení na životě jednotlivců.	Může způsobit porušení právních předpisů vedoucí k negativním dopadům na velkou skupinu osob (pokuta až 20 mil. EUR nebo 4 % celkového ročního obratu - viz čl. 83/5 GDPR).	Může zapříčinit porušení právních předpisů vedoucí k zahájení trestního stíhání.	Může vést k narušení vyšetřování trestné činnosti nebo soudní řízení (méně závažná kriminalita, krátkodobě, v jednotlivých případech).	Může zapříčinit rozsahem, formou nebo místem omezené protesty na úrovni významné části správního území obce s rozšířenou působností, jejichž řešení si může vyžádat aktivaci krizového řízení na úrovni kraje.	Může vytvářet negativní obraz ČR ve světě.	Může způsobit dočasné zastavení nebo podstatné narušení důležitých činností organizace nebo poškodit rozvoj nebo prosazování cílů a zájmů organizace.	Může závažně ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní negativní publicity.	Může přímo nebo nepřímo vést ke ztrátám vyšším než 2 % a nižším či rovným 10 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace). Pozn. v případě PZS je hranice ztráty stanovena na 0,25 % HDP.	Může způsobit závažné omezení, narušení či nedostupnost nezbytných služeb pro více než 25 000 osob (v rámci kategorie provozovatelů základních služeb se může lišit dle právní úpravy pro jednotlivá odvětví viz vyhláška č. 437/2017 Sb.).
Ostatní, ISVS, GDPR, ZKB - VIS, ISZS, ZKB - KII, ISZS, ZUI	4 kritická **	Může vést k přímému ohrožení či ztrátě života skupiny osob.	*žádné vodítko*	*žádné vodítko*	Může vést k závažnému, dlouhodobému narušení schopnosti vyšetřovat trestnou činnost, popřípadě zpochybnění soudních řízení a rozhodnutí (závažná kriminalita, celkové zpochybnění systému).	Může zapříčinit hromadné nepokoje, např. generální stávku, nebo jinak závažně narušit veřejný pořádek s celostátními dopady.	Může negativně ovlivnit nebo poškodit diplomatické vztahy a tím způsobit nevýhodu pro zájmy ČR.	Závažným způsobem může zasáhnout do fungování celé organizace a může vést až k ukončení činnosti.	Může závažně a dlouhodobě ovlivnit vztahy s jinými organizacemi nebo veřejností s následkem celostátní či nadnárodní negativní publicity, s dlouhodobými účinky a požadavky přijetí politické odpovědnosti.	Může přímo nebo nepřímo vést ke ztrátám přesahujícím 10 % ročního rozpočtu, popř. obratu organizace (v závislosti na typu organizace). Pozn. v případě KII je hranice ztráty stanovena na 0,5% HDP.	Může způsobit rozsáhlé omezení poskytování nezbytných služeb nebo jiného závažného zásahu do každodenního života postihujícího více než 125 000 osob.
Ostatní, ISVS, GDPR, ZKB - VIS, ISZS, ZKB - KII, ISZS, ZUI		Narušení bezpečnosti informací v oblasti "důvěrnosti" může způsobit újmu zájmům České republiky anebo nevýhodnost pro zájmy České republiky a zároveň je informace typově uvedena v seznamu utajovaných informací (§ 2 písm. a) zákona č. 412/2005 Sb.). Na základě tohoto dopadu by se za splnění dalších legislativně stanovených podmínek mělo jednat o utajované informace. Pro určení odpovídajícího stupně utajení je třeba postupovat v souladu se zákonem č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti. A to za splnění dalších stanovených podmínek, např. uvedených v nařízení vlády č. 522/2005 Sb.								

** V případě, že je v některém z parametrů bezpečnosti (dostupnost, důvěrnost, integrita) dosaženo max. úrovně dopadu "Vysoká", měl by správce zvážit zařazení informačního systému mezi významné informační systémy (VIS), případně mezi informační systémy základní služby (ISZS).*
- Podmínkou pro zařazení systému mezi VIS je současné naplnění definice v § 2 písm. d) zákona č. 181/2014 Sb., a alespoň jednoho oblastního kritéria podle přílohy č. 2 k vyhlášce č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích a zároveň alespoň jednoho dopadového kritéria uvedeného v § 4 vyhlášky č. 317/2014 Sb., o významných informačních systémech a jejich určujících kritériích.
- Podmínkou zařazení systému mezi ISZS je naplnění definice v § 2 písm. i) a j) zákona č. 181/2014 Sb., a současné naplnění odvětvových kritérií a alespoň jednoho dopadového kritéria uvedeného v příloze vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatelů základních služeb.

*** V případě, že je v některém z parametrů bezpečnosti dosaženo úrovně dopadu "Kritická", měl by správce zvážit zařazení informačního nebo komunikačního systému mezi prvky kritické informační infrastruktury (KII), případně mezi informační systémy základní služby (ISZS).*
- Podmínkou zařazení systému mezi KII je současné naplnění definice v § 2 písm. b) zákona č. 181/2014 Sb., a alespoň jednoho odvětvového kritéria v odvětví V1., oblasti G. Kybernetická bezpečnost podle přílohy k nařízení vlády č. 432/2010 Sb., a kritériích pro určení prvku kritické infrastruktury a zároveň alespoň jednoho průřezového kritéria uvedeného v § 1 nařízení vlády č. 432/2010 Sb., o kritériích pro určení prvku kritické infrastruktury.
- Podmínkou zařazení systému mezi ISZS je naplnění definice v § 2 písm. i) a j) zákona č. 181/2014 Sb., a současné naplnění odvětvových kritérií a alespoň jednoho dopadového kritéria uvedeného v příloze vyhlášky č. 437/2017 Sb., o kritériích pro určení provozovatelů základních služeb.

Poznámka ke sloupci „Ochrana osobních údajů":
Požadavky na zpracování osobních údajů v cloudových službách musí dle nařízení GDPR vycházet z hodnocení rizik daného scénáře zpracování pro práva a svobody fyzických osob. V případě zjištění vysokého rizika budou správci povinni provést tzv. „posouzení vlivu zpracování dat na ochranu osobních údajů" (DPIA, viz čl. 35), a zajistit adekvátní bezpečnostní opatření a mechanismy ochrany. Přitom předpokládáme využití některého ze schválených „kodexů chování" (viz čl. 40 GDPR) daným zpracovatelem a jeho cloudovou službou. Regulátor (ÚOOÚ) očekává, že do doby účinnosti nařízení GDPR bude schváleno několik kodexů chování, které vytvoří vhodný rámec standardizace pro vyšší úrovně dopadů zpracování osobních údajů.

Seznam použitých zkratek:
GDPR - nařízení Evropského parlamentu a Rady (EU) č. 2016/679 o ochraně fyzických osob v souvislosti se zpracováním osobních údajů a o volném pohybu těchto údajů a o zrušení směrnice 95/46/ES (obecné nařízení o ochraně osobních údajů)
ISVS - zákon č. 365/2000 Sb., o informačních systémech veřejné správy a o změně některých dalších zákonů
ISZS - informační systém základní služby podle § 2 písm. j) zákona č. 181/2014 Sb.
KII - kritická informační infrastruktura podle § 2 písm. b) zákona č. 181/2014 Sb.
PZS - provozovatel základní služby podle § 2 písm. k) zákona č. 181/2014 Sb.
ÚOOÚ - Úřad pro ochranu osobních údajů
VIS - významný informační systém podle § 2 písm. d) zákona č. 181/2014 Sb.
ZKB - zákon č. 181/2014 Sb., o kybernetické bezpečnosti a o změně souvisejících zákonů (zákon o kybernetické bezpečnosti)
ZUI - zákon č. 412/2005 Sb., o ochraně utajovaných informací a o bezpečnostní způsobilosti