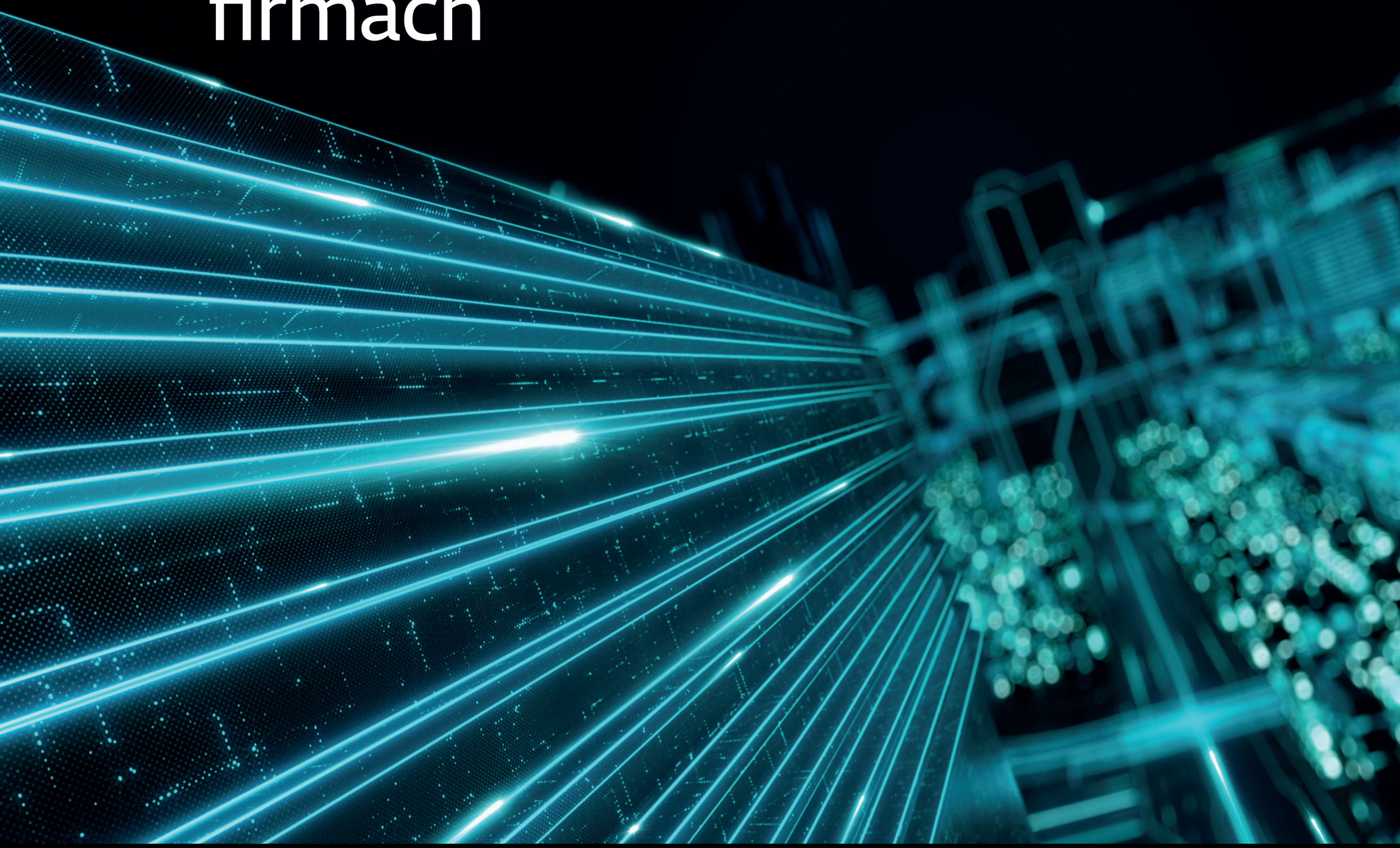
ENJOY SAFER TECHNOLOGY™

OCHRANA DAT

v malých a středně velkých firmách



kapitola 3

Posouzení rizik zabezpečení údajů

V této kapitole

- Proces posouzení rizika
- Identifikace operací zpracování údajů
- Vyhodnocení potenciálního dopadu úniku dat
- Identifikace možných hrozeb ochrany údajů
- Vyhodnocení rizika pomocí matice

Kapitola 3

POSOUZENÍ RIZIK ZABEZPEČENÍ ÚDAJŮ

V této kapitole se dočtete, jak aplikovat postupy pro řízení rizika na zabezpečení údajů.

Posouzení rizika

Posouzení rizika je první fází v postupu řízení rizika a skládá se z:

- Identifikace aktiv (hmotných i nehmotných)
- Analýzy hrozeb (včetně dopadu a pravděpodobnosti)
- Posouzení zranitelnosti (tj. jaké kontroly jsou nedostatečné nebo zcela chybí)

Obdobně, posouzení rizik zabezpečení údajů potom obsahuje:

- Identifikaci operací zpracování údajů (jak a kde se dané údaje v rámci vaší firmy používají)
- Vyhodnocení potenciálního dopadu na firmu (pokud dojde ke kompromitaci dat)
- Identifikaci možných hrozeb a vyhodnocení pravděpodobnosti (výskytu, včetně frekvence)
- Vyhodnocení rizika (pro posouzení, jaké kontrolní mechanizmy by měly být implementovány)

Krok 1:
Identifikace operací zpracování údajů

Údaje v rámci společnosti mají různé rizikové profily, které nejsou založené jen na obsahu dat, ale také na tom, jakým způsobem s daty daná společnost pracuje. Dříve než začnete posuzovat rizika, je důležité, abyste porozuměli, jakým způsobem se údaje v rámci vaší firmy zpracovávají. V typicky malé nebo střední firmě se obvykle jedná o následující operace, které se týkají:

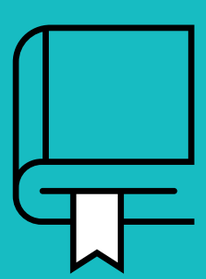
Lidských zdrojů, jako je správa výplat, přijímání nových a udržení stávajících zaměstnanců, záznamy o školení, vyhodnocení pracovních výsledků a podobně.

Správy zákazníků a dodavatelů, což jsou informace o zákaznících, objednávkách, fakturách, seznamy e-mailových adres, údaje pro marketing nebo smlouvy s prodejci.

Bezpečnosti zaměstnanců a fyzického zabezpečení, jako jsou různé bezpečnostní protokoly o aktivitě zaměstnanců, záznamy o návštěvách, video monitorování atd.

U každé operace zpracování údajů si položte následující otázky:

- Jaké osobní údaje se zpracovávají?
- Za jakým účelem se zpracovávají?
- Kde zpracovávání probíhá?
- Kdo je za zpracování odpovědný?
- Kdo má k údajům přístup?



Zásada minimálních práv je osvědčený postup, kdy je koncovým uživatelům udělena pouze minimální úroveň přístupu nezbytná pro výkon jejich konkrétní pracovní funkce.

Krok 2:
Vyhodnocení potenciálního dopadu na firmu

Dále musíte určit potenciální dopad kompromitace nebo porušení ochrany údajů na firmu. Porušení nebo kompromitace může mít vliv na důvěrnost dat (například neoprávněný přístup), jejich integritu (například neoprávněná modifikace) nebo na dostupnost (například ransomwarový útok).

Společnosti musí chránit důvěrnost, integritu a dostupnost údajů. V informační bezpečnosti se to označuje jako C-I-A diagram (viz kapitola 2).

Typicky je potenciální dopad daného rizika obvykle vyjádřen ve smyslu škody, kterou by společnost utrpěla, jako je ztráta nebo zničení fyzického aktiva (server, kopírka nebo vozidlo atd.)

- Dopad na firmu může být i nepřímý. V případě citlivých osobních údajů je totiž subjekt (např. zákazník), jehož údaje byly odcizeny nebo kompromitovány, přímou obětí. V takových případech může být ukradena identita nebo finanční aktivum jednotlivce a /nebo napadeno jeho soukromí. Dopad na firmu je méně přímý, ale i tak potenciálně velmi nákladný a může mimo jiné zahrnovat:
- Ztrátu zákazníků a příjmu
- Poškození značky a negativní PR
- Regulační pokuty a soudní spory
- Náklady spojené s oznámením úniku údajů
- Forenzní analýzy a obnovy

TIPY

Dopad na firmu může být klasifikován jako nízký, střední nebo vysoký. Nicméně konkrétní definice úrovně dopadu bude jedinečná pro každou firmu a měla by obsahovat jak objektivní (kvantitativní), tak subjektivní (kvalitativní) opatření.

Krok 3
Identifikace možných hrozeb a vyhodnocení pravděpodobnosti

Hrozbou mohou být jakékoliv události nebo okolnosti, přírodní nebo uměle vytvořené, které mohou negativně ovlivnit důvěrnost, integritu a dostupnost osobních nebo citlivých dat. Může jít o kybernetické útoky, náhodné ztráty nebo krádeže firemních IT zařízení, interní hrozby, požáry a záplavy, zemětřesení, vlivy extrémního počasí, pracovní spory a podobně. Firmy musí identifikovat možné hrozby a vyhodnotit pravděpodobnost (včetně frekvence výskytu). Musíte mít jistotu, že máte hrozby zařazeny do konkrétně definovaných oblastí, včetně hrozeb ze síťových a technických zdrojů (software/ hardware), souvisejících procesů a postupů, lidských zdrojů a hrozby vyplývající z rozsahu zpracování.

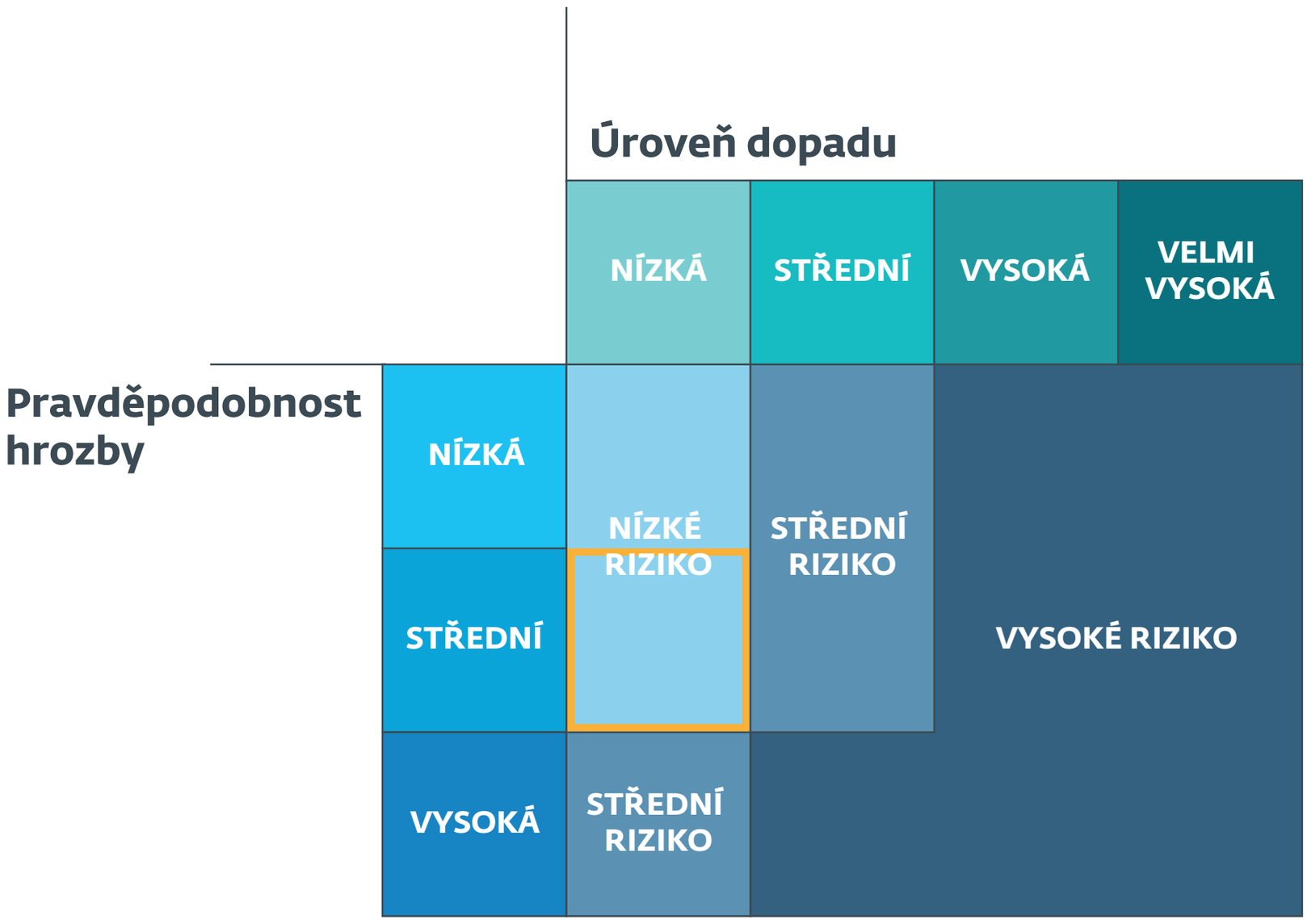
TIPY

Pro každou identifikovanou hrozbu můžete pravděpodobnost klasifikovat obdobným způsobem jako u dopadu na firmu: nízká, střední a vysoká. Při vyhodnocování pravděpodobnosti výskytu hrozby je potřeba zvážit jak pravděpodobnost výskytu hrozby obecně, tak i to, jak často je pravděpodobné, že se hrozba vyskytne během určité doby (například během jednoho roku).

Krok 4
Vyhodnocení rizika

Jako poslední budete hodnotit riziko spojené s každou operací a v závislosti na výsledku hodnocení implementovat vhodné technologické kontrolní mechanizmy a organizační postupy.

Obrázek 3-1 zobrazuje obecnou šablonu pro vyhodnocení rizika a příklad vyhodnocení vybrané operace zpracování dat.



Pravděpodobnost hrozby

Pro konkrétní operaci zpracování projděte seznam možných hrozeb a vyhodnoťte jejich pravděpodobnost. Výsledná pravděpodobnost by měla být součtem hodnot ze všech hrozeb ze seznamu.

- **Nízká** – Není pravděpodobné, že hrozba nastane.
- **Střední** – Je důvodná šance, že hrozba nastane.
- **Vysoká** – Je pravděpodobné, že hrozba nastane.

Úroveň dopadu

Pro konkrétní operaci zpracování vyhodnoťte možný dopad na důvěrnost, integritu a dostupnost dat (C-I-A diagram). Výsledná úroveň dopadu je nejvyšší dopad ze tří.

- **Nízká** – Drobné obtíže, které lze bez problému překonat.
- **Střední** – Zásadní obtíže, které lze překonat i přes několik nesnází.
- **Vysoká** – Zásadní důsledky, které lze překonat, ale s vážnými obtížemi.
- **Velmi vysoká** – Zásadní nebo dokonce nezvratné důsledky, které nelze překonat.

Výsledná úroveň rizika

- **Nízká**
- **Střední**
- **Vysoká**

Příklad

Operace zpracování: Marketing/Reklama
Zpracovávané údaje: Kontaktní údaje (např. jméno, poštovní adresa, telefonní číslo, e-mail)
Klasifikace údajů: Osobní údaje
Účel zpracování: Propagace zboží a speciálních nabídek potenciálním zákazníkům
Subjekty údajů: Zákazníci

Pravděpodobnost hrozby

Síťové a technické zdroje (HW, SW): Střední
Procesy a postupy: Nízká
Zúčastněné lidské zdroje: Střední
Obchodní oddělení a rozsah zpracování: Střední
Výsledná pravděpodobnost: Střední

Úroveň dopadu

Posouzení úrovně dopadu na důvěrnost: nízká; na integritu: nízká; na dostupnost: nízká
Výsledná úroveň dopadu: Nízká

Výsledná úroveň rizika:

- **Nízké riziko** – zpracování dat pro marketing/reklamu představuje nízké riziko, měli byste implementovat odpovídající technická a organizační opatření.

Obrázek 3-1: Matice posouzení rizik pro operace zpracování dat