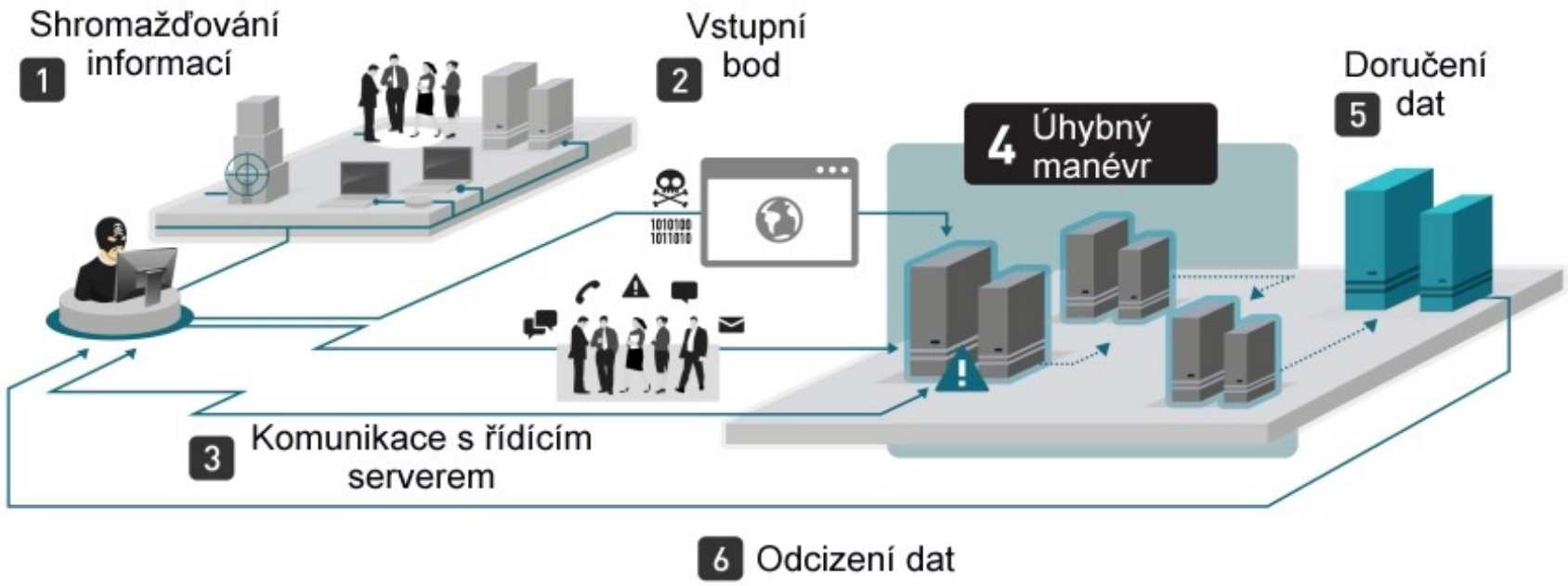
GORDIC®

Posuzování na základě rizika

Ing. Jaroslav Balcar, MBA, LL.M.

Obecné schéma sofistikovaných kybernetických útoků



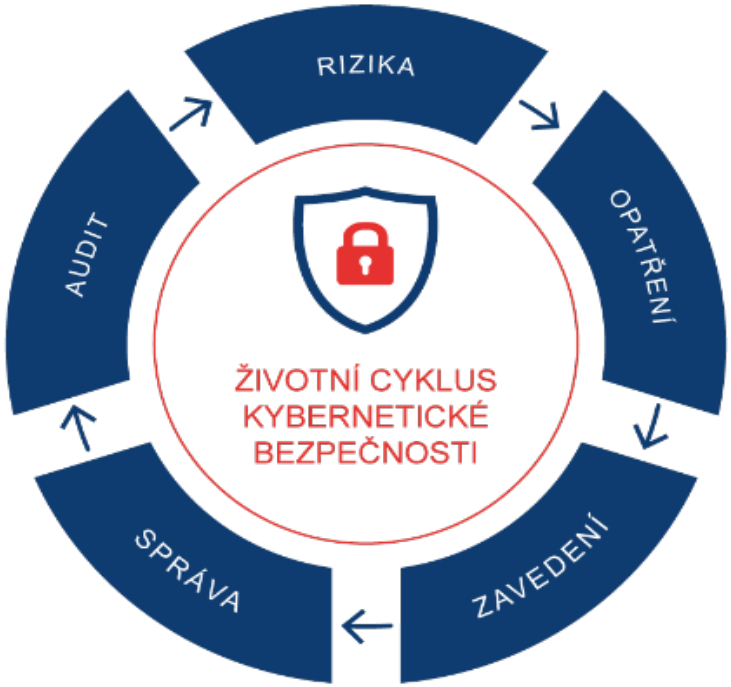
Hlavní principy:

- **Informovanost** - o potřebě bezpečnosti
- **Odpovědnost** - nést osobní odpovědnost
- **Reakce** - jednat včas a vzájemně spolupracovat
- **Hodnocení rizik** - provádět hodnocení rizik
- **Dopad na SÚ** – hodnocení rizik pro SÚ způsobených únikem
- **Návrh a implementace bezpečnosti** - zahrnout mezi základní prvky informačních systémů a sítí
- **Management bezpečnosti** - komplexní přístup
- **Opětovné hodnocení** - opětovně hodnotit bezpečnost informačních

Vše souvisí se vším

Obecné principy kybernetické bezpečnosti

Pro naplnění požadavků legislativy je vhodné vycházet z obecného modelu Demingova cyklu, definuje záměry a cíle, organizační a řídící strukturu, technická opatření, procesní integraci a dokumentační strukturu.

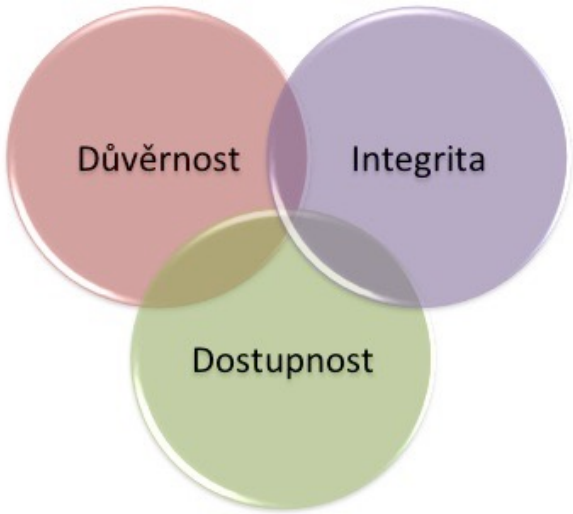


Rozdělení aktiv:

- **Primárním aktivem** se rozumí informace nebo služba, kterou zpracovává nebo poskytuje informační systém …
- **Podpůrným aktivem** se rozumí technické aktivum, zaměstnanci a dodavatelé podílející se na provozu, rozvoji, správě nebo bezpečnosti informačního systému …
- **Technickým aktivem** se rozumí technické vybavení, komunikační prostředky a programové vybavení informačního systému …

Hodnocení aktiva garanty aktiv:

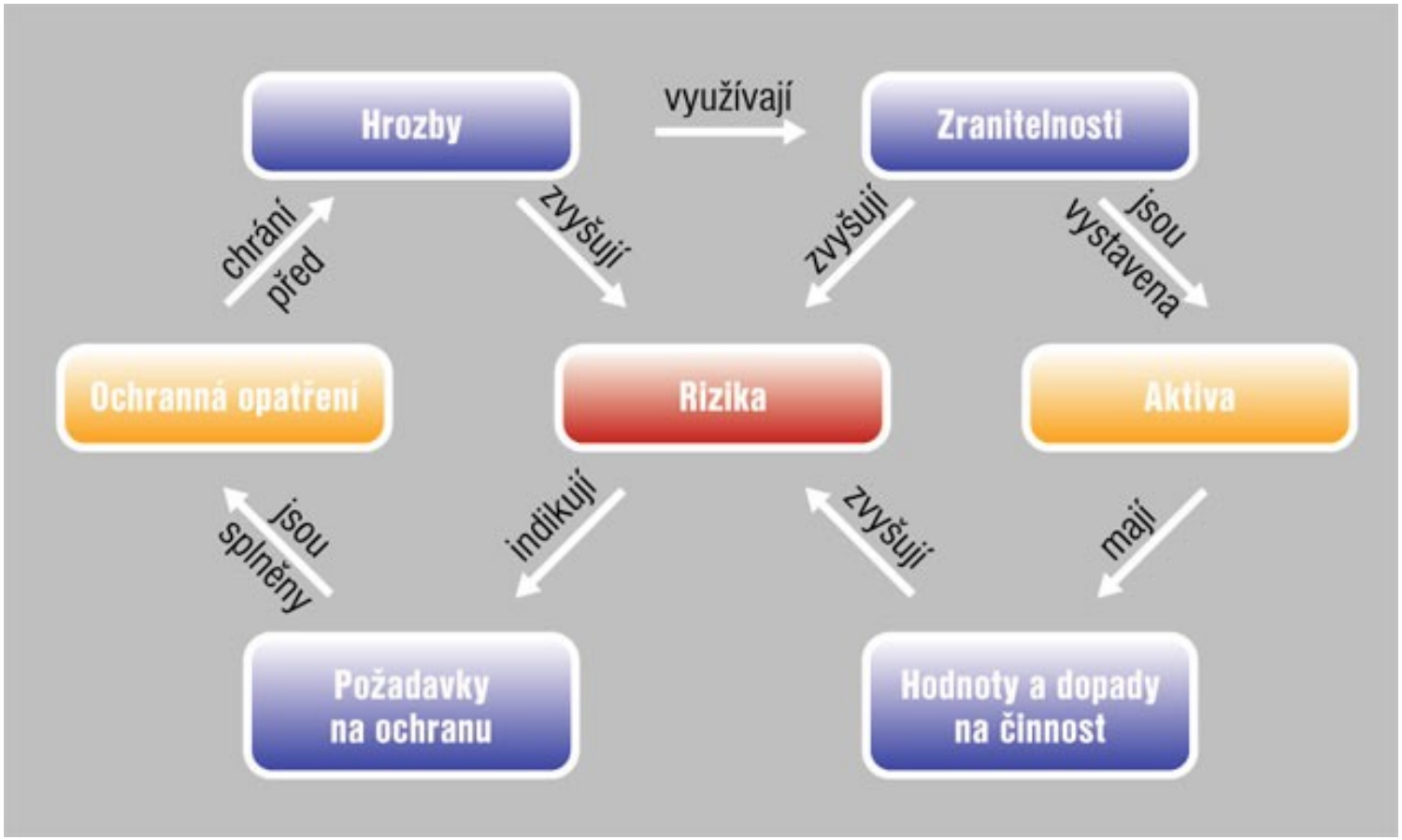
- **Důvěrnost:** k informacím mají přístup pouze oprávněné osoby
- **Integrita:** je zajištěna správnost a úplnost informací a jsou jasně stanoveny pravomoci a práva k pozměňování informací.
- **Dostupnost:** data a jiné z okamžiku jejich potřeby.
- **GDPR požaduje také odolnost systémů a služeb zpracování?**



Definice pojmů:

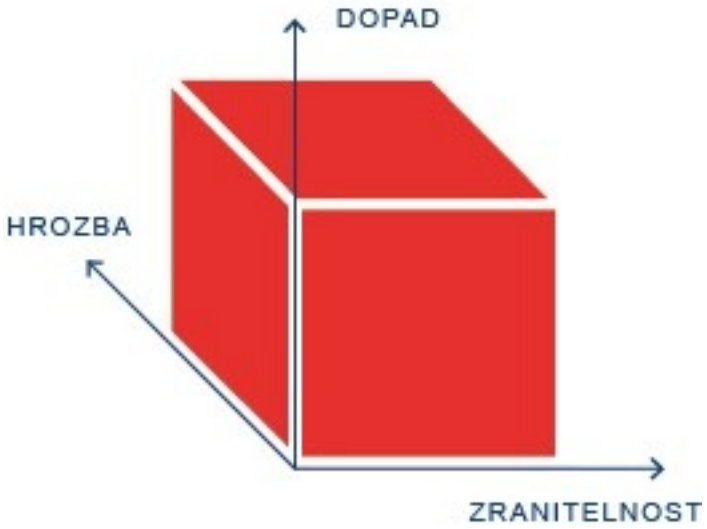
- **Rizikem** se rozumí možnost, že určitá hrozba využije zranitelnosti informačního systému kritické informační infrastruktury, komunikačního systému kritické informační infrastruktury nebo významného informačního systému a **způsobí poškození aktiva**
- **Hodnocením rizik** se rozumí proces, při němž je určována významnost rizik a jejich přijatelná úroveň

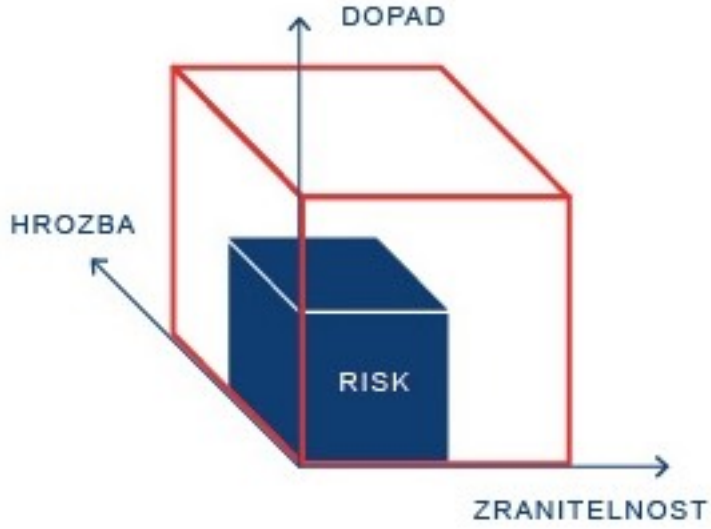
Aktiva a analýza rizik



Implementace bezpečnostních opatření přináší:

- Snížení hrozeb, kterým musí organizace čelit
- Snížení rozsahu negativních dopadů
- Snížení míry zranitelnosti organizace





Článek 32 Zabezpečení zpracování

1. S přihlédnutím ke stavu techniky, nákladům na provedení, povaze, rozsahu, kontextu a účelům zpracování i k různě pravděpodobným a různě závažným rizikům pro práva a svobody fyzických osob, provedou správce a zpracovatel vhodná technická a organizační opatření, aby zajistili úroveň zabezpečení odpovídající danému riziku, případně včetně:

a) pseudonymizace a šifrování osobních údajů;

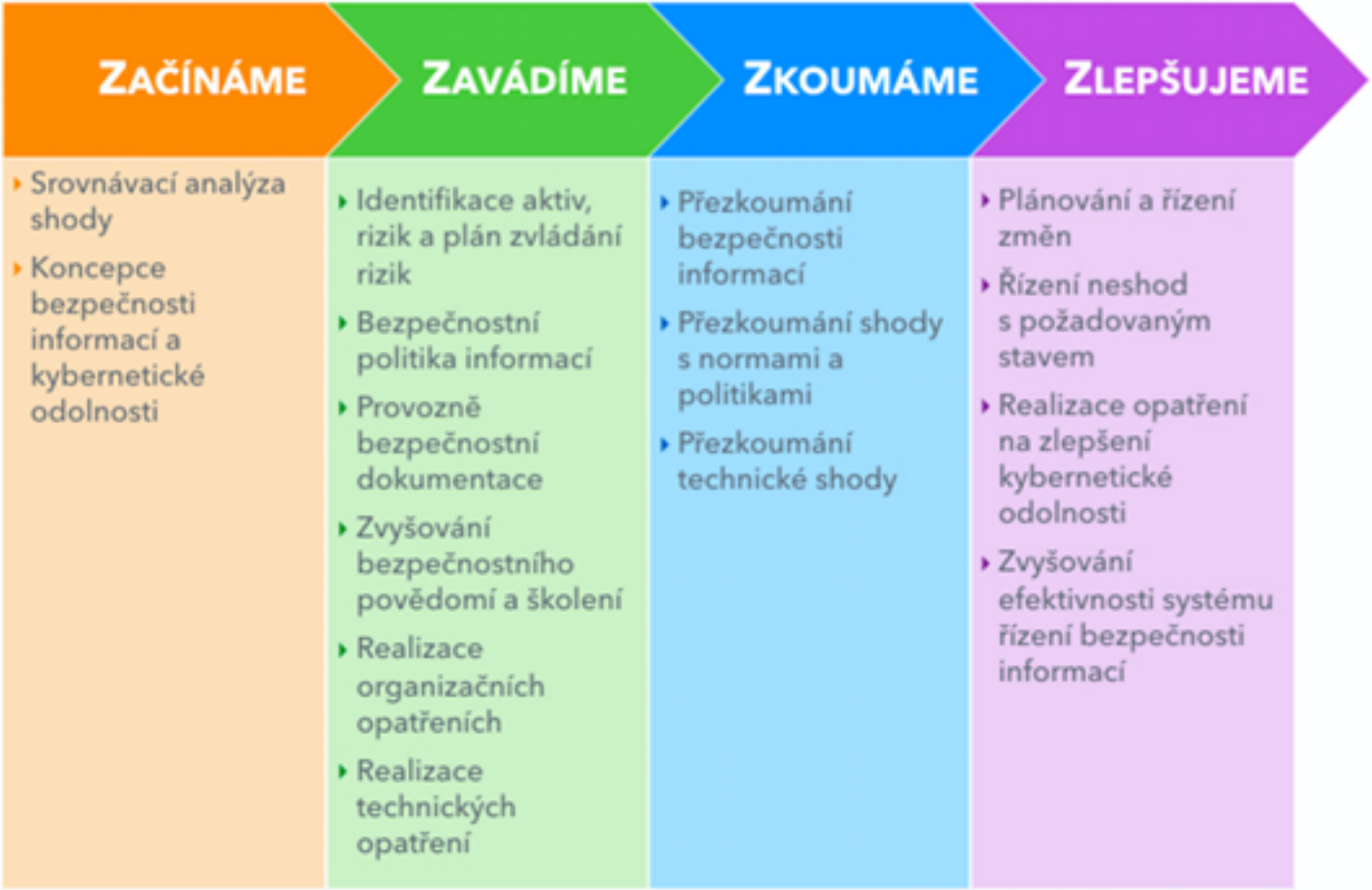
b) … důvěrnost, integritu, dostupnost a odolnost systémů a služeb zpracování;

d) procesu pravidelného testování, posuzování a hodnocení účinnosti zavedených technických a organizačních opatření pro zajištění bezpečnosti zpracování.

Článek 35 Posouzení vlivu na ochranu osobních údajů

1. Pokud je pravděpodobné, že určitý druh zpracování, zejména při využití nových technologií, bude s přihlédnutím k povaze, rozsahu, kontextu a účelům zpracování bude mít za následek **vysoké riziko pro práva a svobody fyzických osob,** provede správce před zpracováním posouzení vlivu zamýšlených operací zpracování na ochranu osobních údajů. Pro soubor podobných operací zpracování, které představují podobné riziko, může stačit jedno posouzení.

GORDIC® | Konsolidace SŘBI, ZoKB a GDPR



GORDIC®

Děkujeme za pozornost

KYBEZ Platforma kybernetické bezpečnosti