Univerzita Karlova

# Kyberbezpečnost by design

## Od jednotlivých systémů k řízení změn celé organizace

**Marek Kalika, Jakub Malina**
Univerzita Karlova

Digitální transformace univerzit 2026 | 9. 9. 2026

# Úvod - Proč nestačí řešit bezpečnost až na konci

**Dnešní stav:**

- bezpečnost když je, tak jako „dodatečný doplněk“
- penetrační test týden před spuštěním, pokud to není přímo start živého provozu
- nejasné odpovědnosti za data, kde vždy je odpovědný ten druhý

**Dopady:**

- vyšší náklady na provoz, opravy, změny, úpravy
- zpoždění projektu
- nesoulad s legislativou, NIS2
- bezpečnostní incidenty

---

**Hlavní myšlenka – „**Nejlevnější zranitelnost je ta, která nikdy nevznikne“

Univerzita Karlova

# Kde začíná „by design“?

**Při programování? Při technickém návrhu? Při analýze? V jaké fázi?**


Řízené rozhodování o změně začíná už **zachycením podnětu a záměru.**

---

**Security by Design začíná v prvním okamžiku, kdy lze charakter změny ještě ovlivnit.**

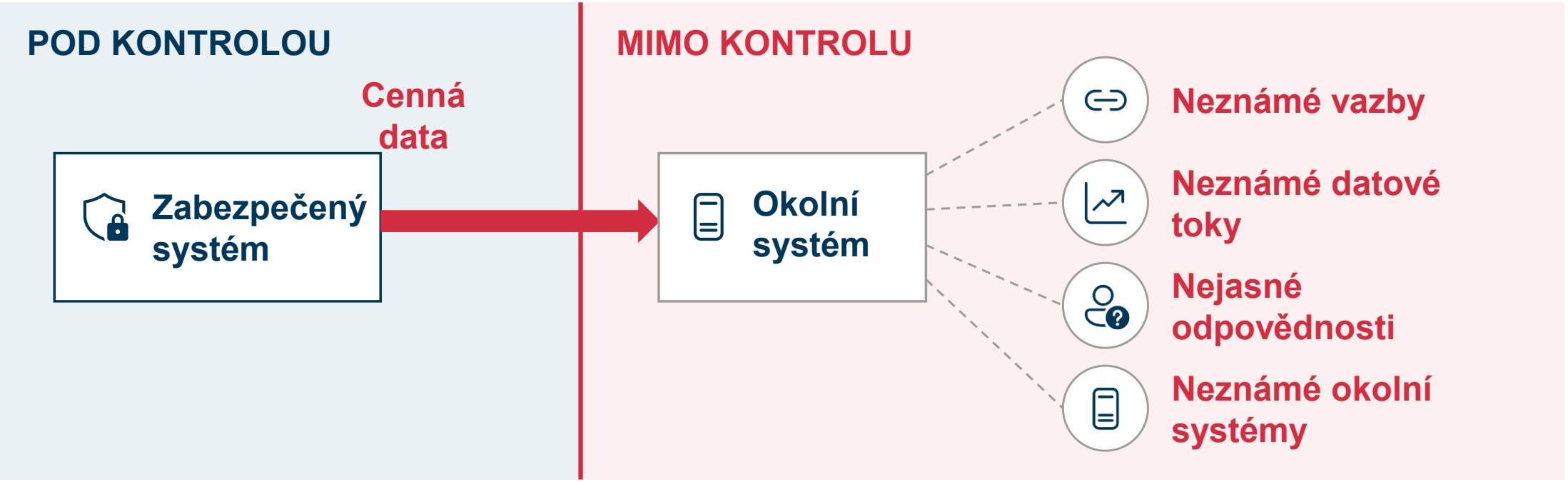
Univerzita Karlova

# Bezpečnost není jediný legitimní požadavek


**Cílem není izolovaně maximalizovat jeden požadavek, ale přijmout vědomé, zdůvodněné a kontrolovatelné rozhodnutí.**

Univerzita Karlova

# Izolovaně bezpečný systém nestačí




**Lokální optimum není bezpečnost organizace.**

Univerzita Karlova

# Projekt jako zásah do fungování univerzity


**Enterprise architektura umožňuje vidět projekt jako zásah do fungování univerzity, nikoliv jako samostatný seznam úkolů.**

# Projektů mnoho a portfolio nikde?

## VÝCHOZÍ STAV

- projekty vznikající na různých místech
- rozdílná úroveň popisu a připravenosti
- obtížně porovnatelné priority
- nejasné souhrnné kapacitní nároky
- slabě viditelné duplicity a závislosti

## BUDOVANÁ SCHOPNOST

- společná evidence
- jednotné projektové karty a metadata
- fáze a přechody na další stupeň
- společné posouzení priorit a dopadů
- vazba na enterprise architekturu

Přibližně **200** centrálních projektových položek a záměrů v Akčním plánu IT.

Univerzita Karlova

# Jak se ze seznamu stává portfolio

Mapování změn → Konsolidace položek → Projektová karta → Společná metadata → Odborné a kapacitní posouzení → Rozhodnutí o portfoliu

## PROJEKTOVÁ KARTA: STANDARDIZOVANÝ INFORMAČNÍ VSTUP

- motivace a řešený problém
- vlastnictví a odpovědnosti
- legislativa a termíny
- dotčené agendy, data a aplikace
- náklady a kapacity
- rizika a závislosti

**Portfolio nevzniká sepsáním projektů. Vzniká jejich společným posouzením, prioritizací a rozhodováním.**

Univerzita Karlova

# Metadata strukturují rozhodování

## PRIORITA

- termíny
- legislativní tlak
- význam pro věcné vlastníky

## KOMPLEXITA

- rozsah a kapacity
- počet zapojených stran
- náročnost realizace

## ARCHITEKTONICKÝ DOPAD

- průřezovost
- dopad na agendy, data a aplikace
- význam pro klíčové celky

**Ukazatele poskytují společný podklad. Nerozhodují místo lidí.**

# Rozhodování: stejná logika, přiměřený rozsah

| 1. PODKLADY | 2. POSOUZENÍ | 3. ROZHODNUTÍ | 4. AKTIVACE DALŠÍ FÁZE |
|---|---|---|---|
| • výstupy fáze<br>• metadata projektu<br>• rizika, dopady a závislosti | → • připravenost<br>• naplnění požadavků<br>• dostupnost kapacit<br>• smysluplnost dalšího postupu | → • pokračovat<br>• pokračovat s podmínkami<br>• doplnit nebo přepracovat<br>• pozastavit, sloučit či ukončit | → • potvrzení odpovědností<br>• přidělení kapacit<br>• stanovení podmínek<br>• zahájení dalších prací |

**PŘIMĚŘENOST** →

Projekty malého rozsahu a/nebo komplexity

Komplexní, prioritní a architektonicky významné projekty

**Rozsah podkladů a posouzení odpovídá fázi, povaze, komplexitě, dopadu a rizikům projektu.**

# Každý přechod fáze rozhoduje o dalších podmínkách

**Právě zde se Security by Design stává součástí skutečného řízení změn.**

**KYBERBEZPEČNOST | OCHRANA OSOBNÍCH ÚDAJŮ | EA | DATA | LEGISLATIVA | AI**

| podnět | záměr | analýza a příprava zadání | příprava realizace | realizace | vyhodnocení | provoz |
|---|---|---|---|---|---|---|
| **Má smysl podnět rozpracovat?** | **Má změna vlastníka, účel a prioritu?** | **Víme, co a za jakých podmínek realizovat?** | **Je realizace připravena a zajištěna?** | **Jsou výstupy připraveny k ověření a akceptaci?** | | **PŘEVZETÍ DO PROVOZU** **Je řešení dlouhodobě provozuschopné?** |
| Aktivujeme: rozpracování záměru | Aktivujeme: analytika a podle potřeby technického vlastníka | Aktivujeme: projektového manažera a přípravné kapacity | Aktivujeme: interní vývoj, dodavatele, projektový tým a finance | Aktivujeme: QA, akceptaci a přípravu ukončení projektu | | Aktivujeme: provozní odpovědnosti, podporu, dohled a provozní rozpočet |

Rozsah zapojení jednotlivých oblastí odpovídá fázi a charakteru projektu.

**Portfolio řídí priority, připravenost projektů i přidělování limitů a kapacit.**

# Nejsme v cíli. Budujeme podmínky.

## CO UŽ MÁME

- společný přehled projektových změn
- jednotnou projektovou informaci
- fáze a rozhodovací brány
- společné prioritizační fórum
- vazbu portfolia na enterprise architekturu
- řízení kapacit a odpovědností

## CO MUSÍME DOPLNIT

- jednotná kritéria bezpečnostního posouzení
- systematické zapojování odborných rolí
- architektonická a datová pravidla
- projektový reporting
- programové a strategické řízení oblastí
- průběžné vyhodnocování přínosů a rizik

**Bezpečnost by design není checklist na konci projektu. Je to schopnost organizace klást správné otázky a přijímat odpovědná rozhodnutí ve správný čas.**


# Děkujeme za pozornost!

**Marek Kalika**
**Jakub Malina**

Ústav výpočetní techniky
Univerzita Karlova

Petrská 3, 116 36 Praha 1

marek.kalika@ruk.cuni.cz
jakub.malina@ruk.cuni.cz
**www.cuni.cz**

Univerzita Karlova