ProID

# Kryptografie v organizaci a nejčastější chyby v nastavení

**Ing. David Říhošek**
ProID by Monet+

solutions by MONET+

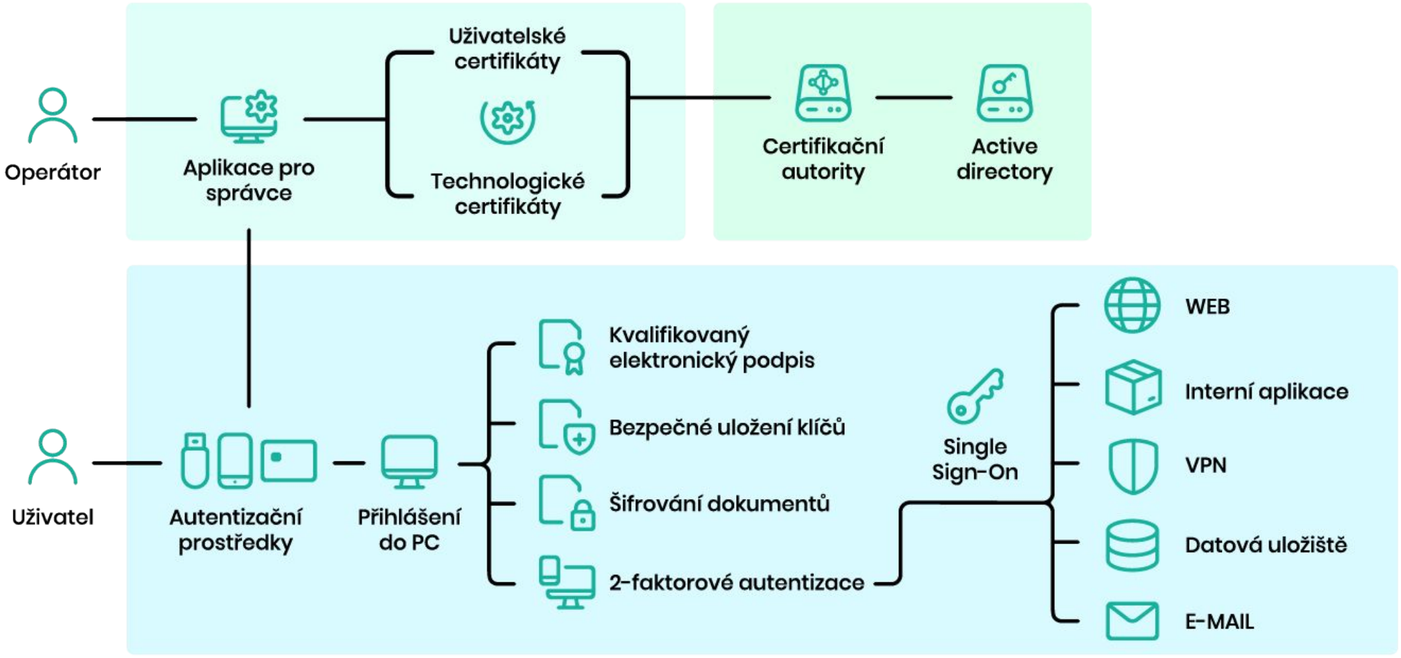
# 80 %

organizací používá ke správě digitálních klíčů doménové certifikační autority a PKI.
Nerozumí jim však, nemají je správně nastavené a neumí je spravovat.

**To znamená potenciální bezpečnostní riziko.**

# Kryptografie a bezpečnost v praxi

- Práce s kryptografickým materiálem zajišťuje Certifikační autorita a PKI infrastruktura.
- Tu je třeba vybudovat a doplnit o nástroje pro koncové uživatele.
- Administrátoři pak potřebují aplikace pro správu životního cyklu certifikátů a klíčů.



# Jak vypadá organizace

## před zavedením produkčního PKI

solutions by MONET +

# Před produkčním provozem PKI

- Bez PKI, Bez CA
- Testovací CA
  - Velké množství šablon certifikátů
  - Vydané testovací certifikáty
  - Většinou se nevyužívá odvolání certifikátů
  - Z části nedostupné CRL/AIA
  - Bez konsolidace oprávnění uživatelů i správců
  - Bez údržby
  - Bezpečnostní riziko
- Nepovedený decommissioning
  - Pouze vypnutí stroje

# Nejčastější chyby,

## se kterými se setkáváme v praxi při řešení projektů

solutions by MONET +

# Digitální klíče a certifikáty

- Používání nepodporovaných kryptografických algoritmů
- Používání nepodporovaných délek šifrovacích klíčů
- Publikace šablon certifikátů, podle kterých se však nevydává žádný certifikát
- Nefunkční nebo nedostupná cesta k certifikátu certifikační autority (AIA/CRL)
- Nezajištěné privilegované účty (oprávnění pro správu certifikační autority/správu šablon/žádostí o certifikáty atd.)
- Dodržování vydaných doporučení
- Aktualizace systémů

# Uložení kryptografického materiálu a certifikátů

- Digitální certifikáty a klíče jsou ukládány do málo zabezpečených úložišť
  - Vždy je třeba zvážit pro a proti
- Certifikační autority nejsou dostatečně odděleny od zbytku sítě, popřípadě nemají vícevrstvou architekturu tam, kde je to třeba
- Kořenové certifikační autority nejsou dostatečně chráněny
- Není zajištěna fyzická bezpečnost CA a striktní přístupová oprávnění pro správce CA
- Chybějící notifikace končící platnosti certifikátů, možnost expirace

# Ochrana záloh operačních systémů

- Ochrana privátních klíčů v úložišti systému
- Zálohy je třeba chránit stejně nebo i důkladněji jako primární systémy
- Virtualizace, správce virtualizační platformy, správce záloh
- Fyzická bezpečnost

# Autentizace a ochrana přístupů

solutions by MONET +

# Nastavení oprávnění, sdílené účty

- Správci používají sdílené uživatelské/administrační účty
- Správcovské účty administrátorů mohou být chráněny méně než uživatelské účty
- Oprávnění jsou nastavena na konkrétní účty místo skupin
- Jeden správcovský účet má oprávnění napříč všemi systémy organizace

# Slabá hesla a nechráněné přístupy

- Zaměstnanci používají slabá, snadno prolomitelná hesla.
- Používají stejné heslo do více systémů zároveň.
- Hesla různě sdílejí – přeposílají e-mailem, píšou si je na papírek u počítače apod.
- U dokumentů se nepoužívá elektronický podpis
- Nešifruje se připojení do VPN, firemních systémů a sítí

# Dvoufaktorová autentizace v nezabezpečených počítačích

- Vynucené používání dvoufaktorového přihlášení pro uživatele
- Zadní vrátka pro správce
  - Vzdálené přístupy
  - Používání hesel
  - Doménová politika
  - Key logger
- Záložní přístup pro případ výpadku PKI

# Dokumentace a bezpečnostní politiky

- V organizacích často chybí dokumentace a zpracované postupy
  - Bezpečnostní
  - Havarijní
  - Provozní
- Nejsou definovány bezpečnostní politiky
- Nejsou definovány role a zodpovědnosti, např. **Manažer bezpečnosti, Správe domény** atd.

# S čím vám rádi pomůžeme

- Provést revizi PKI případně provést řízené odstavení a vybudovat nové PKI.
  - Aplikace doporučených změn
- Zavedení nástrojů pro bezpečné přihlašování a ověřování identity uživatelů a správců
- Soulad s doporučeními vydanými důvěryhodnými autoritami, správné používání kryptografických klíčů a digitálních certifikátů.
- Revize bezpečnostních plánů a politik.


solutions by MONET +

# Děkuji!

Potřebujete vyřešit kyberbezpečnost
ve vaší organizaci?

**Kontaktujte nás.**

**www.proid.cz | info@proid.cz**