




IAM



Identita & přístup: proč na IAM záleží?

Mario Minarovský
CREDIBILIS

Agenda

1. Prečo IAM
2. Základy a pojmy
3. Prepojenia, väzby
4. Implementácia & metriky
5. Q&A





IAM (Identity & Access Management)

- Súbor procesov, politík a technológií na správu identít a prístupov
- Zahŕňa
 - Identita (kto som)
 - Autentifikácia (ako to dokážem)
 - Autorizácia (čo smiem)
 - Audit (čo som urobil)
- Nezahŕňa
 - Len "IT nástroj" – je to organizačná schopnosť
 - Jednorazový projekt – je to nepretržitý cyklus



Prečo IAM práve teraz

- Cloud, hybrid a SaaS rozptýlili perimetrickú bezpečnosť
- Práca odkiaľkoľvek a dodávateľské reťazce zvyšujú riziko
- Regulácie a audity vyžadujú preukázateľné riadenie prístupov
- Identita je nová perimetrická hranica (Zero Trust)



Kľúčové domény IAM

IGA – Identity Governance & Administration

- Životný cyklus (Joiner–Mover–Leaver)
- Certifikácie prístupov, SoD

AM – Access Management

- SSO, MFA, adaptívna autentifikácia
- Politiky – RBAC/ABAC

PAM – Privileged Access Management

- Trezor účtov, schvaľovanie, session recording



IAM × kyberbezpečnosť

- Zero Trust: veríme až po overení; neustála verifikácia kontextu
- Least privilege & just-in-time prístup namiesto trvalých práv
- Detekcia a reakcia: logy z IAM sú zdroj pre SOC a foreznu analýzu
- Zníženie priestor na útok: MFA, passwordless, segmentácia prístupu



IAM × fyzická bezpečnosť (converged security)

- Prepojenie digitálnych identít s prístupom do budov (PACS)
- Jednotný JML: odchod = zrušenie IT aj dverových práv
- Zdieľané princípy: identita, autentifikácia (badge/biometria), audit
- Scenáre: návštevy, dodávatelia, 24/7 prevádzky, citlivé zóny



Najčastejšie chyby v IAM

- Práva sa iba pridávajú – chýba odobranie a recertifikácia
- Trvalé privilegované účty bez schvaľovania a monitoringu
- Viacero zdrojov o identite (HR, Excel, manuál)
- Jednorazový projekt bez vlastníkov procesov



Normy & rámce

- ISO/IEC 27001/27002: identita, autentifikácia, správa prístupov (Annex A)
- NIST SP 800-63 (digitálna identita), NIST SP 800-53 (AC, IA domény)
- NIS2: riadenie rizík, identita a prístupy ako povinné opatrenia
- GDPR: minimalizácia, nevyhnutnosť prístupu, auditovateľnosť



Rýchly plán implementácie (90 dní)

1. Základy

- ✓ Zdroj údajov (HR/ERP) a JML proces
- ✓ Mapovanie aplikácií & rizík

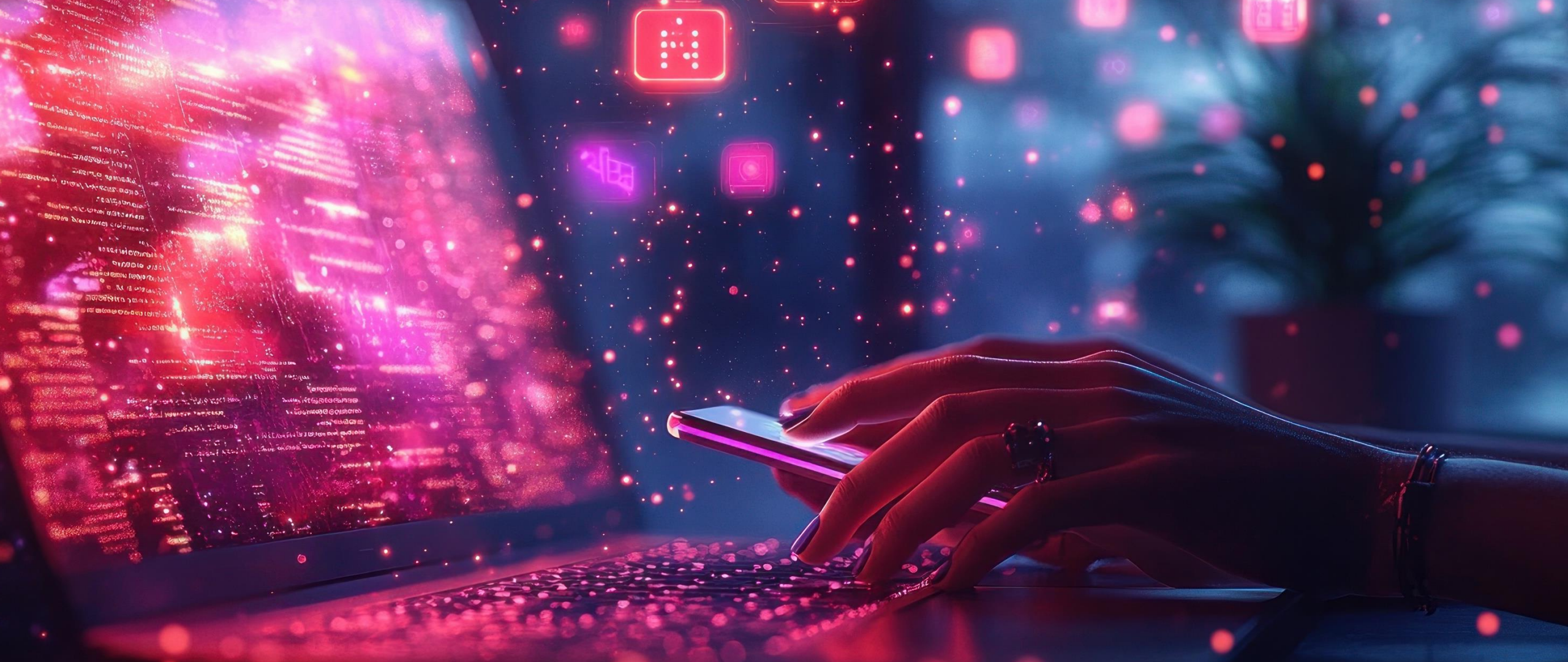
2. Kontroly

- ✓ MFA pre všetkých, SSO pre kľúčové systémy
- ✓ Privilegia: trezor + JIT

3. Správa

- ✓ Role/RBAC pre 3–5 kľúčových tímov
- ✓ Prvá recertifikácia prístupov





Záver

Zhrnutie & odporúčania

- Identita je nový perimetr – IAM je strategická schopnosť
- Začnite s ľuďmi a procesom, technológia je až tretia
- MFA, SSO, JML a PAM prinášajú rýchly prínos
- Zladte IAM s ISO 27001/NIS2 a fyzickou bezpečnosťou





DISKUSIA.



**Ďakujem za Vašu pozornosť.
info@credibilis.sk**

