



# Zkušenosti MSK se ZKB a ISO 27001

Zpracoval(a): Pavel Žák

Datum: X. XX. 2023

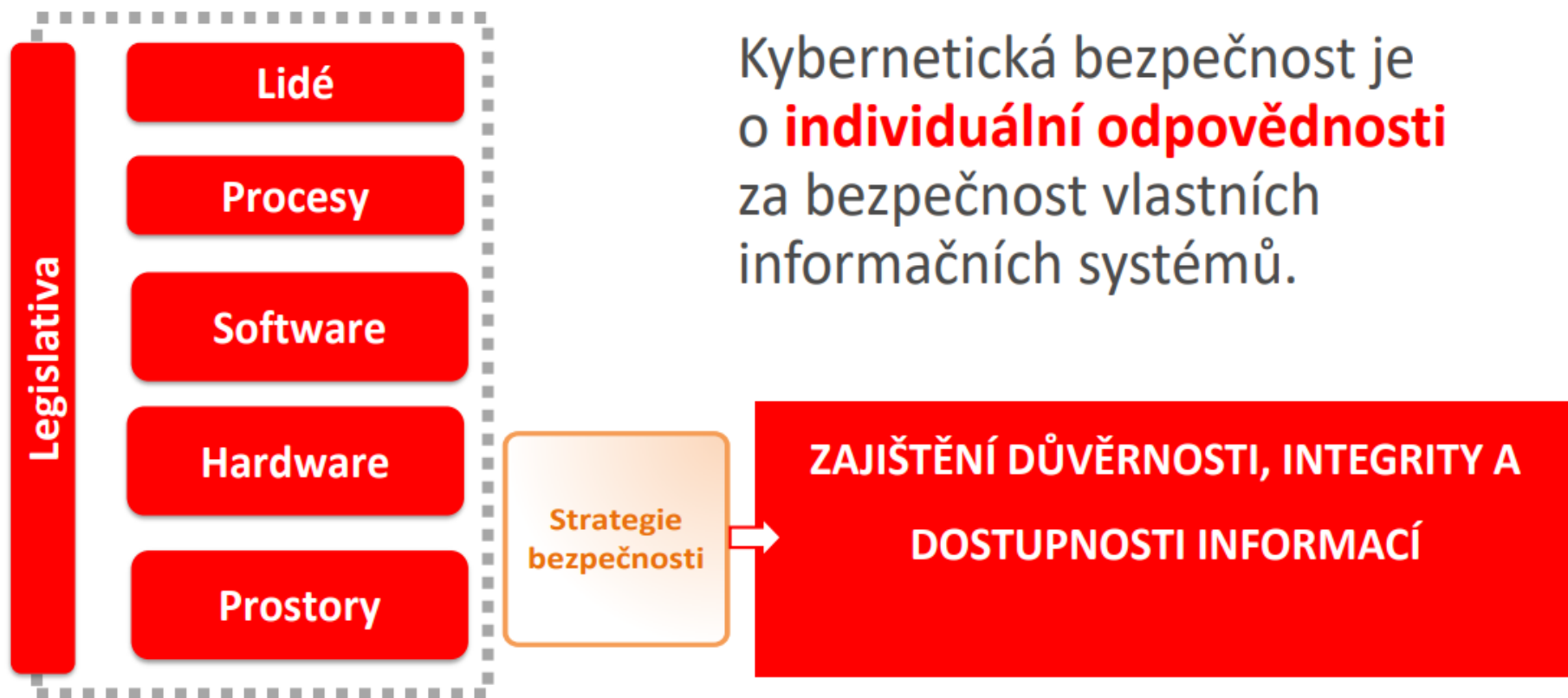


*Zavedli jsme systém řízení kvality  
a systém environmentálního řízení a auditu*



## Kybernetická bezpečnost a jak začít...

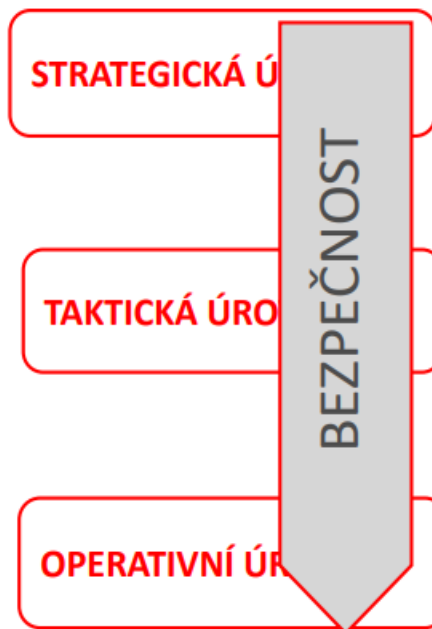
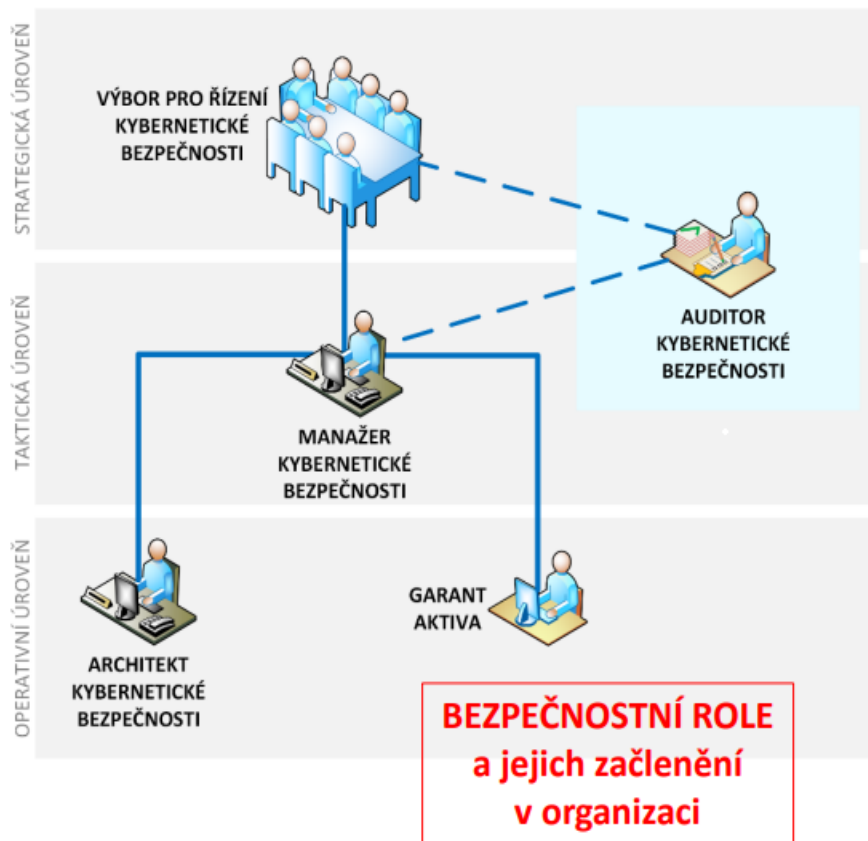
- ▶ *Rozdílová analýza (Připravenost)*
- ▶ *Analýza prostředí (Road mapa)*







# ORGANIZAČNÍ OPATŘENÍ



**Bezpečnost se buduje ze shora !!!**



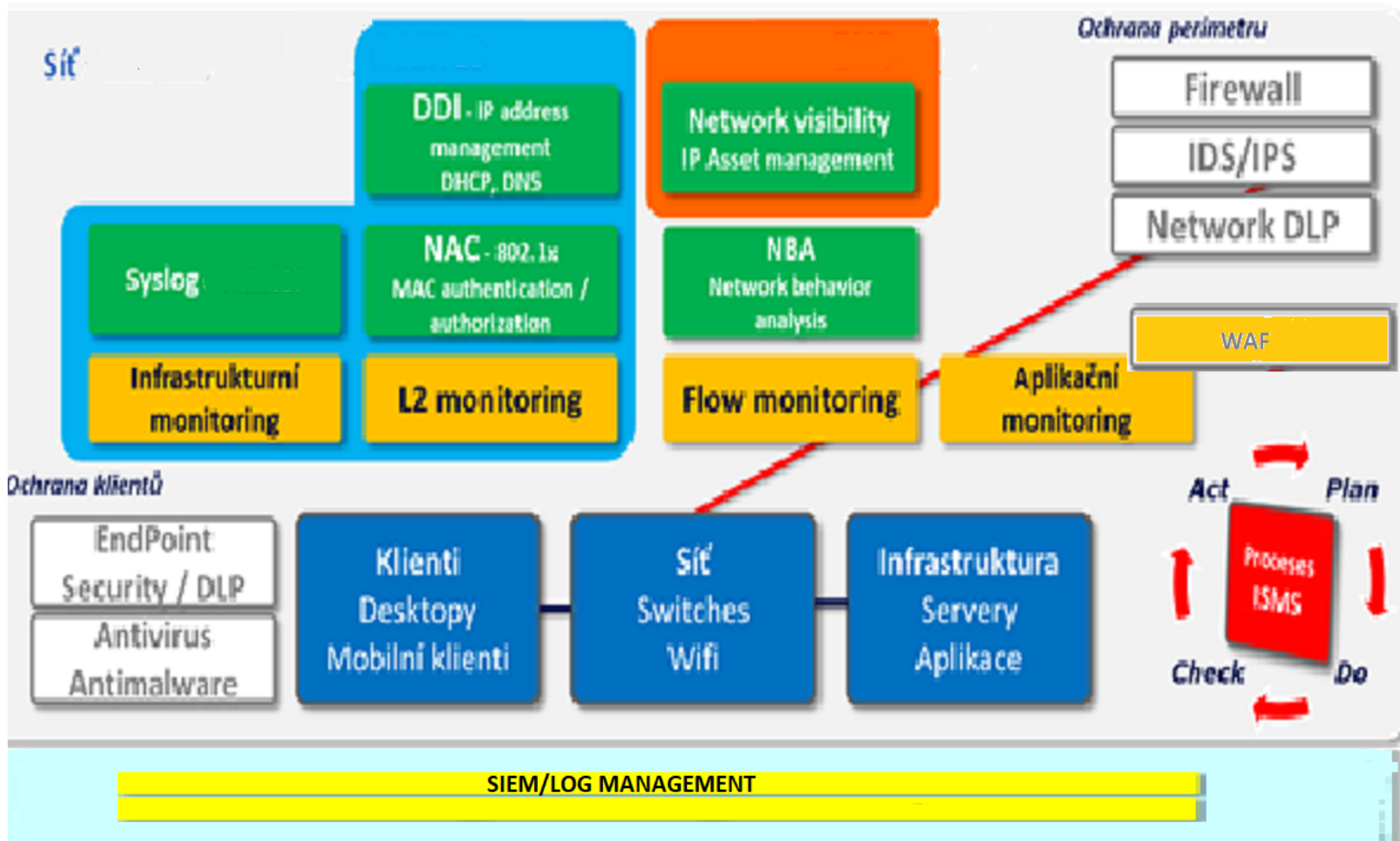
# TECHNICKÁ OPATŘENÍ

---

- ▶ *Správa identit*
- ▶ *Ochrana koncových zařízení /Servery*
  - *EndPoint Security*
  - *Šifrování*
- ▶ *Infrastruktura*
  - *Perimetr (Firewall/WAF)*
  - *Segmentace sítě / NAC 802.1X / IPAM*
- ▶ *Datová úložiště*
  - *Struktura dat / SW pro analýzu OU*
- ▶ *Doba trvání*



# TECHNICKÁ OPATŘENÍ






# TECHNICKÁ OPATŘENÍ

---




- ▶ *Monitoring*
  - ▶ *Provozní monitoring*
  - ▶ *Monitoring síťového provozu*
  - ▶ *Kontrola DNS provozu*
  - ▶ *SIEM /Logmanager*
  
- ▶ *Externí SOC*






# JINÉ PRAKTICKÉ POZNATKY



Vítejte > Hledat opakovanou činnost > Opakovaná činnost

Všechny organizace    

Vítejte

Správa konfigurací

Helpdesk

Správa incidentů

Správa problémů


Řízení změn



Provozní deník


**Opakované činnosti**

- ▶ Nová opakovaná činnost
- ▶ Hledat opakovanou činnost
- ▶ Požadavky z opakovaných činností

Hledat objekty třídy Opakovaná činnost Na základě vašich preferencí jsou zastaralá data skrytá ▲

Přidat nové kritérium +  and  

Celkem objektů: 11  **Nový...** **Další akce** 

Stránek:  30 objektů na stránku

Opakovaná činnost	Organizace	Služba	Podkategorie služeb	Datum počátku
Fyzická kontrola serveroven	MSK - řešitelé	Kontroly ISMS	Servery	2022-01-17
Kontrola bezpečnostních aktualizací OS	MSK - řešitelé	Kontroly ISMS	Servery	2022-01-19
Kontrola přístupů do serveroven	MSK - řešitelé	Kontroly ISMS	Bezpečnost	2022-01-21
Kontrola redukčního poměru disk.pole A348-SSD	MSK - řešitelé	Kontroly ISMS	Servery	2022-05-24
Kontrola systémového času	MSK - řešitelé	Kontroly ISMS	Sítě	2022-01-18
Kontrola vzdálených přístupů dodavatelů	MSK - řešitelé	Kontroly ISMS	Vzdálené přístupy	2022-01-20
Platnosti certifikátu ISE	MSK - řešitelé	Elektronický podpis a certifikáty	Požadavek na službu	2024-01-15
Přezkoumání seznamu smluv	MSK - řešitelé	Kontroly ISMS	Dokumentace	2022-01-19
Revize kapacitního plánu	MSK - řešitelé	Kontroly ISMS	Dokumentace	2022-01-19
Údržba NB pro nahližení do spisu (pro odbory VŽ a ÚPS)	MSK - řešitelé	Pracovní stanice a mobilní zařízení	Instalace a aktualizace programového vybavení na stanicích uživatelů	2021-11-10



## ZÁVĚR

---

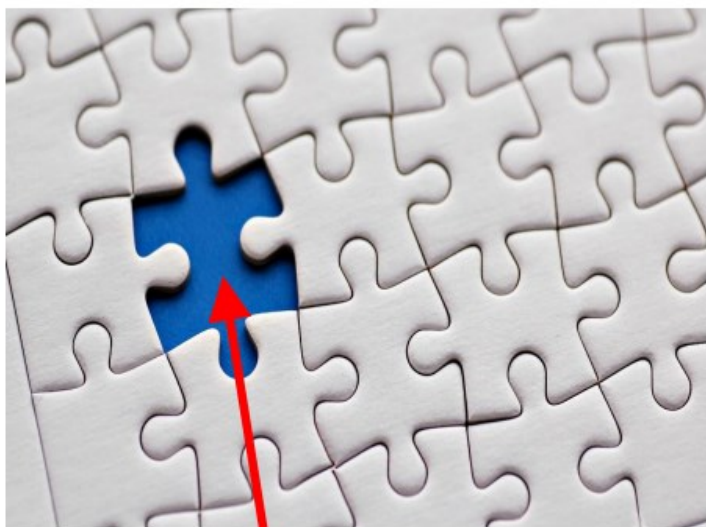
Směrnice NSI 2 a budoucího ZKB jsou zaměřeny na prevenci, detekci a reakce na kybernetické útoky, zvýšení povědomí o kybernetických hrozbách, posílení spolupráce mezi orgány státní správy a soukromým sektorem.

Čeká nás toho hodně .....

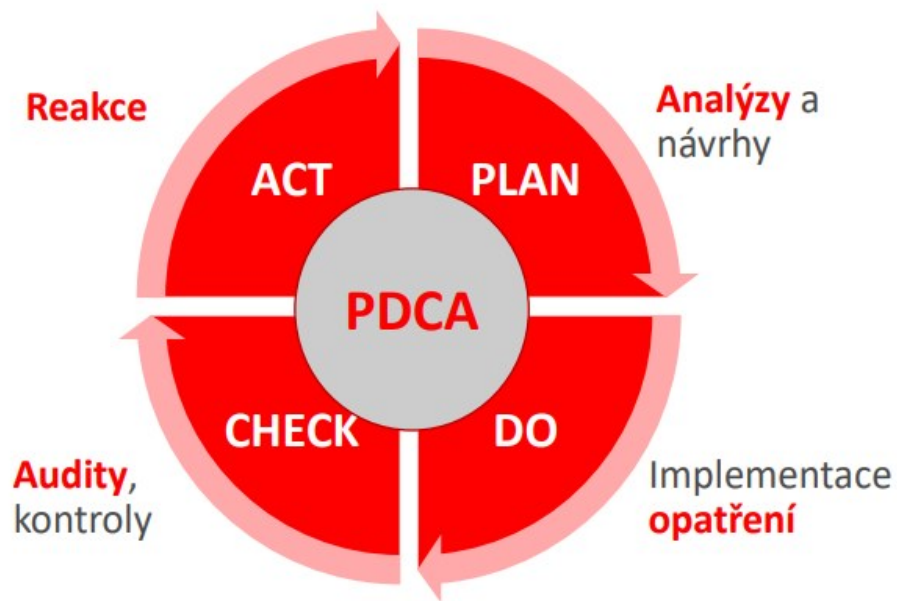




# ISMS /ZoKB



**ZRANITELNOST**



Používáme metodiku a doporučení  
**ČSN ISO/IEC 27001-27003:2014**



# DĚKUJI ZA POZORNOST