

Preventivní ochrana informací

(privilegovaní uživatelé)

Záměr

Ochrana informací v informačních systémech je velmi důležitým a sledovaným aspektem, který je podpořen řadou zákonů a vyhlášek. Velkou hrozbou pro organizace, jsou uživatelé s privilegovanými přístupy, které mají k místům, kde jsou data uložena a spravována. Ochrana informací je prováděna tradičně kombinací tří přístupů: Preventivní, Detektivní a Administrativní.



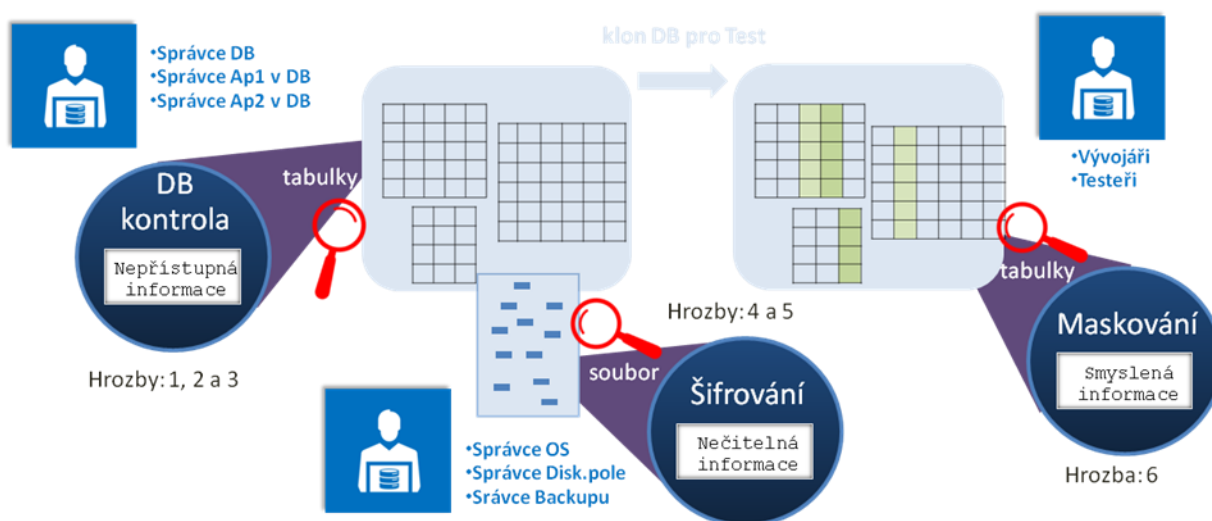
Každá organizace investuje nemalé úsilí a prostředky do ochrany informací. Zejména Administrativní opatření a často nově připravované Detektivní opatření (monitoring a audit) se v mnoha organizacích již realizují. V tuto chvíli však existuje řada hrozeb od privilegovaných uživatelů, které lze eliminovat, nebo alespoň snížit riziko, pomocí vhodné Preventivní ochrany. Tento dokument popisuje hrozby, návrhy Preventivní ochrany a její přínosy z pohledu privilegovaných skupin a současně naznačuje způsob implementace, včetně ověřujícího pilotního provozu.

Hrozby a vhodné preventivní opatření

1. Do sdílené databáze přistupuje několik aplikací, které využívají privilegia s vysokým přístupem k datům
 - **Omezení přístupu jen na objekty, ke kterým dana aplikace má a musí mít přístup**
2. Uživatel přistupující do databáze dostane mnohdy vyšší přístup, než skutečně potřebuje
 - **Umožnit sledovat a analyzovat oprávnění a role pro přístup do databáze a optimalizovat je na nezbytně nutné**
3. Databázový správce je zodpovědný za správu a zálohování dat z konkrétní tabulky
 - **Omezení privilegií s nemožností číst, kopírovat data z tabulky**
4. Správce Operačního systému pracuje se DB soubory databáze, které může číst nebo i upravovat
 - **Znečitelnění vybraných DB souborů pomocí šifrování**
5. Správce záloh s uloženými daty může restaurovat data v nové databázi, kterou si pro tento účel připraví.
 - **Znečitelnění vybraných DB souborů pomocí šifrování**

6. Organizace poskytne dodavateli aktuální stav databáze, se kterou bude jeho aplikace komunikovat, aby se předešlo překvapením a zkrátila se doba na dodání a otestování nové verze aplikace.
 - **Datová věta bude smyšlená, aby nedošlo ke zneužití informací. Bude zamaskovaná dle centrálně spravovaných a auditovatelných pravidel a nebude mít vliv na výkonový test aplikace.**

Privilegovaní uživatelé a hrozby



Návrh ověření preventivních opatření ve vaší organizaci

- Pilotní ověření navrhujeme realizovat na jedné z vašich databází, pro kterou bude vytvořen testovací klon dat
- Pokud má organizace omezené HW prostředky, tak jí nabídneme databázovou infrastrukturu postavenou v Oracle Demo Centru a pouze na začátku budeme potřebovat data ve vaší organizaci připravit (na vašem anebo našem Oracle HW) v souladu s vaší legislativou (data mohou být ostrá, anonymizovaná nebo syntetická, ale taková, aby bylo příslušné ověření průkazné pro vaší organizaci)
- Doporučujeme provést veškeré testy na nejnovější verzi Oracle Database 12c.
- Pro jednotlivé testy bude připraven projektový plán: cíle/KPI, časování, nároky na součinnost ze strany vaší organizace, popis jak bude ověření realizováno a odhad nákladů na implementaci
- Dodáme vám odhad nákladů pro potenciální budoucí implementaci včetně licencí a to včetně každé oblasti řešení (DB kontrola, Šifrování, Maskování)