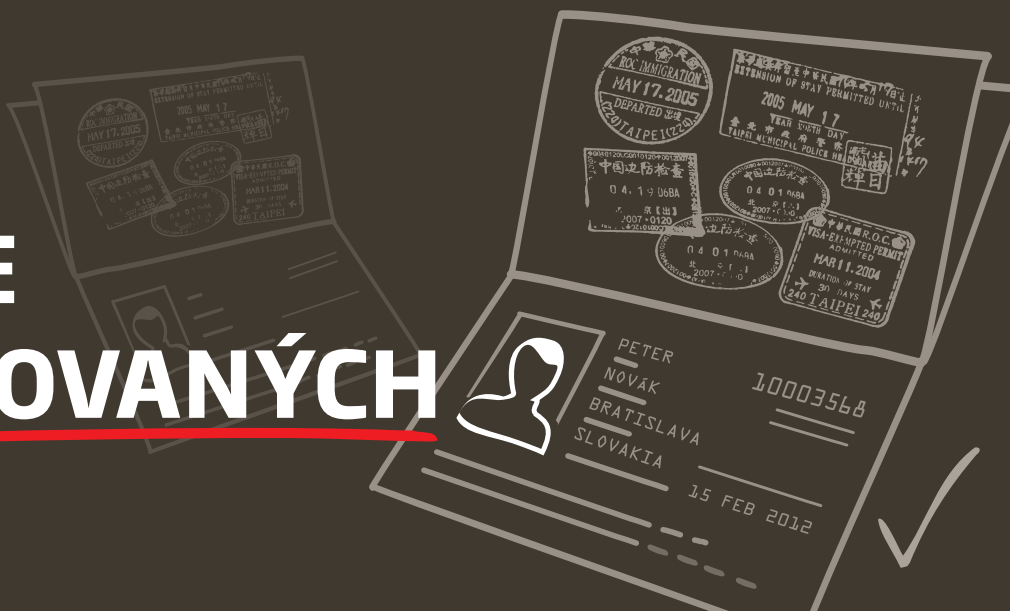
# RIADENIE PRIVILEGOVANÝCH IDENTÍT




## SÚ PRIVILEGOVANÍ POUŽÍVATELIA IT RIZIKOM?

Spoločnosti väčšinou prevádzkujú v rámci svojej IT infraštruktúry množstvo serverov, databáz, virtuálnych serverov, sieťových zariadení a aplikácií. Tieto komponenty spravujú privilegovaní používatelia, či už interní zamestnanci spoločnosti, externisti alebo dodávatelia. Títo používatelia majú takmer vždy neobmedzené oprávnenia pri prístupe k informačným aktívam spoločnosti, pretože poznajú heslá k privilegovaným účtom, ako je „root" v Unix/Linux systémoch, „Administrator" vo Windows systémoch alebo „SYS" v Oracle databázach.

Spoločnosti v rámci svojej bezpečnostnej politiky a stratégie aplikujú riešenia, ktoré pokrývajú hrozby vyplývajúce z činnosti štandardných používateľov. Avšak hrozby vyplývajúce z činnosti privilegovaných používateľov vo väčšine prípadov nie sú pokryté a pritom sa jedná o činnosti, ktoré predstavujú pre spoločnosť a jej aktíva najvyššie riziko.

**Výhody aktívneho riadenia privilegovaných účtov:**

- zníženie rizika odcudzenia údajov a tým zvýšenie ochrany svojho podnikania
- eliminovanie sabotáží a najkritickejších hrozieb pre prevádzku IT
- súlad s legislatívnymi požiadavkami

## AKÉ PROBLÉMY A POŽIADAVKY RIEŠIME?

- **Bezpečné uloženie citlivých informácií.** V tomto prípade sa jedná o heslá k privilegovaným účtom, ale v princípe je možné ukladať ľubovoľné dokumenty. Produkty využívajú certifikované riešenie ako bezpečné úložisko, ktoré napĺňa atribúty pre zabezpečenie dôvernosti, integrity a dostupnosti.
- **Interné a externé hrozby**, keďže produkty kontrolujú činnosti privilegovaných používateľov v rámci organizácie alebo aj mimo nej, ako sú externisti alebo dodávatelia. Na základe rôznych štúdií sú hrozby vyplývajúce z činnosti interných zamestnancov pre spoločnosť najkritickejšie.
- **Strata citlivých informácií**, keďže prístup k privilegovaným účtom, heslám a aj systémom je riadený, tak je možné minimálne identifikovať, ktorým kanálom (napríklad export Oracle databázy) došlo k strate citlivých informácií.
- **Dohľad nad činnosťami privilegovaných používateľov**, keďže systém spravuje zoznam privilegovaných používateľov a zoznam systémov, ku ktorým pristupujú. Okrem toho je možné aplikovať aj riešenie, ktoré monitoruje činnosti privilegovaných používateľov a aj umožňuje nahrávať ich aktivity.

## O PRODUKTOCH SPOLOČNOSTI CYBER-ARK

Balík produktov Privileged Identity Management (PIM) spravuje privilegované účty, heslá a monitoruje aktivity, ktoré sú s nimi vykonávané. Skladá sa z nasledujúcich produktov:

- **Secure Digital Vault.** Základný produkt, ktorý obsahuje patentovanú technológiu poskytujúcu bezpečné úložisko pre všetky používané informácie. Sú to politiky, nastavenia, heslá, nahraté činnosti a podobne.
- **Enterprise Password Vault (EPV).** Na základe zadefinovaných politík spravuje produkt heslá privilegovaných používateľov. Môže realizovať aj automatické zmeny hesiel na cieľových systémoch.
- **Application Identity Manager (AIM).** Riešenie eliminuje nutnosť umiestňovať heslá (napríklad na prístup do databázy) v zdrojových kódoch aplikácií, v skriptoch a konfiguračných súboroch.
- **Privileged Session Manager(PSM).** Produkt umožňuje monitorovať a nahrávať aktivity privilegovaných používateľov. Používa sa najmä na monitoring pri vzdialenom prístupe externistov a dodávateľov do infraštruktúry spoločnosti.
- **On-Demand Privileges Manager (OPM).** Produkt je určený pre Unix/Linux systémy a pomocou neho je možné dosiahnuť vysokú granularitu prístupových oprávnení až na úroveň povolených alebo zakázaných príkazov, ktoré môže používateľ spúšťať.

---

Architektúra balíka produktov PIM je modulárna a zároveň centrálne spravovaná. Jednotlivé produkty je možné nasadzovať postupne a pritom sú spravované centrálne pomocou jednotného administratívneho rozhrania. Nasadenie produktov PIM môže byť postupné s minimálnym dopadom na prevádzku. V úvodnej fáze môže byť nasadený produkt EPV na správu hesiel privilegovaných používateľov vo vybratých systémoch. Po odladení technológie a pracovných postupov je možné pridať ďalšie systémy a prípadne nasadiť aj produkty AIM, OPM, alebo PSM.
Produkty sú integrovateľné s inými riešeniami, najmä s riešeniami na zabezpečenie silnej autentifikácie (tokeny, čipové karty, certifikáty), s riešeniami z oblasti Identity Management, firemnými adresármi (LDAP server, Microsoft doména), systémami na dohľad a zber logov (SIEM), a aj ticketovacími riešeniami.

## AKÁ JE PRIDANÁ HODNOTA TEMPEST?

Firma TEMPEST je jediným partnerom spoločnosti Cyber-Ark na Slovensku. Má k dispozícii pracovníkov s certifikátom Cyber-Ark PIM (Privileged Identity Management) Professional Engineer.

Spoločnosť TEMPEST dokáže poskytnúť ucelené portfólio produktov a služieb z oblasti aplikačnej i analytickej bezpečnosti. Okrem technologického nasadenia produktov z balíka PIM kladieme dôraz na vypracovanie pracovných postupov, ktoré musia byť v súlade s bezpečnostnou politikou spoločnosti i regulatórnymi požiadavkami. V tejto oblasti má TEMPEST dlhoročné skúsenosti a množstvo pracovníkov s medzinárodne uznávanými certifikátmi CISM (Certified Information Security Manager), CISA (Certified Information Systems Auditor) a CISSP (Certified Information Systems Security Professional).

Cyber-Ark®
Security That Empowers People

Tempest
IT makes sense