Izkušnje obvladovanja privilegiranih dostopov v bančnem okolju

Janko Zorman, Simon Feldin

AGENDA

1. Kaj je PAM? – Simon Feldin
2. Izkušnje iz prakse – Janko Zorman
3. Vprašanja

KAJ JE PAM?

- Privilegiran uporabnik je uporabnik z administratorskimi pravicami na določenem sistemu
- Ali imate seznam vseh privilegiranih računov in kdo jih lahko uporablja?
- Imate vpogled nad kdo, zakaj in kdaj je dostopal do vaših sistemov? (zunanji partnerji?)
- Veste kaj točno se je naredilo med posameznim dostopom?
- Je zaupanje dovolj?

KAJ JE PAM?

- **PAM – privileged account management**
- **PAM je sistem, ki omogoči upravljanje, nadzor in popolno revizijsko sled nad rabo privilegiranih uporabniških računov in dostopov do IT sistemov**
- **Privilegirani dostopi MORAJO biti nadzirani**

KAJ JE PAM?

- PAM mora ščititi vaše sisteme pred nepooblaščenim privilegiranim dostopom
- PAM mora omogočati dodeljevanje privilegiranih dostopov do sistemov za katere ima uporabnik dovoljenje
- PAM mora ukiniti dostope, ki jim poteče veljavnost
- PAM mora onemogočiti neposredno povezovanje s privilegiranimi dostopi
- PAM mora voditi popolno revizijsko sled nad dodeljevanjem in rabo priveligranih dostopov

KAJ JE PAM?

- **Komponente PAM sistema**
  - **Access Manager – zagotavlja nadzor dostopa do privilegiranih dostopov preko centralno definiranih politik**
  - **Password Vault – varna hramba gesel privilegiranih dostopov**
  - **Session Manager – beleži vso aktivnost, ki se odvija med privilegiranimi dostopi**

PRAKTIČNE IZKUŠNJE

STATISTIKA INFORMACIJSKE VARNOST

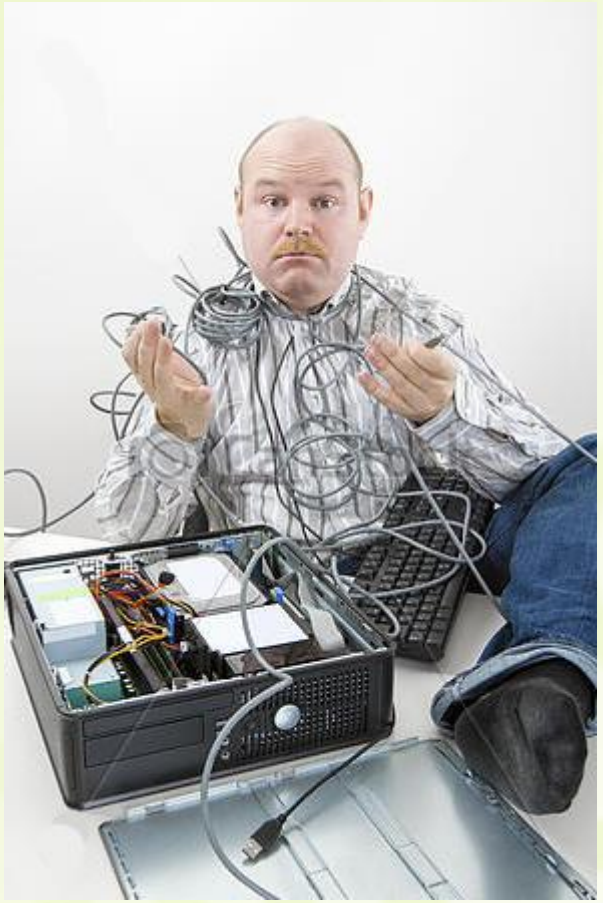
- **Nenadzorovani privilegirani računi so lahka tarča**
  - **80% vdorov vključuje privilegirane poverilnice**
  - **82% vdorov je posledica zlorabe notranjih informacij**
  - **Čas potreben za odkritje vdora je več kot 1 teden**
- **Varnost privilegiranih računov v podjetjih**
  - **73% testnih/default računov je aktivnih v produkcijskem okolju**
  - **55% uporabniških računov po prenehanju pogodbenega razmerja je še vedno aktivnih**

Vir: Forrester Research: Wave report in Privileged Access Management
Verizon Data Breach Investigations Report (DBIR)
Thycotic 2018 Global state of privileged access management risk & compliance

IZZIV ?

- Zmanjšati tveganje pred notranjimi in zunanjimi grožnjami
- Kako imeti boljši nadzor nad dostopi do IT okolja
- Kdo, kdaj in kaj
- Povečana produktivnost (Lažje upravljanje privilegiranih dostopov, revizijske sledi, …)
- Poenostaviti skladnost

PRIMER IZ PRAKSE



REZULTAT ANALIZE

- Ni znakov vdora
- Ni znakov okužbe
- Manjkajo ključne sistemske mape in datoteke
- Na sistemu sta bila prijavljena 2 uporabnika

REŠITEV IN DOSEŽEN REZULTAT

- Večja varnost (upravljanje dostopov ter uporabniških poverilnic; gesel ne pozna nihče)
- Pridobitev podrobnih informacij (kdo, kdaj in kaj)
- Večja učinkovitost (pohitritev odobritev ter nastavitev dostopov od IT okolja)
- Zagotovitev skladnosti
- Uporaba „point-and-click“ orodij
- Enostavnost uporabe

VPRAŠANJA ?