Tehnične specifikacije za PAM

# Uvod:

Na MIZŠ želimo vpeljati programsko rešitev PAM (Privileged Access Management), za potrebe upravljanja in nadzora privilegiranih uporabnikov. Rešitev mora zadostiti kriterijem, ki so opisani v nadaljevanju.

# Splošno:

* transparentni princip delovanja
* na voljo kot namenska strojna oprema, ki bo postavljena v način visoke razpoložljivosti za strojno rešitev
* visoka razpoložljivost v načinih master/slave, in master/master
* podpora za integracijo z drugimi sistemi tako na nivoju aplikacij, kakor tudi z avtentikacijskimi mehanizmi
* rešitev mora zagotavljati šifriranje nosilnega medija s preverjanjem pristnosti ob zagonu

# Session Manager:

* vzpostavljanje sej s katerimkoli odjemalcem, ki polno podpira zahtevan protokol (RDP, SSH,)
* nadzor privilegiranih uporabnikov/uporabniških računov
* omogočena mora biti prijava v račun, ne da bi bilo geslo ciljnega sistema razkrito do končnega uporabnika
* omejevanje dostopa samo do elementov do katerih ima uporabnik pravico dostopa
* grupiranje uporabnikov/ciljnih naprav (npr. uporabniki z enakimi pravicami dostopa do naprav so v isti grupi)
* primarna in sekundarna avtentikacija na podlagi domenskih podatkov
* snemanje sej uporabnikov (možnost enkripcije zajetih podatkov); zbiranje metapodatkov o sejah;
* hranjenje posnetih sej na napravi, zunanji podatkovni napravi ali traku
* velikost video posnetkov sej ne sme presegati 3MB na minuto snemanja
* pošiljanje obvestil administratorjem/uporabnikom preko elektronske pošte
* rešitev brez namestitev klientov na ciljne naprave
* zagotavljanje revizijske sledi; beleženje izvedenih dejanj in časovno žigosanje
* zagotavljanje skladnosti z regulativami npr. GDPR
* nadzor vzpostavljenih sej v realnem času; ogled uporabnikovih dejanj v živo, prekinitev seje
* možnost omejevanja seje na podlagi aktivnosti uporabnika
* seznami dovoljenih in prepovedanih ukazov znotraj nadzorovanih sej in obveščanje v primeru kršitve le-teh
* prepoznavanje vnesenih ukazov in prikazanih vsebin (imena datotek, map) ter obveščanje in/ali prekinitev seje v primeru dostopanja do vsebin za katere uporabnik nima pooblastil
* dostop do naprav na podlagi podanega zahtevka, ki ga mora potrditi eden ali več administratorjev (approver-jev); zgodovina odobrenih dostopov
* časovna omejitev dostopa
* zgodovina dostopov po uporabnikih
* integracija z zunanjimi sistemi za identifikacijo/avtentikacijo (AD/LDAP/Radius)
* uvoz podatkov iz CSV datotek
* dvofaktorska avtentikacija primarnih uporabniških računov (RSA, SecureKey) – priporočeno (upošteva se 5 točk v merilu za najugodnejšo ponudbo)
* priprava poročil
* integracija z SIEM sistemi

# Password Manager:

* administrativno upravljaje z gesli
* gesla shranjena v certificiranem trezorju
* hramba SSH ključev
* redne menjave/rotacije gesel uporabnikov in/ali aplikacij
* nadzor nad kompleksnostjo gesel (dolžina, posebni znaki, male in velike črke, številke, prepovedani znaki)
* upravljanje z gesli ciljnih naprav (npr. periodično menjavanje gesla); se stalno dopolnjuje
* upravljanje gesel aplikacij in storitev (Application-to-application)
* možnost uporabe zunanjih trezorjev
* breaking glass mehanizem; pošiljanje kriptirane elektronske pošte, ki vsebuje spremenjeno geslo/SSH ključ ciljne naprave administratorjem

# Zahteve glede velikosti okolja:

* rešitev mora omogočati vsaj 25 hkratnih sej uporabnikov pri povezavi s ciljnimi sistemi

# Ostalo:

* integracija naprav v sistem naročnika
* vzdrževanje naprave (care package) za 3 leta, ki naj vsebuje prijavo napak od ponedeljka do petka v režimu 8x5. Odzivni čas 4 ure, čas popravila naslednji delovni dan.

Predmet javnega naročila je tudi možnost naročnika, da v času trajanja pogodbe dodatno, po dejanskih potrebah, naroča dodatne ure za vzdrževanje oz. svetovanje (skupaj do največ 360 ur), ki niso zajete v prejšnjih alinejah. Naročnik dodatnih ur ni dolžan naročiti oz. se naročajo po potrebi. Cena za uro vzdrževanja in svetovanja ter količina je v obrazcu Predračun zato posebej navedena.