



METODICKÉ USMERNENIE č. 2/2022

o zabezpečení bezpečnosti prevádzky sieťovej služby vzdialenej plochy

Článok 1

Úvodné ustanovenia

1. Účelom tohto metodického usmernenia je zabezpečenie jednotného postupu pri zabezpečení bezpečnosti používania sieťovej služby vzdialenej plochy (Remote Desktop Services, ďalej len „RDS“). Metodické usmernenie je určené na definovanie spôsobu zabezpečenia bezpečnosti prevádzky služby vzdialenej plochy pomocou protokolu RDP pre študentov a zamestnancov Fakulty elektrotechniky a informačných technológií Žilinskej univerzity v Žiline (ďalej len „FEIT UNIZA“).

Článok 2

Všeobecné zásady zabezpečenia bezpečnosti RDS

1. Všeobecné zásady zabezpečenia bezpečnosti prevádzky RDS sú:
 - a) silné heslá pre účty s prístupom k vzdialenej ploche, heslo by malo mať aspoň 8 znakov. Malo by obsahovať malé písmená a – z, veľké písmená A – Z, číslice 0 – 9 aj špeciálne znaky,
 - b) pravidelná aktualizácia operačného systému, ktorá zabezpečuje že komponenty sa automaticky aktualizujú najnovšími bezpečnostnými opravami,
 - c) obmedzenie počtu používateľov, ktorí sa môžu prihlásiť pomocou vzdialenej pracovnej plochy,
 - d) nastavenie politiky uzamknutia účtu.

Článok 3

Postup zabezpečenia RDP

1. Zablokovanie priameho prístupu RDP ku klientom alebo serverom pre siete mimo UNIZA pomocou firewallu.
2. Používatelia, ktorých zariadenia, nie sú pripojené do univerzitnej siete, môžu využiť autorizovaný vzdialený prístup VPN UNIZA na pripojenie sa do univerzitnej siete.

Článok 4

Zodpovednosť

1. Zodpovednosť za zabezpečenie bezpečnosti RDS má používateľ.

Článok 4

Záverečné ustanovenie

2. Metodické usmernenie č. 2/2022 nadobúda platnosť dňom podpisu dekanom FEIT a účinnosť dňom jeho zverejnenia.

V Žiline dňa 14.03.2022

prof. Ing. Pavol Špánik, PhD.
dekan FEIT