

## Uživatelská IP-bezpečnost Inetu MU

Jaroslav Měcháček, ÚVT MU

V měsíci září byla na intranetovém serveru `inet.muni.cz` implementována možnost omezit přístup k aplikacím na základě aktuální IP adresy klienta. Komunikace mezi klientem (webový prohlížeč) a serverem je zabezpečena transportním protokolem SSL, takže odposlech hesla po trase je téměř vyloučen. Existuje však mnoho jednodušších způsobů, jak získat přístupové heslo uživatele. Jako příklad lze uvést použití softwaru pochybného původu, přihlašování se z počítačů typu "internetová kavárna" nebo pouze cizí pohled na klávesnici v době, kdy uživatel píše svoje heslo.

Pokud má uživatel intranetového serveru pocit, že by za určitých okolností mohlo dojít ke zcizení a následnému zneužití jeho hesla, může využít možnosti omezení/povolení přístupu pouze z vybraných IP adres.

V systému jsou jednotlivé aplikace označeny stupněm důvěrnosti dat, se kterými pracují. Toto členění určuje administrátor systému a uživatel je nemůže ovlivnit. Přehledný seznam všech aplikací a stupně jejich důvěrnosti je k dispozici na <https://inet.muni.cz/app/sys/duvernost>, stupeň důvěrnosti je také zobrazován v záhlaví stránek aplikací. V menu jsou položky, k nimž nemá uživatel aktuálně přístup, odlišeny jinou grafikou a barvou.

Aktuálně jsou definovány 4 stupně/úrovně důvěrnosti:

- 0 - Konfigurace IP adres
- 10 - Citlivá data
- 20 - Osobní data
- 30 - Veřejná data

Každá úroveň má přiřazen číselný kód, přičemž čím nižší je číslo, tím důvěrnější jsou zpracovávaná data.

Každý uživatel má možnost s použitím aplikace "Konfigurace IP adres" (<https://inet.muni.cz/app/sys/ipsecconfig>) přiřadit ke každému stupni důvěrnosti množinu IP adres, z nichž je povoleno aplikace daného stupně spouštět. Při přístupu z jiných adres jsou požadavky zamítnuty.

Platí následující pravidla:

- Není-li úrovni 0 přiřazena žádná adresa, jsou všechny IP adresy strojů, z nichž uživatel k aplikacím přistupuje, považovány za adresy úrovně 0, tj. IP bezpečnost není aktivní a uživatel může k libovolné aplikaci přistupovat odkudkoli.
- Pokud je IP adresa přiřazena k úrovni  $N$ , pak lze samozřejmě z této adresy také spouštět aplikace úrovní vyšších než  $N$ .
- Pokud uživatel přiřadí adresy pouze k některým úrovním důvěrnosti, jsou všechny IP adresy, které neodpovídají tomuto nastavení, klasifikovány jako adresy úrovně  $N + 1$  (kde  $N$  je maximální nastavená úroveň). □