

OPEN-SOURCE TECHNOLOGIE SE ZAMĚŘENÍM NA INFRASTRUKTURU, KYBERBEZPEČNOST A OCHRANU DAT



Centrum
přírodovědných
a technických oborů

Univerzita J. E. Purkyně v Ústí n. L.
Přírodovědecká fakulta UJEP
Pasteurova 3632/15
400 96 Ústí nad Labem

RNDr. Jan Krejčí, Ph.D.
E-mail: jan.krejci@ujep.cz
Tel.: +420 739 274 400
Kancelář: 7.04

PŘEDSTAVENÍ VÝZKUMU/TECHNOLOGIE

Cílem vyvinuté technologie je poskytnutí ucelené finančně dostupné alternativy k ekonomicky nákladným a funkčně předimenzovaným řešením určeným pro velké korporátní heterogenní sítě v oblasti managementu infrastruktury a bezpečnosti sítě a dat. Poskytovatel je schopen realizovat i jednotlivé dílčí prvky řešení.

POTENCIÁLNÍ UŽIVATELÉ

Tyto materiály je vhodné využít v MSP, v orgánech státní správy, ve školních a vzdělávacích institucích či v neziskovém sektoru pro malé sítě do 500 uživatelů.

VÝHODY TECHNOLOGIE A VYUŽITÍ NA TRHU

V současné době jsou vybírány open-source technologie s dlouhodobou plánovanou podporou s ohledem na udržitelnost provozu. Servis a správa může být realizována buď vlastními pracovníky společnosti, pracovníky VaV instituce či ve spolupráci s partnerskými technologickými společnostmi v regionu. S ohledem na platnou legislativu je zajištění kybernetické bezpečnosti prvořadým úkolem každého subjektu. Analýza, návrh a testování nezávislou institucí (provider/inventor) nejsou ovlivněny výrobci v daných technologických oblastech. Implementace open-source bezpečnostních technologií zvyšuje efektivitu ochranného perimetru síťové infrastruktury při minimalizaci finanční náročnosti a je dostupná i malým uživatelům – viz cílová skupina.

DOPLŇUJÍCÍ INFORMACE

Realizace (třeba i dílčího) řešení je podmíněna, ve vazbě na zvolený rozsah řešení, odpovídajícími postupnými úkony:

- analýza a penetrační testování stávajícího stavu,
- analýza potřeb,
- teoretický návrh a harmonogram implementace bezpečnostních open-source technologií,
- implementace bezpečnostních open-source technologií v laboratorních podmínkách,
- optimalizace síťové infrastruktury,
- implementace bezpečnostních open-source technologií v ostrém prostředí zadavatele,
- penetrační testování nasazené infrastruktury,
- korekce nasazení dle aktuálních potřeb.