ISP Cyber COP

Fáze vývoje technologie

Fáze 3

Validace technologie a její přenesení do reálného prostředí. Testování technologie mimo laboratoř a její úprava pro externí podmínky.

Status IP ochrany

Strategie pro hledání partnera

Licencování

Instituce

jctt Jihočeské Univerzitní a Akademické centrum transferu technologií

Jihočeská univerzita v Českých Budějovicích

Motivace

Ochranu počítačových sítí proti hackerským útokům lze zajistit různými dostupnými produkty či službami. Pro velká datová centra či jiné instituce může být zajištění bezpečnosti těchto sítí značně finančně náročné. Motivací pro vývoj produktu ISP CyberCop bylo vytvořit levné, bezpečné, spolehlivé a snadno škálovatelné řešení umožňující detekci nejběžnějších síťových útoků.

Popis

Produkt ISP CyberCOP je sondou v síťovém provozu, která dokáže detekovat problém, rozeznat druh kybernetického útoku, zabránit takovému útoku na tuto síť a připojená zařízení a upozornit na tuto situaci. Systém funguje tak, že analyzuje data procházející počítačovou sítí prostřednictvím zmíněné sondy. Ta předává informace o síťovém provozu s využitím protokolu IPFIX síťovým detektorům, které z poskytnutých dat odhalí základní typy síťových útoků jako např. port-scan, password cracking, DDOS, posílání spamu atd. a reportují o tomto správci sítě či uživateli. Systém je založen na platformě Apache Kafka určené pro zpracování velkých dat a umožňuje snadné a efektivní škálování systému. Řešení je tedy velmi jednoduše přizpůsobitelné pro malé i velké firmy a provozovatele internetového připojení.

Komerční využití

Potenciálními uživateli jsou veškeré subjekty, které potřebují ochránit své počítačové sítě před síťovými útoky. Tedy např. datová centra, poskytovatelé internetové sítě či telekomunikační společnosti.