Politika čistoty dat systému Warden

Čistota dat

Čistota dat v případě projektu Warden označuje fakt, že veškeré události poskytované zapojeným účastníkům jsou nabízeny v nejlepší dostupné kvalitě a pocházejí z ověřených zdrojů. Události jsou získávány z vnitřních služeb sdružení CESNET (např. honeypoty), z dat poskytovaných členskými sítěmi sdružení a dalšími zapojenými účastníky, kteří procházejí registrací a kontrolou zasílaného obsahu. Další zdroje událostí představují služby třetích stran jako jsou hlášení ze systému N6 provozovaného CERT Polska.

Spolupráce s ověřenými službami.

Spolupráce s ověřenými službami znamená, že události jsou do systému Warden přijímány ze služeb provozovaných důvěryhodnými a spolehlivými partnery, případně jsou součástí služeb poskytovaných samotným provozovatelem systému.

Výběr partnerských organizací

Všechny partnerské organizace posílající informace do systému Warden jsou vybírány na základě předchozí spolupráce a dobrých zkušeností.

Ověřování partnerů

Každý klient posílající události do systému Warden musí být na základě předchozí dohody zaregistrován administrátorem systému. Nutnou podmínkou této registrace je platný certifikát. Klienti pak mohou po registraci zasílat informace z předem nahlášeného IP rozsahu.

Po dokončení registrační procedury je klient po určitou dobu připojen k testovacímu serveru, který slouží pro odladění případných problémů s odesílajícím klientem. Dále je po tuto dobu ověřována kvalita zasílaných dat. Po ukončení testovacího období je klient připojen k produkčnímu serveru.

Kontrola událostí při přijetí

Při každém přijetí událostí od klientů probíhá na Warden serveru jejich základní kontrola. Je ověřována formální správnost informací, tedy skutečnost, že mají všechna pole události očekávané hodnoty (např. IP adresa správný formát). Také je kontrolována validita událostí z pohledu vlastního systému Warden. Jedná se zde především o ověření, zda vůbec existuje typ zasílané události.

Kontrola stavu databáze událostí

V rámci systému Warden provádí jeho provozovatel (sdružení CESNET) pravidelné kontroly databáze událostí. V rámci těchto kontrol je ověřováno, zda zasílané události odpovídají obsahem kladeným požadavkům na definované typy a mají korektní časové známky, Dále je například ověřováno, zda události pocházejí z rozsahů IP adres, které se mohou vyskytovat v internetu. Také je při těchto kontrolách ověřována aktivita (živost) klientů.

Veškeré zjištěné nedostatky jsou v rámci kontrol automaticky reportovány osobám odpovědným za stav klientů posílajících události do systému Warden. Do doby, než je zjednána náprava nedostatků, jsou chybné události tohoto klienta označeny jako neplatné.