

BAESE

Benchmarking and Analytic Evaluation of IDSs in Specified Environments

Programm / Ausschreibung	FORPA, Forschungspartnerschaften NATS/Ö-Fonds, FORPA NFTE2015	Status	abgeschlossen
Projektstart	01.03.2016	Projektende	31.08.2019
Zeitraum	2016 - 2019	Projektlaufzeit	42 Monate
Keywords			

Projektbeschreibung

Intrusion Detection Systems (IDSs) sind ein essentieller Teil einer funktionierenden Sicherheitsinfrastruktur heutiger Computernetze. Sie sollen in der Lage sein Cyber-Angriffe und unbefugten System-zugriff zu erkennen und ggf. zeitnahe zu unterbinden. Während es viele Produkte mit unterschiedlichen Ansätzen am Markt gibt ist ein ungelöstes Problem, wie man die geeignetste Lösung für eine spezifische Infrastruktur auswählt, und wie diese optimal konfiguriert werden kann. Ziel des Projektes ist daher die Erarbeitung eines Konzepts, einer Methodik und Demoimplementierung eines Systems zur herstellerunabhängigen Evaluierung von IDSs unter realistischen Bedingungen. Dabei stehen analytische Modelle, zur Bewertung und der systematische Vergleich dieser in spezifischen Netzwerkinfrastrukturen, außerhalb von laufenden Produktivsystemen im Vordergrund. Dazu werden einerseits Netzwerkverhaltensmodelle zur synthetischen Datengenerierung entwickelt und andererseits ein Testbed, das die Evaluierung der optimalen Nutzung von unterschiedlichen IDSs ermöglicht.

Projektpartner

- AIT Austrian Institute of Technology GmbH