Fraunhofer
FKIE

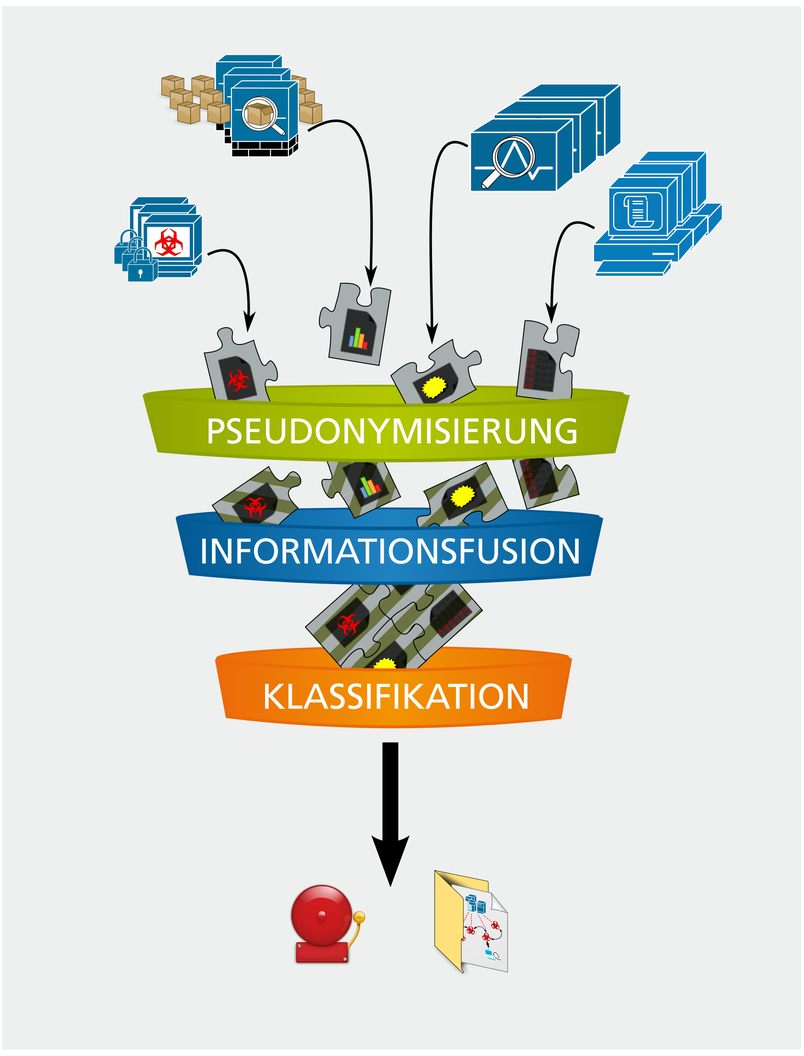
FRAUNHOFER-INSTITUT FÜR KOMMUNIKATION, INFORMATIONSVERARBEITUNG UND ERGONOMIE

VERTEILTES KOOPERATIVES MONITORING ZUR NETZWERKANOMALIE-ERKENNUNG

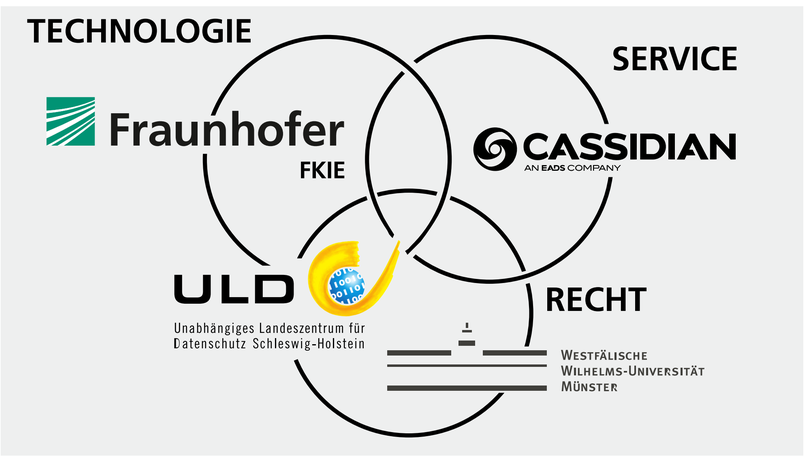
Till Elsner, Michael Meier, Arnold Sykosch, Matthias Wübbeling
{till.elsner, michael.meier, arnold.sykosch, matthias.wuebbeling}@fkie.fraunhofer.de

MonIKA

Das Internet ist für die heutige Gesellschaft von zentraler Bedeutung. Diese kritische Infrastruktur wird zunehmend durch verteilte Angriffe Bedroht. Durch kooperatives Monitoring werden Anomalien erkennbar, die einer begrenzten lokalen Sicht verborgen bleiben. Der hierzu notwendige, kontinuierliche Datenaustausch birgt die Gefahr der Offenlegung sensibler oder geheimer Informationen. Ziel des MonIKA-Projekts ist es, eine aus technischer, rechtlicher und organisatorischer Sicht praxistaugliche Lösung für diese Herausforderung zu bieten. Im Projektkonsortium wird hierzu ein Framework zum Austausch und zur Analyse von sicherheitsrelevanten Daten über organisatorische Grenzen hinweg entwickelt, welches sowohl auf administrative als auch auf rechtlich Anforderungen abgestimmt ist. Die Kernkonzepte Pseudonmysierung, Informationsfusion und Klassifikation harmonisieren dabei die Bedürfnisse nach dem Schutz von Privatsphäre und sensiblen Daten einerseits und der Konsolidierung und Analyse andererseits. Das resultierende Model stellt eine umfassende Datenbasis zur Erkennung von Anomalien bereit, die von einem lokalen Beobachtungspunkts nicht erkennbar wären.



Konzeptionelle Architektur des MonIKA-Projekts zur Anomalieerkennung in Internet-Infrastrukturen

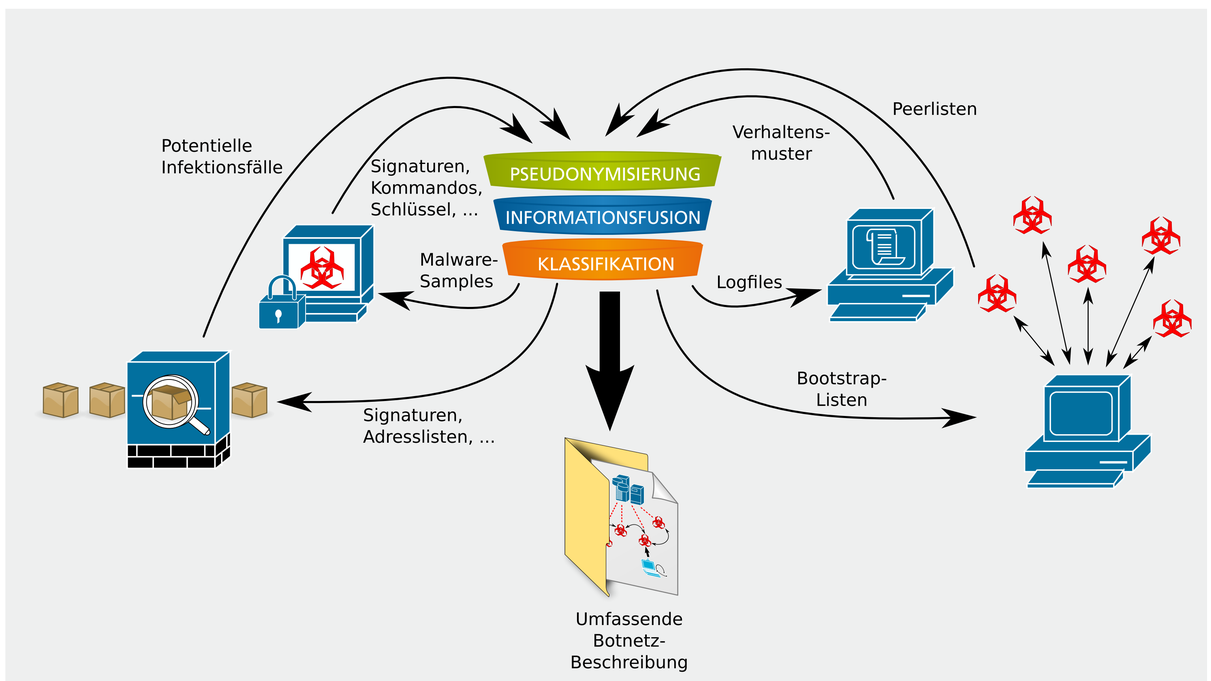


Sichten der Projektpartner innerhalb des MonIKA-Projekts.

Pseudonymisierung

Regulatorische Vorgaben und Vertraulichkeitsanforderungen aller beteiligter Parteien verlangen nach einer Lösung zum Austausch von Informationen nach dem Need-to-know-Prinzip. Maßgeschneiderte Pseudonymisierungsschemata erlauben die exakte Definition der Informationen, welche in bereitgestellten Daten noch enthalten sein dürfen. Beispielsweise müssen keine Informationen über konkrete IP-Adressen zugängig gemacht werden wenn lediglich die Information über Subnetz-Zugehörigkeit erforderlich ist. Speziell gestaltete Pseudonyme erlauben diese Art der Interpretationsbegrenzung für Daten.

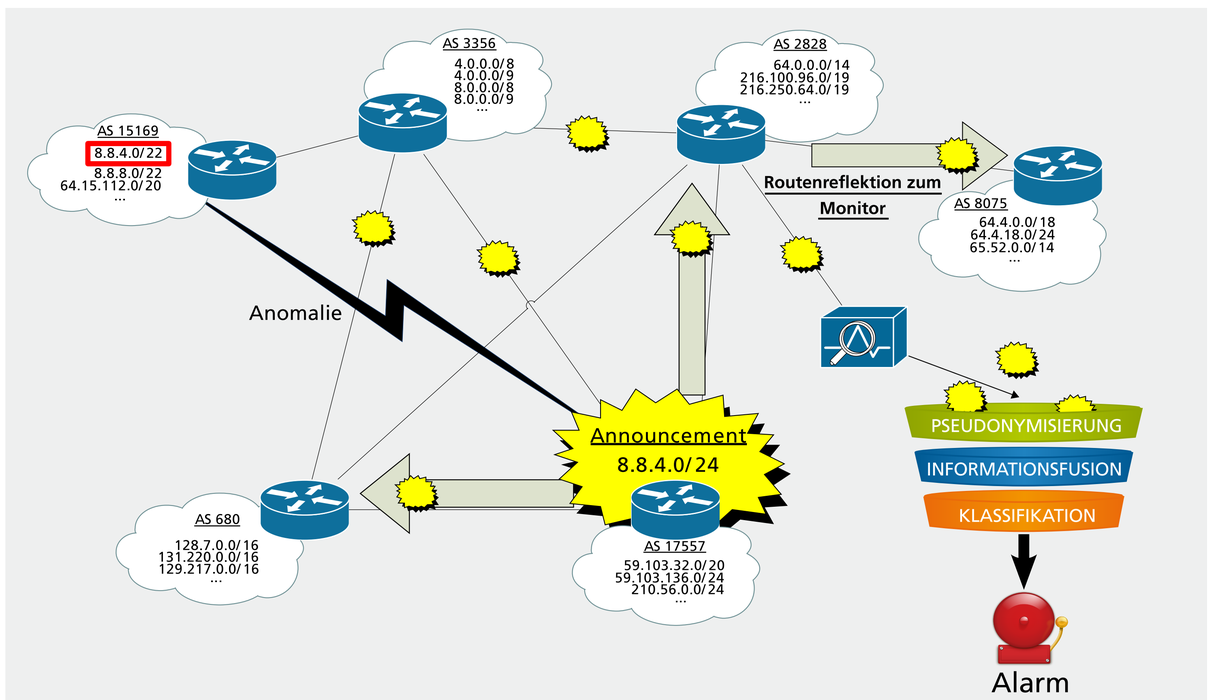
Fusion von Botnetz-Daten



Fusion von Botnetz-Daten zum besseren Verständnis von Teilinformationen.

Die Beschreibung der Merkmale von Botnetzen können durch die Heterogenität der beteiligten Systeme und die große Vielfalt genutzter Techniken sehr unterschiedlich ausfallen. Der Verbund von heterogener Sensorik kann daher der Detektion von Botnetzen in besonderem Maße dienen. MonIKA ermöglicht den Austausch von Informationen zwischen Sensoren verschiedener Art zur Steigerung der Effizienz und aggregiert alle verfügbaren Informationen zu umfassenden und informationsreichen Lagebildern erkannter Botnetze.

Klassifikation von BGP-Anomalien



Detektion von BGP-Anomalien durch Daten verschiedener Beobachtungspunkte.

Anomalien im Inter-Domain-Routing werden durch Fehlkonfigurationen, Hardwareausfälle und Angriffe verursacht. MonIKA nutzt geografisch verteiltes Monitoring, um sowohl gezielte Angriffe als auch Fehlkonfigurationen frühzeitig erkennen zu können. Auftretende Konflikte werden, soweit möglich, durch Klassifikationsalgorithmen untersucht und klassifiziert. Die manuelle Untersuchung nicht klassifiziertbarer Konflikte unterstützt den automatisierten Prozess und dient der Verbesserung der Klassifikationsalgorithmen.

Fraunhofer FKIE
Westfälische Wilhelms-Universität Münster
CASSIDIAN AN EADS COMPANY
ULD Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein
GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung