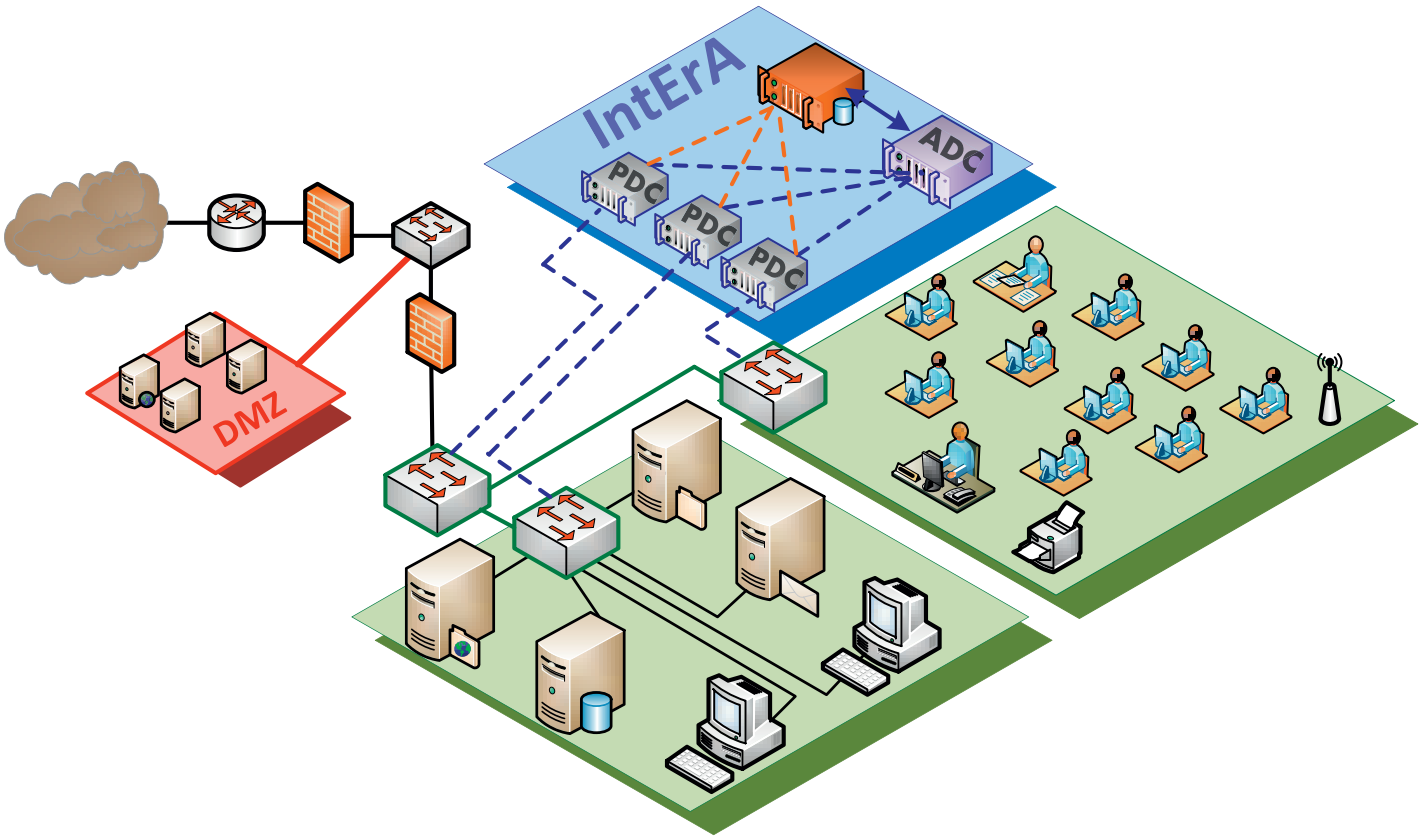
IntErA

Intelligente Erkennung von Cyber-Attacken auf IT-Infrastrukturen



Überblick

Das Framework IntErA wird eine Weiterentwicklung des anomalie-basierten Ansatzes aus dem Vorgängerprojekt SecMonet zu einem hybriden, selbstlernenden und dadurch äußerst flexiblen Intrusion Detection System (IDS) darstellen. Es wird in der Lage sein, den Netzwerkverkehr in zwei Stufen zu analysieren, wobei bereits bekannte Angriffe durch Musterabgleich mit geringstmöglichem Aufwand detektiert, neue Muster für bisher unbekannte Anomalien erzeugt werden, und sich somit selbstlernend dem veränderlichen Zustand des Netzwerkes kontinuierlich anpassen. Einer der Schwerpunkte der Forschungsarbeiten wird auf der Verfolgung von Strategien zur Verteilbarkeit und Parallelisierung der einzelnen Komponenten und deren Module liegen, um größtmögliche Skalierbarkeit gewährleisten zu können.

Hochschule Fulda
University of Applied Sciences

Prof. Dr. Ulrich Bühler
u.buehler@informatik.hs-fulda.de
T 0661 9640-325

M.Sc. Maher Salem
maher.salem@informatik.hs-fulda.de
T 0661 9640-225

Hochschule Fulda
Fachbereich Angewandte Informatik
Forschungsgruppe Network & Data Security (NDSec)
Marquardstraße 35
36039 Fulda

www.hs-fulda.de/NDSec

Hintergrund

Cyber-Attacken erfolgen zunehmend in allen digitalen Kommunikationsnetzen und bedrohen existenzielle Werte von Unternehmungen und persönliche Daten der Bürgerinnen und Bürger nicht nur in sozialen Netzwerken. Datenschutz und Privatsphäre müssen trotz Internet, Mobilfunk und Heimnetzwerken in einem angemessenen Umfang gewährleistet sein. Das Erkennen solcher Angriffe schon während ihrer Entstehung ermöglicht das frühzeitige Ergreifen entsprechender Gegenmaßnahmen und bietet daher Schutz vor dem Verlust vertraulicher Daten.

Vorgehensweise

Der zu entwickelnde Prototyp soll die sehr umfangreichen Netz- und Hostdaten verschiedener IT-Infrastrukturen (Mobilfunknetze, Cloud Computing, Smart Meter und Grid, Soziale Netze, Webcam, Heimnetzwerke) effektiv sammeln, die Infektionswege von Malware analysieren, unbekannte Anomalien frühzeitig detektieren und diese in Form speziell erzeugter Anomalie-Signaturen in einer adaptiven Datenbank hinterlegen. Der hybride Ansatz ermöglicht so einen optimalen Schutz auch vor bisher unveröffentlichten Schwachstellen (Zero-Day Vulnerabilities). Das intelligente IDS IntErA besteht aus den Komponenten „Pattern-based Detection Component" (PDC), „Anomaly-based Detection Component" (ADC) und der adaptiven Pattern-Datenbank (siehe Abbildung).

Während die Komponente PDC eine Vorfilterung und Normalisierung der erhaltenen Netzwerkdaten durch Abgleich mit den in der Pattern-Datenbank hinterlegten Muster der detektierten Anomalien durchführt, eruiert die Komponente ADC Abweichungen von einem robusten normalen Netzzustand auch unter Analyse verschiedener Payload-Informationen und generiert weitere bzw. adaptiert vorhandene Muster. Durch die kaskadierte Integration des hybriden Systems mit weitestgehender Parallelisierung der Funktionalitäten der Komponenten wird die effiziente Überwachung einzelner Netzwerksegmente in IT-Infrastrukturen mit hoher Skalierbarkeit erreicht und Cyber-Attacken frühzeitig erkannt.

Ausblick

Auf der Grundlage von IntErA werden unterschiedliche Produkte weiter entwickelt, wie. z. B. Apps für Smartphones oder Plug-ins für Webanwendungen. Auch ist vorgesehen, das Framework als hardwarebasiertes eigenständiges Produkt zu konzipieren und so als Appliance zur Verfügung zu stellen. Die verteilte Installation mehrerer adaptiver Pattern-Datenbanken im Netzwerk wird die Erkennungsrate neuer Angriffe wesentlich erhöhen.

GEFÖRDERT VOM

Bundesministerium für Bildung und Forschung

Projektpartner

Das Projekt wird in enger Zusammenarbeit mit dem Partnerunternehmen IT-Security@Work GmbH durchgeführt. Beteiligt sind weiterhin EDAG GmbH & Co. KG und Wissenschaftler der Hochschule Fulda und der Universität Kassel.

IntErA

IntErA is a further research project in Network and Data Security group at the University of Applied Sciences Fulda. The Framework consists of pattern-based detection component (PDC), anomaly-based detection component (ADC), and an adaptive pattern-database. These components are interconnected using secure communication protocols and they are able to interact in a parallel scenario. The component PDC will continuously receive the network traffic and match it with the database to detect unknown attacks earlier and filter them accordingly. Then the ADC component will examine the traffic data intensively by comparing it (in consideration of payload) with a robust predefined normal network behavior model to generate an adaptive pattern and store it in the pattern-database. The main goal is to develop a tool to uncover unknown Cyber-Attacks in an early state. This project is funded by the German Federal Ministry of Education and Research (BMBF).