



idalab setzt **Verfahren der Anomalieerkennung** ein,  
um Hackerangriffe zu bekämpfen.

## MIND - Maschinelles Lernen zur Bekämpfung von Hackerangriffen

Erkennung unbekannter Hackerangriffe in Echtzeit durch den Einsatz  
Maschinellen Lernens in Intrusion Detection Systemen

### Intrusion Detection Systeme (IDS)

Technischer Fortschritt führt insbesondere in der Informationstechnologie  
zu einem stark anwachsenden Datenaustausch, der die Gefahr neuartiger  
Angriffe auf Computersysteme ansteigen lässt. Herkömmliche passive,  
regelbasierte Techniken reichen zum Schutz vor solchen Einbruchsarten  
nicht mehr aus: Sie können unbekannte Attacken nicht erkennen und  
nicht angemessen auf sie reagieren.

Intrusion Detection (ID) ist ein Ansatz zur aktiven Überwachung von Com-  
putersystemen. Als Intrusion Detection System (IDS) bezeichnet man eine  
Zusammenstellung von Werkzeugen, die den gesamten Aufdeckungspro-  
zess von der Ereigniserkennung über die Auswertung bis hin zur Eskala-  
tion und Dokumentation unterstützt.

Klassische IDS erkennen bereits bekannte Einbruchs- und Manipula-  
tionsversuche auf Basis von Signaturen (Fingerabdrücken), die im System  
hinterlegt werden. Während ein solches Vorgehen für bekannte Angriffe  
gut geeignet ist, versagt es bei neuen Angriffsmustern. Die Zeitspanne  
zwischen einer neuen Angriffsart und deren Identifizierung ist jedoch in  
der Praxis entscheidend.

Die Herausforderung für moderne Intrusion Detection Systeme besteht  
darin, diese Instrumente um eine aktive Komponente zu erweitern: Über  
automatisierte Anomalieerkennungsverfahren werden Angriffe oder Miss-  
brauchsversuche im Moment des Geschehens erkannt und gemeldet. Sie  
sind somit in der Lage, unbekannte Einbruchsarten aufzudecken und in  
Zukunft zu berücksichtigen.

#### Ziel

Optimierung von Intrusion Detection Systeme-  
men (IDS) zur aktiven Verhinderung von  
Hackerangriffen auf Rechnersysteme

#### Lösung

Einsatz moderner statistischer Lernver-  
fahren zur automatischen Erkennung neuer  
Angriffsszenarien

#### Anwendung

Erhöhung der Computersicherheit, Überwa-  
chung von Transaktionsströmen

#### Branche

IT-Sicherheit, Banken

Passive Verfahren zum Schutz vor unbekann-  
ten Hackerangriffen reichen heute nicht mehr  
aus, um Computersysteme zu schützen.

Zur aktiven Überwachung werden heute  
Intrusion Detection Systeme eingesetzt: Sie  
erkennen über automatisierte Anomalieerken-  
nungsverfahren Angriffe im Moment des  
Geschehens.

## Maschinelles Lernen für Intrusion Detection (MIND)

Das Bundesministerium für Bildung und Forschung (BMBF) fördert seit 2004 das Kooperationsprojekt MIND. Ziel des Projekts ist es, durch den Einsatz moderner statistischer Verfahren des Maschinellen Lernens neuartige IDS-Systeme zu entwickeln. Dabei stehen zwei Aspekte im Fokus:

1. Signifikante Senkung der falschen Alarme bei gleichzeitig hohen Trefferquoten für echte Angriffe.
2. Erkennung unbekannter Angriffe durch moderne Anomalieerkennungsverfahren vor dem Schadensfall.

Die Techniken des Maschinellen Lernens sind für beide Fragestellungen besonders gut geeignet. Sie können hochpräzise und sensibel Vorhersagen treffen, so dass sich das Verhältnis falscher Alarmen und entdeckter Angriffen gut kontrollieren lässt.

Noch größere Bedeutung haben diese Techniken für die Erkennung unbekannter Angriffe: Über Anomalieerkennungsverfahren werden unbekannte Einbrüche identifiziert, der hohe zeitliche und intellektuelle Aufwand für die Erstellung von Signaturen entfällt. Das System lernt, sich selbstständig und dynamisch an veränderte Infrastrukturen und Rahmenbedingungen anzupassen. Dies stellt einen entscheidenden Beitrag zur Kostenreduktion, Effizienzsteigerung und Anwendbarkeit von IDS dar.

idalab ist im Rahmen des Projekts damit befasst, moderne Lernverfahren für den Echtzeiteinsatz in Intrusion Detection Systemen einsatzfähig zu machen. Darüber hinaus unterstützt idalab aktiv die Umsetzung einer prototypischen Implementierung der Ergebnisse.

Die gewonnenen Erkenntnisse sind nicht auf den Bereich der Computersicherheit beschränkt, sondern können überall dort zum Einsatz kommen, wo große Datenmengen überwacht und Unregelmäßigkeiten frühzeitig und zuverlässig erkannt werden müssen.

Die Partner im Projekt sind Fraunhofer Institut FIRST, idalab GmbH und St. Petersburg Institut der Russischen Akademie der Wissenschaften als Auftragnehmer von FIRST, Siemens AG und IT Service Omikron GmbH.

Im Verbundprojekt MIND werden statistische Verfahren des Maschinellen Lernens für die Entwicklung moderner Intrusion Detection Systeme eingesetzt.

Die Techniken des Maschinellen Lernens zeigen hohe Trefferquoten für echte Angriffe und senken gleichzeitig signifikant die Anzahl falscher Alarme. Sie sind besonders geeignet für die Identifizierung unbekannter Angriffe.

idalab bringt diese Lernverfahren zum Echtzeiteinsatz in Intrusion Detection Systemen und unterstützt die Umsetzung einer prototypischen Implementierung der Ergebnisse.

### Wer ist idalab?

idalab ist eine Unternehmensberatung für Statistik. Wir beraten in datenbezogenen Fragestellungen, analysieren Daten mit modernsten Forschungsmethoden und entwickeln spezifische Statistik-Software.

### Ansprechpartner

Dr. Sebastian Mika

**idalab GmbH**  
Sophienstr. 24  
10178 Berlin  
Germany



T +49.30.81 45 13-0 · F +49.30.81 45 13-10  
www.idalab.de · info@idalab.de

Geschäftsführer  
Dr. Sebastian Mika  
Dipl.-Psych. Malte Friedrich-Freksa