



FIDeS

Frühwarn- und Intrusion Detection System

Auf Basis von heterogenen Methoden der Künstlichen Intelligenz wird ein Frühwarnsystem entwickelt, das die Analyse von Angriffen und die Durchführung von Gegenmaßnahmen unterstützt.



**SICHERHEIT UND
ZUVERLÄSSIGKEIT**

01000001001000011011001
10010001000111100100001
00100100100110010001010
00011001101000111010011

Innovation durch Intelligenz
Software macht's!

10001100101110
11000001010100

IKT 2020
Softwaresysteme

10001100100110
110000101010000
1011
1100

Geschäftsprozesse im Internet/Intranet als Zielscheibe professioneller Hackerangriffe

Viele sicherheitskritische Geschäftsprozesse wie z.B. finanzielle Transaktionen werden heute elektronisch abgebildet; ein Ausfall der Kommunikation oder unerlaubte Zugriffe auf Geschäftsprozesse können hier zu einem erheblichen finanziellen Schaden oder zumindest zu einem Imageverlust für die betroffenen Unternehmen führen. Das Internet muss zunehmend als gemeinsame kritische Infrastruktur betrachtet werden. Neben der stärkeren Sensibilisierung von Mitarbeitern für die Gefahren geht es strukturell um die Frage, wie sich Angriffe von professionellen Datenspionen frühzeitig erkennen lassen. Ein leistungsstarkes Konsortium von 7 Partnern aus Wirtschaft und Wissenschaft hat sich mit dem Forschungsprojekt FIDeS zum Ziel gesetzt, ein umfassendes Assistenzsystem zur Früherkennung von Angriffen aus dem Internet und in lokalen Netzen zu entwickeln. Das Assistenzsystem soll nachvollziehbare Erklärungen für einen Angriff liefern. Es soll Angriffswissen, angreifbare Systeme und Systemkomponenten sowie Gegenmaßnahmen erläutern und im Falle eines Angriffs mit dem Nutzer interagieren.

Internet-Analyse-System (IAS)

Ausgangspunkt von FIDeS ist das bestehende Internet-Analyse-System (IAS) der Fachhochschule Gelsenkirchen. Anders als Firewalls an den Übergängen des offenen Internets zu internen gesicherten Intranets besteht das IAS aus Sonden, die den Netzverkehr an Kommunikati-



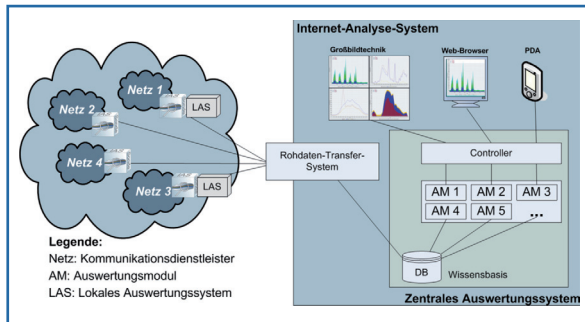
onsleitungen in definierten Teilnetzen des Internets abgreifen und Kommunikationsparameter auf verschiedenen Ebenen messen. Durch ein Zusammenführen vieler lokaler Sichten erstellt es eine globale Beschreibung des Sicherheitszustandes des Internets. Das IAS soll nun um verschiedene Komponenten und Verfahren auf Basis von Methoden der Künstlichen Intelligenz (KI) erweitert werden.

Einsatz von Methoden der Künstlichen Intelligenz

Das Frühwarn- und Intrusion-Detection-System FIDeS wird prototypisch auf Basis von neuesten Forschungsergebnissen zu Verfahren der Künstlichen Intelligenz (KI) entwickelt. Um Angriffssituationen/-muster rechtzeitig identifizieren zu können, soll das System verschiedene Eigenschaften besitzen:

Frühwarnfunktionalität: Wesentlich für das Frühwarnsystem ist die Möglichkeit der Vorhersage von Angriffen. Basis für die rechtzeitige Erkennung unbekannter Angriffe sind so genannte Attack Patterns, also Angriffsmuster, die bei den bislang bekannten Angriffen als typische Angriffstechniken identifiziert wurden. Ein Beispiel ist das Einschleusen von Code oder von Programmargumenten in Internet-Sever. Die in FIDeS eingesetzten KI-Methoden repräsentieren aus solchen Attack Patterns bestehende Taktiken bzw. Angriffs-Strategien, die auch die Wahl der Gegenmaßnahmen bestimmen. Verbunden damit ist ferner die „Erklärungsadäquatheit“, d. h. der Sicherheitsverantwortliche erhält nicht nur die Warnung, dass es sich um einen Angriff handelt, sondern auch die Erklärung dazu. Da ein Angriff oft aus mehreren Schritten besteht, kann er meist schon vorhergesagt werden, bevor er vollständig durchgeführt worden ist.

Verwendung und Bereitstellung von zusätzlichem Expertenwissen: Nicht immer wird ein herkömmliches Intrusion Detection System (IDS) die Angriffssituation selbstständig erkennen bzw. richtig deuten können. Die meisten IDS und insbesondere solche zur Anomalieerkennung verursachen zum Teil Fehlalarme (false positives) oder erkennen die Angriffe nicht (false negatives). Aus diesem Grunde muss auch dem



Sicherheitsverantwortlichen die Möglichkeit gegeben werden, sein Fachwissen über Systeme und Angriffe dem IDS zur Verfügung zu stellen. Da das Fachwissen aber nicht über Textbausteine eingegeben wird, sondern manuell von den Technikern, variieren die Texte, so dass eine einfache regelbasierte maschinelle Auswertung nicht möglich ist. Um die in diesen Texten enthaltenen Informationen für die Lernverfahren nutzbar zu machen, können KI-Verfahren des Textverstehens eingesetzt werden. Durch die eingeschränkte (von technischen Begrifflichkeiten beherrschte) Domäne und eine niedrige Variabilität der Texte sind flache und effiziente Verfahren der Textanalyse anwendbar.

Die Sicherheitsverantwortlichen der Unternehmen benötigen gerade im Falle professioneller Angriffe auf die IT-Systeme konkrete Handlungsanweisungen. Deshalb soll das Fachwissen in einem verteilten Expertensystem Sicherheitsverantwortlichen und Netzbetreibern zur Verfügung gestellt werden, um nicht nur Angriffe erkennen, sondern auch geeignete Gegenmaßnahmen ergreifen zu können.

Behandlung neuer Protokolle: In diesem Projekt werden nicht nur die verbreiteten Internet-Protokolle wie z.B. HTTP und FTP behandelt, sondern auch neuere Protokolle wie z.B. VoIP (Voice over IP) oder SOAP. Hierdurch können neben Angriffen auf Internetknoten auch Sicherheitsvorfälle, die von mobilen Endgeräten ausgehen, und missbräuchliche Zugriffe auf sicherheitskritische, IT-gestützte Geschäftsprozesse von Unternehmen erkannt werden.

Analyse von Log-Dateien: Bei der Überwachung von Netzen werden an Firewalls verschiedenste Daten in Log-Dateien mit protokolliert. Die Log-Dateien können aufgrund der Fülle und

der Verschiedenheit der Daten sehr umfangreich sein, so dass eine manuelle Selektion kritischer Indikatoren unmöglich ist. Viele dieser Daten sind allerdings auch für eine weitere Untersuchung nicht mehr relevant, weil sie beispielsweise durch bereits an den Firewalls abgewehrte und damit fehlgeschlagene Angriffe verursacht wurden. Ziel ist die Entwicklung eines Analyse-Moduls für Log-Dateien, mit welchem abweichende Zugriffsmuster ermittelt werden können.

Effizientes Erkennen von Angriffen: Es soll aufgrund von zusätzlichen off-line Lernverfahren möglich sein, die gelernten kritischen Muster in Echtzeit und neue Angriffe möglichst effizient und frühzeitig zu erkennen.

Angemessene Darstellung von Analyseergebnissen: Missbräuchliche Zugriffe müssen rechtzeitig durch den Sicherheitsverantwortlichen/Administrator erkannt werden. Die Analyseergebnisse müssen dafür angemessen und übersichtlich dargestellt sowie ein Mechanismus für die Alarmierung im Falle eines Angriffs gefunden werden. Nutzbare Sicherheitstechnologien zu entwickeln, gehört zu den schwierigsten und bislang nicht hinreichend gelösten Problemen der IT-Sicherheit. Aus diesem Grunde sollen auch Usability-Fachleute an der Entwicklung der Benutzungsoberflächen beteiligt werden.

Simulator zum Testen des Frühwarnsystems: Es wird ein Simulator entwickelt, mit dem Angriffsszenarien unter realistischen Zeit- und System-Zwängen erzeugt werden. Dieser Simulator dient zur funktionalen Validation und zur Sicherstellung des hinreichenden Abdeckungsgrades des Frühwarnsystems. Es wird erwartet, dass mit diesem Simulator auch andere Intrusion-Detection-Systeme getestet werden können.

Projektdaten:

Förderprogramm:

IKT 2020 / Forschung für Innovationen

Förderschwerpunkt:

Sicherheit und Zuverlässigkeit

Förderkennzeichen: 01IS08022

Fördervolumen: 2,7 Mio. €

Laufzeit: 01.09.2008-31.08.2011

Projektkoordinator:

Prof. Dr. Otthein Herzog
Am Fallturm 1
28359 Bremen

Telefon: +49 (0)421 218-7090
Fax: +49 (0)421 218-7196
E-Mail: herzog@informatik.uni-bremen.de
Internet: www.tzi.de

Projektpartner:

Technologie-Zentrum Informatik (TZI), Universität Bremen
mobile solution group GmbH, Bremen
Institut für Internet-Sicherheit if(is), Fachhochschule Gelsenkirchen
ZF Friedrichshafen AG, Lemförde
T-Systems Enterprise Services GmbH, Darmstadt
Nicos AG, Münster
algorithmica technologies GmbH, Bremen

Weitere Informationen:

Projektträger des BMBF
Softwaresysteme und Wissenstechnologien
im Deutschen Zentrum
für Luft- und Raumfahrt e.V. (DLR)
Rutherfordstr. 2
12489 Berlin

Telefon: (030) 67055 741
Internet: www.pt-it.pt-dlr.de

Herausgeber:

Bundesministerium für Bildung
und Forschung (BMBF)
Referat Öffentlichkeitsarbeit
11055 Berlin

100011001001100000101001100
01001111011011001110001100100011
1100011001101000111010011110
011101001011011010101110111010010110010110

Stand April 2009