



Frühwarn-System für Bundesministerium für Bildung und Forschung

FIDeS soll Regierungsdaten vor Angriffen aus dem Internet schützen

11.06.2009 | Redakteur: Peter Schmitz



Das Frühwarn- und Intrusion Detection System FIDeS soll mit KI-Methoden Angriffe aus dem Internet erkennen und abwehren.

Das Bundesministerium für Bildung und Forschung hat die nicos AG ausgewählt, zusammen mit sechs weiteren Projektpartnern das Frühwarn- und Intrusion Detection System „FIDeS“ zu entwickeln. Das System soll in der Lage sein, Angriffe von professionellen Datenspionen via Datennetz zu analysieren und die Durchführung von Gegenmaßnahmen unterstützen.

Aktuelle Intrusion Detection Systeme (IDS) helfen zwar durchaus dabei die Netzwerksicherheit zu verbessern, aber sie leiden nach der Meinung vieler Experten vor allem unter zwei Problemen. Zum einen arbeiten die Systeme meist signaturbasiert und können daher nur Angriffe entdecken, für die es bereits eine Signatur gibt. Zum zweiten tauchen in den Logs moderner IDS oft auch eine große

Masse an Fehlalarmen auf. Aus dieser Masse an Daten müssen Sicherheitsverantwortliche noch immer größtenteils manuell die tatsächlichen Angriffe herausfiltern.

Das Assistenzsystem FIDeS soll an diesen beiden Problempunkten ansetzen und dabei auf Basis von neuesten Forschungsergebnissen zu Verfahren der Künstlichen Intelligenz (KI) Lösungen entwickeln. Ziel ist es, die Angriffserkennung und die anschließende forensische Analyse zu verbessern.

Um Angriffssituationen aus Inter- und Intranet rechtzeitig zu identifizieren, soll das System u.a. über eine Frühwarnfunktionalität verfügen, die Systemkomponenten der Angreifer erkennen und Gegenmaßnahmen vorschlagen kann. Dabei wird FIDeS so konzipiert, dass es über Lernverfahren die kritischen Muster erkennt und analysiert.

Bildergalerie



Klicken Sie auf ein Bild um die Bildergalerie zu öffnen (1 Bilder)

Künstliche Intelligenz als Basis von FIDeS

Das im Auftrag des Bundesamts für Sicherheit in der Informationstechnik (BSI) vom Institut für Internet-Sicherheit der FH Gelsenkirchen entwickelte Internet-Analyse-System (IAS) soll als Kernsystem die statistische Anomalie-

Erkennung im Netzwerk übernehmen. So soll FIDeS dann in der Lage sein, Angriffe zu entdecken, die normale IDS übersehen. Das IAS überwacht dazu eine Vielzahl an Daten im Paketstrom und definiert so das Normalverhalten der Netzwerkkommunikation.

Abweichungen von diesem „Normalzustand“ können dann als Anomalien gemeldet und von FIDeS ausgewertet werden. Dazu gleicht das System die Daten mit normalen Intrusion Detection Systemen wie Snort und anderen Datenquellen ab.

Durch den Einsatz von Verfahren der KI ist gewährleistet, dass das IAS in der Lage ist das Normalverhalten der Netzwerkkommunikation an beliebigen Standorten zu erkennen. Außerdem kann das IAS sich so auch bei größeren Veränderungen im überwachten Netzwerk mit der Zeit anpassen und muss nicht aufwändig von Hand neu konfiguriert werden.

Projektpartner aus Wirtschaft und Forschung

Die nicos AG wurde vom Bundesministerium für Bildung und Forschung für diesen Expertenkreis von Projektpartnern ausgesucht, da das deutsche Unternehmen eine umfangreiche Expertise in den Segmenten International Network Operating (WAN), Data Protect & Security (IT Security), Data Backup und Storage sowie System Control aufweist.

„Wir sind stolz darauf, dass das Bundesministerium für Bildung und Forschung uns als Partner für dieses hochsensible Projekt gewinnen wollte. Dies spiegelt unser Know-How wider und zeigt ein Vertrauen insbesondere in unsere Kompetenz“, so Thomas Brosch, Vorstand der nicos AG.

Weitere Projektpartner sind das Technologie-Zentrum Informatik und Informationstechnik der Uni Bremen, das Institut für Internet-Sicherheit der FH Gelsenkirchen, die ZF Friedrichshafen AG, T-Systems, die mobile solution group, sowie Algorithmica Technologies GmbH.

Copyright © 2009 - Vogel Business Media