h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

HOCHSCHULKOMMUNIKATION

Simon Colin
Pressesprecher

Tel +49.6151.16-38036
Fax +49.6151.16-38900
simon.colin@h-da.de www.h-da.de

GEMEINSAME PRESSEMITTEILUNG
04.10. 2017

Wie kann ein Angriff auf IT-Systeme nachgewiesen werden? Forschungsgruppen entwickeln Methoden der forensischen Netzwerkanalyse

Darmstadt/Frankfurt am Main – Eine vollständige Absicherung der IT-Infrastruktur in Unternehmen und anderen Einrichtungen ist auch beim Einsatz neuester Technologien nicht möglich. Angriffe auf Computer-Netzwerke sind im Nachhinein nur schwer nachvollziehbar: Aufgrund der großen Datenmengen in einem Netzwerk ist eine Speicherung von Daten über den Angriff für eine spätere Analyse kaum durchführbar; die Daten werden zumeist gelöscht und das Netzwerk neu aufgesetzt. Im Forschungsprojekt „Forensische Netzwerkanalyse mittels Complex Event Processing (ForCEPs)“ untersuchen Wissenschaftlerinnen und Wissenschaftler der Hochschule Darmstadt (h_da) und der Frankfurt University of Applied Sciences (Frankfurt UAS) neue Methoden zur Speicherung und Analyse der Netzwerkdaten, um Angriffe frühzeitig erkennen und zurückverfolgen zu können. Das Projekt ist auf einen Zeitraum von vier Jahren angelegt und wird bis August 2021 vom Bundesministerium für Bildung und Forschung gefördert.

„Spätestens seit dem Angriff auf die IT-Infrastruktur des Deutschen Bundestages im Jahr 2015 ist klar, wie wichtig es ist, Angriffe anhand gespeicherter forensischer Informationen analysieren zu können. Damit soll einerseits der Angriff abgewehrt und andererseits die Schwachstellen im System geschlossen werden, so dass künftige Angriffe keinen Erfolg mehr haben. An diesem Punkt setzt unser Projekt an: Wir entwickeln mit modernen Datenverarbeitungstechnologien Methoden zur IT-forensischen Netzwerkanalyse“, beschreibt Prof. Dr. Martin Kappes, Leiter der Forschungsgruppe für Netzwerksicherheit, Informationssicherheit und Datenschutz an der Frankfurt UAS, die Bedeutung des Projekts. ForCEPs nutzt mit „Complex Event Processing (CEP)“ eine moderne Technologie zur Verarbeitung großer Datenmengen.

„IT-forensische Untersuchungen in einem Netzwerk erfolgen oft unter erheblichem Zeitdruck, weil diese nicht ohne Weiteres abgeschaltet werden können. Zudem sollten Institutionen Datenquellen bereits vor einem Sicherheitsvorfall datenschutzkonform eingerichtet haben. Folglich ist ein standardisiertes Vorgehen bei netzwerkforensischen Untersuchungen essenziell“, erklärt Prof. Dr. Harald Baier vom Fachbereich Informatik der Hochschule Darmstadt, der eine Arbeitsgruppe zu Internet-Sicherheit und digitaler Forensik leitet. ForCEPs entwickelt daher ein Vorgehensmodell zur Netzwerkforensik auf Basis des Leitfadens „IT-Forensik“ des Bundesamtes für Sicherheit in der Informationstechnik.

Die Frankfurt UAS übernimmt die Gesamtprojektleitung, zudem die Bereiche Systemarchitektur, verteilte Sensorik und Datenspeicherung sowie Detektionsalgorithmen zur Realzeiterkennung von Angriffen und Datenschutz. Die Hochschule Darmstadt leitet die Anforderungsanalyse an netzwerkforensische Daten, identifiziert relevante Datenquellen, konzipiert und implementiert die Vorverarbeitung der Daten sowie die

h_da
HOCHSCHULE DARMSTADT
UNIVERSITY OF APPLIED SCIENCES

HOCHSCHULKOMMUNIKATION

Simon Colin
Pressesprecher

teilautomatisierten forensischen Analysen. Als ein zentrales Ergebnis entwickelt sie das Vorgehensmodell.

In ForCEPs sind zahlreiche Praxispartner eingebunden: Hessisches Landeskriminalamt, Software AG, „media transfer AG", BES Data Terminals GmbH, Frankfurter Verband für Alten- und Behindertenhilfe e.V. sowie Institut für Datenschutz, Arbeitsrecht und Technologieberatung „d+a consulting" (IDA). Als wissenschaftliche Partner sind die Universität Cádiz, Spanien, sowie die Technische Universität Darmstadt in das ForCEPs-Konsortium eingebunden.

Das Projekt „IngenieurNachwuchs 2016: Forensische Netzwerkanalyse mittels Complex Event Processing" (Förderkennzeichen 13FH019IA6) wird im Rahmen des Förderprogramms „Forschung an Fachhochschulen" vom Bundesministerium für Bildung und Forschung gefördert.

Kontakt:
Hochschule Darmstadt, Fachbereich Informatik, Prof. Dr. Harald Baier, Telefon: +49 6151-16-30089, E-Mail: harald.baier@h-da.de, www.dasec.h-da.de

...

Frankfurt University of Applied Sciences, Fachbereich 2: Informatik und Ingenieurwissenschaften, Prof. Dr. Martin Kappes, Telefon: +49 69 1533-2791,
E-Mail: kappes@fb2.fra-uas.de, www.frankfurt-university.de/?3208