**Universitätsleitung**

Abteilung Kommunikation und Marketing

# Pressemitteilung

| | |
|---|---|
| Auskunft erteilt | Katrina Jordan<br>0851 509-1439 |
| Telefax | 0851 509-1433 |
| E-Mail | kommunikation<br>@uni-passau.de |
| Datum | 22. September 2017 |

## EU-Projekt zu Cyber-Sicherheit: Passauer Team macht Computer immun gegen Attacken

**Ein europaweites Team um Prof. Dr. Siegfried Handschuh rüstet kleine Behörden und Unternehmen gegen Cyber-Angriffe: Die Forscherinnen und Forscher setzen auf Systeme, die sich selber heilen können – und zwar Mithilfe von Methoden der maschinellen Verarbeitung von Sprache. Die EU-Kommission fördert das Projekt.**

Über die Attacke auf den Deutschen Bundestag vor zwei Jahren wurde viel berichtet. Doch auch kommunale Verwaltungen und der Mittelstand kämpfen zunehmend mit Angriffen aus dem Cyberspace. „Es herrscht Krieg da draußen“, sagt Prof. Dr. Siegfried Handschuh, Inhaber des Lehrstuhls für Informatik mit Schwerpunkt Digital Libraries and Web Information Systems. Noch etwas macht diesen Organisationen zu schaffen: Die neue Rechtsprechung, die manche Anbieter verpflichtet, gravierende Störungen an eine Kontaktstelle beim Bundesamt für Sicherheit in der Informationstechnologie (BSI) zu melden. Doch das Passauer Forschungsteam hat herausgefunden, dass gerade der Mittelstand und kleine Behörden meist nicht über Expertinnen und Experten für IT-Sicherheit verfügen.

### System, das sich selber heilt

Gemeinsam mit einem europaweiten Forschungsteam arbeitet Prof. Dr. Handschuh an einer Lösung: ein System, das sich selber heilt, vor Attacken schützt und verdächtige Vorfälle automatisch an nationale und EU-Behörden meldet. „Unsere Cybersecurity-Lösung analysiert den Zusammenhang des Angriffs, erkennt damit automatisch den Vorfall, visualisiert diesen und ermöglicht den Informationsaustausch mit wichtigen nationalen und EU-basierten Autoritäten.“

Ein Beispiel: Die Mitarbeiterin einer Stadtverwaltung will eine Mail schreiben. Sie stößt auf Probleme, denn eine Taste schlägt nicht richtig an. Sie meldet dies der Technik. Die Technik geht nun alle möglichen Ursachen durch, etwa ob es sich um ein Software- oder Treiberproblem handelt. Bis erkannt wird, dass es sich um eine Attacke handelt, haben die Hacker das System bereits übernommen.

**Maschinen lernen Text und Kontext**

Das Forschungsteam um Prof. Dr. Handschuh will das System gegen solche Vorfälle wappnen, indem es möglichst viele Muster solcher Angriffe in die Maschine einspeist, das System der Kommunalverwaltungen also auf solche Attacken trainiert. Die Verwaltungen sind untereinander vernetzt, so dass die Maschinen auch Informationen zu Vorfällen anderswo austauschen können und so voneinander lernen können. Die Forscherinnen und Forscher arbeiten mit „Advanced Big Data Analytics“ und Methoden des Natural Language Processing (NLP), der Erfassung natürlicher Sprache. NLP erkennt und analysiert Sprache, um den Sinn zur weiteren Verarbeitung zu extrahieren. Die Maschinen lernen also, nicht nur Texte, sondern auch die Zusammenhänge zu verstehen.

„Stellen Sie sich einen Gang zum Arzt vor“, sagt Projektmitarbeiter Dr. Adamantios Koumpis. „Sie schildern Ihre Symptome. Der Arzt geht nun sein Wissen und seine Erfahrungen mit bestimmten Krankheiten durch und zieht daraus Schlüsse. Seine Diagnose könnte aber noch genauer sein, wenn er auch das Wissen und die Erfahrungen weiterer Ärzte einbeziehen könnte.“ Und nicht nur das: Der Patient, also das System, soll sich selbst heilen können. Im obigen Beispiel also hätte das System die Attacke schnellstmöglich erkannt, die Schwächen behoben – und die Mitarbeiterin der Stadtverwaltung hätte keinerlei Probleme mit ihrer Tastatur.

**Beteiligt sind Expertinnen und Experten europaweit**

Noch etwas unterscheidet den Ansatz des Passauer Forschungsteams von der Konkurrenz: „Wir verwenden eine mehrsprachige Semantikunterstützung, um Sprachbarrieren im EU-Kontext zu berücksichtigen“, erklärt Prof. Dr. Handschuh. Zu diesem Zweck arbeiten die Passauer europaweit mit Expertinnen und Experten zusammen. Folgende Einrichtungen sind beteiligt:

Universität Oulu, Finnland
Universität Wien, Österreich
Caris Research Ltd, Großbritannien
3RDPLACE SRL, Italien
DashSoft ApS, Dänemark
PERACTON LIMITED, Irland
Innovative Secure Technologies P.C., Griechenland
ANDRIESSEN JEFFREY ELBERTUS BARTHOLOMEUS, Niederlande
ANCITEL SPA, Italien
Open Technology Services S.A., Griechenland
Stadtverwaltung von Rom, Italien
Stadtverwaltung von Larissa, Griechenland

*Für dieses Projekt werden im Rahmen der Finanzhilfevereinbarung Nr. 740723 Fördermittel aus dem Programm der Europäischen Union für Forschung und Innovation "Horizont 2020" bereitgestellt.*

**Rückfragen zu dieser Pressemitteilung** richten Sie bitte an das Referat für Medienarbeit, Tel. 0851 509-1439.