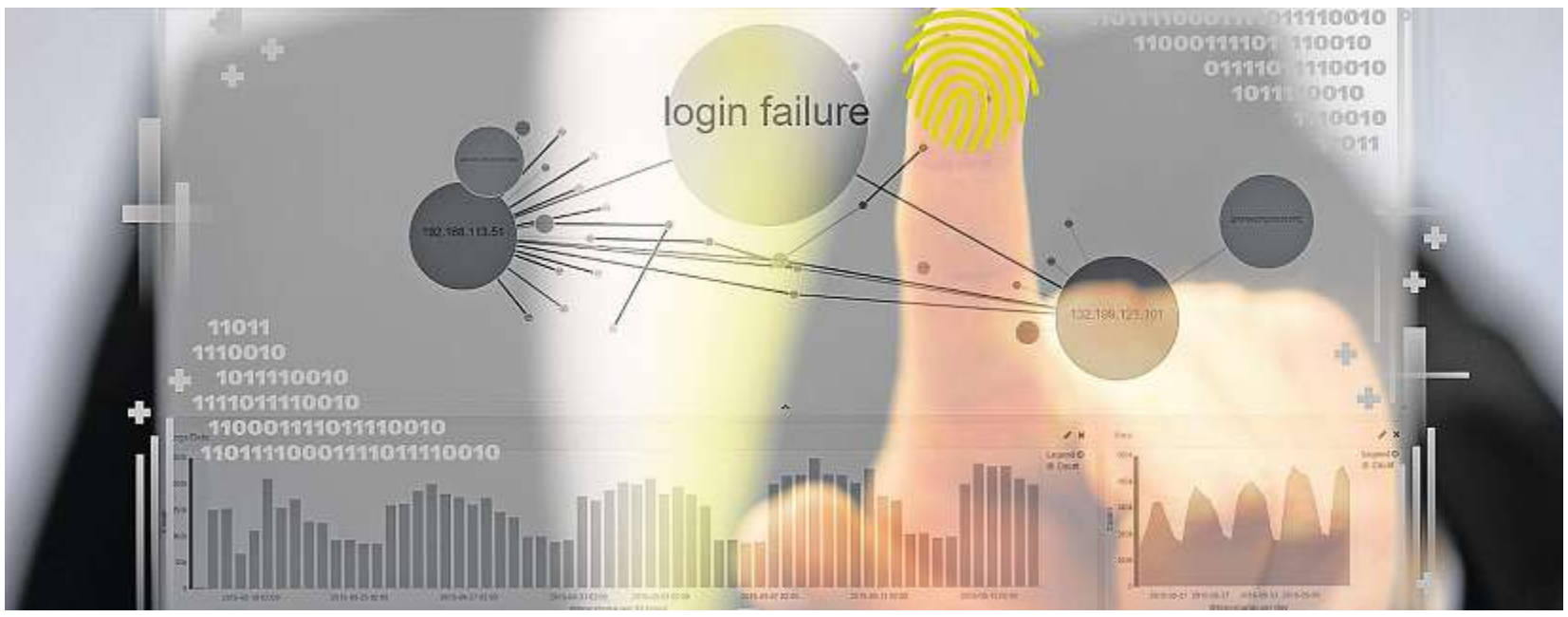
IT & KOMMUNIKATION

Schutz vor Cyberkriminellen und Spionage

Regensburger Forscher entwickeln Werkzeuge zur Erkennung digitaler Angriffe.



Das Projekt „DINGfest“ wird mit über 2,4 Millionen Euro gefördert. Foto: Universität Regensburg

REGENSBURG. Noch vor wenigen Jahren wurden IT-Systeme vornehmlich isoliert und innerhalb leicht zu schützender Grenzen betrieben. Derartige Systeme konnten nur innerhalb eines einzelnen Unternehmens oder in einem festen Organisationskontext kommunizieren. Diese Situation hat sich jedoch stark verändert. Moderne IT-Systeme gleichen eher fragilen Gebilden. Sie nutzen vielfältige, flexible, virtualisierte und hochgradig vernetzte Anwendungen. Komplexe und speziell auf ein Unternehmen oder auf eine Organisation zugeschnittene Angriffe nehmen in der jüngeren Vergangenheit zu. Die Angriffe verdeutlichen die Anfälligkeit und das Missbrauchspotenzial von IT-Systemen in drastischer Weise. In der deutschen Wirtschaft verursacht Computerkriminalität inzwischen jährliche Schäden von mehr als 10 Milliarden Euro. Eine Absicherung der IT-Systeme gegen Cyberangriffe und Cyberspionage ist daher für Wirtschaft und Gesellschaft entscheidend, um die Fortschritte und Chancen der Digitalisierung auch künftig nutzen zu können.

Vor diesem Hintergrund finanziert das Bundesministerium für Bildung und Forschung bis Ende Mai 2019 ein Verbundprojekt mit über 2,4 Millionen Euro, das neue Verfahren erforschen soll, um einerseits mit innovativen IT-forensischen Aufklärungsmethoden Angriffsszenarien untersuchen und verstehen zu können. Andererseits sollen mit diesen Erkenntnissen Möglichkeiten geschaffen werden, um solche Angriffe schon im Vorfeld und in Echtzeit erkennen und verhindern zu können.

Koordiniert wird das Forschungsprojekt mit dem Namen „DINGfest“ (**D**etekt**I**on, Visualisieru**NG**, **f**or**e**nsische Aufbereitung von **s**icherhei**t**svorfällen) von Prof. Dr. Günther Pernul vom Lehrstuhl für Wirtschaftsinformatik I der Universität Regensburg, die in dem Konsortium auch den größten Partner stellt. Zudem sind der Lehrstuhl Informatik I der Friedrich-Alexander-Universität Erlangen-Nürnberg sowie die Universität Passau an dem Projekt beteiligt. Vonseiten der freien Wirtschaft werden sie von Innowerk-IT aus Passau, den Regensburger Unternehmen Nexis sowie R-Kom und der Rechtsanwaltskanzlei Paluka, Sobola Loibl & Partner unterstützt, die sich um die datenschutzrechtlichen Aspekte der Projektarbeit kümmern.

Zusammen widmen sich die verschiedenen Projektpartner der Detektion schädlicher Systemzustände, der forensischen Analyse digitaler Spuren sowie der vertrauensvollen und pseudonymisierten Meldung von Sicherheitsvorfällen. Gemäß dem IT-Sicherheitsgesetz sind Betreiber kritischer Infrastrukturen unter anderem dazu verpflichtet, dem Bundesamt für Sicherheit in der Informationstechnik erhebliche IT-Störungen zu melden. Diese Meldung kann aber auch anonym erfolgen, um drohende Imageschäden durch die öffentliche Aufmerksamkeit zu verhindern. Zusätzlich ist im Projekt die Entwicklung eines modularen SW-Werkzeugkastens im Open-Source-Modell geplant. Diese Tool-Sammlung soll den Anforderungen an die Analyse komplexer IT-Infrastrukturen gerecht werden. Die einzelnen Module werden mit offenen Schnittstellen ausgestattet, die Dritte an eigene Anforderungen anpassen können. Insbesondere KMUs sollen von diesem Angebot profitieren. Sie können den entstandenen Software-Demonstrator als Open Source nutzen und als Startpunkt für eigene Produktentwicklungen und Dienstleistungen verwenden. Neben den technischen Details wird sich das Projekt auch intensiv den organisatorischen und juristischen – insbesondere datenschutzrechtlichen – Implikationen widmen.

Die große Innovationskraft des neuen Verbundvorhabens liegt in der Entwicklung solcher zentraler Module zur Erkennung und Analyse von Sicherheitsvorfällen und ihrer Meldung. Die geplanten Analysemodule erweitern bereits für sich genommen den Stand der Technik. Der große Nutzen entsteht erst im reibungslosen Zusammenspiel aller Komponenten als gut sortierter Werkzeugkasten. *(wz)*

INTERVIEW

Gespräch mit Klaus Eckel, Bereichsleiter Technik bei der R-Kom GmbH & Co. KG

Den Imageverluste verhindern

Was ist die Rolle Ihres Unternehmens innerhalb des Projekts „DINGfest“?

Klaus Eckel: Die Rolle der R-Kom besteht darin, Daten aus unseren aktiven Systemen bereitzustellen und unsere Erfahrungen aus der Praxis einzubringen. Für die Datenakquisition sind Schnittstellen zu definieren und zu entwickeln, die es erlauben, relevante Daten abzugreifen, ohne die laufenden Systeme zu beeinflussen. Bei der Auswertung können wir auf Erfahrungen bei der Entwicklung von Systemen zurückgreifen, die Fraud (Betrug) bei Sprachdiensten oder DDoS (Distributed Denial of Service) bei IP-Diensten zeitnah erkennen, grafisch darstellen und automatisiert an die Spezialisten der R-Kom melden.

Welche Chancen bietet die Projektarbeit für die R-Kom selbst?

Wir betreiben ein öffentliches Telekommunikationsnetz, das als kritische Infrastruktur einzustufen ist – insbesondere wenn man die angeschlossenen Teilnehmer wie Polizei, Krankenhäuser und Energieversorger betrachtet. Wir sehen in dem Projekt die Chance, IT-forensische Erkenntnisse über Angriffe auf aktive Telekommunikationssysteme sowie Erkenntnisse über Bedrohungsszenarien in verschiedenen Netzbereichen zu gewinnen und wollen erforschen, wie diese durch automatisierte Analysemethoden möglichst frühzeitig und zuverlässig erkannt werden können. Unser Ziel ist es, die Ergebnisse aus „DINGfest“ zur Optimierung der aktuell eingesetzten Erkennungssysteme zu nutzen.

Klaus Eckel
Bereichsleiter Technik bei R-Kom

Welches Potenzial bietet das Projekt für die Unternehmen der Region?

Jeder erkannte Angriff bedeutet für ein Unternehmen einen immensen Gewinn. Es kann ein unmittelbarer kommerzieller Schaden – beispielsweise durch Spionage und den damit oftmals verbundenen Imageverlust durch Veröffentlichung – von vertraulichen Daten abgewendet werden. Weiterhin werden die forensischen Methoden von besonderem wirtschaftlichem Interesse sein. Wenn es zur Beweissicherung genügt, die automatisiert erzeugten, verdächtigen Datenströme zu sichern, statt das gesamte System über Tage oder gar Monate einzufrieren und damit den EDV-Betrieb stillzulegen, kann dies über die weitere Existenz eines Unternehmens entscheiden. Nicht zu unterschätzen ist außerdem die Möglichkeit der anonymisierten Meldung von Vorfällen, was den angesprochenen Imageverlust verhindern kann. Dem Bundesamt für Sicherheit in der Informationstechnik werden zudem zuverlässiger auch kleinere Schadensfälle gemeldet, was die Entwicklung von effektiven Gegenmaßnahmen erst ermöglicht. Die Ergebnisse werden nach Projektende allen interessierten Unternehmen, Organisationen, Behörden und Forschungseinrichtungen zur Nutzung und Weiterentwicklung zur Verfügung gestellt.

Wie verläuft die Zusammenarbeit zwischen den sieben Partnern verschiedener Branchen in der Praxis?

Schon im Kick-off wurde deutlich, dass alle Projektpartner sich optimal ergänzen, sehr gut harmonieren und mit vollem Engagement dabei sind. Insbesondere hat mich die professionelle Projektleitung durch den Lehrstuhl für Wirtschaftsinformatik der Uni Regensburg beeindruckt.

Das Interview führte Julia Rummel