



Westfälische Hochschule, Standort Gelsenkirchen

# Internet- Sicherheit

Schutz vor virtuellen Angriffen

## Ansprechpartner

Prof. Dr. Norbert Pohlmann  
Westfälische Hochschule  
Fachbereich Informatik und Kommunikation  
Neidenburger Straße 43  
45897 Gelsenkirchen  
Tel.: +49 (0)209 9596 - 515  
+49 (0)209 9596 - 763  
Fax: +49 (0)209 9596 - 427  
norbert.pohlmann@w-hs.de  
www.internet-sicherheit.de



Westfälische Hochschule  
Technologietransfer  
Neidenburger Straße 43  
45897 Gelsenkirchen  
Tel.: +49 (0)209 9596 - 458  
Fax: +49 (0)209 9596 - 563  
technologietransfer@w-hs.de  
www.w-hs.de/technologietransfer

**Prof. Dr. Norbert Pohlmann**

Das Institut für Internet-Sicherheit – if(is) – ist eine innovative, unabhängige und wissenschaftliche Einrichtung der Westfälischen Hochschule, die sich mit aktuellen und relevanten IT-Sicherheitsthemen gemeinsam mit namhaften Industrie- und Hochschulpartnern für mehr Sicherheit im Internet auseinandersetzt.

Neben der Forschung und Entwicklung ist das if(is) ein kreativer Dienstleister auf dem Gebiet der Internet-Sicherheit sowie Ratgeber für Industrie, Medienlandschaft und Endverbraucher. Begleitend zur aktiven und praxisnahen Forschung gelingt es den Informatikern des Instituts immer wieder, Ausgründungen ihrer Forschung erfolgreich im Markt zu platzieren:

Die Innovationen des if(is) finden ihren Weg in die Wirtschaft und leisten dadurch einen großen Beitrag zur Steigerung der IT-Sicherheit von Unternehmen und Institutionen.

Auch die Förderung und Weiterentwicklung der anwendungsbezogenen Lehre und Ausbildung im Bereich der IT- und Internet-Sicherheit sind wichtige Aufgaben. So ist der Masterstudiengang Internet-Sicherheit – als duales Studium oder Vollzeitstudium – bundesweit einzigartig und entlässt seine Absolventen als High-Potentials der Branche mit hervorragenden Jobperspektiven. Seit der offiziellen Eröffnung 2005 hat sich das kreative Forscherteam unter der Leitung von Prof. Norbert Pohlmann schnell zu einer der bedeutendsten Kompetenz-Teams für Internet-Sicherheit entwickelt und sich stets den Herausforderungen der Branche erfolgreich gestellt. Erklärtes Ziel aller Mitarbeitenden ist es, einen Mehrwert an Vertrauenswürdigkeit und Sicherheit im Internet herzustellen und dadurch jedermann ein angemessenes Niveau an Internet-Sicherheit zugänglich zu machen.



## Forschungsbereiche im Institut für Internet-Sicherheit

### **Blockchain-Technologie**

Das Institut für Internet-Sicherheit ist Kompetenzzentrum für Blockchain und steuert Entwicklungsgruppen aus Hochschulen, Behörden und Unternehmen neben Methoden der Blockchain-Technik konkrete Anwendungen zum sicheren Umgang mit Zeugnissen, Qualifikations- und Leistungsnachweisen bei, die in der Hochschule zentral und dezentral ausgestellt und durch Blockchain-Sicherheit digital zur Verfügung gestellt werden können. Studierende und Absolventen können ihre Nachweise dadurch elektronisch führen, ohne Studienbescheinigungen oder Zeugnisse kopieren und beglaubigen lassen zu müssen.

### **Vertrauenswürdige IT-Systeme**

Das Ziel von vertrauenswürdigen IT-Systemen ist, sie verlässlicher und sicherer zu machen. Vertrauenswürdig bedeutet in diesem Zusammenhang, dass die Hard- oder Software sich exakt nach definierten Vorgaben verhält.

### **Zahlungssysteme und Banktransaktionen**

Die zunehmende wirtschaftliche Bedeutung des Internets und die Nutzung von mobilen Geräten zieht auch eine Veränderung des Zahlungsverkehrs mit sich. Daher ist es notwendig, dass Sicherheit und Vertrauenswürdigkeit eine angemessene Höhe haben, damit wir als Kunden die Vorteile auch weiterhin ohne Bedenken nutzen können.

### **Security for Smart Car, Smart Grid, Smart Traffic, Smart Home and Internet of Things**

Der Forschungsbereich „Security for Smart Car, Smart Grid, Smart Traffic, Smart Home“ widmet sich dem Sicherheitsbedarf des Internet der Dinge und seiner smart objects. Die Mitarbeitenden forschen an zahlreichen Projekten des wachsenden Themas IoT.

### **Strukturelle Analyse des Internets**

Bei der Interneterforschung geht es darum, eine solide Wissensbasis sowie umfangreiches Know-how über das Internet zu erlangen. Ein wichtiger Schritt in diese Richtung ist die detaillierte Analyse von Kommunikationsprotokollen.

### **Botnetze**

Im Rahmen dieses Projektes analysieren wir die Funktionsweisen von Botnetzen, mit besonderem Augenmerk auf die Struktur der C&C-Steuerkanäle. Diese Information kann dann genutzt werden, um Bot-Infektionen möglichst frühzeitig zu erkennen. Unsere Forschung zielt dabei insbesondere auf die Erkennung in Hochgeschwindigkeitsnetzen.

### **Internet-Kennzahlen-System**

Der Forschungsbereich Internetkennzahlen erstellt ein Kennzahlensystem, um die Komplexität der kritischen Infrastruktur Internet zu analysieren, den aktuellen Zustand zu beobachten sowie die zukünftige Entwicklung abschätzen zu können. Das erste Projekt ist der Deutsche Internet-Index.

### **Mobile Security**

Der steigenden Mobilität widmet sich der Forschungsbereich Mobile Security. Erforscht werden die Möglichkeiten mobile Endgeräte innovativ und sicher in Unternehmensnetzwerke und den Alltag zu integrieren.

### **Identity Management**

Der Forschungsbereich Identity Management untersucht die Entwicklungen des Identity Managements, aber vor allem auch neue Möglichkeiten, sichere Identitäten zu verwenden.

### **Internet-Frühwarnsysteme**

Das Internet-Frühwarnsystem oder Internet-Lagebild vereint alle Analysekomponenten wie IAS, LVS und weitere if(is)-Projekte sowie Partnerprojekte.

### **Cloud Computing**

Cloud Computing ist ein wichtiger Teil der IT und des Internets. In diesem Forschungsbereich beschäftigt sich das if(is) mit Maßnahmen zur Sicherheit und Vertrauenswürdigkeit von Cloud-Diensten.

### **Soziale Netze**

Nutzer müssen immer schneller und umfassender in der Lage sein, die Vertrauenswürdigkeit sozialer Dienste richtig einzuschätzen, lernen entsprechend darauf zu reagieren und ein gesundes Maß an Misstrauen zu zeigen. Um auf diesem Gebiet für mehr Transparenz zu sorgen, forscht das Institut für Internet-Sicherheit in dem Bereich der sozialen Netze.