Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE
TECHNICAL REPORT

Positionspapier aus Forschungssicht

Sicherheitstechnik im IT-Bereich

Michael Waidner, Michael Backes, Jörn Müller-Quade

CISPA Center for IT-Security, Privacy

EC SPRIDE
EUROPEAN CENTER FOR
SECURITY AND PRIVACY BY DESIGN

KASTEL

Kompetenzzentren für IT-Sicherheit

IMPRESSUM

Kontaktadresse:
Fraunhofer-Institut für
Sichere Informationstechnologie SIT
Rheinstraße 75
64295 Darmstadt
Telefon 06151 869-213
Telefax 06151 869-224
E-Mail info@sit.fraunhofer.de
URL www.sit.fraunhofer.de

Bibliografische Information der Deutschen Nationalbibliothek
Die Deutsche Nationalbibliothek verzeichnet diese Publikation in der Deutschen Nationalbibliografie; detaillierte bibliografische Daten sind im Internet über http://dnb.d-nb.de abrufbar.

Hrsg. Michael Waidner
Runder Tisch der Bundesregierung | Sicherheitstechnik im IT-Bereich
Positionspapier aus Forschungssicht
Sicherheitstechnik im IT-Bereich
(SIT-TR-2013-04)
Michael Waidner, Michael Backes, Jörn Müller-Quade
Copyright Titelbild: iStockphotos.com/scotspencer
ISSN 2192-8169

Runder Tisch der Bundesregierung
Sicherheitstechnik im IT-Bereich

Positionspapier aus Forschungssicht

9. September 2013

Prof. Dr. Michael Waidner[1,2]
Institutsleiter Fraunhofer SIT,
Direktor EC SPRIDE und CASED
michael.waidner@sit.fraunhofer.de

Prof. Dr. Michael Backes[3,4]
Max Planck Fellow,
Direktor CISPA
backes@mpi-sws.org

Prof. Dr. Jörn Müller-Quade[5]
Leiter des Instituts für Kryptographie und Sicherheit (IKS),
Direktor KASTEL
mueller-quade@kit.edu

(1) Fraunhofer-Institut für Sichere Informationstechnologie (SIT)
Rheinstraße 75, 64295 Darmstadt

(2) Technische Universität Darmstadt
Mornewegstraße 30, 64289 Darmstadt

(3) Universität des Saarlandes
Campus E1 1, 66123 Saarbrücken

(4) Max-Planck-Institut für Softwaresysteme (MPI-SWS)
Campus E1 5, 66123 Saarbrücken

(5) Karlsruher Institut für Technologie (KIT)
Am Fasanengarten 5, Geb. 50.34, 76131 Karlsruhe

Im vorliegenden Papier fassen die drei Autoren ihre Position zum Thema "Sicherheitstechnik im IT-Bereich" zusammen. Mit den aufgeführten Standpunkten vertraten die Wissenschaftler die Anliegen der Forschung gegenüber Staat und Wirtschaft beim gleichnamigen Runden Tisch der Bundesregierung am 09.09.2013 in Berlin.

Inhalt

1 Vorbemerkung

1.1 IT-Sicherheit erfordert Forschung

In Wirtschaft und Verwaltung besteht großer Nachholbedarf in der Umsetzung von IT-Sicherheitslösungen. Selbst elementare Techniken wie Dateiverschlüsselung, Identitätsmanagement oder sichere Nachrichtenübertragung werden nur unzureichend eingesetzt.

IT-Sicherheit erfordert aber weit mehr als die Umsetzung bekannter Techniken. Es müssen auch zahlreiche Fragen der angewandten und der Grundlagenforschung beantwortet werden.

Einige Beispiele:

- IT-Sicherheitslösungen sind oft schwer zu benutzen, sehr komplex, sehr aufwendig. Die systematische Erschaffung von IT-Sicherheitslösungen, die benutzbar sind und von den Nutzern als wertvoll erkannt und angenommen werden, ist ein offenes Problem.

- IT-Produkte und Systeme sind fast immer fehlerbehaftet und dadurch angreifbar. Der Entwurf sicherer Systeme, der automatisierte Test auf Unsicherheit, der Nachweis von Sicherheit sind offene Probleme.

- IT-Produkte können Trojanische Pferde enthalten. Wie kann man dies zuverlässig und automatisiert erkennen und verhindern?

- Wie kann man im Internet tatsächlich sicher und unbeobachtbar kommunizieren, im Allgemeinen oder zumindest vis-a-vis Massenüberwachung durch fremde Dienste? Auf dem Papier existieren viele Techniken zur Verschlüsselung und Anonymisierung, aber keine davon skaliert ausreichend für alle Nutzer in Deutschland, EU, weltweit.

- Wie geht man mit dem Konflikt zwischen Privatsphärenschutz einerseits und Online Social Networks, Big Data, Ubiquitären und mobilen Systemen andererseits um?

- Angriffe, insb. zur Industriespionage, erfolgen oft durch Innentäter (Angestellte, Partner) oder unter Ausnutzung unbekannter Schwachstellen im System. Wie kann man solche Angriffe schnell und automatisiert erkennen und verhindern?

- Wie kann Sicherheit mit minimalen Ressourcen und minimalen Interaktionsanforderungen (eingebettete IT, Industrie 4.0) erreicht werden?

- Wie misst man Sicherheit (oder Unsicherheit)? Wie wertet man Sicherheitsdaten effizient und bedeutungsvoll aus?

- Im Allgemeinen setzt Cloud Computing voraus, dass die Nutzer dem Betreiber vollständig vertrauen. Die Kryptographie kennt Ansätze, wie diese Anforderung an das Vertrauen reduziert werden kann – aber wie macht man sie praktisch nutzbar?

- Heutige Kryptographie und Protokolle sind nur gegen heutige Angreifer sicher. Wie kann Sicherheit auch in Zukunft erreicht werden?

1.2 Deutschland ist ein wichtiger und erfolgreicher Forschungsstandort

Deutschland verfügt über eine sehr aktive und erfolgreiche Forschungslandschaft zu IT-Sicherheit bzw. Cybersecurity.

An der ACM CCS 2013 in Berlin, einer der beiden derzeit weltweit wichtigsten akademischen Forschungskonferenzen zur IT-Sicherheit, stellt Deutschland nach den USA das zweitgrößte Kontingent (sowohl eingereichte als auch akzeptierte Papiere).

Dank der Förderung durch Bund und Länder in die Bildung von Zentren (insb. Land Hessen, BMBF) und in wichtige Themen (z.B. Cloud Computing, KRITIS) gibt es mehrere exzellente, international sichtbare Forschungszentren. Insbesondere zu nennen sind die drei vom BMBF geförderten Zentren in Darmstadt, Karlsruhe und Saarbrücken, aber auch beispielsweise Bochum und München. Darüber hinaus sind an vielen deutschen Hochschulen und Forschungseinrichtungen weitere exzellente Forscherinnen und Forscher tätig. Viele Firmen in Deutschland, insbesondere KMUs, sind sehr in der Sicherheitsforschung engagiert.

2 Empfehlungen

2.1 Klarheit und Transparenz zu Gefahren und Risiken, Dauerhafte und tragfähige Strategie

- Der Auftrag an den Runden Tisch ist sehr umfassend. Dieser Auftrag sollte präzisiert und den Teilnehmern Zeit und Freiraum zur Schaffung einer tragfähigen Strategie gegeben werden.

- Viele der Betroffenen (Bürger, Industrie, Staat) erwarten eine realistische Einschätzung der tatsächlichen Gefahren und Risiken. Die Wissenschaft kann hier im Sinne unabhängiger Sachverständiger einen regelmäßigen Beitrag leisten.

2.2 Umfassende digitale Souveränität ist nicht realistisch, aber es gibt sinnvolle Annäherungen an eine Souveränität

- Eine vollständige Unabhängigkeit von IT-Produkten und -Diensten aus dem Ausland ist unrealistisch:

    - Der Technologievorsprung z.B. der USA und der Kostenvorteil z.B. Chinas sind praktisch nicht einzuholen.

    - Deutsche Nutzer wollen an der global vernetzten Welt teilnehmen und wollen und müssen daher auch Dienste aus dem Ausland verwenden.

    - Als exportorientierte Nation sind wir auf einen offenen, freien Handel angewiesen.

Die folgenden beiden Ansätze sind aber sinnvolle Möglichkeiten mehr Souveränität zu erreichen:

2.2.1 Ausgewählte Speziallösungen *hergestellt* in Deutschland

- Souveränität in einzelnen Bereichen ist herstellbar bzw. existiert bereits.

    - Vorhanden: Sehr viele IT-Sicherheitslösungen der deutschen Software-Industrie, insbesondere von KMUs.

    - Möglich: Linux-Distribution, Intermediäre Dienste, Router, deutsche/europäische PKI.

- Flankierende regulatorische Maßnahmen sind erforderlich, um solchen Lösungen im deutschen (idealerweise: europäischen) Markt einen Vorteil zu verschaffen. Deutschland sollte hier für und in Europa eine Vorreiterrolle spielen.

- Dies erfordert teilweise signifikante Investitionen und die Bildung von Konsortien aus Industrie und Forschung.

2.2.2 Alle Lösungen *überprüfbar* durch Test-Labore

- Generelle und bei Beschaffungen der öffentlichen Hand verpflichtende Überprüfbarkeit der Sicherheit *aller* IT-Lösungen, egal wo sie produziert bzw. erbracht werden.

- Dies umfasst Produkte, Dienste und Herstellungsmethoden (Security by Design!)

- Setzt technische Mindeststandards und verpflichtende Testmethoden und Testwerkzeuge voraus (wenn möglich automatisiert!)

    - Verschafft der deutschen (europäischen) Industrie und Forschung automatisch einen Vorteil für nationale Produkte, Dienste und Testwerkzeuge

    - Sicherheit und Annahmen zur Sicherheit müssen für Marktteilnehmer sichtbar sein (Standards, Siegel, Produkt-Zertifikate)

    - Unsicherheit muss in geeigneter Form zu Haftung führen

- Finden trojanischer Funktionalität ist ansatzweise machbar, wenn die Testlabore Zugang zu Source Code / zur Dienstplattform haben

    - Verpflichtung zur Offenlegung gegenüber ausgewählten, glaubwürdigen, nationalen Test-Laboren (z.B. TÜV, Fraunhofer).

- Ansätze existieren, aber letztlich besteht hier ein sehr großer Forschungsbedarf: Finden von Trojanischen Pferden, vollautomatische Analyse, Security by Design

2.3 Entwicklung sicherer IT erfordert geeignete Infrastruktur

- Neue Testmethoden und -werkzeuge (siehe Abschnitt 2.2) erfordern sehr großen Forschungsbedarf und liefern sehr große Marktchancen für neue Produkte.

- Datenbank mit Fakten und Annahmen zur Sicherheit von Komponenten zur leichteren Integration. Hier besteht ebenfalls Forschungsbedarf: Definition von Sicherheit, Integration von Sicherheit.

- Beides erfordert signifikante Forschung: Security and Privacy by Design ist Fokus der drei BMBF-Zentren!

2.4 Nutzung sicherer IT erfordert Vertrauensinfrastruktur

- Bekannte Sicherheitsmechanismen (z.B. sichere E-Mail) werden zu selten eingesetzt. Ein Grund ist das Fehlen geeigneter Infrastrukturen.

- F&E zu einfachem, national / global einsetzbarem Schlüsselaustausch, z.B. basierend auf staatlicher Infrastruktur (nPA) oder basierend auf anderen Vertrauensmodellen.

- F&E zu einfacher, kostengünstiger und sicherer E-Mail

- F&E zu sicherem DNS, sicherem SSL/TLS-Next, sicheren Plattformen usw.

2.5 IT-Sicherheit braucht eine umfassende Forschungsagenda

- Zahlreiche offene Probleme für Grundlagen- und angewandte Forschung (Abschnitt 1)

    - Vieles in der IT-Sicherheit ist bekannt,
      noch mehr ist unbekannt!

- Koordinierte Strategie und Förderung auf Bundes-/Landes- und EU-Ebene (z.B. im Rahmen von Horizon 2020)

- Bewährtes Instrument: Zentrenbildung (dadurch erhält man die kritische Masse und erreicht Wettbewerbsfähigkeit gegenüber der internationalen Konkurrenz)

- Bewährtes Modell: Verzahnung der Forschungseinrichtungen mit der Industrie (insb. KMUs) und der öffentlichen Hand (z.B. dem BSI) bei angewandter Forschung.