PROF. DR. BERNHARD M. HÄMMERLI

Acris GmbH und Hochschule Technik+Architektur (HTA)
Luzern

Statement zur KRITIS-Forschung

KRITIS ist in Deutschland einerseits mit Studien aus Beratungshäusern erforscht worden, andererseits wurden auf der Ebene der IT-Security Lösungen zu aktuellen und dringlichen Problemen entwickelt. Zwar wird zum Glück IT-Security nicht mehr mit Kryptologie verwechselt, jedoch gibt es noch immer keine umfassende Forschungsagenda zu KRITIS. Auf europäischer Ebene sind bereits einige Forschungsvorhaben abgeschlossen, andere sind noch in Arbeit oder Vorbereitung. Die abgeschlossenen Forschungen konnten wesentliche Problemstellungen identifizieren und umreißen, jedoch ist es noch nicht vollständig gelungen, die Forscher aus verschiedenen Bereichen wie IT, Ingenieurwissenschaften, Security, Simulation, Politikwissenschaften oder Kryptologie in einem Team für die neue Aufgabe zu begeistern. Ein Grund mag wohl in starren Strukturen und der stark disziplinär orientierten akademischen Meinung über forschungswürdige Themen liegen. Inzwischen ist nicht zuletzt aufgrund von Entwicklungen in Technik und Organisation kritischer Infrastrukturen, aber auch aufgrund einer durch terroristische Handlungen veränderten Bedrohungslage der Bedarf nach KRITIS jedoch unbestritten. Ein Lösungsweg aber ist nach wie vor noch sehr vage und offen. Für den jungen KRITIS–Bereich ist es daher eine Herausforderung, sich neben den gewachsenen Strukturen zu behaupten!

Architekturelle Forschung

Die heutigen Infrastrukturen sind sektorweise gewachsen. Die wichtigsten Sektoren sind Energie, Telekommunikation, Finanzen und Anwendungssektoren wie z. B. Gesundheitswesen, Rettungswesen, Verwaltung und andere mehr. In den Sektoren sind mehrere gegenseitig im Wettbewerb stehende Firmen, die je ihre eigene Infrastruktur vorwärts treiben. Für den Telekommunikationssektor bieten beispielsweise in Deutschland folgenden Firmen im Wettbewerb Dienstleistungen an: Deutsche Telekom, COLT, Arcor, O_2 sowie verschiedene kleinere, sektorale und regionale Anbieter. Die Vernetzung und Gesamt-Architektur der kritischen Infrastrukturen als ganzes ist deshalb eher organisch und über längere Zeiträume gewachsen und wenig auf Robustheit und Widerstandsfähigkeit optimiert, obwohl jeder einzelne Betreiber in seinem Bereich – im Rahmen der notwendigen Wirtschaftlichkeitsüberlegungen – sein Bestes für die Widerstandsfähigkeit und Robustheit gibt. Das heißt, dass die Teilinfrastrukturen hinsichtlich dieser Aspekte zwar sicherlich optimiert sind, jedoch nicht deren Vernetzung. Hier hat insbesondere die mathematische Forschung der vergangenen Jahre wesentliche Defizite aufgezeigt.

Die Forschung kann aufgrund dieser Beobachtungen Strukturen und Migrationspfade untersuchen und vorschlagen, die für die Begegnung neuer Bedrohungen geeignet sind. Unmittelbare Forschungsfelder können etwa die Untersuchung der Robustheit verschiedener Zentralisierungs- und Vernetzungsgrade der Infrastrukturen, ihrer IT-Anteile und ihrer Steue-

rungen sein sowie die Abkoppelbarkeit von Teilsystemen zu autarken, selbst geführten Systemen sowie die Selbstüberwachung und –reparatur komplexer Systeme sein. Wesentlicher Bestandteil der Konzeption und Umsetzung von Überwachungs- und Leitfunktionen in heterogenen KRITIS-Netzen sind hierbei die Identifikation der erforderlichen Granularität und Detailgrad der Informationen, die auf einer bestimmten Stufe innerhalb eines Sektors und zwischen den Sektoren ausgetauscht werden müssen, da hier vielfach auch zwischen Konkurrenten potenziell vertrauliche Daten ausgetauscht werden müssen. Auch die Vertrauenswürdigkeit entsprechender technischer Verfahren und Informationssysteme muss eingehend untersucht und vielfach signifikant verbessert werden. Als besondere Erhöhung der Komplexität kommt hinzu, dass für verschiedene Krisengrade die auszutauschenden Informationen anders aussehen und eine andere Vertraulichkeits- oder Geheimschutz-Einstufung haben.

Technisch können im Idealfall vernetzte Systeme bei einer Störung automatisch aufgetrennt werden und als selbständige Systeme weiterlaufen oder gar autonom eine Krisenbewältigung einleiten, wenn das menschliche Reaktionsvermögen hierzu nicht ausreicht. Um bei Großschadensereignissen oder drohenden Schäden geeignet reagieren zu können, muss zudem auch gewährleistet werden, dass hinreichende Informationen auch staatlichen Stellen zur Verfügung stehen und diese sich untereinander austauschen können. So können etwa Lagezentren (z.B. nach Bundesländern und Bund) zur Erfassung und Koordinierung Nachrichten über Betriebszustände, Schäden und zu erwartende Anomalien automatisch zur Verfügung gestellt werden.

Unmittelbares Ziel verbesserter Informationssysteme und Forschung im Bereich der Leittechnik und Vernetzung muss dabei sein, unvermeidbare Ausfälle soweit möglich lokal begrenzt zu halten, wobei die Krisenheftigkeit die Größe des betroffenen Gebietes bestimmt. Dominoeffekte sollten nicht mehr möglich sein, ebenso sollten zentrale „Single Points of Failure“ auf ein sinnvolles Minimum reduziert werden.

So sind die Ursachen für die Stromausfälle an der Ostküste der USA und Kanadas 2003 und in Italien in „Single Points of Failure“ zu suchen, deren Wirkung erst durch Dominoeffekte verheerend wurde und die durch ein besseres Verständnis der zugrunde liegenden Netzcharakteristika und Informationsaustausch vermieden oder in ihrem Schweregrad stark hätten eingeschränkt werden können. Neben physikalischen Schäden sind jedoch auch die IT-Aspekte selbst seit langem Ursache für gravierende Schadensereignisse. In der Schweiz wurde am 7. Februar 2005 bei der SBB Bundesbahn der Release-Einzug des Softwareupdates zum Verhängnis. Fehlfunktionen der Software und kaskadierende Dominoeffekte führten zum Ausfall des Bahnhofs Zürich und aller Züge in dessen Umgebung für 4 Stunden[1]. Am 27. Juli 2001 hatte ebenfalls in der Schweiz der Release-Einzug bei Swisscom Mobile und in einer redundant geführten Mobiltelefon-Vermittlungsanlage einen Komplettausfall der Mobiltelefonie für 36 Stunden bewirkt.

Gerade in diesem Bereich sind neben der Informatik auch andere Fachgebiete angesprochen: Neben den Ingenieurwissenschaften (z.B. Mess- und Regelungstechnik, Nachrichten- und Elektrotechnik) sind hier auch Mathematik und Physik (insbesondere z.B. statistische Physik zur Untersuchung des Verhaltens komplexer Systeme) zu gemeinsamen Anstrengungen gefordert.

[1] Schweizer Eisenbahn-Revue 4/2005 Seiten 196/197 oder NZZ 9. Februar 2005 Nr. 33 Seite 47

Forschungsbedarf hinsichtlich Lagezentren

Das Systemdesign sowohl innerhalb der Infrastrukturen wie auch des Lagezentrums, das Information Engineering – d.h. das Festlegen, welche Informationen, wie gespeichert, verteilt und ausgetauscht werden dürfen und sollen - und die Vertraulichkeits- bzw. Geheimschutz-Einstufung[2] der Informationen unter anderem auch nach Krisengrad müssen erforscht und bedarfsgesteuert geklärt werden. Aufgrund der in weiten Teilen wettbewerblichen Strukturen innerhalb der Infrastrukturen und der Gefahren für Betriebssicherheit einerseits und wirtschaftlicher Nachteile andererseits ist ein wesentlicher Teil des Information Engineering die Gewährleistung der Vertraulichkeit der verwendeten Information und die Vertrauenswürdigkeit der hierzu verwendeten Systeme. Beides sind essenzielle Aspekte und bedürfen einer engen Abstimmung mit den involvierten Partnern[3]. Neben wissenschaftlichen und technischen Anforderungen gilt es hier zudem auch die betreffenden Organisationen und deren Abläufe einzubeziehen, was z.B. sektorweise erfolgen kann. Beim Information Engineering ist speziell auf die Reduktion und Kompression der anfallenden Datenmengen Wert zu legen, da oftmals die Aufnahmefähigkeit menschlicher Entscheidungsträger ein wesentlicher Schwachpunkt derartiger Systeme darstellen muss.

Beispiel: Der Stillstand der gesamten Schweizerischen Bundesbahn SBB für die Dauer von drei Stunden am 22. Juni 2005 wurde ausgelöst durch Fehlentscheidungen: Mit ca. 18.000 Sicherheitsmeldungen pro Minute war das Krisenpersonal überfordert und legte den Fokus der Aktivitäten falsch[4]. Dies führte auch zu Fehlentscheidungen, die die Katastrophe verursachten. Laut Untersuchungsbericht hätte die Energieversorgung jedoch bei idealen Entscheidungen ausgereicht, um das ganze Netz zu versorgen.

Das kürzlich abgeschlossene Europäische Forschungsprojekt Safeguard[5] hat im Bereich der Internettechnologien die Informationsverdichtung in einem kleinen Netzwerk erfolgreich behandelt. Fazit: Es gibt Forschungsansätze, jedoch verlangt die Dimension von KRITIS eine neue Ebene des Problemstudiums, die große und sehr große Systeme berücksichtigt und zusätzlich die verschiedenen Sektoren integrieren kann.

Gerade im Bereich der Informations- und Leitsysteme und Lagezentren spielen mithin die Mensch-Maschine-Interaktion und Erkenntnisse aus kognitiver und Organisationspsychologie bei der Gestaltung der Informationssysteme eine wesentliche Rolle. Die Modellierung und Simulation von zum Teil auf kontinentaler Ebene miteinander vernetzter Systeme stellt zudem erhebliche Anforderungen an effiziente algorithmische und heuristische Verfahren und deren Realisierung; auch hier ist daher der ausgeprägte Querschnittcharakter der KRITIS-Forschung klar erkennbar.

---

[2] Eine Geheimschutz-Einstufung bzw. das jeweils privatwirtschaftliche Pendant wird in der IT-Sicherheit verwendet, um Informationen nach Vertraulichkeitsgrad zu sortieren, von öffentlich vertraulich bis streng geheim in zumeist 3 bis 6 Stufen.

[3] Gemeint ist eine Public Private Partnership (PPP), wie sie in verschiedenen Ländern gelebt wird. Die USA betreiben vom DHS (Department for Homeland Security) gefördert diverse Information Sharing and Analysis Centres für die sektorielle Risikoanalyse und Lageerkennung.

[4] Die SBB hat mitgeteilt, dass künftig im ersten Schritt die Isolation des Problems vorgenommen werden soll, indem die Verfügbarkeit des Restnetzes (hier über 95 %) im Fokus bleibt. Siehe auch: Schweizer Eisenbahn-Revue 8-9/2005 Seiten 373-379

[5] http://www.ist-safeguard.org/

Entwicklung eines Indikatorensystems zur KRITIS-Evaluation

Die Entwicklung von messbaren Indikatoren, die eine Bewertung der KRITIS-Aktivitäten und mithin auch eine Bewertung der Effektivität von Anstrengungen in der Forschung und Entwicklung erlauben, bedarf ihrerseits international abgestimmter Forschungsaktivitäten, um sicherzustellen, dass die erfassten Kenngrößen in der Tat die gewünschte Zielrichtung reflektieren. Dabei ist zu beachten, dass diese Indikatoren vom Dezentralisierungsgrad und Entwicklungsgrad der Region (etwa bezüglich der Stabilität der Energieversorgung in einer geographischen Region) stufengerecht angepasst werden müssen, um ein Beurteilungssystem fair zu gestalten. Ferner sollte ein solcher Ansatz das betriebliche Risikomanagement unterstützen, indem nachvollziehbare Risikoindices für Krisenlagen definiert werden, die wiederum als Grundlage für die Bewertung und Einführung von Maßnahmen und deren Kosten herangezogen werden können. In diesen Bereich fällt auch die Entwicklung von Musterszenarien zur Überprüfung des vorgeschlagenen Beurteilungssystems.

Beispiele für Indikatoren[6] können im Telekommunikationssektor der Datendurchfluss und die Verzögerungszeit (Latency) sein. Speziell dabei ist, dass eine Frühwarnung und die Synergie bei der Fehlersuche nur dann Vorteile bringen, wenn eine genügende Menge an statistischen Erfahrungswerten vorliegt und diese Verfahren dynamisch in Anpassung an sich ändernde Strukturen in den einzelnen Infrastruktur-Sektoren nachgeführt werden können.

KRITIS Middleware Forschung

KRITIS Middleware ist das fehlende Element zwischen dem „Top down"-Ansatz der politischen Diskussion und dem „Bottom up"-Ansatz der Hersteller und Dienstleister. Die KRITIS Middleware muss auf verschiedenen Ebenen entwickelt werden und soll vor allem die bestehenden Elemente sinnvoll verbinden. Die Forschung betrifft vor allem Schnittstellen und Protokolle.

Beispiel: Die Verbindung zwischen den betrieblichen Funktionen Business Continuity Planning (BCP), Disaster Recovery Planning (DRP), IT-Sicherheit und der staatlichen CIP Aufgabe sind zu definieren und weiter zu entwickeln. Dabei sollen Beiträge zur Entwicklung von der Integration der komplexen kritischen Infrastruktur und ihrer Schnittstellen in einen nationalen oder übernationalen Plan Forschungsbestandteil sein, ebenso wie die Grundlagenforschung für wirksame „Information Sharing and Analysis Centres" (ISAC), welche den Informationsaustausch in einer Public Private Partnership zwischen Staat und Privatwirtschaft bezüglich Risiken, Verletzlichkeiten und Vorfällen organisieren.

[6] Klaus Julisch und Christopher Krüger, Detection of Intrusion and Malware, and Vulnerability Assessment, Springer-Verlag 2005, Seite 103. Produkteinsatzstudien für verschiedene solche Werkzeuge.

Einsatz und Konfiguration von unterstützenden Werkzeugen

Neue Technologien und aktuelle Produkte bieten Werkzeuge[7] für starke Widerstandskraft gegen Angriffe und Robustheit gegen schleichende Änderungen. Unter dem Begriff Robustheit wird die Desensibilisierung gegen Veränderung verstanden, das heißt, dass eine robuste Infrastruktur voll funktionstüchtig bleibt, auch wenn viele Parameter etwas aus dem Lot geraten. Dazu gehören beispielsweise das Erzwingen von Weisungen und Richtlinien (Policy Enforcement) sowie die Überwachung von Schlüsselindikatoren (Key Performance Indikatoren - KPI) zur automatischen und frühzeitigen Feststellung von außerordentlichen Betriebssituationen. Der angemessene Einsatz und die Integration solcher Werkzeuge sind eine große Herausforderung für die Wirtschaft und sollen aus der Forschung unterstützt werden.

Forschung bezüglich Sicherheitskultur

Eine neue Sicherheitskultur, die auf die heutige Situation mit dem *Leben unter permanenter Bedrohung* und dem *Betrieb während andauernder und laufend neuer Attacken* angepasst ist, sowie die hierfür erforderlichen technischen Grundlagen muss entwickelt und auf regionale Besonderheiten abgestimmt werden. Vielfach sind Infrastruktur-Systeme und die ihrem Betrieb zugrunde liegenden Analysen noch auf rein stochastische Bedrohungsmodelle ausgerichtet, wie sie etwa durch Naturkatastrophen oder technische Schäden (Materialermüdung, etc.) verursacht werden. Dahingegen sind gerade im Hinblick auf die kontinuierlich verstärkte Vernetzung der Infrastrukturen auch gezielte Angriffe wie Sabotageakte und terroristische Handlungen auch in die relevanten Bedrohungsanalysen zumindest einzubeziehen. Insbesondere sind das natürliche Maß an Vertrauen mit der Bedrohungslage auszubalancieren und der Konflikt zwischen Sicherheit, informationeller Freiheit und – in einigen Fällen – Privatsphäre neu zu überdenken. Ohne diese kritische Gegensicht können zu rigide Sicherheitsmaßnahmen die Grundidee westlicher Demokratien nachhaltig gefährden.

Derzeit befassen sich verschiedene philosophische und soziologische Studien[8] zunehmend mit dem Wert der Privatheit und für das Setzen von Grenzen für die alles kontrollierende Sicherheit. Benjamin Franklin meinte dazu: “They that can give up essential liberty to obtain a little temporary safety deserve neither liberty nor safety.” Kurz: Es ist wirklich außerordentlich wichtig, dass jede Einschränkung der Freiheiten wohl bedacht und überlegt ist. Für den rein technischen Teil der Infrastrukturen ist die Sicherheit unproblematisch. Jedoch überall wo Verflechtungen mit Personen vorkommen sind Aufzeichnungen auf ihre Problematik zu untersuchen (z.B. Airport Security).

Beispiel: Spam-Mails machen heute bis zu 50 % des Mail Verkehrs aus und könnten in bestimmten Situationen eine Denial of Service Attacke auslösen. Eine starke Authentisierung würde unentdecktes Spamming verunmöglichen. Jedoch wäre es dann nicht mehr möglich

[7] Speziell sind hier alle Werkzeuge gemeint, die umfassendes Multisystem Monitoring und Security Information Management integrieren und zu höherwertiger information aufbereiten.
[8] Arbeiten von Vordenkern sind etwa: Prof. Dr. Beate Rössler, Der Wert des Privaten, Frankfurt Surkamp 2001,
Focus „Der Wert des Privaten“ Digma, 2. Jahrgang Heft 3, Schulthess 2002
Schwerpunkt „Informationsfreiheit“ Digma, 4. Jahrgang Heft 4, Schulthess 2004

mit einer temporären E-Mail Adresse eine anonyme[9] Anfrage zu machen, wie z. B. nach einer Krankheit oder anderen privaten Angelegenheiten.

Forschungsmethodik und Forschungseigenheiten

Ein neu aufkommendes Gebiet wie KRITIS, das eine unbestreitbare Bedeutung für die Gesellschaft hat, braucht eine starke multidisziplinäre und transnationale Ausrichtung. Es kann mit den üblichen Forschungsansätzen des Informatikbereichs alleine nicht angegangen werden. Vielmehr sind neue wissenschaftliche Denkmuster und interdisziplinäre Kooperationen gefragt, um die vielfältigen Fragestellungen einer Lösung zuzuführen. Der Durchbruch im Bereich von KRITIS ist für die Gesellschaft wichtig und ist der Maßstab, an welchem diese Aktivitäten in Forschung und Umsetzung unmittelbar gemessen werden.

Beispiel: Heute fokussiert die wissenschaftliche Forschung in der Informatik immer noch sehr stark auf die Optimierung und Weiterentwicklung disziplinärer Themen und Subthemen. Die Forderung, die Forschung in KRITIS interdisziplinär von allen Zweigen des Engineering über Politikwissenschaften, Komplexitätstheorien, Soziologie weiter zu gestalten ist aktuell im CIIP[10] Handbook[11] klar gefordert als Bestandteil der Forschungsagenda.

Anmerkung zum „Nationalen Plan zum Schutz der Informationsinfrastrukturen“

Das Studium des kürzlich erschienenen „Nationalen Plans zum Schutz der Informationsinfrastrukturen“ NPSI des Bundesinnenministeriums[12] bestätigt den Forschungsbedarf hinsichtlich der Informationsinfrastrukturen. Die anderen kritischen Infrastrukturen und deren Informationsanteile sind im NPSI nicht direkt abgedeckt.

Literaturhinweise:

- Andreas Wenger und Jan Metzger, International CIIP Handbuch 2004, ETH Zürich, ISBN 3-905641-92-5 oder www.isn.ethz.ch/crn
- European CIIP Newsletters of EU’s CIIRCO (**C**ritical **I**nformation **I**nfrastructure **R**esearch **CO**ordination Action) Project, www.ci2rco.org, 2005
- Critical Infrastructure Protection & Civil Emergency Planning: Dependable Structures, Cybersecurity and Common Standards, edited by Centre for International Security Policy CISP, Bern Switzerland
- Critical Infrastructure Protection (CIP) - Status and Perspectives. Preprints of the First German Informatics Workshop on CIP, Frankfurt am Main 2003

Weitere Informationen: Fachgruppe KRITIS der GI, http://www.gi-fb-sicherheit.de/fg/kritis

[9] Die Zahl der Publikationen zu berechtigter Anonymität sind nicht ausserordentlich zahlreich, aber sehr wichtig. Siehe auch Schwerpunkt „Anonymität“ Digma 4. Jahrgang Heft 1, Schulthess 2004

[10] CIIP, Critical Information Infrastructure Protection, steht hier für den Teilbereich von KRITIS, der in Deutschland „kritische Informationsinfrastrukturen“ genannt wird.

[11] Andreas Wenger und Jan Metzger, International CIIP Handbuch 2004, ETH Zürich, ISBN 3-905641-92-5 oder www.isn.ethz..ch/crn , Seiten 356/357

[12] http://www.bmi.bund.de/Internet/Content/Nachrichten/Pressemitteilungen/2005/08/Nationaler__Plan__zum__Schutz_der_Informationsinfrastrukturen.html

Lebenslauf

Bernhard M. Haemmerli ist Professor für Kommunikation und Informationssicherheit and der Hochschule Technik+Architektur in Luzern. Er hat das Exekutive-Master-Programm „Informationssicherheit“ und die regionale Cisco-Akademie mit dem Angebot der CCNA und CCNP aufgebaut. Er ist Gründungsmitglied der ersten Stunde der Fachgruppe KRITIS der Gesellschaft für Informatik (GI) und designierter Präsident der Information Security Society Switzerland ISSS / FGSec (Swiss Chapter of ACM). Er ist Geschäftsführer von Acris GmbH, welche Beratungsleistungen für CIIP und Informationssicherheit anbietet und Kongresse zu diesen Themen organisiert. Er arbeitet in verschiedenen technischen und politischen Arbeitsgruppen zur Förderung der Informationssicherheit und CIIP. Ausserdem ist er Herausgeber der Zeitschrift Digma (privacy and security) und des European CIIP Newsletter www.ci2rco.org.

Kontakt

bmhaemmerli@acris.ch und bmhaemmerli@hta.fhz.ch
Tel: 0041 79 541 7787, Fax: 0041 310 5918
Bodenhofstrasse 29, CH-6005 Luzern
HTA Luzern, Technikumstrasse 21, CH 6048 Horw