Mainz, 15.10.2015

EIN UNÜBERSCHAUBARER MARKT?

ZERTIFIZIERUNGSANGEBOTE UND IHRE ANFORDERUNGEN

Dr. Rolf Dahm

RKW Rheinland-Pfalz e.V.

Das RKW – ein Netzwerk mit langer Tradition!

- 1921 gegründet, seit 1950 eingetragener gemeinnütziger Verein mit Sitz in Frankfurt, seit 1990 auch in den neuen Bundesländern
- 12 rechtlich selbständige, föderal gegliederte Landesorganisationen als Mitglieder
- Bundesweit ca. 3.000 Mitglieder aus Unternehmen und Verbänden
- RKW RLP mit Schwerpunkt KMU in RLP
  - Rationalisierungs- und Innovationsmöglichkeiten
  - Technologietransfer Forschung zum Mittelstand
  - Regionale Unternehmernetzwerke und Arbeitskreise
  - Modellprojekte, Beratung, Weiterbildung für KMU
  - Zertifizierungen (akkreditiert / nicht-akkreditiert)
  - Kommunale Beratungen und Projekte
  - Beraterregistrierung und -qualifizierung

ad personam

- Dr. Rolf Dahm
  - Promotion Theoretische Physik, Mainz
  - langjährige freiberufliche Beratungstätigkeiten IT (ab 1994), Projektmanagement und Systemtheorie / -analyse
  - derzeitige Tätigkeiten:
    - Geschäftsführender Gesellschafter (Software-Unternehmen, 1999) mit Schwerpunkten „Verteilte Anwendungen“ und „Software als Medizinprodukt“
    - Forschung Mathematische Physik, Algebren- / Gruppentheorie, Projektive und Algebraische Geometrie [http://www.researchgate.net/profile/Rolf_Dahm]
- RKW – ehrenamtliche Tätigkeiten:
  - Vorsitz Vorstand und Präsidium RKW RLP e.V. [http://www.rkw-rlp.de/]
  - Vorstandsbereich III:
    - Technologietransfer, Intellectual Property („IP“)
    - Cluster / Netzwerke
    - Existenzgründungen, insbesondere im Technologiebereich
  - Mitglied des Bundesvorstands RKW e.V. [http://www.rkw.de]
  - Präsidiumsvorsitz RKW CERT [http://www.rkw-cert.de/]

Agenda und Zusammenhänge

Ein unüberschaubarer Markt: Zertifizierungsangebote und ihre Anforderungen

- Vortragstitel und Hintergründe
  - Was will uns dieser Titel wohl sagen?
  - Standortbestimmung – ein Bild!
  - Transfer des Bildes auf Informationssicherheit und IT
- Übertragungen der Bild-„Facetten“:
  - strukturell: IT und „Sicherheit“
  - ökonomisch: Markt bzgl. Informations- / IT-Sicherheit
  - technisch: Sicherheitsbereiche
  - gesellschaftlich: Einordnung
- Ausblick
  - Fazit und Handlungsbedarf

Agenda und Zusammenhänge

Ein unüberschaubarer Markt:
Zertifizierungsangebote und ihre Anforderungen

- Vortragstitel und Hintergründe
  - Was will uns dieser Titel wohl sagen?
  - Standortbestimmung – ein Bild!
  - Transfer des Bildes auf Informationssicherheit und IT
- Übertragungen der Bild-„Facetten“:
  - strukturell: IT und „Sicherheit“
  - ökonomisch: Markt bzgl. Informations- / IT-Sicherheit
  - technisch: Sicherheitsbereiche
  - gesellschaftlich: Einordnung
- Ausblick
  - Fazit und Handlungsbedarf

Vortragstitel und Hintergründe

- Begriffe und Verknüpfungen in den Überschriften:
  - „Transparenz“
  - „Vertrauen“
  - … ein „und“ dazwischen…
  - „Datenschutz- und Sicherheitsaudits“
- und im Vortragsthema:
  - „unüberschaubarer Markt“ mit nachfolgendem Fragezeichen
  - inhaltliche Anforderungen von Zertifizierungsangeboten
- SEHR viele Facetten des „Themas Informationssicherheit“!
- Typische Situation:
  Jetzt stehe ich als K-/M-Unternehmer davor und ich bin etwas überfordert, diese Informationsflut für mich zu sortieren…
  Was benötige ich denn überhaupt und wozu? Hilft‘s mir?

Vortragstitel und Hintergründe – ein Bild!

- Versuch einer Orientierung / eines Transfers mittels eines ähnlich komplexen Bildes:

Vortragstitel und Hintergründe – ein Bild!

RKW Rheinland-Pfalz e.V. DER VORSTAND

- Versuch einer Orientierung / eines Transfers mittels eines ähnlich komplexen Bildes:

Gregory Phillips, 15.1.2004
GNU Free Documentation License v1.2

- Diamant – Facetten und Sichtweisen
  - strukturelle Sichtweise:
    - Kristallklasse O_h [Schoenflies] bzw. $4/m\bar{3}2/m$ [Hermann-Mauguin]
    - Raumgruppe hexakisoktaedrisch
  - ökonomische Sichtweise:
    - Angebot / Nachfrage (Produkt ist doch klar!?)
    - Preis / Leistung
  - technische Sichtweise:
    - extrem harter Kohlenstoff, ggf. noch Aufbewahrung / Fassung
  - gesellschaftliche Sichtweise:
    - Status und Psyche Besitzer, emotionale Bindung
    - Herkunft des Diamanten
- Es fehlen aber noch zwei Begriffe: Transparenz und Vertrauen!

Vortragstitel und Hintergründe – ein Bild!

- Wie kommen diese beiden Begriffe ins Spiel?
- Audit und Zertifizierung als Grundlage:
  - Grundlegende Standards: Reinheit, Einschlüsse, Farbe, etc.
  - Unabhängige Prüfung (Messung, Begutachtung)
  - Zertifikaterstellung

Vortragstitel und Hintergründe – ein Bild!

RKW Rheinland-Pfalz e.V. DER VORSTAND

- Wie kommen diese beiden Begriffe ins Spiel?
- Audit und Zertifizierung als Grundlage:
  - Grundlegende Standards: Reinheit, Einschlüsse, Farbe, etc.
  - Unabhängige Prüfung (Messung, Begutachtung)
  - Zertifikaterstellung
- … und dann: Der Diamant ist ein **kein** Diamant, sondern ein kubischer Zirkonia mit Brilliantschliff…!
  - strukturelle Sichtweise:
    - Kristallklasse $Fm\bar{3}m$ [Hermann-Mauguin]
    - Raumgruppe kubisch
  - ökonomische Sichtweise:
    - Angebot / Nachfrage (Produkt war doch nicht klar!)
    - Preis / Leistung sehr schlecht
  - technische Sichtweise:
    - Zirconiumdioxid, ggf. noch Aufbewahrung / Fassung
  - gesellschaftliche Sichtweise:
    - ??? je nach Kontext: ggf. Auftakt zu einem emotionalen Absturz!

Gregory Phillips, 15.1.2004
GNU Free Documentation License v1.2

Vortragstitel und Hintergründe – Bildtransfer!

- Transfer auf Informationssicherheit und IT:
  - strukturelle Sichtweise:
    - Informationssicherheit – systemische Verortung IT und von „Sicherheit“ als Informationssicherheit
    - Überschaubarkeit und Komplexität
  - ökonomische Sichtweise:
    - Markt – gibt es den?
    - Was ist Angebot, was ist Nachfrage?
    - Preis / Leistung
  - technische Sichtweise:
    - Informationssicherheit und IT-Technik
    - bottom-up-Ansätze zur Informationssicherheit
    - Transparenz und Vertrauen
  - gesellschaftliche Sichtweise:
    - Datenschutz und Informationssicherheit
    - nochmal: Transparenz und Vertrauen
  - WICHTIG: Facetten und Beschreibung, kein umfassender Lösungsversuch!

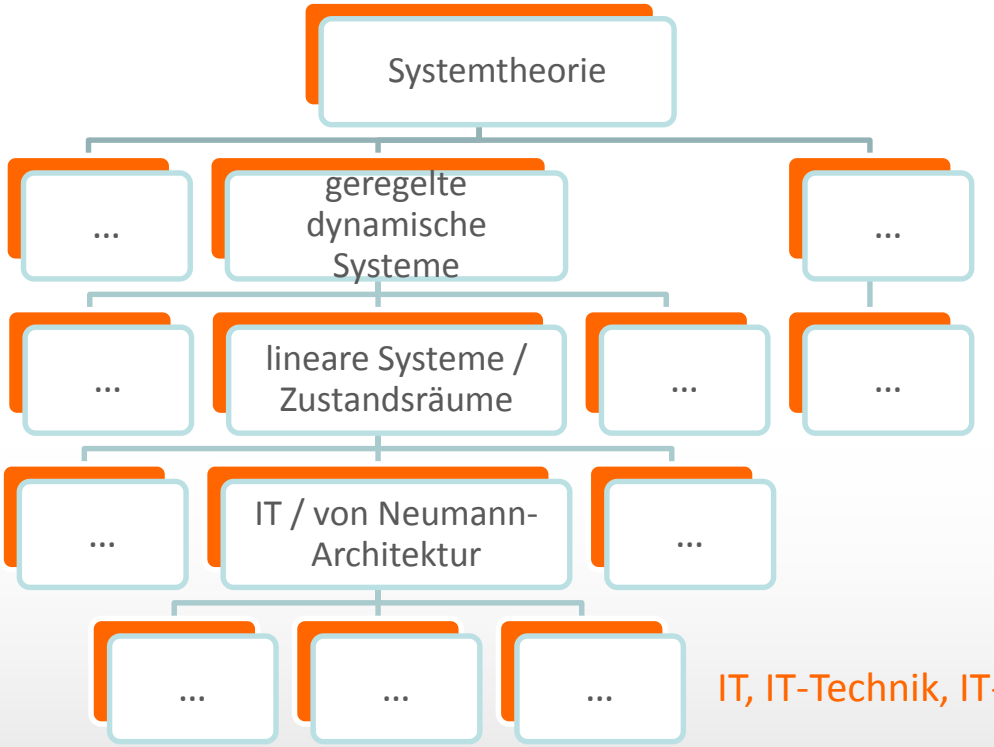
Agenda und Zusammenhänge

Ein unüberschaubarer Markt:
Zertifizierungsangebote und ihre Anforderungen

- Vortragstitel und Hintergründe
  - Was will uns dieser Titel wohl sagen?
  - Standortbestimmung – ein Bild!
  - Transfer des Bildes auf Informationssicherheit und IT
- Übertragungen der Bild-„Facetten“:
  - strukturell: IT und „Sicherheit“
  - ökonomisch: Markt bzgl. Informations- / IT-Sicherheit
  - technisch: Sicherheitsbereiche
  - gesellschaftlich: Einordnung
- Ausblick
  - Fazit und Handlungsbedarf

Übertragungen – strukturell: IT

- Verortung Informationssicherheit und IT (exempl.)



IT, IT-Technik, IT-Technikkonzepte

- es gibt ein „INTERN“ und ein „EXTERN“ bzgl. IT/IT-Technik und Konzepten!

Übertragungen – strukturell: IT

- Verortung Informationssicherheit und IT (Forts.)
  - Reduktion auf (IT-)Technik zwar vertrieblich vorteilhaft, aber prozessual / sozial / gesellschaftlich äußerst problematisch
  - WICHTIG (aus Systemkontext) sind auch übergreifende Bereiche!
    - PERSONELLE Maßnahmen
    - Datenschutz auch als ideeller Wert (digitale Grundrechte!)
    - organisatorische Maßnahmen (Abläufe, Prozesse, …)
    - ggf. baulich-physische Maßnahmen
    - ggf. weitere technische Maßnahmen
  - somit KLAR:
    - Neoliberale BWL (naive Kostenminimierung) als natürlicher Gegner
    - heutiges Bildungsniveau (Naturwissenschaften/IT) als natürlicher Gegner
    - übergreifender, ggf. sogar volkswirtschaftlicher Handlungsbedarf
    - übergreifendes, interdisziplinäres Wissen erforderlich
    - stufenweiser Zugang (da systemische Forderungen) erforderlich!
  - damit auch KLAR (vielfach „IST“-Situation):
    - Vertriebsthema für Produkt- / Konzeptbesitzer
    - hoher Aufwand / hohe Kosten beim Interessenten / Nachfrager

Übertragungen – strukturell: IT

- WICHTIG bzgl. „Ist“-Zustand:
  - Inhalt der Diskussion sind komplexe Systeme, daher gibt es keine minimalen „objektiven“ oder rein technische Lösungen
  - derzeit vielfach technikgetriebene Lösungen nach
    - Marktangeboten (interessengesteuert)
    - vorhandenem Wissensstand
  - leider viel zu wenig öffentliche Diskussion
  - man glaubt immer noch an evolutionäre Entwicklungen („Papier nach IT“)
  - viele glauben „an den Markt“ quasi als neue heilsbringende Religion
  - vielfach undifferenzierte Medienberieselung, Details oft nur im Internet
- Zwei dringend erforderliche Klarstellungen:
  - Globale IT-Netzwerke verhalten sich ESSENTIELL anders als ein Keller mit Patienten- oder Stasi-Akten!
  - „Gemeinwohlgedanke des Staates“ ist in herstellerdominierten Technikumgebungen nicht anwendbar!

Übertragungen – strukturell: IT

- REVOLUTIONÄRE ZEIT (systemische Aspekte):
  - IT wandert nicht nur in jeden Prozeß, sondern auch in alle Bereiche der Gesellschaft und in die Privatsphäre
  - Rechtsgüter werden mangelhaft oder gar nicht „virtualisiert“
    - Elektronische Signatur
    - Gesundheitskarte
    - Digitale Identität/Privatsphäre, usw. [SEHR lange Liste]
  - hersteller- und technikgetriebene Faktenschaffung wird a priori zugelassen (Bsp. Smartphones und Hersteller-Inseln/-Ökosysteme, BYOD)
  - Öffentlichkeit / Politik reagiert nur zäh aufgrund großartiger und SEHR wichtiger Arbeit von Datenschützern und/oder Privatpersonen
  - Wissen heute oft virtuelles Online-Wissen („ich frag‘ mal Google…“)
  - Teile der Wissenschaft als Profiteure / Komplizen („endlich Daten…“)
  - dramatischer Umbau der individuellen Werte
  - keinerlei Ethikdiskussion analog der Medizin („Anwendung am Menschen“)
  - Staaten spielen scheinbar mit / profitieren (Geheimdienstdiskussion)

Übertragungen – strukturell: IT

- Systemische Aspekte / Angriffspotential und Mythos Beherrschbarkeit

Beispiel Pavlovic / Fauser [arxiv:1402.4414v2 math.CT]

- Software-Modellierung durch Zustandsmodelle auf kontinuierlichen und metrischen Zustandsräumen
- Prozesse als Co-Algebren
- Struktur-Abbildungen spezifizieren Zustandsübergänge
- …

- Kategorientheorie (d.h. harte Mathematik)

Übertragungen – strukturell: IT

- Systemische Aspekte / A
  Mythos Beherrschbarkei

  Beispiel Pavlovic / Fauser [arx
  - Software-Modellierung du
    und metrischen Zustandsr
  - Prozesse als Co-Algebren
  - Struktur-Abbildungen spe
  - …

  - Kategorientheorie (d.h. ha

2 General testing framework

We begin by reviewing the testing framework from [46].

2.1 Idea

Given a family of systems Σ, a family of tests Θ, and a type Ω of observations, we call a map

$$\Sigma \times \Theta \xrightarrow{\mathbb{T}} \Omega \tag{1}$$

a *testing correlation*, or just *testing*. The observation $\mathbb{T}(S,t)$ is often written in the infix form $S \models t$. The observations can be boolean, like 'true'/'false', or 'pass'/'fail'; but they can also be quantities obtained from a measurement, e.g. in the interval $[0,1]$, or on the real line $\mathbb{R}$. Each test is assumed to yield a single observation. In the simplest case, we may use testing to distinguish a given system $S \in \Sigma$ from a reference system $R \in \Sigma$. The two systems are observably different if there is a test $b \in \Theta$ such that the observation $R \models b$ is different from the observation $S \models b$. Otherwise, if the two systems induce the same observations for all tests, then they are *observationally indistinguishable*, and we write

$$S \sim R \iff \forall t \in \Theta.(S \models t) = (R \models t)$$

Developing this idea in [43], E.F. Moore suggested that minimal representations of automata can be built over the equivalence classes of their observationally indistinguishable states. This idea was elaborated categorically in [46], by identifying each equivalence class of systems that are observationally indistinguishable from $S \in \Sigma$ with the map $S \models (-) : \Theta \to \Omega$. Such maps can be thought of as the *observable behaviors* of systems. The family L of observable behaviors of systems from Σ can thus be obtained as the image in Ω^Θ of the mapping that

Übertragungen – strukturell: IT

- Systemische Aspekte / A
  Mythos Beherrschbarkei

  Beispiel Pavlovic / Fauser [arx
  - Software-Modellierung du
    und metrischen Zustandsr
  - Prozesse als Co-Algebren
  - Struktur-Abbildungen spe
  - …

  - Kategorientheorie (d.h. ha

2 General testing framework

We begin by

2.1 Idea

Given a fami
we call a ma

a *testing cor*
in the infix f
or 'pass'/'fai
e.g. in the i
a single obse
a given syste
observably di
different fron
same observa
and we write

Developing t
of automata
indistinguish
tifying each
able from S
as the *observ*
systems from

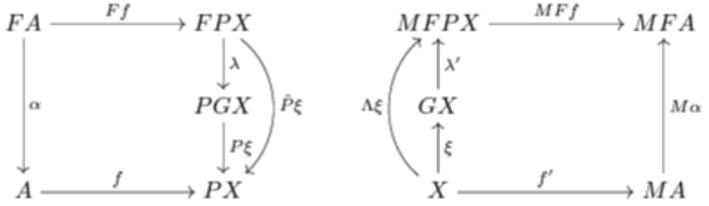
(a) The predicate functor $P : \mathcal{S}^{op} \to \mathcal{T}$ lifts to $\hat{P} : (\mathcal{S}_G)^{op} \to {}_F\mathcal{T}$

$$\frac{X \xrightarrow{\xi} GX}{\hat{P}\xi : FPX \xrightarrow{\lambda} PGX \xrightarrow{P\xi} PX}\ \text{LIFT} \qquad (3)$$

(b) $\hat{P}$ has in general no adjoint, but there is a correspondence

$$\frac{\alpha \longrightarrow \hat{P}\xi}{\Lambda\xi \longrightarrow M\alpha}$$

where $\Lambda : \mathcal{S}_G \to \mathcal{S}_{MFP}$ is the functor mapping the coalgebra $\xi : X \to GX$ to $X \xrightarrow{\xi} GX \xrightarrow{\lambda'} MFPX$. λ' is the twisted distributivity law.



(4)

(c) If $\mathcal{T}$ is a regular category, and $F : \mathcal{T} \to \mathcal{T}$ preserves reflexive coequalizers, then ${}_F\mathcal{T}$ is a regular category. Every F-algebra homomorphism $\alpha \xrightarrow{f} \hat{P}\xi$ has a regular epi-mono factorization.

(d) If $\mathcal{S}^{op}$ is a regular category, and MFP preserves weak pull backs, then every twisted coalgebra homomorphism $f' : \Lambda\xi \to M\alpha$ has a regular epi-mono factorization, which induces a coalgebra $\ell : L \to MFPL$ as the

Übertragungen – strukturell: IT

- Systemische Aspekte / Angriffspotential und Mythos Beherrschbarkeit

Beispiel Shandilya / Simmons / Shiva [J Comp Netw Comm 2014]

- Angriffsgraphen („attack graphs“)
- Systemmodellierung und potentielle System-Exploits
- System(re-)konstruktion / -modellierung zur Analyse
- Bestimmung / Tests des Antwortverhaltens
- …

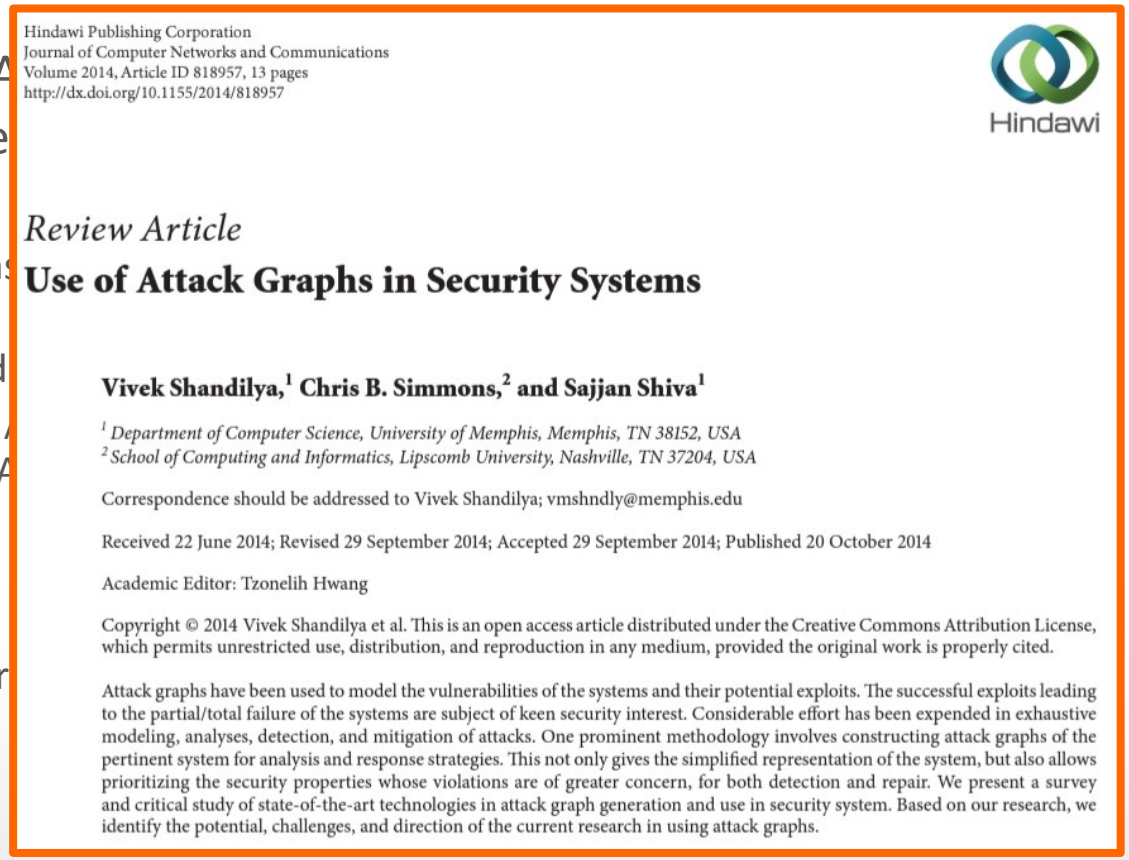
- Graphentheorie (d.h. harte Mathematik)

Übertragungen – strukturell: IT

- Systemische Aspekte / A
  Mythos Beherrschbarke

  Beispiel Shandilya / Simmons
  - Angriffsgraphen („attack
  - Systemmodellierung und
  - System(re-)konstruktion /
  - Bestimmung / Tests des A
  - …

  - Graphentheorie (d.h. har



Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2014, Article ID 818957, 13 pages
http://dx.doi.org/10.1155/2014/818957

Hindawi

Review Article

Use of Attack Graphs in Security Systems

Vivek Shandilya,[1] Chris B. Simmons,[2] and Sajjan Shiva[1]

[1] *Department of Computer Science, University of Memphis, Memphis, TN 38152, USA*
[2] *School of Computing and Informatics, Lipscomb University, Nashville, TN 37204, USA*

Correspondence should be addressed to Vivek Shandilya; vmshndly@memphis.edu

Received 22 June 2014; Revised 29 September 2014; Accepted 29 September 2014; Published 20 October 2014

Academic Editor: Tzonelih Hwang

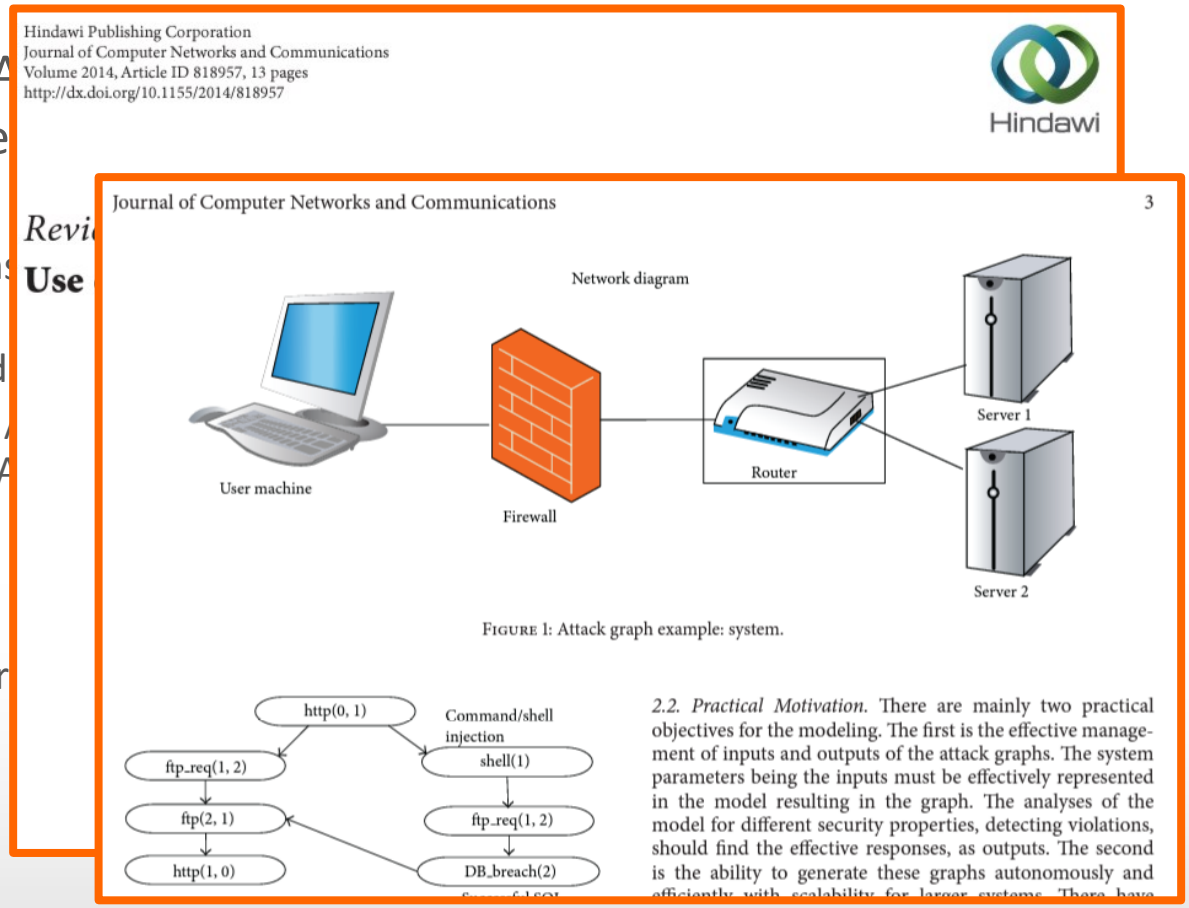
Attack graphs have been used to model the vulnerabilities of the systems and their potential exploits. The successful exploits leading to the partial/total failure of the systems are subject of keen security interest. Considerable effort has been expended in exhaustive modeling, analyses, detection, and mitigation of attacks. One prominent methodology involves constructing attack graphs of the pertinent system for analysis and response strategies. This not only gives the simplified representation of the system, but also allows prioritizing the security properties whose violations are of greater concern, for both detection and repair. We present a survey and critical study of state-of-the-art technologies in attack graph generation and use in security system. Based on our research, we identify the potential, challenges, and direction of the current research in using attack graphs.

Übertragungen – strukturell: IT

- Systemische Aspekte / A
  Mythos Beherrschbarke

Beispiel Shandilya / Simmons
- Angriffsgraphen („attack
- Systemmodellierung und
- System(re-)konstruktion /
- Bestimmung / Tests des A
- …

- Graphentheorie (d.h. har



Hindawi Publishing Corporation
Journal of Computer Networks and Communications
Volume 2014, Article ID 818957, 13 pages
http://dx.doi.org/10.1155/2014/818957

Hindawi

Journal of Computer Networks and Communications 3

Network diagram

User machine
Firewall
Router
Server 1
Server 2

FIGURE 1: Attack graph example: system.

http(0, 1)
Command/shell injection
ftp_req(1, 2)
shell(1)
ftp(2, 1)
ftp_req(1, 2)
http(1, 0)
DB_breach(2)

2.2. Practical Motivation. There are mainly two practical objectives for the modeling. The first is the effective management of inputs and outputs of the attack graphs. The system parameters being the inputs must be effectively represented in the model resulting in the graph. The analyses of the model for different security properties, detecting violations, should find the effective responses, as outputs. The second is the ability to generate these graphs autonomously and

Übertragungen – strukturell: IT

- Systemische Aspekte / Angriffspotential und Mythos Beherrschbarkeit

Beispiel Graph-Operad-Logic X ,
Dynamische Systembeschreibungen, [Tallinn 2013, http://www.astralgo.com/]

- Angewandte Kategorientheorie auf 3-schichtige Informationssysteme
- Graphen und logische Systeme
- Systemverhalten anhand Transformationseigenschaften
- Dynamische Systemmodellierung entlang Differentialgleichungen
- Dynamische algebraische Systemmodellierungen
- …

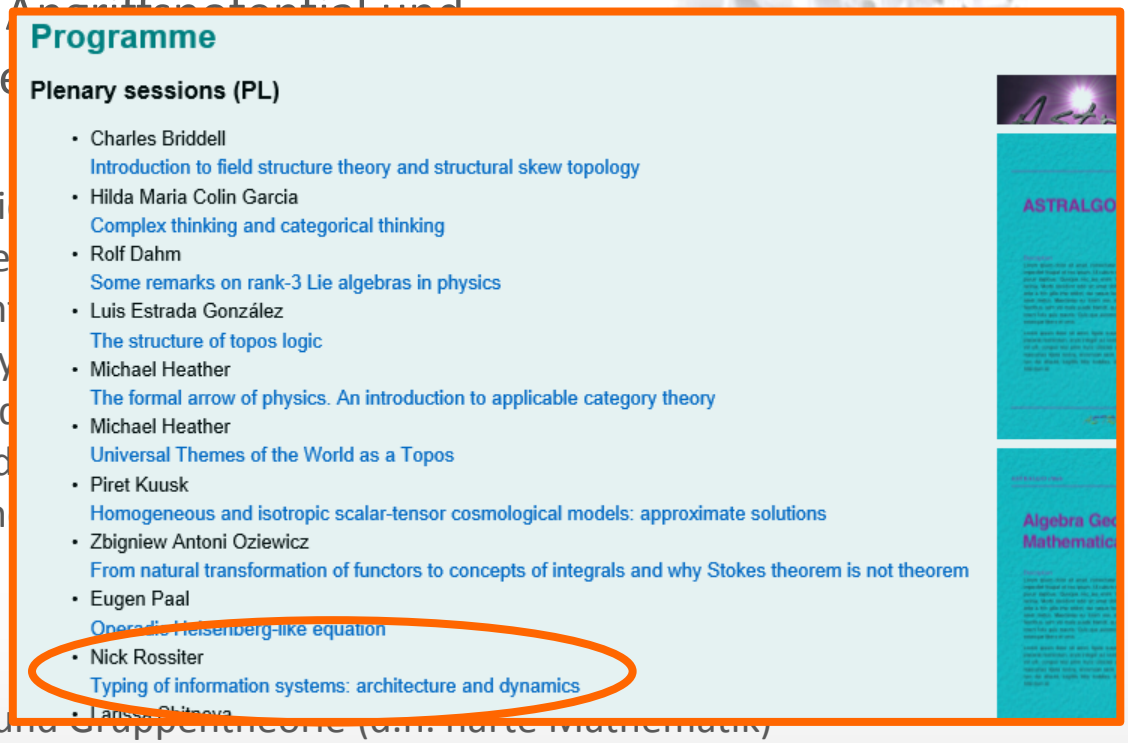
- Kategorien-, Algebren- und Gruppentheorie (d.h. harte Mathematik)

Übertragungen – strukturell: IT

- Systemische Aspekte / A
  Mythos Beherrschbarke

  Beispiel Graph-Operad-Logi
  Dynamische Systembeschre
  - Angewandte Kategorien
  - Graphen und logische Sy
  - Systemverhalten anhand
  - Dynamische Systemmod
  - Dynamische algebraisch
  - …

  - Kategorien-, Algebren- und Gruppentheorie (d.h. harte Mathematik)



Programme

Plenary sessions (PL)

- Charles Briddell
  Introduction to field structure theory and structural skew topology
- Hilda Maria Colin Garcia
  Complex thinking and categorical thinking
- Rolf Dahm
  Some remarks on rank-3 Lie algebras in physics
- Luis Estrada González
  The structure of topos logic
- Michael Heather
  The formal arrow of physics. An introduction to applicable category theory
- Michael Heather
  Universal Themes of the World as a Topos
- Piret Kuusk
  Homogeneous and isotropic scalar-tensor cosmological models: approximate solutions
- Zbigniew Antoni Oziewicz
  From natural transformation of functors to concepts of integrals and why Stokes theorem is not theorem
- Eugen Paal
  Operadic Heisenberg-like equation
- Nick Rossiter
  Typing of information systems: architecture and dynamics
- Larissa Shitneva

Übertragungen – strukturell: IT

- Systemische Aspekte / A
  Mythos Beherrschbarke

  Beispiel Graph-Operad-Logi
  Dynamische Systembeschre
  - Angewandte Kategorien
  - Graphen und logische Sy
  - Systemverhalten anhand
  - Dynamische Systemmod
  - Dynamische algebraisch
  - …

  - Kategorien-, Algebren- und Grupp

Übertragungen – strukturell: IT

- Systemische Aspekte / Angriffspotential und Mythos Beherrschbarkeit

Weitere Beispiele in Kürze:

- Zitat aus einem externen Audit (!) für Medizinprodukte, ISO 13485:
  „Mathematik ist, wenn die Tafel voll ist, viele kleine Buchstaben
  als Indizes verteilt sind und keiner weiß, was gemeint ist…“
  [Lead-Auditor anläßlich der Vollständigkeitsprüfung des Datenmodells eines Medizinprodukts]
- Anti-Viren-Software prüft / stellt wegen geringer Effizienz auf Call-Graphen um
- Mathematikkonferenz, Goslar 2015:
  BigData und Markt-/Käuferverhalten als Transformationstheorie im $\mathbb{R}^{2057}$
  (Vektoren und Statistik) → DATENSCHUTZ?
- Sprachanalyse und quaternionische Wavelets 2014 (Ethik-Diskussion abgewürgt!)

Übertragungen – strukturell: IT

- Systemische Aspekte / Angriffspotential und Mythos Beherrschbarkeit

  - white/black hacking („handwerkliche Antwort der Informatiker…“)
  - Vertrauen auf Zahlentheorie bei der Verschlüsselung (u.a. Teilbarkeit)
  - jüngste Schlagzeilen:
    - Android-Hacks (Betriebssystem Schmacht-Phones)
    - Schad-Software im Apple-Store
    - Firmware-Schädlinge (Iran, USB-Sticks, Router, …)
    - Lecks DSL-Router
    - Backdoors in Weitverkehrsdatenverteilern (Backbone-Router)
    - angelsächsische und asiatische Geheimdienstprogramme
    - Satellitenkontrolle
  - … (beliebig fortsetzbar)

Übertragungen – strukturell: IT

- The „way out“: A. C. Clarke‘s Drittes Gesetz

> “Any sufficiently advanced technology is indistinguishable from magic.”
>
> [„Jede hinreichend fortschrittliche Technologie ist von Magie nicht zu unterscheiden.“]

- Nun sind wir beim „Glauben“ und „Vertrauen“ angelangt, **aber wer soll‘s denn nun richten?**

Übertragungen – ökonomisch: Markt

- Aus Überschriften: Transparenz, Vertrauen, Markt
  - Warum hier Transparenz und Vertrauen?
  - Warum „unüberschaubarer Markt?“?
- Klärung der Begrifflichkeit „Transparenz“
  - Transparenz [Wöhe, Allgemeine BWL (1996)]

    „Markttransparenz: Alle Anbieter und Nachfrager sind (stets) vollkommen informiert.“

  - Bei Informationstechnologien? KMU? Endkunden? Größere Unternehmen? Hier ist wohl jedes Wort der Definition problematisch!
  - Und weiter: [Wöhe, Allgemeine BWL (1996), S. 632]

    „Fehlende Markttransparenz schafft Freiräume im Wettbewerb!“

  - Produktpolitik (aus Anbietersicht) sollte also Inhomogenitäten schaffen, dies auch unterstützt durch das eher komplexe Grundthema!
  - Ökonomischer Kontrapunkt zu dem eigentlich deterministischen Thema!

Übertragungen – ökonomisch: Markt

- Klärung Begrifflichkeit „Vertrauen“
  - Vertrauen [Wöhe, Allgemeine BWL (1996)]

    – / –

  - ? – also Wikipedia: [http://www.wikipedia.de/, 1.9.2015]

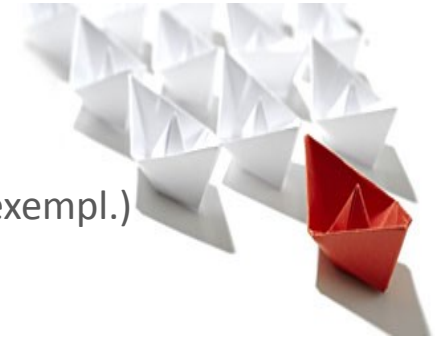
    „**Vertrauen** ist in psychologisch-persönlichkeitstheoretischer Perspektive definiert als subjektive Überzeugung von der (oder auch als Gefühl für oder Glaube an die) Richtigkeit, Wahrheit bzw. Redlichkeit von Personen, von Handlungen, Einsichten und Aussagen eines anderen oder von sich selbst (Selbstvertrauen). Zum Vertrauen gehört auch die Überzeugung der Möglichkeit von Handlungen und der Fähigkeit zu Handlungen. Man spricht dann eher von Zutrauen. Als das Gegenteil des Vertrauens gilt das Misstrauen.“

  - na – eher schwammig in einer wohldefinierten Welt der Information und der IT…

Übertragungen – ökonomisch: Markt

- Interpretation „Vertrauen“
  - bisher eher negative Interpretation
    - eigentlich wohldefiniert und deterministisch, z.T. reine Ingenieurkunst, warum kommen solche subjektiven Begriffe/Wertungen ins Spiel?
  - aber: positive Interpretation
    - wir kennen uns aus und wissen, was wir tun und benötigen
    - schrittweise Verbesserung der Zielerreichung und Erhöhung der Systemunterstützung
    - 6-Augen-Prinzip (intern, Berater, Auditor)
- mündet offensichtlich einmal mehr in Clarke‘s Drittem Gesetz!
- „Glauben“ und „Vertrauen“ statt exaktem Wissen und Sicherheit
  - Unternehmer gegenüber Fachabteilungen und Technokraten (intern/extern)
  - Unternehmer gegenüber Anbietern derartiger Technologien
  - Endkunden gegenüber Unternehmen allgemein
  - Unternehmen allgemein gegenüber wenigen Technologiekonzernen
  - Endkunden / Unternehmen gegenüber Politik / Gemeinwesen (Ordnungshoheit)
  - …

Übertragungen – ökonomisch: Markt



- Warum Glauben und Vertrauen? (exemplarisch)
  - Wissensstand der Akteure (**beide** Markt-Seiten!)
  - Abkopplung Management (BWL) vom operativen Betrieb
  - betriebsinterne Sparmaßnahmen „an den falschen Stellen“ (exempl.)
    - Weiterbildung
    - Personalauswahl
    - Ressourcenbeistellung
  - falsche Annahmen über Vorsatz anderer Personen, Wertigkeit eigener Informationen und die (technischen) Möglichkeiten der anderen Marktteilnehmern
- Einige wenige Beispiele der jüngsten Zeit:
  - Bundestag: Handlungen der Akteure und Systeme
  - Angriffe / Verseuchung Android oder Firmware USB-Sticks
  - Angriff / Verseuchung Apple-Store
  - HSV: Manager hat Rucksack im Park vergessen
  - NSA/weitere Geheimdienste: Vorsatz, Spionage (z.B. Smartphones, Biometrie, Kommunikationsnetze, Satelliten, …)

Übertragungen – ökonomisch: Markt

- Def. „Markt“ als Zusammentreffen von Angebot und Nachfrage, dazu Abgrenzungen
  - sachlich: Abgrenzung nach Gütern und/oder Gütergruppen
  - räumlich: Einkaufsgewohnheiten
  - personell: Markt konstituiert sich aus den im Markt agierenden Anbietern und Nachfragern
- Wer ist das?
  - Angebote von
    - System-/IT-Herstellern
    - Beratungsunternehmen
    - Ämtern/Behörden und z.T. Kammern
  - Nachfrage durch …?
  - Und: Vertrauen in Angebote?
  - Helfen Audits? Zertifikate? Und wenn ja, welche?

Übertragungen – ökonomisch: Markt

- Damit: Zertifikat (wieder Wikipedia, Excerpt)

Zertifikat (von lat. certus „sicher, bestimmt“ und facere „machen“) steht für:

- Allgemein eine Beglaubigung
- Allgemein eine Bescheinigung
- […]
- in der Informatik die Verifikation einer (meist asymmetrischen) Verschlüsselung, siehe Digitales Zertifikat
- […]
- im Verbraucherschutz ein Mittel zur Sicherstellung von Qualitäts- oder Nachhaltigkeitsstandards von Produkten, siehe Gütesiegel
- […]
- in der IT-Branche der Nachweis einer Qualifikation, siehe Liste der IT-Zertifikate

- oha: Letztes Link! Wieder Wikipedia:

Übertragungen – ökonomisch: Markt

IT-Zertifizierungen sind Nachweise einer Qualifikation in der Branche der Informationstechnik. Sie werden von verschiedenen Organisationen angeboten. Diese Organisationen bescheinigen dem Zertifikatsinhaber Kenntnisse auf einem Gebiet. Die meisten Zertifikate enthalten keine Note, sondern nur ein „hat bestanden“.

- Liste enthält > 50 Anbietern, meist Hersteller, auch Meta-/ „Standards“-Zertifizierungen (z.B. ITIL) mit mehreren hundert Angeboten…
- allein bei Sicherheitszertifizierungen findet man…

Übertragungen – ökonomisch: Markt

CompTIA Security+
CCNA Security – Cisco Certified Network Associate
CCNP Security – Cisco Certified Network Professional Security
CCIE Security – Cisco Certified Internetwork Expert
MCSA: Security (Server 2003/XP)
MCSE: Security (Server 2003/XP)
CIW Security Professional
CIW Security Analyst
eCCPM - ELearnSecurity Certified Professional Penetration Tester
SSCP – Systems Security Certified Practitioner
CISSP – Certified Information Systems Security Professional
TISP – Teletrust Information Security Professional
GIAC – Global Information Assurance Certification
OPSA – OSSTMM (Open Source Security Testing Manual) Professional Security Analyst
OPST – OSSTMM (Open Source Security Testing Manual) Professional Security Tester
RSA[13] Certified Archer Administrator

RSA Certified SecurID Administrator
RSA Certified Administrator
RSA Certified Systems Engineer
RSA Certified Instructor
TICSA – TruSecure ICSA Certified Security Associate
SCNS – Security Certified Network Specialist
SCNP – Security Certified Network Professional
SCNA – Security Certified Network Architect
CISA – Certified Information Systems Auditor
CISM – Certified Information Security Manager
CSSA – Certified SonicWALL Security Administrator
CEH – Certified Ethical Hacker (www.eccouncil.org)
CISE - Certified Information Security Expert (Indien) [14]
OSCP - Offensive Security Certified Professional
OSCE - Offensive Security Certified Expert
OSWP - Offensive Security Wireless Professional
ITSB+
CPSSE - Certified Professional for Secure Software Engineering

- Aber: Hauptsächlich Tummelplatz von Herstellern…
- Wie sieht die Nachfrage-Seite des „Marktes“ aus?

Übertragungen – ökonomisch: Markt

- Konzerne / Großunternehmen, großer Mittelstand:
  - eigene IT-/QM-Abteilungen
  - Compliance / Organisationsgrade konzernintern, dabei Datenschutz und Datensicherheit teils mehr „auf dem Radar“, teils weniger
  - teils nach Normen / „best practice“, meist nach Herstellern, teils zertifiziert
- Krankenhäuser / „kritische Infrastruktur“: Abenteuer pur
- Kleinst- / Klein- und kleine / mittlere mittelständische Unternehmen:
  - wenig „awareness“ oder Problembewußtsein, Auflagen sind hinderlich
  - IT wird „mitgemacht“ (kleine DL, Verwandschaft, Nachbar, Student, …)
- „Bürger“: Generationen „Y“ und „Z“ weitgehend desinteressiert und oft ahnungslos…
- Staat wird mitunter nicht mehr als objektiv/unabhängig und vertrauenswürdig angesehen
- und IMMER: SEHR TEUER und AUFWENDIG! Nutzen meist unklar!

Übertragungen – ökonomisch: Markt

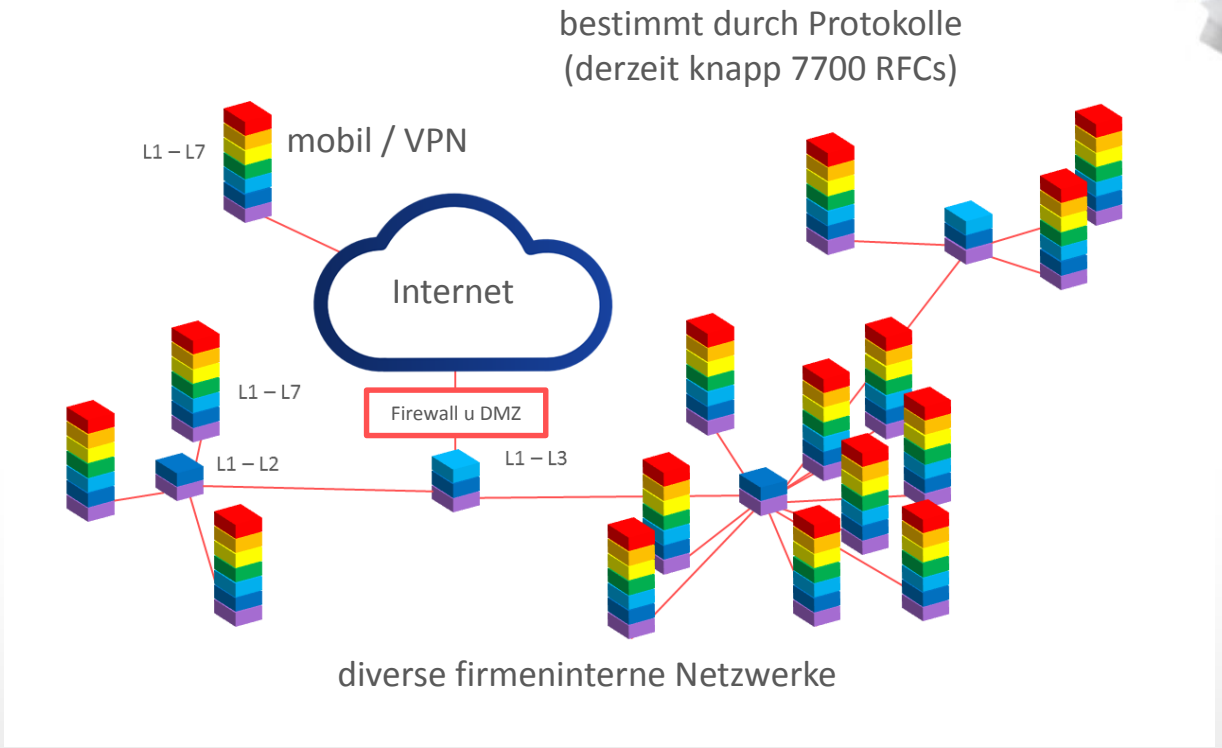
- Und nun?
- Transparenz funktioniert nur beschränkt, daher zurück zu Clarke‘s Drittem Gesetz und „Vertrauen“!
- Wem kann man vertrauen?
  - „dem Markt“, vor allem den Anbietern? … na ja, Markt eben…
  - dem eigenen Wissen / Gefühl? … na ja…
  - dem Wissen mancher (Fach-)Angestellter? … na ja… vielleicht schon eher…
  - den Infrastrukturanbietern? … na ja…
  - dem Staat? … na ja… und weiter? …?
- Wer/was bleibt? ? ?:
  - Unabhängige Beauftragte mit starken Durchgriffsrechten (Bund, Land, Firmen)
  - WENIGE anerkannte und durchsetzbare Standards, dazu gute Berater, Auditoren und WENIGE transparente und kostengünstige Zertifikate!
  - Dreistufiges RKW-Konzept – Impulsgespräch, Erhebung (generalistisch), Spezialisten
  - vor allem: Durchsetzung anerkannter Standards durch Gesellschaft / Politik!

Übertragungen – technisch: Sicherheitsbereiche

- Informationssicherheit und IT 2015:
  - schleichender IT-Einzug in alle Bereiche
    - initial IT als Hilfsmittel / „tool set“ (Rationalisierung)
    - danach schnell auch Kommunikation und Dateitransfer
    - dann Marketing-Plattform („World Wide Web“)
    - nun immer mehr allumfassende Lebensbegleitung… (mobil, IoT)
  - mittlerweile scheinbare Inversion der Werthaftigkeit
    - IT als Rückgrat / Schwerpunkt der Prozessbildung (XY 4.0)
  - technik- und herstellergetrieben, Sicherheit und Datenschutz meist nachfolgend, gesellschaftliche Diskussion fehlt nahezu
  - IT wird mehr und mehr als eine Modellierung gesellschaftlicher und wirtschaftlicher Prozesse gesehen und eingesetzt
  - Regelung meist „durch den Markt“, eine aktive Regelung durch Bürger und Politik oft erst nachfolgend (wenn überhaupt)
  - Systemimplementationen / -konfigurationen bestimmen oft die Regeln
- Und nun? Informationssicherheit? Datenschutz? Technik?

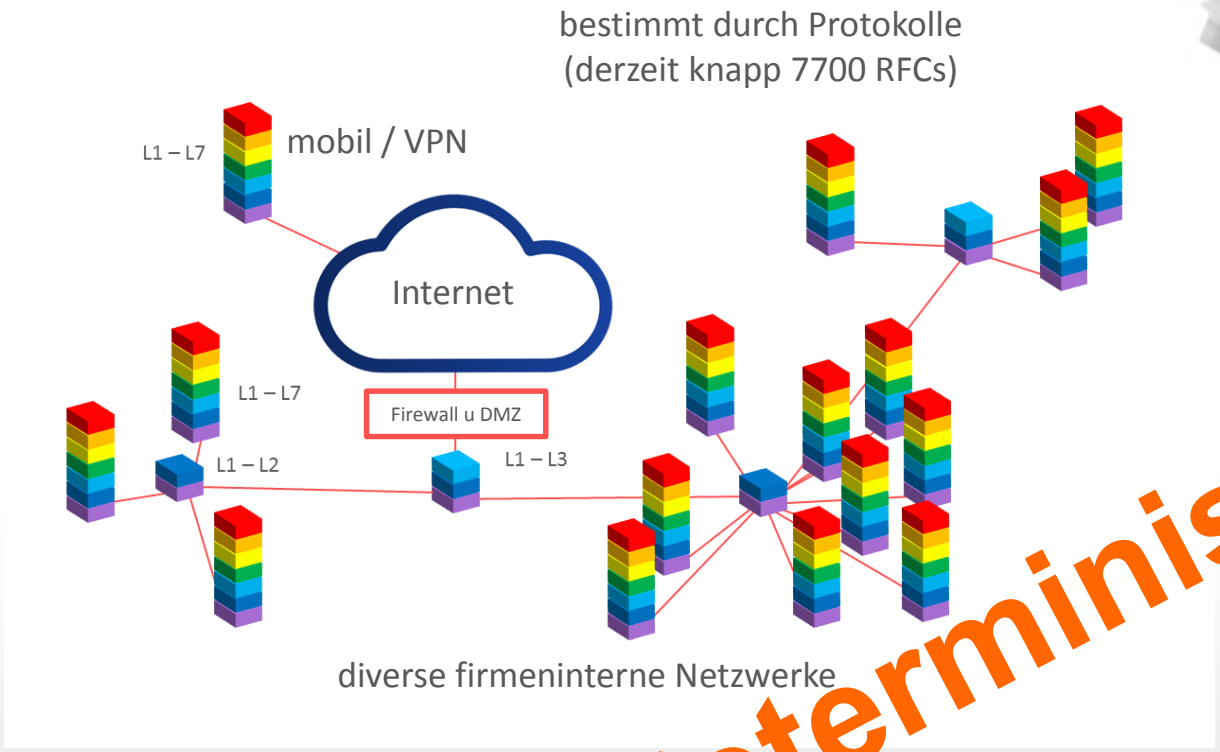
Übertragungen – technisch: Sicherheitsbereiche

- Bild IT-Infrastruktur:



Übertragungen – technisch: Sicherheitsbereiche

- Bild IT-Infrastruktur:



deterministisch

Übertragungen – technisch: Sicherheitsbereiche

- Zentraler Begriff: ISMS – was ist das?
  - Managementsystem (allgemein):
    - Alle Regelungen, die für die Steuerung und Lenkung zur Zielerreichung der Institution / des Unternehmens sorgen
  - ISMS verkürzt „information security management system“
  - Teil des Managementsystems, der sich mit Informationssicherheit beschäftigt
  - umfaßt die Bereiche (Komponenten)
    - Management-Prinzipien
    - Ressourcen
    - Mitarbeiter
    - Sicherheitsprozeß (Leitlinie, Konzept, Organisation)
  - benötigt Lebenszyklusmodell (z.B. PDCA)
- Idee: Normierung / Standardisierung und Dokumentation
  - äußerst begrüßenswert, wenn machbar
  - je nach Betriebsgröße und Unternehmer problematisch
  - ISO 9001 in KMU vielfach schon Hindernis oder „overkill“

Übertragungen – technisch: Sicherheitsbereiche

- Zentraler Begriff: ISMS – was ist das?
  - Managementsystem (allgemein):
    - Alle Regelungen, die für die Steuerung und Lenkung zur Zielerreichung der Institution / des Unternehmens sorgen
  - ISMS verkürzt „information security management system“
  - Teil des Managementsystems, der sich mit Informationssicherheit beschäftigt
  - umfaßt die Bereiche (Komponenten)
    - Management-Prinzipien
    - Ressourcen
    - Mitarbeiter
    - Sicherheitsprozeß (Leitlinie, Konzept, Organisation)
  - benötigt Lebenszyklusmodell (z.B. PDCA)
- Idee: Normierung / Standardisierung und Dokumentation
  - äußerst begrüßenswert, wenn machbar
  - je nach Betriebsgröße und Unternehmer problematisch
  - ISO 9001 in KMU vielfach schon Hindernis oder „overkill“

QM-Grundlage erforderlich!

Übertragungen – technisch: Sicherheitsbereiche

- Konsequenzen:
  - Angebote des Marktes an Unternehmen (insbes. KMU ohne QM-System) sind oft sinnlos und Geldmacherei
  - diverse Anbieter ohne QM-Hintergrund
    - machen zwar Geld, liefern aber wenig bis keinen Wert an Unternehmen (Fassade, aber Werthaftigkeit?)
    - oft isolierte (technische) Lösungen ohne Zusammenhang
  - hohe Einstiegserfordernisse und zusätzliche Kosten für Unternehmen
  - aus verschiedenen Gründen wenig öffentliche Wertschätzung
  - für Kleinst- und Kleinunternehmen sehr weit ab vom Tagesgeschäft und der Betriebsorganisation
- Reprise: Idee der Normierung / Standardisierung und Dokumentation
  - äußerst begrüßenswert, wenn machbar
  - je nach Betriebsgröße und Unternehmer problematisch
  - ISO 9001 in KMU vielfach schon Hindernis oder „overkill“

Übertragungen – technisch: Sicherheitsbereiche

- Grundlagen der Normierung(en) (exemplarisch)
  - Familie ISO/IEC 27000 – 27019, 27030 – 27044 (nicht EN!), IT-Sicherheit, aus dem angelsächsischen Raum
    - regeln viele Aspekte rund um ISMS
  - Common Criteria (CC, umfaßt ISO/IEC 15408, …, ISO/IEC TR 15446)
    - Schwachstellenminimierung Hardware/Software/„IT-Produkte“, Vertrauenswürdigkeit, Evaluationsgegenstände/Schutzprofile
  - COBIT, Val IT, Risk IT (ISACA, globale NGO, seit 1976)
    - Kontrolle von Risiken und Risikomanagement-Aspekte
  - ITIL (OCG, GB) für Personen und ISO/IEC 20000 (Organisationen)
    - Aspekte IT-Service Management **aus Sicht IT-Dienstleister**
  - ISO EN 13485 und IHE
    - Harmonisierte Norm für Medizinprodukte und -Software
    - europäischer Standard, umfaßt weitere Normen
    - IHE als Empfehlung der EU-Kommission 07/2015 mit 27 Profilen
  - ISO 80001
    - Norm für Medizinprodukte und –Software **in Netzwerken**

Übertragungen – technisch: Sicherheitsbereiche

- Grundlagen der Normierung(en) (exemplarisch)
  - Familie ISO/IEC 27000 – 27019, 27030 – 27044 (nicht EN!), IT-Sicherheit, aus dem angelsächsischen Raum
    - regeln viele Aspekte rund um ISMS
  - Common Criteria (CC, umfaßt ISO/IEC 15408, …, ISO/IEC TR 15446)
    - Schwachstellenminimierung Hardware/Software/„IT-Produkte“, Vertrauenswürdigkeit, Evaluationsgegenstände/Schutzprofile
  - COBIT, Val IT, Risk IT (ISACA, globale NGO, seit 1976)
    - Kontrolle von Risiken und Risikomanagement-Aspekte
  - ITIL (OCG, GB) für Personen und ISO/IEC 20000 (Organisationen)
    - Aspekte IT-Service Management **aus Sicht IT-Dienstleister**
  - ISO EN 13485 und IHE
    - Harmonisierte Norm für Medizinprodukte und -Software
    - europäischer Standard, umfaßt weitere Normen
    - IHE als Empfehlung der EU-Kommission 07/2015 mit 27 Profilen
  - ISO 80001
    - Norm für Medizinprodukte und –Software **in Netzwerken**

bottom up / best practice

Übertragungen – technisch: Sicherheitsbereiche

- Bundesamt für Sicherheit in der Informationstechnik (BSI) hat den Komplex 27xxx aufgearbeitet / erklärt:
  - Grundschutz BSI 100-1 bis 100-4 [http://www.bsi.bund.de/gshb]
  - Kataloge

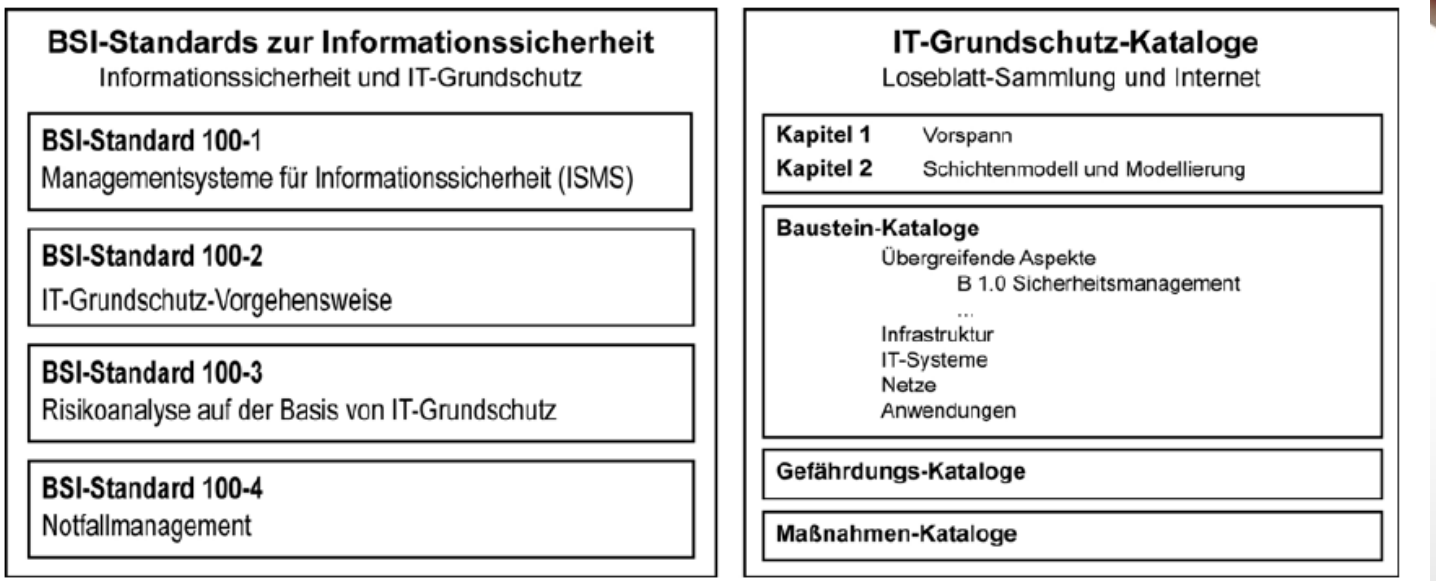


Abbildung 1: Übersicht über BSI-Publikationen zum Sicherheitsmanagement

Übertragungen – technisch: Sicherheitsbereiche

- Bundesamt für Sicherheit in der Informationstechnik (BSI) hat den Komplex 27xxx aufgearbeitet / erklärt:
  - Grundschutz BSI 100-1 bis 100-4 [http://www.bsi.bund.de/gshb]
  - Kataloge

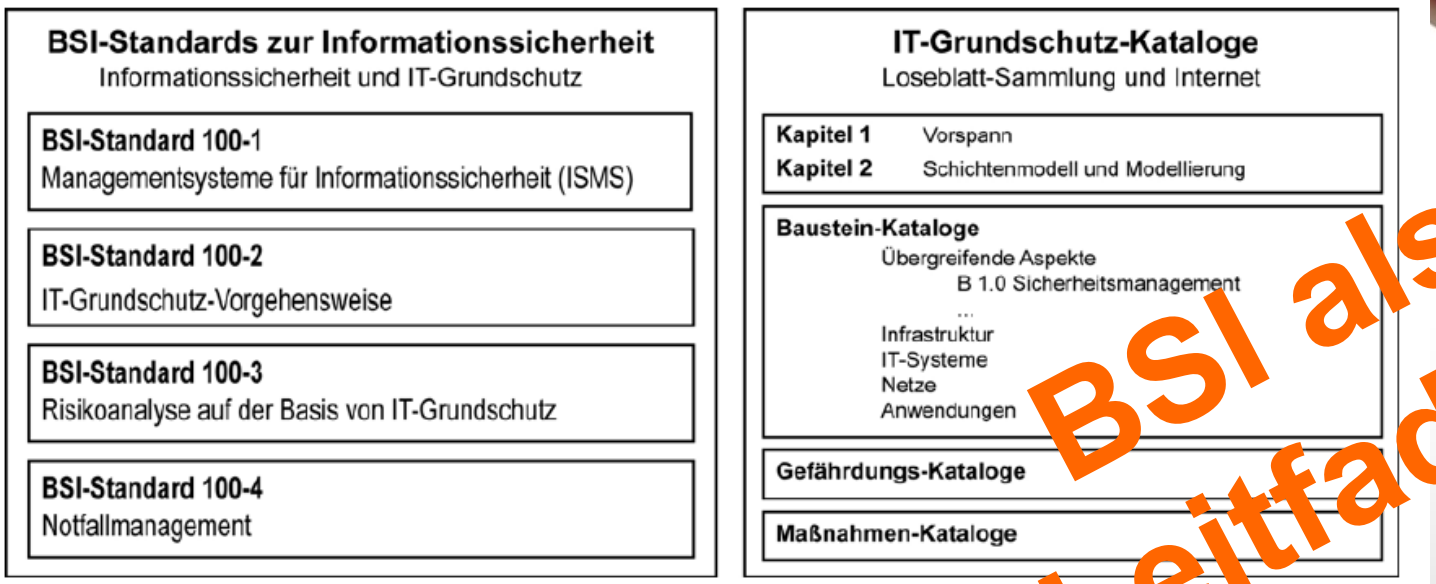


Abbildung 1: Übersicht über BSI-Publikationen zum Sicherheitsmanagement

BSI als Leitfaden

Übertragungen – technisch: Sicherheitsbereiche

- Bemerkungen / Notwendigkeiten aus Sicht RKW RLP:
  - Markt alleine kann wird die Problematik sicher nicht lösen
  - permanente Erhöhung / Verschärfung schon der grundlegenden QM-Normen hängt gerade KMU immer mehr ab
    - ISO 9001:2008 → ISO 9001:2015
    - ISO EN 13485:2012 → ISO 13485:2015
    - …
  - fehlende Akzeptanz läßt sich nicht durch Marktverhalten regulieren

- Investitionsanreize für Unternehmen?
  - Großunternehmen / Konzerne: Compliance, Außenfassade / Marketing
  - KMU:
    - Verhältnis Kosten / Nutzen sehr fragwürdig
    - wenig nutzbar, sogar oft hinderlich im operativen Betrieb
  - Krankenhäuser / kritische Infrastruktur: KEINE! Nur Druck durch Gesetze…

Übertragungen – gesellschaftlich: Einordnung

- Bemerkenswert: Udo di Fabio, ehem. BVG [phoenix, „Im Dialog“, 4.10.2015]
  - Grundgesetz fordert allgemein eine ordnungspolitische Rahmengebung durch die Politik! („vernünftige Regulierung“!)
  - Infrastruktur der Marktwirtschaft als SOZIALE Marktwirtschaft!
- Wie sieht das bei Informationssicherheit, IT oder Technologie aus?
  - Großunternehmen / Konzerne / Lobbies bestimmen weitgehend IT- und Technologiebereiche (IT, Medizin, Medizintechnik, „Social Networks“, Automotive, Industrie 4.0, …)
  - Mobile IT / Wissensabfluß wird leider noch nicht als disruptiv / problematisch wahrgenommen
  - Gestaltungsfunktion der IT für die Gesellschaft wird ansatzweise diskutiert, aber nicht als Problem / „game changer“ wahrgenommen
  - Datenabfluß wird diskutiert, KnowHow-Abfluß wenig wahrgenommen
  - Gründungen / KnowHow wird von Konzernen / Industrie früh absorbiert und Wissen verballhornt oder gar stillgelegt…
  - Ökonomische Regeln durch Finanzsystem beeinflußt, nicht durch Leistung/Produktion
  - …

Übertragungen – gesellschaftlich: Einordnung

- Stand aus Sicht KMU heute? (Meinungen)
  - Großunternehmen / Konzerne / Lobbies bestimmen immer dominanter IT- und Technologiebereiche, Oligopol-Bildung ist problematisch (Bsp. ITK-Infrastruktur, Web-Anbieter, Cloud, …)
  - es gibt wenig echte Standards, noch weniger offene Standards…
  - wenn Standards, dann oft nicht durchgesetzt, damit schwerer Marktzugang von KMU mit hohen Hürden (stattfindende Verdrängung und Oligopole)
  - auch grundlegende Standards werden mittelfristig unbezahlbar für KMU [wenig Vertreter in normativen Gremien, wenig Einflußmöglichkeiten]
  - Großkonzerne / Industrie werden als Innovationsgeber gehandelt (auch bei IT) – ist das wirklich die Realität?
  - Zukunft/Positionierung von Gründungen / KnowHow-Manifestation immer schwieriger und hype-abhängiger…
  - Konzerne sammeln KnowHow („Algorithmen“) schon bei Studenten und sogar Schülern ein („Pizza-Parties“)
  - …

Agenda und Zusammenhänge

Ein unüberschaubarer Markt:
Zertifizierungsangebote und ihre Anforderungen

- Vortragstitel und Hintergründe
  - Was will uns dieser Titel wohl sagen?
  - Standortbestimmung – ein Bild!
  - Transfer des Bildes auf Informationssicherheit und IT
- Übertragungen der Bild-„Facetten“:
  - strukturell: IT und „Sicherheit“
  - ökonomisch: Markt bzgl. Informations- / IT-Sicherheit
  - technisch: Sicherheitsbereiche
  - gesellschaftlich: Einordnung
- Ausblick
  - Ansätze und Handlungsbedarf

Ausblick – Ansätze und Handlungsbedarf

- Arbeitsansätze (exemplarisch):
  - Diskussion der Realität, nicht der Medienbilder oder der publizierten Marketing-Konzepte
  - viel mehr und intensivere öffentliche Diskussion („quo vadis“) des Struktur- und Rechtstransfers auf IT
  - bitte, bitte keine naive Technologiegläubigkeit!
  - Stärkung der Beauftragten (BfD, LfD, Firmen, …)
  - offene Standards in IT mit strikter Durchsetzung (speziell bei öffentlichen Beschaffungen und Einsatz öffentlicher Gelder!)
  - wenige grundlegende, substantiierte Standards und Zertifizierungen, kein „Markt“ von Standards und Zertifikaten
  - wenn KMU als wichtig im Land angesehen wird, dann werden Schutzfunktionen für Kleinst-/Kleinunternehmen und für den kleinen Mittelstand benötigt (hilflos gegenüber IT-Markt und Konzernen!)
  - breite Information und Sensibilisierung herstellen
  - Bildung als Wert gegenüber Technologie- und Markt-Hypes

Ausblick – Ansätze und Handlungsbedarf

- Echtes Dilemna für KMU
- Gute Orientierung: BSI und Publikationen als Richtschnur!
- Stufenweiser Zugang RKW RLP für Endkunden und KMU:
  - Breite Sensibilisierung und Information („RKW-Impulsgespräche“) in Kooperation mit weiteren Interessierten
  - wenige transparente und breit akzeptierte Grundlagen:
    - QM-Standard (ISO 9001, Prozesse)
    - danach enge Leitlinien z.B. durch BSI-Grundschutz
  - Einordnung für KMU (Tages-Check durch Generalisten, keine Spezialisten)
  - nachfolgend spezialisierte Beratungen NACH BEDARF und Zertifizierungen
  - Kooperation der Wissensträger anstatt Marktverhalten („wir machen das aber auch…“)

Kontakt

RKW Rheinland-Pfalz e. V.
Martinsstraße 17
55116 Mainz

Wir suchen jederzeit weitere interessierte Unternehmen als gemeinnützige Unterstützer und Mitstreiter!

Dr. Rolf Dahm
r.dahm@rkw-rlp.de

I www.rkw-rlp.de
T 06131 - 893 77 71
E info@rkw-rlp.de