Westfälische
Wilhelms-Universität
Münster

Über Agenten und Trittbrettfahrer: Web-Sicherheit als öffentliches Gut

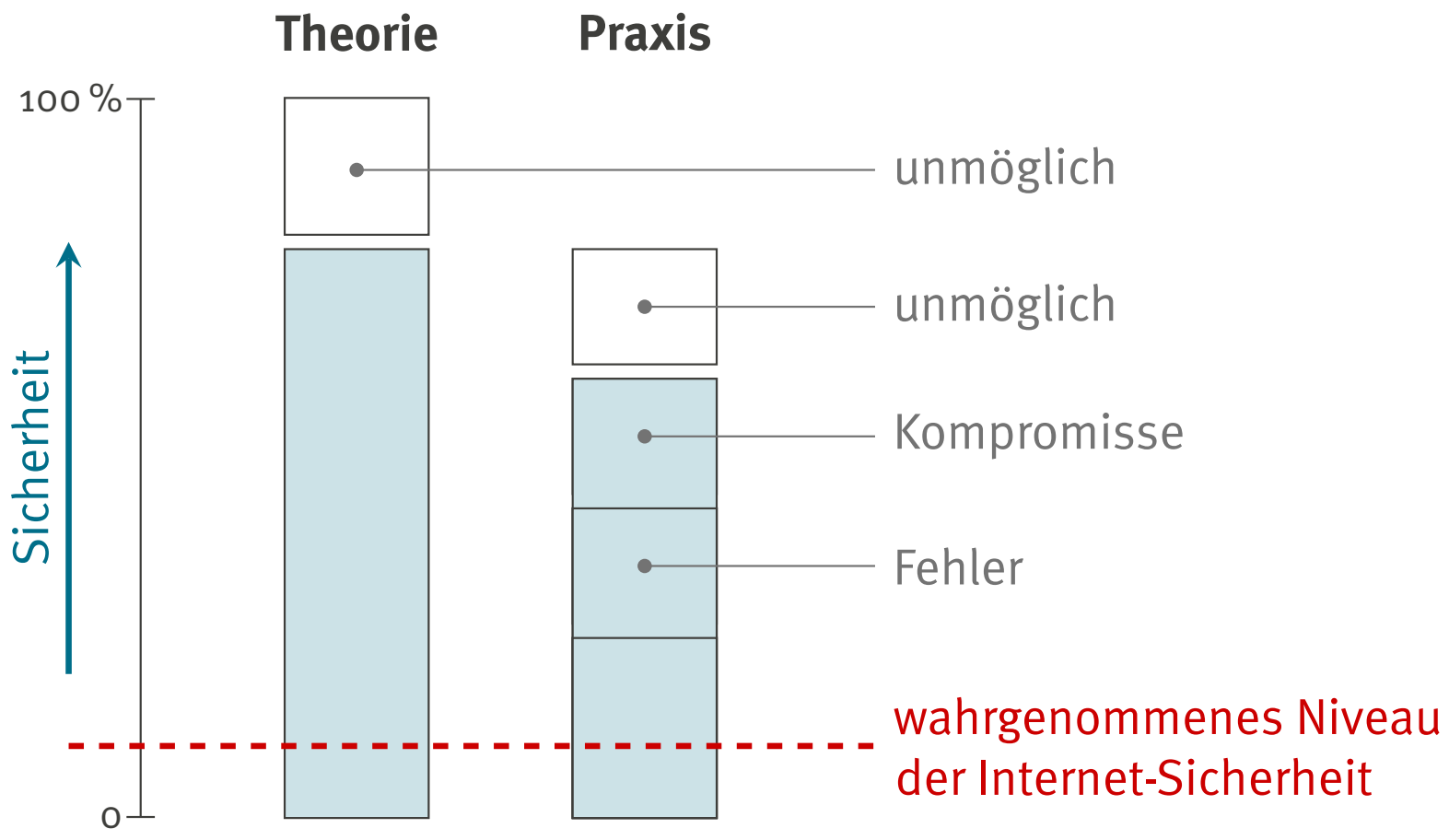
German OWASP Day 2014, Hamburg

wissen.leben
WWU Münster

Rainer Böhme

9. Dezember 2014

Status Quo

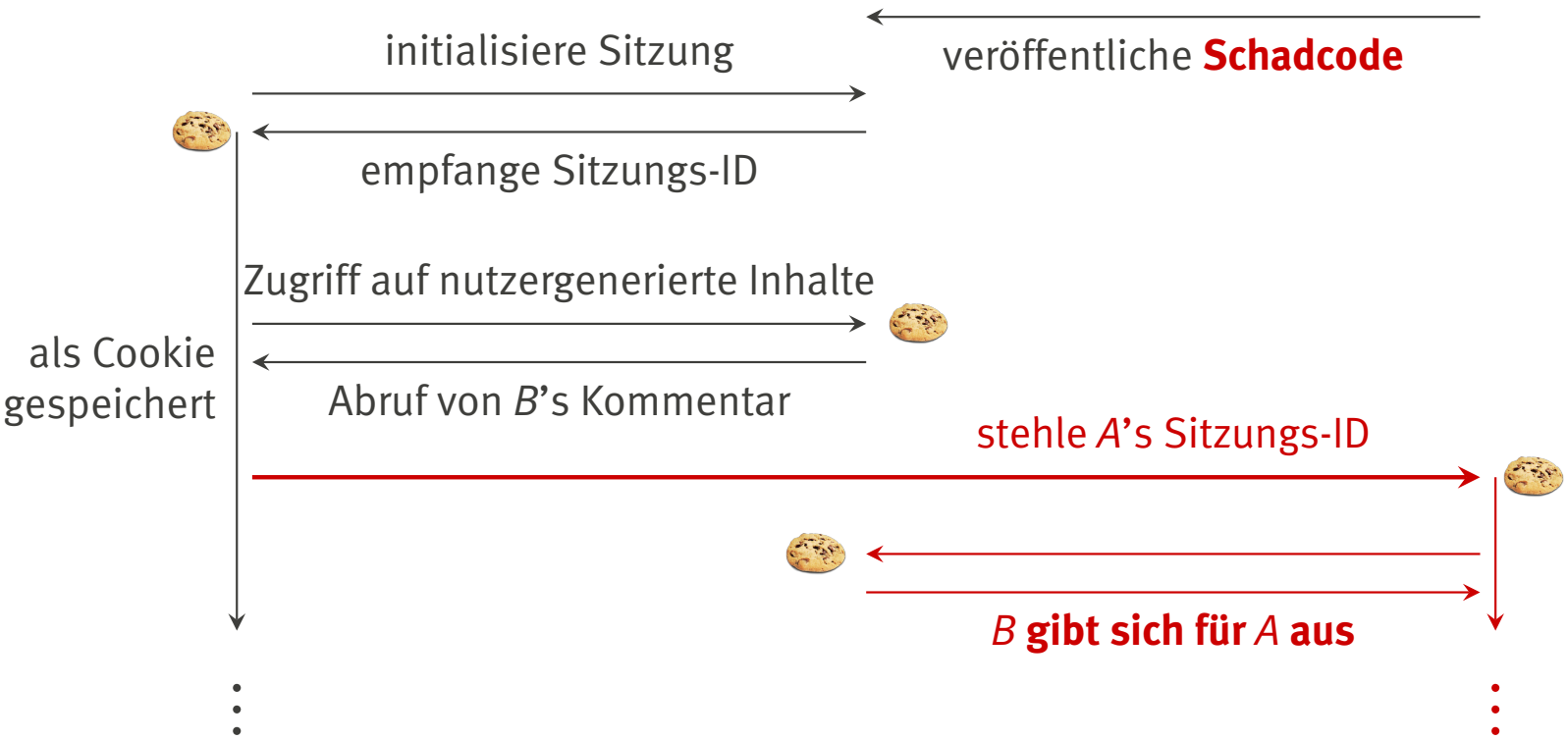


Cross-Site Scripting

Client *A*

Web-Server

Angreifer *B*



Wer ist schuld ?

- Angreifer — klar, aber wer noch ?
- Betreiber der Webseite
- Nutzer
- Microsoft
- Tim Berners-Lee
- Bundesregierung
- NSA
- Adam Smith

Kleine Unternehmenstypologie

„Sicherheitsgeber“

- IT ist strategisches Kapital
- Fokus auf Entwicklung
- Wachstumsstrategie
- Eigenschaften von Informationsgütern bestimmen Entscheidungen bzgl. Sicherheit
- Sicherheit nicht Kernkompetenz

„Sicherheitsnehmer“

- IT ist echte „Commodity“
- Fokus auf effizienter Nutzung
- Reputationen zu verlieren
- Budgetverhandlungen definieren den Spielraum des Sicherheitsmanagements
- Sicherheit nicht Kernkompetenz

Zulieferer Sicherheitsindustrie: Verkauf von Sicherheit ist Kernkompetenz.

Informationsgüter

Eigenschaften

- Grenzkosten der Reproduktion $\rightarrow$ 0
- Heterogene Präferenzen der Nachfrageseite

  Beispiel – 10 % Geschäftsleute, Budget € 1000; 90 % Heimnutzer, Budget € 50

Preisstrategie

- Versioning

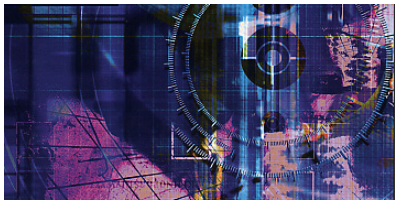
  Problem – Geschäftsleute kaufen Home-Version

Konsequenz

- Marktabgrenzung nach Sicherheitsbedürfnis

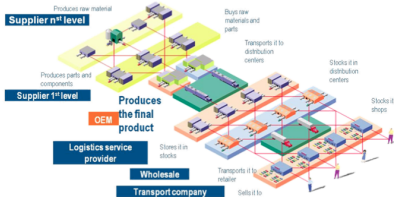
  $\rightarrow$ keine Sicherheit für Heimnutzer

Interdependente Sicherheit



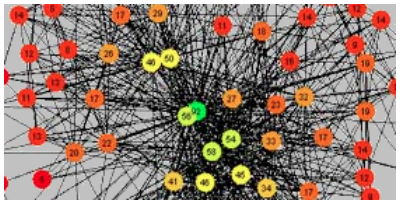
Software Engineering

Sicherheit der Anwendung hängt von der Sicherheit aller ihrer Komponenten ab.



Lieferketten

Die Sicherheit der IT-Systeme von Kunden und Zulieferern bestimmt die eigene Sicherheit.



Informationsaustausch in sozialen Netzen

Die Vertraulichkeit persönlicher Informationen hängt von der Vertrauenswürdigkeit aller Kontakte ab.

Internetsicherheit

Bot-Netze bedrohen unsere Systeme weil andere Netzteilnehmer ihre Rechner ungenügend absichern.

Prinzipien der Netzwerkökonomik

Ökonomik

- Autonome Entscheidungsträger – Agenten – maximieren ihre individuelle Zielfunktion – Nutzen.

$$u_i(a_i)$$

Externe Effekte

- Entscheidungen eines Agenten beeinflussen den Nutzen Anderer.

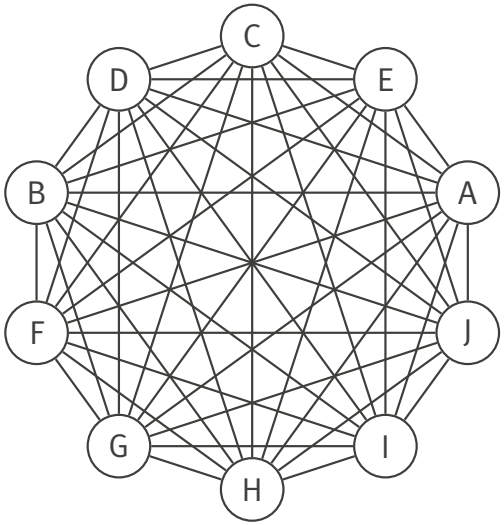
$$u_j(\ldots, a_i, \ldots)$$

Netzwerk-Externalität – Spezialfall

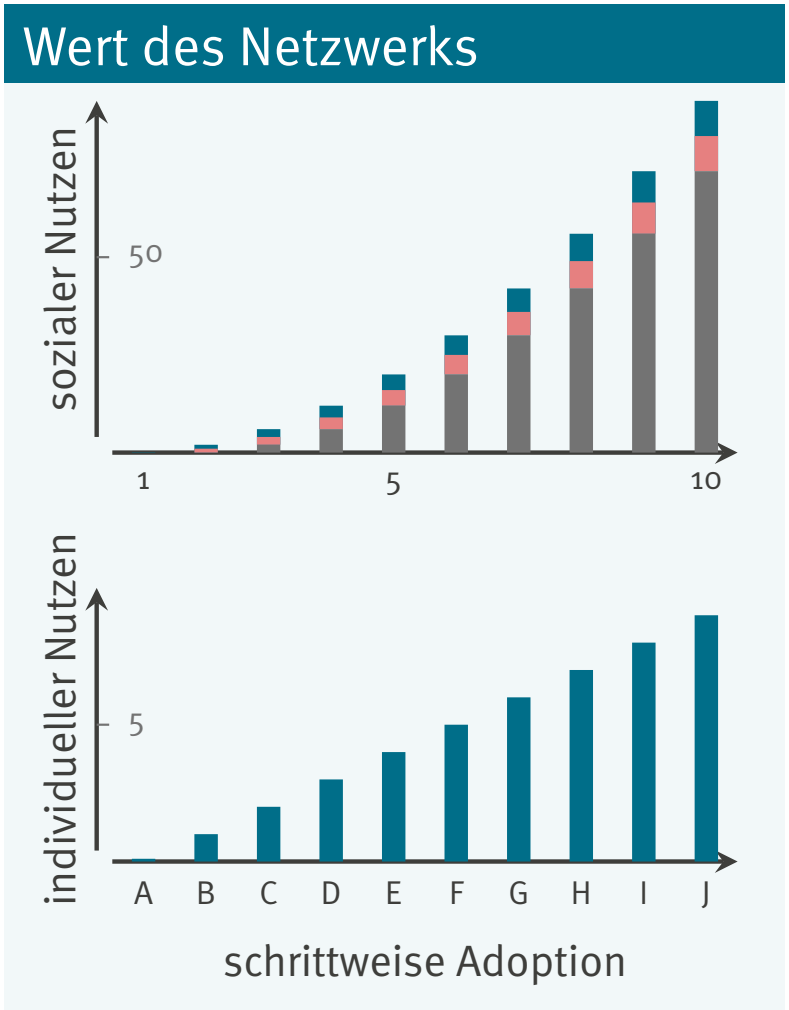
- Binäre Entscheidung: teilnehmen oder nicht teilnehmen.
  Nutzen der Teilnahme an einem Netzwerk wächst mit dem Anteil aller Agenten, die teilnehmen, $q \in [0, 1]$.

Netzwerk-Externalitäten

Verbindungen stiften Nutzen.

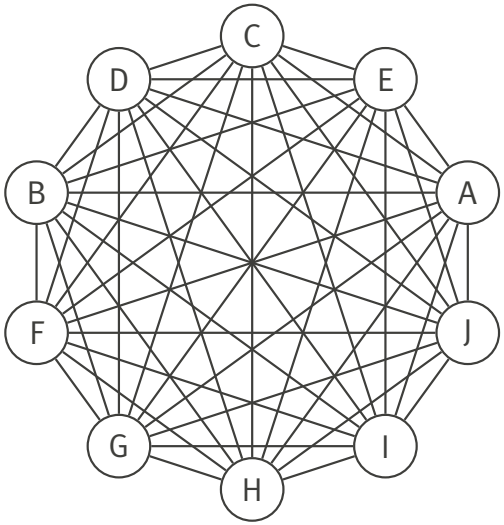


"Der Wert eines Netzwerks wächst schneller als linear in der Anzahl der Nutzer."



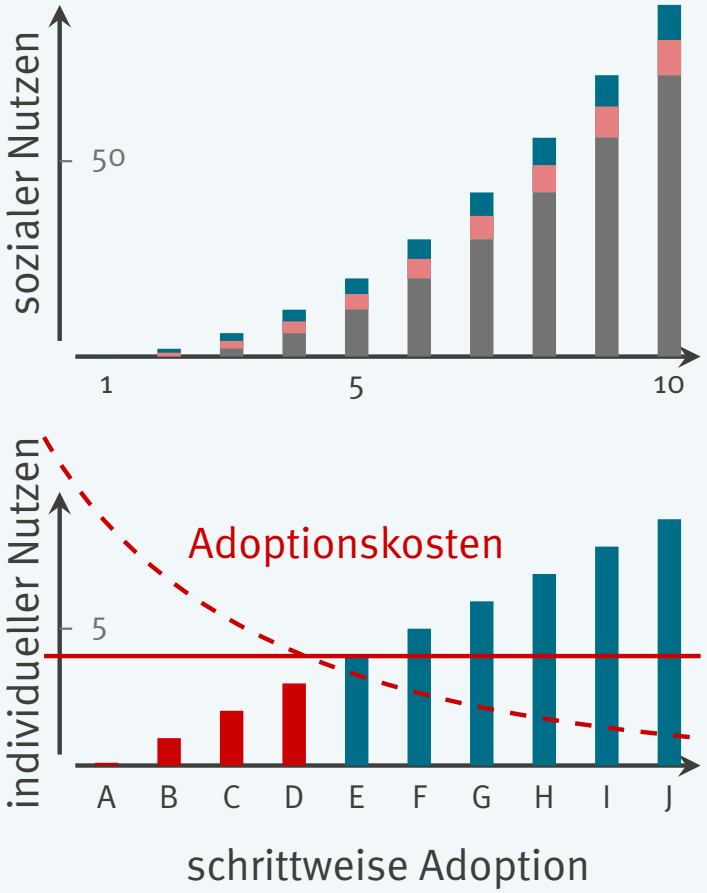
Netzwerk-Externalitäten

Verbindungen stiften Nutzen.



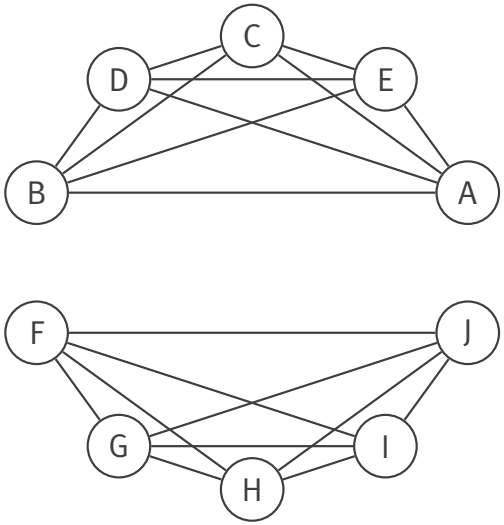
→ kritische Masse

Wert des Netzwerks



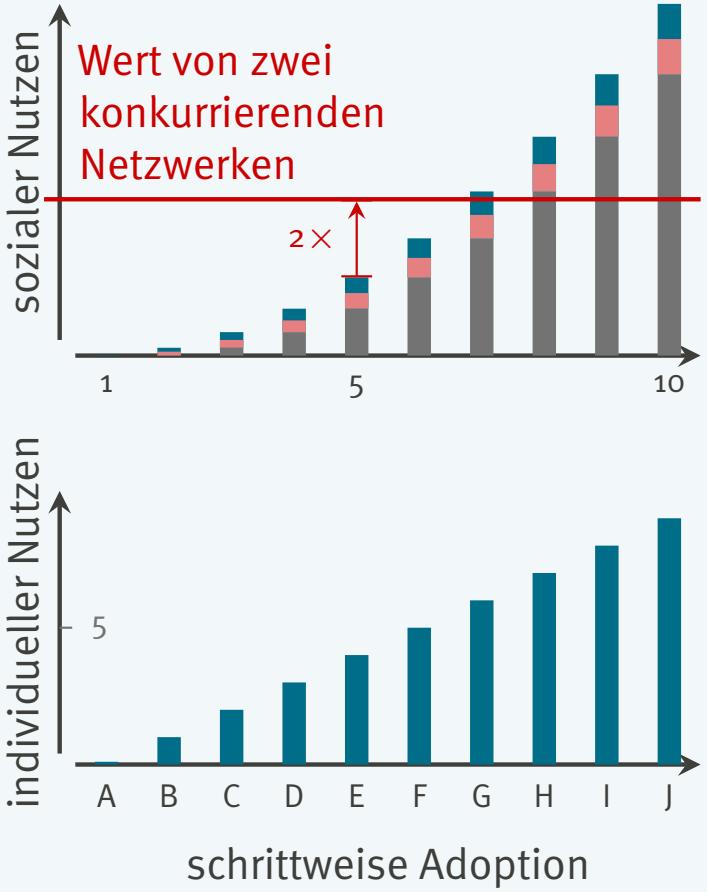
Netzwerk-Externalitäten

Verbindungen stiften Nutzen.



→ natürliches Monopol

Wert des Netzwerks



Strategien für Netzwerkmärkte

Fakten

- Markt belohnt First-Mover mit Monopolrenditen.
- Entwicklungskosten sind „versunken“.

Daumenregeln

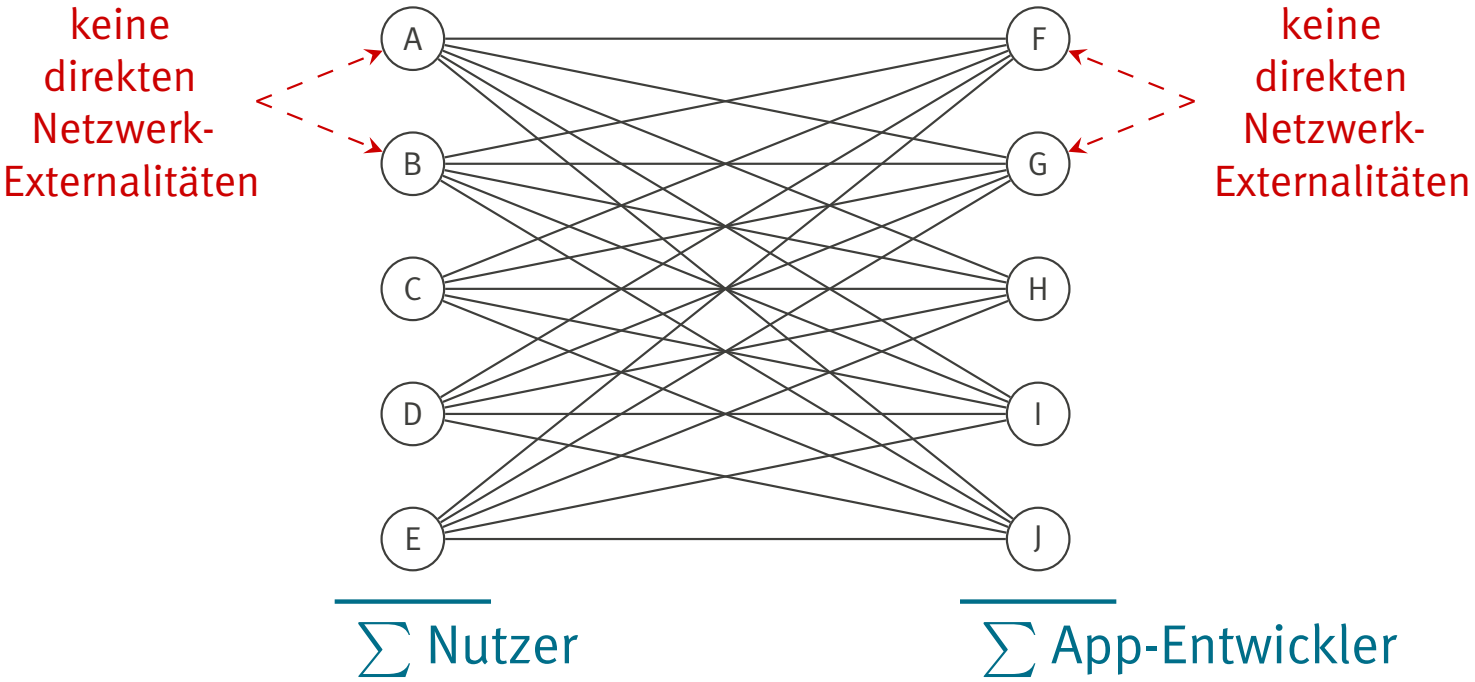
- “Ship today, fix tomorrow”
- Senke Adoptionkosten, steigere individuellen Nutzen
  $\rightarrow$ investiere in sichtbare Features und aggressives Marketing

Konsequenzen für die Sicherheit

- Kurzfristig: Sicherheit kostet Zeit und Geld – Why care ?
- Langfristig: Vorkehrungen treffen, um Sicherheit nachzurüsten – falls nach massivem Erfolg die fehlende Sicherheit zum Problem wird.

Netzwerk-Externalitäten in speziellen Topologien

Verbindungen stiften Nutzen.



Strategien für Plattform-Anbieter

Hofiere Anwendungsentwickler:

- Vermeide komplizierte Zugriffskontrolle.
  Beispiel: Alle Nutzer arbeiten immer mit Admin-Rechten.
- Erlaube Zugriff auf attraktive Ressourcen.
  Beispiele: Display – Adware; Nutzungsdaten – Profiling; Netz – “call home”
- Stelle Dev-Kits bereit, mit denen spielerisch und ohne fundierte Kenntnisse der Plattform lauffähiger Code erzeugt werden kann.

→ Die Konsequenzen für Sicherheit und Datenschutz sind offensichtlich.

Wann und wo in Sicherheit investieren ?

Drei Gründe für „echte“ Sicherheit

1. Wenn fehlende Sicherheit direkt das Geschäft bedroht.
   Beispiele: Betrugserkennung, DDoS gegen die Infrastruktur, Gefährdung von Peering-Beziehungen etc. → Sicherheit für Ihr Geschäft
2. Wenn man bekannt genug ist, so dass fehlende Sicherheit die Reputation und damit indirekt das Geschäft gefährdet.
   Insbesondere: Handeln Sie, wenn Sie sichtbar Nachholbedarf haben oder Vorfälle öffentlich bekannt wurden. → Sicherheit für Ihre Kunden
3. Sicherheit zur Unterstützung der Strategie, z. B. Kunden-Lock-In.
   Beispiel: DRM, bewusste Inkompatibilität → Sicherheit gegen Ihre Kunden

Ein Grund für “Best-Practice”-Sicherheit

- Compliance → Sicherheit, um Haftung zu reduzieren

Meldepflichten für Sicherheitsvorfälle

Erfolgsfaktoren

erfordert Veröffentlichung, im IT-SiG aber nicht vorgesehen

- technikneutrale Rechtsnorm
- echte Sicherheitsverbesserung senkt Reputationsrisiko
- Selbstschutz Betroffener

Anderson et al. 2008

Problembereiche

bestenfalls Hypothese

- Schutzwirkung eines behördlichen Lagebilds nicht erwiesen
- Fragliche Anreize
  - Über-Reporting – „Melden macht frei“
  - Unter-Reporting – Schutzbehauptung: Angriff nicht bemerkt
- Zusätzliche Kontrollen und Sanktionen nötig
- Ausweitung auf Sicherheitslücken

Laube & Böhme 2015

Fazit

„Sicherheitsgeber“

- beste Ausgangslage, um Sicherheit im Cyberspace zu schaffen;
- jedoch kaum Anreize dazu

→ zu viel Fokus auf Sicherheit riskiert den Fortbestand

„Sicherheitsnehmer“

- finden am Markt kaum geeignete Sicherheitslösungen;
- müssen massiv IT einsetzen, um wettbewerbsfähig zu bleiben;
- dabei riskieren sie ihr Geschäft und das Wohl ihrer Kunden.

→ minimiere Sicherheitsausgaben u. d. B. „compliant“ zu sein

Es wäre unfair, jemandem die Schuld zuzuschreiben. Unsicherheit wird uns erhalten bleiben, bis die ökonomischen Ursachen behoben sind.

→ Smart Grids, Autos, Medizin, . . .

immer mehr Sektoren werden wie die IT-Industrie.

Sichere Festtage

Kontakt

Prof. Dr.-Ing. Rainer Böhme

Westfälische Wilhelms-Universität Münster
Institut für Wirtschaftsinformatik
Juniorprofessur für Wirtschaftsinformatik, insb. IT-Sicherheit

Leonardo-Campus 3
48149 Münster

Tel. +49 251 83 38230
Fax +49 251 83 38259

E-Mail rainer.boehme@uni-muenster.de

[In eigener Sache]

2015

JANUARY 20TH

ECONOMICS OF CYBERSECURITY

Online Professional Education

Aim

Identify, measure and understand the economic factors that shape the information security decisions of today's companies.

Team

- *Delft University Technology*: Michel van Eeten, Carlos Gañán
- *Southern Methodist University:* Tyler Moore
- *University of Cambridge:* Ross Anderson
- *University of Münster:* Rainer Böhme

When and Where

The course starts on 20th of January 2015 and lasts four weeks. It will take place in the edX platform.