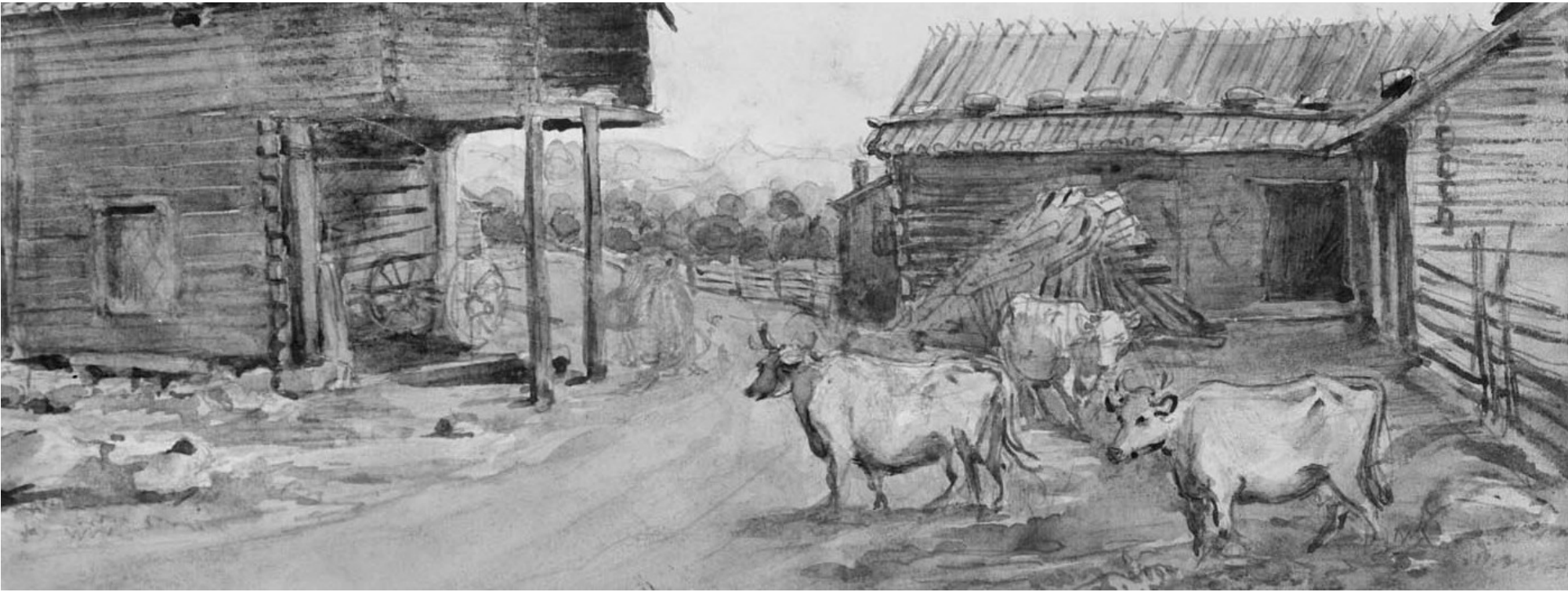
Neue Herausforderungen für die GRC-Organisation durch offenere Unternehmensgrenzen – Langversion

Seminar „Governance, Risk & Compliance“

Moritz Klammler 27. Juni 2014
Karlsruher Institut für Technologie (KIT)



Copyright © 2014 Moritz Klammler

Dieses Werk ist lizenziert unter einer Creative Commons *Namensnennung – Weitergabe unter gleichen Bedingungen 4.0 International* Lizenz.

`https://creativecommons.org/licenses/by-sa/4.0/deed.de`

Dieses Dokument enthält Teile einer gemeinfreien Zeichnung von Fritz von Dardel (1817–1901), sowie Grafiken aus dem *Tango Desktop Project* (`http://tango.freedesktop.org/`), deren Verwendung die Autoren jedermann ohne Auflagen gestatten.

Dieses Dokument und der zugehörige Aufsatz sind zusammen mit dem Quellcode über die Webseite des Autors verfügbar.

`http://klammler.eu/data/jura/kit/grc/`

Gliederung

(1) Fragestellungen

   (a) Datensicherheit und Datenschutz

   (b) Verlässlichkeit von IT-Systemen

   (c) Verantwortung und Haftung

(2) Herausforderungen

   (a) Neue Kommunikationsformen

   (b) Soziale Online-Netzwerke

   (c) Ubiquitäres Rechnen

   (d) Externe IT-Dienstleistungen und verteiltes Rechnen

(3) Fazit

Fragestellungen

(a) Datensicherheit und Datenschutz

(i) Kann ich auf meine unternehmensrelevanten Daten sicher zugreifen?

(ii) Können Unbefugte auf meine unternehmensrelevanten Daten zugreifen?

(iii) Kann ich auf fremde Daten (zB meiner Kunden) zugreifen, auf die ich nicht zugreifen können sollte?

(b) Verlässlichkeit von IT-Systemen

(c) Verantwortung und Haftung

Fragestellungen

(a) Datensicherheit und Datenschutz

(b) Verlässlichkeit von IT-Systemen

- (i) Was machen meine IT-Systeme?
- (ii) Wer kontrolliert meine IT-Systeme?
- (iii) Werden meine IT-Systeme auch in Zukunft liefern, was mein Unternehmen braucht?

(c) Verantwortung und Haftung

Fragestellungen

(a) Datensicherheit und Datenschutz

(b) Verlässlichkeit von IT-Systemen

(c) Verantwortung und Haftung

(i) Was darf mein Unternehmen?

(ii) Wofür ist mein Unternehmen verantwortlich?

(iii) Wie kann mein Unternehmen dieser Verantwortung gerecht werden?

Motivationsbeispiel

BONUS

I found that the company I work for is putting a backdoor into mobile phones

I have found out recently that the remote assistant software that we put in a smartphone we sell can be activated by us without user approval.

We are not using this option, and it is probably there by mistake. But the people who are responsible for this system don't see it as a big deal. Because “We are not going to use it”…

Am I wrong for going ballistic over it?

What would you do about it if it was your workplace?

(1) Diskussion auf StackExchange aus dem Jahr 2012: https://security.stackexchange.com/questions/15076/i-found-that-the-company-i-work-for-is-putting-a-backdoor-into-mobile-phones.

Herausforderungen

BONUS

(a) **Neue Kommunikationsformen**

(b) Soziale Online-Netzwerke

(c) Ubiquitäres Rechnen

(d) Externe IT-Dienstleistungen und verteiltes Rechnen

Analoge Kommunikation

BONUS

- Telefon, Fax, ...
- früher: Staatsmonopole / heute: (teil-)privatisiert
- Vertraulichkeit
  - vor *staatlicher* Willkür geschützt (Art 10 GG)
  - weitere Regelungen im TKG
  - Schutz nur durch Vertrauen
  - Überwachung technisch jederzeit möglich und teilweise auch vorgesehen (zB § 100a StPO)

Digitale Kommunikationsformen der ersten Generation

BONUS

- E-Mail, IRC, ...
- offene Standards für Protokolle (RFC)
- Verwendung vorhandener freier Software oder eigene Implementierung
- Unternehmen hat technische Kontrolle über IT-Infrastruktur
- Anfangs kein Wert auf Vertraulichkeit / Authentizität gelegt

Aktuelle Trends

BONUS

- ICQ, Skype, WhatsApp, ...
- **proprietäre Protokolle**

  → Anwendungen inkompatibel, Abhängigkeit von einem Anbieter
- **nicht einsehbarer Quellcode**

  → keine Kontrolle auf Sickerheitslücken / Hintertüren
- **Lizenzverträge**

  → häufig weitreichende Einschränkung der Benutzerrechte

Skype

BONUS

- extremer Anti-Reverse-Engineering-Aufwand[1]
- Skype (Microsoft) kann sich (oder Dritten) Zugriff auf sämtliche Kommunikationsinhalte verschaffen[1]
- gilt als robust gegenüber Angriffen Dritter[2] (insbesondere durch die Strafverfolgung[3])

(1) *Biondi/Desclaux*, „Silver Needle in the Skype“. In: *BlackHat Europe*. EADS Corporate Research Center. März 2006. URL: https://www.secdev.org/conf/skype_BHEU06.handout.pdf (besucht am 06. 06. 2014).
(2) *Zhu/Fu*, „Traffic analysis attacks on Skype VoIP calls“. In: *Computer Communications* 34.10 (2011), 1202–1212. DOI: http://dx.doi.org/10.1016/j.comcom.2010.12.007.
(3) Aussage von Dr Helmut Kreicker, GBA beim BGH, vom 17. Dezember 2013.

ICQ-Lizenzvereinbarung I

BONUS

Während alle Rechte, Besitzrechte und Beteiligungen an den an ICQ gesandten oder auf den ICQ Services geposteten Informationen, Dokumenten, Inhalten, Bildern, Fotos oder sonstigen Materialien („Materialien“) bei Ihnen verbleiben, **gewähren Sie durch das Versenden oder Posten** solcher Materialien **ICQ**, seinen Konzerngesellschaften, Tochterunternehmen, Bevollmächtigten, Lizenznehmern und Rechtsvertretern hiermit **eine unwiderrufliche, dauerhafte, weltweite Lizenz** zur Nutzung, Reproduktion, Bearbeitung, Vermarktung, Speicherung, Verteilung, Verteilung durch Dritte, öffentlichen und privaten Anzeige, Kommunikation, öffentlichen und privaten Aufführung, übertragung, übertragung durch Dritte, Erstellung abgeleiteter Werke auf der Grundlage der Materialien und zur Werbung für die Materialien (unter Umständen in einer von ICQ nach Belieben bearbeiteten und geänderten Fassung) über die ICQ Services und andere Produkte und Dienstleistungen zu redaktionellen, gewerblichen, werbebezogenen oder sonstigen Zwecken, die ICQ in einem beliebigen, bereits bekannten oder zukünftig erfundenen Medium bestimmen kann.

(1) *ICQ*, „ICQ-Lizenzvereinbarung“. Nov. 2011. URL: https://www.icq.com/legal/eula/de (besucht am 06. 06. 2014).

ICQ-Lizenzvereinbarung II

BONUS

Anfechtungsmöglichkeiten

- Inhaltskontrolle (§ 307 BGB)?

  (−) Anwendbarkeit (kein Verbrauchergeschäft)

  (+) materielle Tatbestandsvoraussetzungen

- Sittenwidrigkeit / Wucher (§ 138 BGB)?

  (+) Anwendbarkeit

  (?) materielle Tatbestandsvoraussetzungen

Alternativen

BONUS

- offene Standards für Protokolle: XMPP („Jabber“), …
- konkurrierende Implementierungen (auch) in freier Software: Pidgin, Empathy, Jitsi, …
- keine Bindung an Anbieter / Lizenzverträge
- Unternehmen kann eigene Infrastruktur einrichten
- Unternehmen kann Quellcode analysieren und adaptieren (lassen)

Herausforderungen

(a) Neue Kommunikationsformen

(b) Soziale Online-Netzwerke

(c) Ubiquitäres Rechnen

(d) Externe IT-Dienstleistungen und verteiltes Rechnen

Soziale Online-Netzwerke

(i) Nutzung zur Mitarbeiterakquise

(ii) Nutzung zum Kundenkontakt

(iii) Private Nutzung durch Mitarbeiter

(iv) Einbindungen auf die Unternehmens-Webseite

Nutzung zur Mitarbeiterakquise

Rechtsnorm

(±) § 28 BDSG – Datenerhebung und -speicherung für eigene Geschäftszwecke

(±) § 32 BDSG – Datenerhebung, -verarbeitung und -nutzung für Zwecke des Beschäftigungsverhältnisses

Zulässigkeit

(+) allgemein zugängliche Quelle

(+) kein berechtigtes Interesse des Arbeitnehmers entgegenstehend

Haltung der Betreiber

(−) StudiVZ[2]

(+) XING

(?) Facebook

(1) *Ernst*, „Social Networks und Arbeitnehmer-Datenschutz“. In: *NJOZ* 23 (2011), 953.

(2) *StudiVZ*, „StudiVZ Allgemeine Geschäftsbedingungen (Version 2.0)“. Dez. 2007. URL: http://www.studivz.net/l/terms/ (besucht am 10. 06. 2014).

StudiVZ-AGB

BONUS

Die Nutzung des StudiVZ-Netzwerkes und seiner Anwendungen darf ausschließlich zu privaten Zwecken erfolgen. Nutzer dürfen daher die Kontaktdaten anderer Nutzer, die über das StudiVZ-Netzwerk zugänglich sind, für keine anderen Zwecke nutzen, als für die eigene private Kommunikation. **Nicht gestattet ist** deshalb z.B. **die Verwendung der Daten eines Nutzers zum Zwecke der Personaldatenerhebung durch Arbeitgeber**, Ausbildungsbetriebe, Personal- bzw. Arbeitsvermittler, Universitäten, Fachhochschulen oder durch vergleichbare öffentliche oder private Bildungseinrichtungen.

(1) *StudiVZ*, „StudiVZ Allgemeine Geschäftsbedingungen (Version 2.0)“. Dez. 2007. URL: http://www.studivz.net/l/terms/ (besucht am 10. 06. 2014).

Nutzung zum Kundenkontakt

- Starke Abhängigkeit von Betreiber bei zentralistischen Netzwerken
  Alternativen: zB Diaspora* (`https://joindiaspora.com/`)
- Mit welchem Account?

Unternehmensprofil

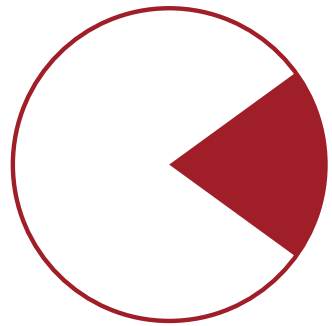
eigenes Business-Profil des Mitarbeiters

privates Profil des Mitarbeiters

Private Nutzung durch Mitarbeiter

- Treuepflicht (§ 241 BGB)
- Verrat von Geschäftsgeheimnissen

Jährlicher Schaden für die deutsche Wirtschaft durch Industriespionage: 2.8 G€



Anteil durch Informationsabfluss durch die eigenen Mitarbeiter: 20 % ≈ 560 M€

- Unternehmen haftet für Urheberrechtsverstöße mit (§ 99 UrhG)
- Verschwendung von Arbeitszeit?

(1) *Weßelmann/Wiele*, „Security Awareness: Der Mensch als Sicherheitsrisiko“. In: *Admin* 3 (2010), 80–83. URL: https://www.admin-magazin.de/Das-Heft/2010/03/Security-Awareness-Der-Mensch-als-Sicherheitsrisiko/ (besucht am 10. 06. 2014).

Einbindungen auf die Unternehmens-Webseite

- zB „Like-Button“ von Facebook
- Plugin; lädt und führt externen Code aus; sendet Daten an die Server des Betreibers
- Betreiber erfährt von *jedem* Besucher:[1]
  - URL
  - IP-Adresse
  - Zeitpunkt des Aufrufs
  - Browser-Signatur (quasi eindeutig[2])
  - Cookie (falls gesetzt) $\mapsto$ User-Account (falls vorhanden)

(1) *Roosendaal*, „Facebook tracks and traces everyone: Like this!“ Tilburg Institute for Law, Technology, und Society, 2011. URL: http://ssrn.com/abstract=1717563 (besucht am 10. 06. 2014).
(2) *EFF*, „Panopticlick“. Electronic Frontier Foundation. 2010. URL: https://panopticlick.eff.org/ (besucht am 10. 06. 2014).

Einschlägige Rechtsnorm

(−) TKG (reiner Datentransport)

(±) TMG (Interaktion zwischen Nutzer und Anbieter)

(+) BDSG (Teledienst lediglich Übertragungsmedium für andere Leistungen)

Verantwortlich für die Verarbeitung

(+) Anbieter des Plugins (Netzwerk-Betreiber)

(+) Verwender des Plugins (Webseiten-Betreiber)

Facebook

Keine Informationen, was mit den Daten geschieht → in aktueller Form rechtswidrig

(1) *Ernst*, „Social Plugins: Der „Like-Button“ als datenschutzrechtliches Problem“. In: *NJOZ* 36 (2010), 1917–1958.

Herausforderungen

(a) Neue Kommunikationsformen

(b) Soziale Online-Netzwerke

(c) Ubiquitäres Rechnen

(d) Externe IT-Dienstleistungen und verteiltes Rechnen

Persönliche mobile Endgeräte

- hohe Rechenleistung und viel Spezial-Hardware

  (Mobilfunk-Modem, Mikrofon, Kamera, GPS-Empfänger, Beschleunigungssensor, ...)

- Statussymbol für Mitarbeiter
- „bring your own device“ (BYOD)
- häufig schlechte Software-Qualität[1,2]
- wenig Kontrolle durch IT-Abteilung

(1) *IBM*, „Mid-year Trend and Risk Report“. IBM X-Force, Sep. 2012. URL: https://www14.software.ibm.com/webapp/iwm/web/signup.do?source=swg-Tivoli_Organic&S_PKG=ov7304&lang=de_DE (besucht am 07. 06. 2014).

(2) *Fahl*, „Ergebnisse eines Android-Sicherheitschecks erschrecken“. In: *Admin* 11 (2013), 110–113. URL: https://www.admin-magazin.de/Das-Heft/2013/11/Ergebnisse-eines-Android-Sicherheitschecks-erschrecken/ (besucht am 10. 06. 2014).

BYOD – Gefahren

Externe Angriffe

- „Leaken“ von sensiblen Daten über „Apps“
- direkte Angriffe auf das Gerät / Daten
- Spionage (zB via Mikrofon & Kamera)
- Einfallstor für weitere Angriffe[1]

Interner Missbrauch

- Mitarbeiterüberwachung

(1) *Genkin/Shamir/Tromer, RSA Key Extraction via Low-Bandwidth Acoustic Cryptanalysis.* Dez. 2013. URL: https://www.cs.tau.ac.il/~tromer/acoustic/ (besucht am 10. 06. 2014).

BYOD – Betriebsvereinbarung

BONUS

I Welche Geräte sind zugelassen?

II Welche Software darf / muss auf dem Gerät installiert werden?

III Welche Maßnahmen soll der Besitzer ergreifen, um das System sicher und aktuell zu halten?

IV Welche beruflichen Tätigkeiten dürfen auf dem Gerät verrichtet werden?

V Welche privaten Tätigkeiten sind zu unterlassen?

VI Welche Unternehmensdaten dürfen auf dem Gerät gespeichert werden?

VII Wie ist das Gerät gegen unbefugten Zugriff zu schützen?

VIII Was soll der Besitzer beachten, wenn er das Gerät vorübergehend Dritten zur Verwendung überlässt oder sich seiner dauerhaft entledigen möchte?

IX Wie ist im Fall eines verlorenen oder gestohlenen Geräts zu verfahren?

X Welche Rechte werden der IT-Abteilung eingeräumt, auf das private Gerät zuzugreifen?

Vernetzte intelligente Mess-, Steuer- und Regelungssysteme

Zwei Szenarien:

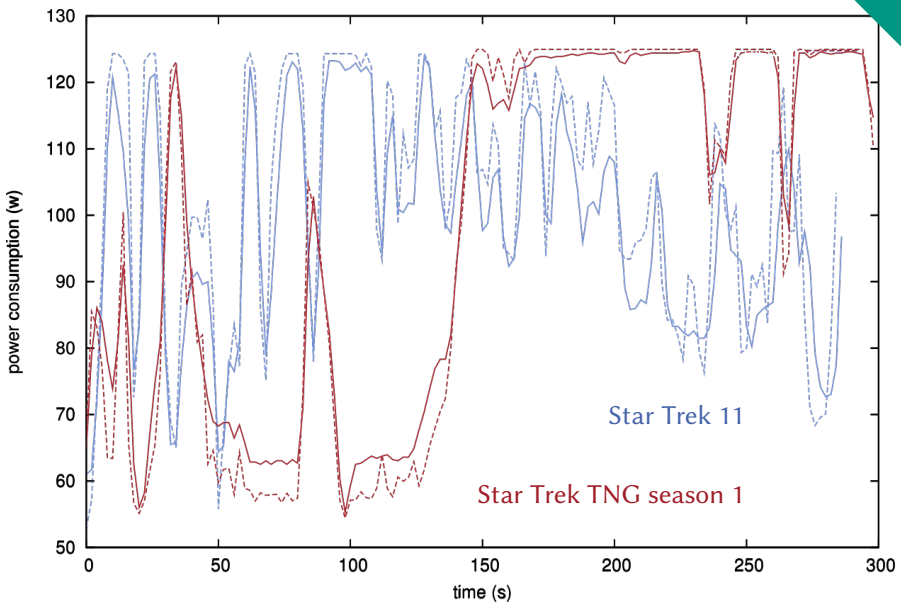
(i) Unternehmen nutzt Technik für sich selbst

(ii) Unternehmen entwickelt / vertreibt Technik als Geschäftszweck

Fallbeispiel: Smart-Meter

BONUS

- hochauflösende Stromverbrauchsmesung
- Sampling-Rate: 0.5 s
- Datenübertragung in Echtzeit
  - unverschlüsselt
  - unsigniert



- massive Erhebung personenbezogener Daten aus dem Kernbereich persönlicher Lebensgestaltung
- Daten sind weder gegen unbefugten Zugriff, noch vor Manipulation (Betrug) geschützt

(1) *Greveler*, „Multimedia Content Identification Through Smart Meter Power Usage Profiles“. Ruhr-Universität Bochum, 2012. URL: https://www.nds.rub.de/research/publications/SmartmeterContentIdent/ (besucht am 10. 06. 2014).

Herausforderungen

(a) Neue Kommunikationsformen

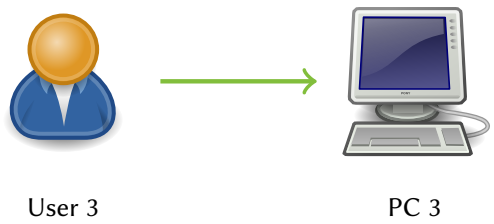
(b) Soziale Online-Netzwerke

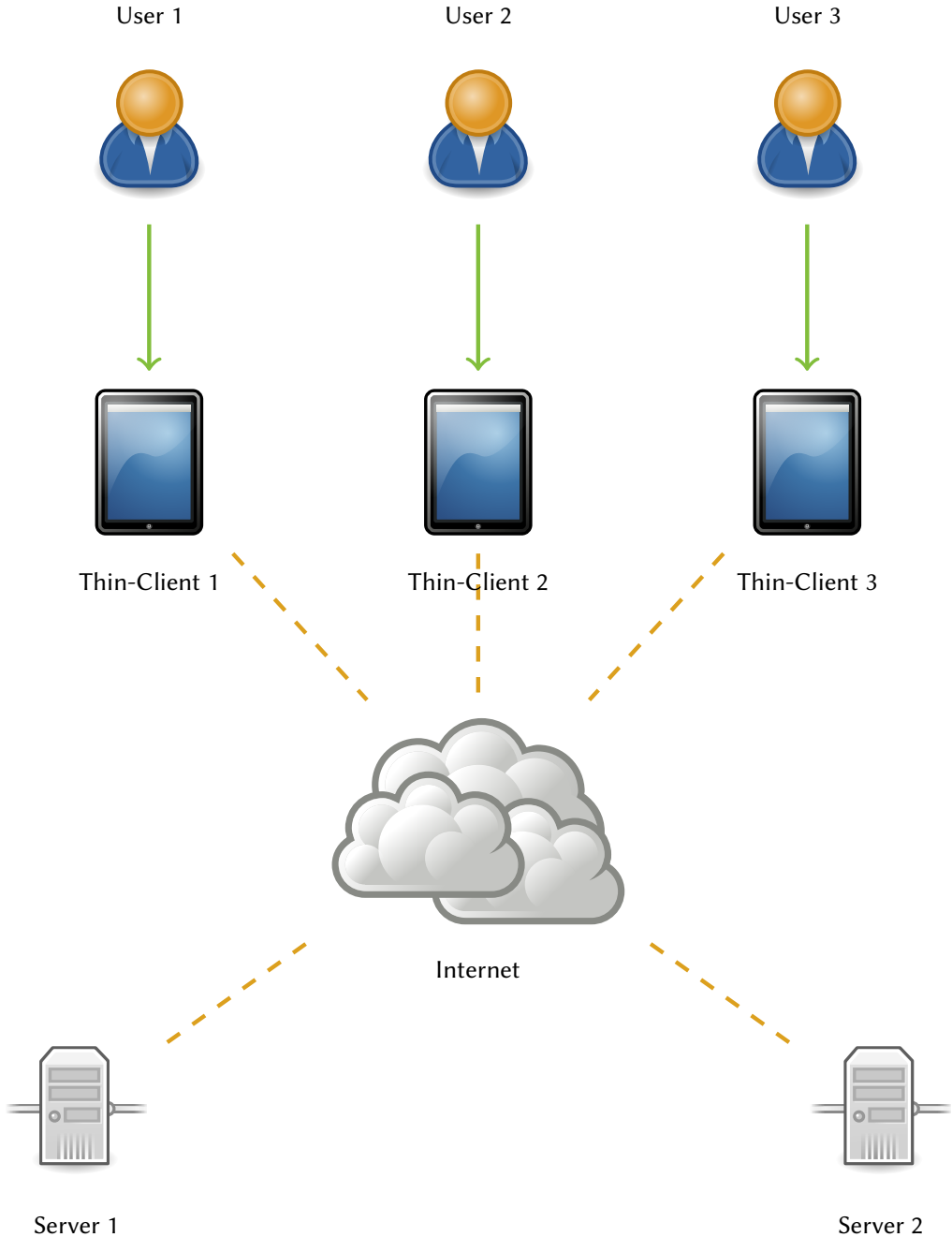
(c) Ubiquitäres Rechnen

(d) Externe IT-Dienstleistungen und verteiltes Rechnen

User 1
PC 1

User 2
PC 2


User 3
PC 3


User 1
User 2
User 3
Thin-Client 1
Thin-Client 2
Thin-Client 3
Internet
Server 1
Server 2

Software as a Service (SaaS)

Anbieter

- ▲ weniger Code zu portieren
- ▲ klar definierter Leistungsumfang („Service“)
- ▲ Urheberrechtsverletzungen „unmöglich“
- ▼ Kosten für Rechenzentrum

Nutzer

- ▲ einfach zu installieren / warten
- ▲ wenig Anforderungen an Rechenleistung
- ▼ keinerlei Kontrolle über die Software
- ▼ permanente Abhängigkeit vom Anbieter (Wechselmöglichkeit?)
- ▼ Anbieter erhält sämtliche Geschäftsdaten

(1) *Stallman*, „What Does That Server Really Serve?“ In: *Boston Review* (März 2010). URL: http://www.bostonreview.net/richard-stallman-free-software-DRM/ (besucht am 10. 06. 2014).

Fazit

- Grenzen zwischen Berufs- und Privatleben verschwimmen
- fast alle Geschäfts- und Lebensbereiche von IT durchdrungen
- IT-Benutzung durch Spezialisten und Laien
- großes Schadenspotential / schwerwiegende Compliance-Verstöße durch unbeholfene Nutzung neuer Technologien
- Risikobewusstsein bei allen Mitarbeitern schaffen
- nicht jeden Trend ungefragt adaptieren

Fritz von Dardel (1817–1901)