UpTimes

Mitgliederzeitschrift der
German Unix User Group

Security als Realpolitik

Backstage beim DANE-RFC

Fachartikel schreiben

guug

2015-2

Inhaltsverzeichnis

Da seid Ihr ja wieder!
Gruß aus der Redaktion

Was gibt's Neues? Wie man eine Redaktionskonferenz auf eine Mailingliste abbildet, zum Beispiel. Die *UpTimes* ist diesmal anders entstanden als die Ausgaben zuvor: Mauerschau auf ein kleines Experiment.

von **Anika Kehrer**

Nur ein Narr
macht keine Experimente.

Charles Darwin

Was Ihr in den Händen haltet, ist ja die Vereinszeitschrift des *German Unix User Group* e.V. Zu ihrem Konzept gehört, für Mitglieder von Mitgliedern gemacht zu sein – darüber hinaus selbstverständlich auch für andere Leser und von anderen Interessierten. Im Jahr 2012 entstand die UpTimes in etwas umgemodelter Form neu [1], und seitdem kümmert sich wieder ein kleines Redaktionsteam via Mailingliste ehrenamtlich um ihre Entstehung, wieder unterstützt von einer beauftragten Chefredaktion, die die Fäden zusammenhält. Vor einem Jahr berichtete die *UpTimes* von ihrem ersten Redaktionstreffen [2].

Ziel ist aber nicht nur, ein tolles Heft zu machen. Publizieren bringt allerlei mit sich (was übrigens in diesem Heft Mathias Weidner in dem Artikel *Fachartikel schreiben* reflektiert), und der eine oder andere interessiert sich dafür – natürlich auch innerhalb der UpTimes-Redaktion. Das Ganze soll also vor allem Spaß machen.

Nun hat aber sicher jeder schon die Erfahrung gemacht, dass konkrete praktische Zusammenarbeit alles andere als trivial ist. Vor allem in Freiwilligen-Communities herrschen erschwerte Bedingungen: Prioritäten, Zeitressourcen und Professionen verteilen sich stark heterogen. Zusammenarbeit kostet oft nicht nur Zeit, sondern auch Nerven. Einfach ist: Einer macht, andere eumeln hinterher. Schöner aber ist: Zusammenarbeit ausprobieren.

Bei der UpTimes sind die Layout-Prozesse stabil und funktionieren gut. Die Überlegung war, wie man den Redaktionsprozess eines verteilten Teams partizipativ gestalten kann, ohne dass die Effizienz nennenswert leidet – also ohne dass der zwangsläufige Overhead das Ergebnis riskiert, nämlich, dass eine Ausgabe Wochen später als geplant oder gar nicht erscheint. Als maßgeblichen Faktor für Risiko identifiziert der Artikel *IT-Sicherheit als Realpolitik* von Dan Geer in diesem Heft „Abhängigkeit". Das trifft hier ebenfalls zu: Wenn mehrere zusammenarbeiten, bewirkt das Abhängigkeit voneinander, unter der das Ergebnis manchmal leidet. Nichts anderes reflektiert der Spruch *Viele Köche verderben den Brei*.

Nix da. Das will ja keiner. Wie also vorgehen, um das Risiko zu minimieren – und zwar möglichst nicht zu Lasten der Partizipationsmöglichkeit? Da den Kern einer Publikation ihre Inhalte bilden, sollten diese auch im Zentrum des Zusammenarbeits-Experiments stehen. Das Mittel war eine *Redaktionskonferenz*. Der Weg war die *Mailingliste*. Bekanntlich erkranken Mailthreads schnell an einem Phänomen, das das Wort „Zerfaserung" gut beschreibt: Nebenthemen poppen auf, das Ursprungsthema gerät aus den Augen, Ergebnisse gehen unter. Ebenfalls wirkt sich erfahrungsgemäß bisweilen nachteilig aus, wenn zu viele Menschen sich beteiligen sollen. Das tritt auch jenseits von Mailinglisten auf. Manche nennen das „CC-Gerödel". :-)

Eingedenk all dessen sah der Versuchsaufbau für das Experiment *Redaktionskonferenz via Mailingliste* also folgendermaßen aus: Auf der Redaktions-Mailingliste gibt es genau einen Thread, der zur Sammlung von Artikelideen dient. Dieser Thread ist kein Diskussions-Thread, sondern listet Thema, kurze Beschreibung und optional zu klärende Fragen sowie konkrete Wünsche für Mithilfe. Die Mithilfe muss fakultativ sein – derjenige, der den Artikel vorschlägt, ist in jedem Fall derjenige, der ihn weiterverfolgt, und zwar gegebenenfalls auch allein.

Wer Input, Feedback oder Mitarbeitsangebote für eine der Artikelideen hat, startet einen neuen Thread, deren Betreffzeile so lautet, wie die Artikelidee im Sammel-Thread. Im Extremfall erhält jedes Artikelprojekt einen Thread. In

diesen Einzelartikel-Threads erfolgen Diskussion, Klärungsbedarf und Kooperationen unter Redakteuren. Empfänger ist hier nicht mehr die große Redaktions-Mailingliste, sondern nur die *Textredakteure* – also diejenigen, die konkret für die redaktionelle Arbeit an diesem Artikel interessieren (gegebenenfalls auch ein Autor). Das Vorgehen baut auf strenge Kommunikationsregeln, auf die sich die Betroffenen per Telefonkonferenz [3] einigten. Ziel war, sich an einzelnen Artikeln mit skalierbarem Aufwand beteiligen zu können (Autorenschaft vs. Kooperation vs. Rat).

Auf diese Weise gab es bei diesem Heft viel mehr Beteiligung an den einzelnen Artikeln. Dadurch, dass die Zahl der Textredakteure überschaubar ist, trat das Funkdisziplin-Problem nicht auf – in kleinem Rahmen funktioniert CC-Gerödel nämlich. Und nicht nur engere Zusammenarbeit lag vor, sondern auch mehr Transparenz zu den Einzelschritten, was zum Entstehung eines einzelnen Artikels gehört. Ob das Verfahren weiterhin funktioniert, wissen wir nicht. Aber wir bleiben dran.

Links

[1] Intro zur ersten neuen UpTimes: *Tag zusammen! UpTimes mit neuer Redaktion*, in: UpTimes 2012-2, S. 3-4. https://www.guug.de/uptimes/2012-2/index.html
[2] Bericht vom Redaktionstreffen: *Eines Tages im Linuxhotel; Erstes Redaktionstreffen der UpTimes*, in: UpTimes 2014-2, S. 10-14. https://www.guug.de/uptimes/2014-2/index.html
[3] Verfahren *Redaktionskonferenz per E-Mail* im GUUG-Wiki (zum Lesen im GUUG-Wiki ist ein Wiki-Account erforderlich): https://wiki.guug.de/uptimes/index?&#redaktionskonferenz_via_e-mail

Über Anika

Anika Kehrer arbeitet seit acht Jahren als Technikjournalistin und ist seit der Wiederauflage der UpTimes im Sommer 2012 von der GUUG als Chefredakteurin beauftragt. Ihr Ziel ist, die UpTimes als Vereinszeitschrift der GUUG in Zusammenarbeit mit dem Redaktionsteam aus GUUG-Mitgliedern als hochwertiges, transparentes und partizipatives Fachmagazin zu gestalten.

/etc
Neues aus dem Verein

Die *GUUG* lebt von den Aktivitäten und Plänen ihrer Mitglieder. An dieser Stelle berichten wir von Neuigkeiten aus allen Bereichen des Vereins. Diesmal geht es um die Weihnachtsaktion, das Frühjahrsfachgespräch, ein Camp für Blinde und die Mitgliederverwaltung.

von **Nils Magnus**

Reden ist Silber,
handeln ist Gold,
gemeinsam handeln ist Dynamit.

Frei nach dem bekannten Sprichwort unbekannter Herkunft.

Weihnachtsaktion 2015 für Mitglieder

Der Verein schenkt seinen Mitgliedern zum Jahresausklang ein Fachbuch von *Open Source Press*. Zur Auswahl stehen fünf Titel zu den Themen *Git*, *Bacula*, je ein Vorbereitungsbuch zur Prüfung *LPIC-2* und *LPI 301*, sowie ein Buch zur Red-Hat-Zertifizierung *RHCSA*. Der Titel der Wahl wird den Mitgliedern kostenlos per Post zugesandt und kommt zusammen mit einem Zugang, über den sich das Buch auch als E-Book lesen lässt.

Mitglieder, die unter dem Weihnachtsbaum in ihrem Buch schmökern wollen, füllen bis zum 20. Dezember 2015 ein Online-Formular aus [1]. Allerspätestens bis zum 29. Dezember 2015 muss die Wahl für dieses Jahr getroffen sein, da die Aktion bis dahin begrenzt ist. Optional haben die Teilnehmer auf diesem Weg gleich auch die Möglichkeit, ihre Kontakt- und Kontodaten für die Mitgliederverwaltung zu aktualisieren.

Erheben der Mitgliedsbeiträge neu geordnet

Die Verwaltung der rund 600 Mitglieder der GUUG ist ein aufwändiges Unterfangen. Um An-, Ab- und Ummeldungen schneller zu bearbeiten und die Abrechnung der Beiträge zu verbessern, hat sich die GUUG professionelle Hilfe besorgt. GUUG-Mitglied Christian Lademann, der in der Vergangenheit seine Zuverlässigkeit als Wahlleiter unter Beweis gestellt hatte, kümmert sich seit Herbst 2015 um die Mitgliederliste und die jährliche Abrechnung.

Ebenfalls neu eingeführt wurde die Vereinsverwaltungssoftware *Jverein* [2], die die bisher selbstentwickelte PHP-Software ablöst. Aufgrund schwieriger Aktenlage hat der Vorstand beschlossen, zunächst die Abrechnungen aus dem Jahr 2014 abzuschließen, was weitgehend erfolgt ist. Anschließend werden Vorstand und Christian Lademann bewerten, inwiefern ausstehende Beiträge aus den Jahren 2012 und 2013 als uneinbringlich abzuschreiben sind. Die Mitgliedsrechnung des laufenden Jahres 2015 steht kurz vor dem Versand oder dem Einzug per SEPA-Lastschrift.

Der Vorstand bittet alle Mitglieder darum, dem Verein die Erlaubnis zu erteilen, die Mitgliedsbeiträge per SEPA-Lastschrift einzuziehen. Für die Mitglieder bedeutet dies kein Risiko, da ein solcher Einzug innerhalb von acht Wochen widerrufen werden kann. Die Kontodaten selbst sind nur in einer von sonstigen Diensten separat geführten Datenbank der GUUG gespeichert. Um die SEPA-Lastschrift zu ermöglichen reicht eine formlose Nachricht per E-Mail an <vorstand@guug.de> oder alternativ die Teilnahme an der Weihnachtsaktion der GUUG [1] bis zum 29. Dezember 2015.

Frühjahrsfachgespräch 2016 in Köln

Die jährliche Hauskonferenz der GUUG, die sich an Administratoren, Systemverwalter, System Engineers, Softwareentwickler, IT-Architekten und Sicherheitspersonal richtet, findet vom 23. bis 26. Februar 2016 an der Universität zu Köln statt. An den ersten beiden Tagen gibt es Praxis-Tutorien zu *OpenStack*, *Puppet 4*, *Ceph*, verteilten Fileservern, *Saltstack* sowie zum Thema *Continuous Delivery*. An den folgenden zwei Tagen stehen mehr als 20 Vorträge aus IT-Operations, Dokumentation, Konfigurationsmanagement, Sicherheit, Storage sowie mehrere Vorträge von Unix-Anwendungen abseits von Linux auf dem Programm.

Die Preise bleiben zum Vorjahr unverändert: 300 Euro für die Konferenz, 600 Euro für beide Tutorientage. Rabatte gibt's für GUUG-Mitglieder und Frühbucher bis zum 29. Januar 2016 sowie für

Studenten. Alle Informationen und das Programm kennt die Website der GUUG [3].

GUUG fördert Dresdner Camp für Sehbehinderte

Das *International Camp on Communication and Computers* (ICC) wendet sich an blinde und sehbehinderte junge Menschen und möchte ihnen Zugang zu und Teilhabe an elektronischer Kommunikation ermöglichen. Die 22. Auflage der Veranstaltung findet vom 25. Juli bis zum 3. August 2016 in Dresden statt. Die GUUG fördert im Rahmen ihres vom Vorstand beschlossenen Förderprogramms die Veranstaltung.

Weiterhin würde es der Vorstand begrüßen, wenn ein GUUG-Mitglied auf dem Camp einen Vortrag über Zugangsmöglichkeiten für sehbehinderte und blinde Anwender zu Unix-Systemen hält. Dafür hat der Vorstand ein weiteres Budget in Höhe von 1.000 Euro für Vorbereitung, Fahrtkosten, Unterbringung und Honorar ausgeschrieben. Interessierte Mitglieder wenden sich an <aktive@guug.de> mit Vorschlägen.

Ankündigung: *OpenPGP Conference* 2016 in Planung

Zusammen mit der Community von *GNU Privacy Guard* (GPG), angeführt von GUUG-Mitglied Werner Koch, und anderen Implementationen des freien Standards *OpenPGP* plant die GUUG die Ausrichtung einer Fachkonferenz im Frühsommer 2016. Themen sollen Ende-zu-Ende-Verschlüsselung von E-Mail, Integration in bestehende und neue Anwendungen sowie Sicherheitsfragen des Formats und Protokolls sein. Details zu Termin, Programm und Sponsoringmöglichkeiten plant die GUUG im Januar 2016 zu veröffentlichen.

Wolfgang Stief zum Social-Media-Manager ernannt

Der Vorstand hat durch Verabschiedung eines Kommunikationskonzepts seine Maßnahmen zur Information von Mitgliedern und interessierter Öffentlichkeit neu geordnet. Eine Maßnahme von mehreren ist das Beschicken von Social-Media-Kanälen. Schon seit einiger Zeit betreut GUUG-Mitglied Wolfgang Stief zenral die Accounts der GUUG bei Twitter, Facebook, Google+ sowie dem GUUG-Blog und postet dort – neben anderen GUUGlern – gelegentlich Amüsantes, Hilfreiches oder Historisches über Unix und dessen Ökosystem.

Diese Außenposten der GUUG sind unter https://twitter.com/guug, https://www.facebook.com/groups/guug.ev/ und https://goo.gl/Rj5wU4 zu erreichen. Mitglieder, die interessante Nachrichten oder Fakten verteilen möchten, wenden sich direkt an Wolfgang unter <stief@guug.de>.

Technik-Team der GUUG schaltet zwei Uralt-Server ab

Auf zwei alten, angemieteten Servern liefen bis vor kurzem noch eine Reihe von internen und externen Diensten der GUUG, darunter der Mailserver, Teile der Website sowie viele kleinere Angebote, die gar nicht mehr im Gebrauch waren. Unter der Federführung von GUUG-Mitglied Thomas Martens sind nun diese zwei Server vollständig leergeräumt. Nach einer kurzen Beobachtungsphase sollen die Server final gesichert, abgeschaltet und gekündigt werden.

Die Dienste der GUUG laufen gegenwärtig auf einer Reihe von virtualisierten *KVM*-Instanzen bei einem weiteren Hoster. Das Team rund um Thomas ist unter <guug-it@guug.de> zu erreichen und sucht regelmäßig Helfer und Mitarbeiter. Aktuelle Themen sind beispielsweise die Konsolidierung von zwei Wikis in eines, die Antispam-Thematik oder eine gemeinsame, zentrale Benutzerverwaltung.

Links

[1] Formular für die GUUG-Weihnachtsaktion 2015: http://goo.gl/forms/EZkuPH7cEI
[2] OSS-Vereinsverwaltungssoftware *jverein*: http://www.jverein.de
[3] Frühjahrsfachgespräch (FFG) 2016: http://guug.de/ffg2016/

Über Nils

Nils Magnus ist seit 2014 Mitglied im Vorstand des *German Unix Users Group* e.V. (GUUG). Beruflich verdingt er sich als Engineer sicherer Systemarchitekturen und Fachautor. Er befasst sich mit Vorliebe mit Cloud-Infrastrukturen auf Basis von Open Source. In seiner Rolle als Veranstalter beim *LinuxTag* und der GUUG organisiert er seit über 15 Jahren Konferenzen und Workshops. Nils lebt in München und manchmal in Berlin.

†

In Gedenken an Carsten Zimmermann

Die GUUG trauert um ihr Mitglied Carsten Zimmermann aus Hamburg. Carsten verstarb im November mit nur 46 Jahren durch einen tragischen Verkehrsunfall kurz nach seinem Umzug nach Friedrichskoog. Im Anschluss an sein Studium an der Universität Hamburg lag Carstens Spezialität im Netzwerk-Design und System-Management, was er mit Herz und Seele ausfüllte. *(Erwin Hoffmann)*

Sein, wo das Internet entsteht
Der RFC für *DANE over SMTP*

Wann hat man schon Gelegenheit, an einem RFC mitzuwirken? Der Autor hat sie ergriffen. Ein Erfahrungsbericht von jemandem, der sein durfte, wo er sein möchte: Wo das Internet entsteht.

von **Patrick Ben Koetter**

Nimmt man die Chance aus der Krise
wird sie zur Gefahr.
Nimmt man die Angst aus der Krise
wird sie zur Chance.

Chinesische Weisheit

Neugierig und unternehmungslustig, wie ich bin, habe ich meinen Mund aufgemacht, als Viktor Dukhovni – Vater und Mitautor des RFC zu *DANE over SMTP* – Rezensenten für seine Drafts suchte. Nach dem ersten Lesen habe ich es gleich einmal bereut. Ich bin zwar englischsprachig aufgewachsen, aber das technische Englisch der IETF-Dokumente stellte mich vor Herausforderungen: Es ist trocken, präzise und formelhaft. Sie sind also nicht gerade die Art Text, die einen unterhaltsam fesselt.

Zudem: Wer formuliert, braucht meist mehrere Anläufe, bis er die Botschaft auf den Punkt bringen kann. Die ersten Entwürfe des RFC waren in meiner Wahrnehmung vom Ringen um die Klarheit der Aussage geprägt, welche Probleme DANE over SMTP lösen kann, und wie genau es das zu tun gedenkt. In dieser Phase habe ich viele E-Mails und Textentwürfe mit Dukhovni ausgetauscht. Ich denke, ich kann sagen, zur Klarheit des Dokuments beigetragen zu haben.

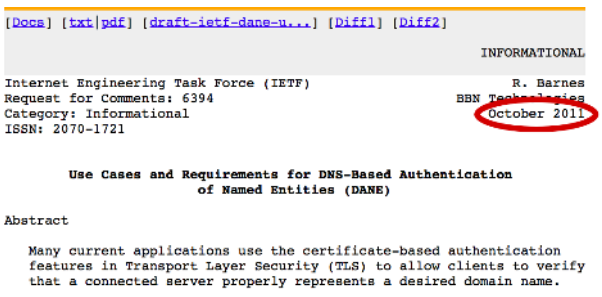
In den technischen Fragen stand ich als Sparringpartner zur Verfügung, wenn der RFC-Hauptautor an konzeptionellen Feinheiten des Proposals feilte. Wobei: Punchingball wäre womöglich zutreffender. Denn einer Koryphäe wie Viktor Dukhovni beim Hin- und Herwälzen von Ideen und Konzepten zu folgen – und dann auch noch brauchbare Antworten zum Pro und Contra zu liefern – hat mich nicht immer im vollen Besitz meiner geistigen Kräfte zurückgelassen. Sozusagen.

Weil ein RFC nicht nur einen *rough consensus*, sondern auch *running code* braucht, habe ich bei der erstbesten Gelegenheit meine eigene sowie die Mailplattform meines Unternehmens auf DANE umgestellt. Geholfen hat mir dabei Carsten Strotmann, dessen Wissen über *DNS* und *DNSSEC* meines bei weitem übersteigt. Seitdem weiß ich wieder, warum es *postmaster* und *hostmaster* als Spezialberufe in der IT gibt. Viktor Dukhovni, Carsten Strotmann und ich fingen dann an, mit DANE zu spielen, um damit vertrauter zu werden. Wir erstellten bewusst falsche Setups, und Dukhovni schrieb Code für *Postfix*, der diese Fehler erkennt und Postfix passend reagieren lässt.

Ein echtes Highlight war, als ich Dukhovni anlässlicher einer DENIC-Tagung, wo wir beide als DANE-Referenten eingeladen waren, persönlich traf – zum ersten mal überhaupt. Wir unterhielten uns den ganzen Abend. Der direkte Austausch hat vieles einfacher und vor allem sehr viel Spaß gemacht.

Engagement beschleunigt Standardisierung

DANE ist eine Prä-Snowden-Idee (Abbildung 1). Ich denke, es ist wichtig, das herauszustellen, denn DANE adressiert Sicherheit, und seit Snowden sind viele neue Sicherheitskonzepte als Reaktion auf Snowdens Veröffentlichungen und das damit gestiegene Bedürfnis zu verbuchen, die eigene Kommunikation vor unberechtigt Zuhörenden zu schützen.


[Docs] [txt|pdf] [draft-ietf-dane-u...] [Diff1] [Diff2]

INFORMATIONAL

Internet Engineering Task Force (IETF) R. Barnes
Request for Comments: 6394 BBN Technologies
Category: Informational October 2011
ISSN: 2070-1721

Use Cases and Requirements for DNS-Based Authentication of Named Entities (DANE)

Abstract

Many current applications use the certificate-based authentication features in Transport Layer Security (TLS) to allow clients to verify that a connected server properly represents a desired domain name.

Abbildung 1: Die Idee zu DANE stammt bereits aus der Prä-Snowden-Ära.

DANE over SMTP ist in Form des RFC 7672 seit Oktober 2014 ein IETF-Standard. Er ist, verglichen

mit den Laufzeiten anderer Standards in der IETF, binnen zwei Jahren und somit in der Tat schnell verabschiedet worden, wenn man sich vergegenwärtigt, dass das IETF zu Zeiten gern sehr, sagen wir mal: ausführlich diskutiert. Diesmal haben sie sich also rangehalten. Und, ja: Die Causa Snowden hat den Prozess der Verabschiedung sicher beschleunigt.

Bedeutsamer scheint mir jedoch, dass Viktor Dukhovni regelmäßig und postwendend Vorschläge der Arbeitsgruppe aufgegriffen, entscheidungsreif diskutiert und in neuen Versionen des Drafts dokumentiert hat. Er hat die Schlagzahl vorgegeben. Binnen Tagesfrist hat er in der Regel Überlegungen, Kritik und Ideen der Arbeitsgruppe als neue Draft-Release an die Gruppe zurückgegeben. 19 Versionen sind so zusammengekommen. Es dürfte nicht Alltag sein, dass einer so viel daran feilt. Für sein Engagement und die fachliche Reife seines Dokuments wurde Viktor auch ausdrücklich von der Arbeitsgruppe gelobt.

Während meiner Zusammenarbeit mit Dukhovni begann eine neue Lernphase für uns, als wir die Zahl an DANE-Nutzern nicht mehr an zwei Händen abzählen konnten. Wir lernten, welche Verständnisprobleme andere bei der Adoption von DANE hatten, und welche Fehler sie dabei machten. Die Fehlerrate war für eine Technologie wie DANE, die auf null Toleranz ausgelegt ist, mit mehr als drei Prozent zu hoch. Wir begannen zu recherchieren, welche Arten von Fehlern auftraten. Beispielsweise stellte sich heraus, dass viele Probleme großer DNS-Provider auf fehlerhafte *DNSSEC*-Implementierungen in (selbstgeschriebenen) DNS-Servern zurückzuführen waren.

Es gab aber auch ausreichend Fehler bei den *TLSA Resource Records*, die man für DANE publizieren muss. Also setzten wir uns hin und schrieben den DANE Validator [2]. Er prüft nicht nur die Existenz von DNSSEC und TLSA, sondern er implementiert die vollständige Logik von DANE over SMTP. Mit diesem Tool ist uns gelungen, die Fehlerrate auf ein unbedeutendes Maß zu reduzieren.

Praxistauglichkeit durch Praxis

Zeitgleich mit dem RFC-Draft schrieb Dukhovni an einer Referenzimplementierung für DANE over SMTP in Postfix. Davon haben beide, Message Transfer Agent und Draft, eindeutig profitiert. So konnte ein in der Praxis brauchbarer Standard herauskommen, der beschreibt, wie sich TLS beim Verbindungsaufbau vor Man-in-the-Middle- und Downgrade-Attacken schützen lässt.

In meinen Augen ist das der wahre Verdienst von DANE over SMTP, dass die Zahl an *Mandatory TLS Policies* endlich steigen wird. Viele Postmaster, mit denen ich gesprochen habe, nutzen höchstens *Opportunistic TLS* und fordern es für bestimmte Ziele nicht zwingend ein (*Mandatory TLS*). Sie meiden TLS, weil es ihnen auf die Füsse fallen könnte: „Lieber unverschlüsselt senden, als Ärger im Betrieb“, ist ihr Motiv. Ich verstehe ihr Problem: Sie scheuen Mandatory TLS, weil es auf Senderseite eine Policy festlegt, die Senden nur dann gestattet, wenn das Ziel bestimmte TLS-Anforderungen erfüllt. Die Kriterien, die zu erfüllen sind, befinden sich aber auf Empfängerseite. Ändern sich dort die Bedingungen, etwa durch ein ausgetauschtes Zertifikat, schlägt die lokale Policy fehl – der Transport zur Zieldomain kommt zum Stillstand.

Mit DANE over SMTP gehört diese Sorge der Vergangenheit an. Die Zieldomain gibt über DNSSEC mit einen TLSA Resource Record bekannt, wie der *STARTTLS*-aktivierte SMTP-Service identifiziert werden kann. Ändern sich die Merkmale und passt die Zieldomain den TLSA-Record entsprechend an, muss der Sender nichts unternehmen: Kein Ärger im Betrieb. Jetzt gibt es hoffentlich mehr Postmaster, die TLS einsetzen.

Security ist zu kompliziert? Nö

In DANE steckt allerdings noch mehr. Die meisten denken bei *DANE* in der Regeln an *DANE over SMTP*. Das ist aber nur eine konkrete Implementierung der DANE-Idee für das Protokoll SMTP. DANE, also das Veröffentlichen einer Policy über eine DNSSEC signierte DNS-Strecke, steht allen Protokollen offen, und auch anderen Anwendungszielen.

Diese Woche wurde ein neuer Typ des DNS Resource Record mit dem Namen *SMIMEA* vergeben. Der gesellt sich zum *OPENPGPKEY Resource Record*. Mit beiden Records kann die Zieldomain PGP-Pubkeys oder *SMIME*-Zertifikate ihrer Mailkonten im DNS veröffentlichen. Gerade der Schlüsselaustausch ist bis heute ein Grund, warum Anwender Ende-zu-Ende-Verschlüsselung meiden: Es ist mühsam, sagen sie. Es ist aufwendig. Sicherheit ist halt kompliziert. „Isso!“, sagen sie.

Nein, is’ nicht so. Sondern wieder einmal ein typischer Fall von *Experten machen ein Interface für Experten* und lassen die Anwender außen vor. Andere bekommen einfache Sicherheit auch hin. Und

Ende-zu-Ende-Verschlüsselung in E-Mail muss dringend aufholen. Die auf DANE aufbauenden Ansätze SMIMEA und Openpgpkey ermöglichen opportunistische Ende-zu-Ende-Verschlüsselung. Wer einen Record für sein Mailkonto erstellt, gibt zu erkennen, dass er Verschlüsselung will. Wer ein entsprechend befähigtes Mailprogramm besitzt, sendet auch beim Erstkontakt automatisch, wenn ein SMIMEA- oder OPENPGPKEYS-Record für den Empfänger erkannt wird.

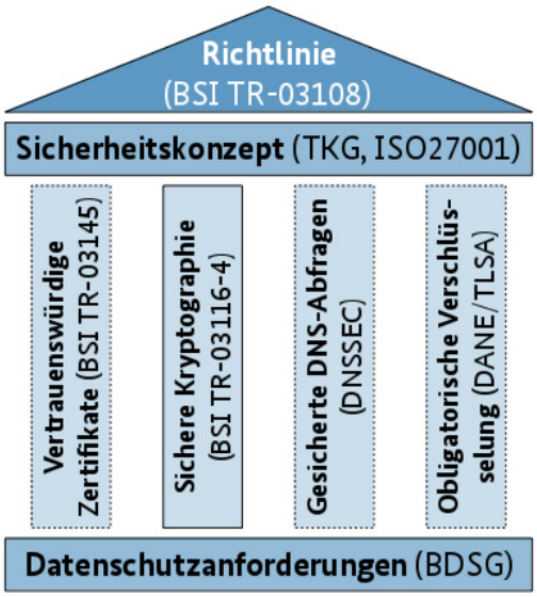


Abbildung 2: Übersicht der BSI-Anforderungen an E-Mail-Diensteanbieter. ©Bundesamt für Sicherheit in der Informationstechnik, 2015 [3]

DANE steht – soweit es SMTP betrifft – in einer Reihe mit *SPF*, *DKIM* und *DMARC*. Sie definieren Prüfkriterien und Policies, die über das eigene Netz hinausreichen. Policies, die Sender oder Empfänger etwas über die zu erwartenden Gepflogenheiten der Domain erzählen. Das ist gut. Vorher mussten wir raten. Jetzt befinden wir uns nicht mehr in einem spekulativen Raum, was denn die andere Seite bei Verstößen gerne haben wollen würde. Oder, wie Karl Valentin sagt: „Mögen hätt ich schon wollen, aber dürfen habe ich mich nicht getraut."

Ein sicheres Internet entsteht

Bei DANE over SMTP entscheidet nicht die Anzahl an Domains, die es adaptieren, über seine Wirkung, sondern die Abdeckung, die DANE-aktivierte Domains erreichen. *Unitymedia* hat 2014 als erster großer Mailprovider in Deutschland seine Plattform DANE-enabled und schützt damit alle seine Kunden. *Web.de* und *GMX* haben dieses Jahr angekündigt, DANE zu adaptieren. Das Bundesamt für Sicherheit in der Informationstechnik hat in seinem aktuellen Entwurf einer neuen technischen Richtlinie von August 2015 angekündigt, Mailprovider in Zukunft nur noch dann zu zertifizieren, wenn sie DANE unterstützen (Abbildung 2, [3]).

Wenn sich das durchsetzt, haben wir etwas ähnliches wie *E-Mail Made in Germany* – aber als offenen Standard. In den USA hat *Comcast* vor kurzem seine Mailplattform DANE-enabled. Hat DANE sich damit durchgesetzt? Nein. Wenn es sich so weiter entwickelt, dauert es aber nicht mehr lange.

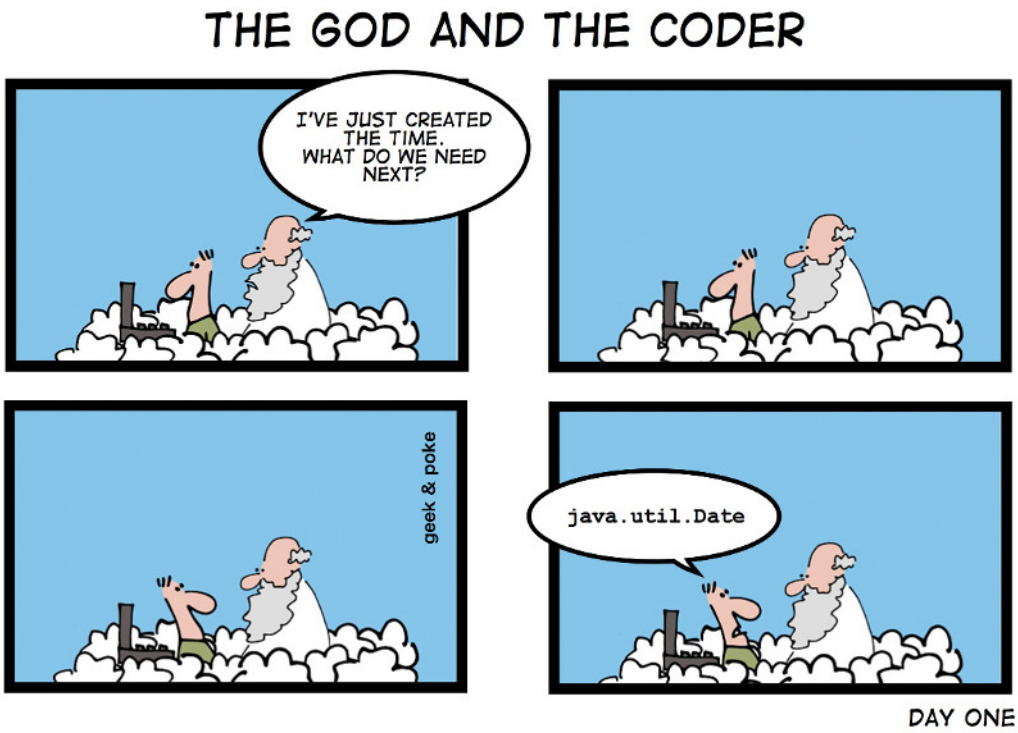
Die Mitarbeit an dem RFC war für mich eine Mischung aus Freude über die Anerkennung der Arbeit, die mir viel bedeutet, geprägt von dem Verantwortungsgefühl, an einem Standard mit weltweit gültige Regeln mitzuwirken, eingepackt in eine Riesenportion Spaß, weil ich mit Menschen, die mir was bedeuten, etwas tun durfte, das mir wichtig ist. Ich durfte da sein, wo ich sein möchte – wo das Internet entsteht.

Links

[1] RFC 7672 *SMTP Security via Opportunistic DNS-Based Authentication of Named Entities (DANE) Transport Layer Security (TLS)*: https://www.rfc-editor.org/rfc/rfc7672.txt
[2] DANE Validator von Patrick Koetter und Viktor Dukhovni: https://dane.sys4.de
[3] BSI TR-03108 *Sicherer E-Mail-Transport*:
https://www.bsi.bund.de/DE/Publikationen/TechnischeRichtlinien/tr03108/index_htm.html

Über Patrick

Patrick ist heute CEO der sys4 AG. Dort leitet er die Geschicke der AG und arbeitet als E-Mail-Experte für ISPs und Unternehmen, die mehr brauchen, als nur E-Mail von der Stange. Begonnen hat seine Liebe zu E-Mail, als er seinen ersten eigenen Server einrichtete und dabei auf *Sendmail* stieß. Das wäre fast das Ende gewesen, wenn er nicht auch noch *Postfix* entdeckt hätte. Danach führte ein Howto über SMTP-Authentifizierung zu dem gemeinsam mit Ralf Hildebrandt geschriebenen *The Book of Postfix*. Das Buch wurde Postfix-Weltbestseller. Patrick engagiert sich weiterhin in vielen Open-Source-Projekten mit E-Mail-Bezug wie *amavisd-new*, *opendkim* und *opendmarc*. Zuletzt lud er nach einem ungewöhnlich fordernden Projekt, das er mit einem eigens zusammengestellten Dreamteam ins Ziel gebracht hatte, dasselbe Team zu einer Firmenidee ein. Alle kamen – und sie gründeten sys4.



Wer macht, hat recht
IT-Sicherheit als Realpolitik

Der amerikanische Regierungsberater Daniel Earl Geer hat den folgenden Text als Keynote auf der *Blackhat* 2014 gesprochen und ihn auf seiner Webseite in Englisch verschriftlicht [1]. Die Übersetzung – eine Leseempfehlung, die Vorschläge zu konkretem politischen Handeln zur Diskussion stellt – erfolgte mit Genehmigung durch den Autor.

übersetzt von **Anika Kehrer**

It's the end of the world as we know it.

R.E.M.

Es gibt drei Berufszweige, die Bescheidenheit lehren: Landwirtschaft, Wettervorhersage, und IT-Sicherheit. Zwei davon übe ich aus, also lasst euch versichern, dass ich das Folgende in aller Bescheidenheit vorbringe. Bescheiden zu sein heißt übrigens nicht, ängstlich oder schüchtern zu sein. Stattdessen kann eine bescheidene Person ihre Meinung ändern, und sei es eine noch so entschiedene Meinung, sobald sie sich widerlegt findet.

IT-Sicherheit genießt heute hohe Aufmerksamkeit. Jeder Vortragende, jeder Autor und jeder Praktiker, der sich je gewünscht hat, sein Thema möge ernst genommen werden, hat nun seinen Willen. IT-Sicherheit ernst zu nehmen ist aber bekanntlich nicht dasselbe, wie sie auch nützlich, schlüssig oder dauerhaft anzuwenden. Das Thema war nie weiter vorn an der politischen Front als heute. Und das ist noch gar nichts.

Ich wünschte, eine einzelne Person könnte immer noch das große Ganze im Blick haben, alles Wichtige mitbekommen und wenig übergehen, wenn überhaupt. Es ist nicht möglich. Diese Phase ging irgendwann in den letzten sechs Jahren zu Ende. Ich selbst habe versucht, auf dem Laufenden zu bleiben, aber es wäre unehrlich zu behaupten, dass es mir in Bezug auf mein eigenes Land gelungen wäre, geschweige denn in Bezug auf andere Länder. Nicht nur hat IT-Sicherheit das Maximum an Aufmerksamkeit erreicht, sondern sie ist auch in fast alle Bereiche vorgedrungen.

Wissen macht mündig

Wieso ist das wichtig? Ich selbst lege keinen Wert auf die Vor- oder Nachteile einer Technologie, solange ich nicht verstehe, wie sie funktioniert. Wenn ich Marketingmaterial sehe, das mir all die tollen Vorteile auflistet, lässt mich das immer an die Worte von George Santayana denken: „Skepsis ist die Keuschheit des Intellekts. Es ist eine Schande, sie zu früh oder dem erstbesten preiszugeben." [2] *Reine Zauberei!* ist keine Antwort, die ein Security-Mensch akzeptiert. Stattdessen sag mir, wie es funktioniert. Dann – und erst dann – sag mir, warum du dich für diese Technologie entschieden hast, um ein Ziel zu erreichen.

Dieses Bedürfnis gründet bei mir zum Teil in der alten und wohlbegründeten Überzeugung, dass jede Sicherheitstechnologie *dual use* ist. Vielleicht haftet diese Zweischneidigkeit jedem Tool an, vom Skalpell über den Hammer bis zur Gaskartusche. Aber Tools der IT-Sicherheit ist sie inhärent. Und ich behaupte, dass man Tools der IT-Sicherheit heute eher offensiv begreift. Der im Januar 2014 ausgeschiedene stellvertretende Direktor der NSA, John Chris Ingly, sagte mal zu mir: „Wenn wir IT-Sicherheit wie Fußball bemessen würden, stünde es nach 20 Minuten 462 zu 456." Ein sehr offensives Spiel also. Für mich ist diese Bemerkung eine Bestätigung von höchster Stelle dafür, dass IT-Security als dual-use gilt, und dass Innovationen, wie sie sich nur Staaten leisten können, offensiven Charakters sind [3].

Dieser Essay folgt aus der Tatsache, dass IT-Sicherheit an Bedeutung gewinnt. Ich sage nicht, dass ich das letzte Wort habe. Aber ich sage, dass wir nicht mehr nur irgendein Brettspiel spielen, wenn wir von IT-Sicherheit reden. Ich sage, dass das Politische heute der wichtigste Aspekt ist. Ich sage, wenn einmal ein Themenbereich – zum Beispiel IT-Sicherheit – in fast jeden Lebensbereich hineinreicht, dann erweitert sich die Schere zwischen guter und schlechter Politik, und die Einfachheit von Lösungen schwindet.

IT-Sicherheit und Politik

Die vier Wahrheiten der Politik sind:

- Die wichtigsten Ideen sind unsympathisch.
- Die sympathischsten Ideen sind unwichtig.
- Nicht für jedes Problem gibt es eine gute Lösung.
- Jede Lösung hat Nebenwirkungen.

Diese vier Wahrheiten dürften auch für den Zusammenhang von IT-Sicherheit und täglichem Leben gelten. Im Lauf meines Lebens hat sich die öffentliche Erwartungshaltung an die Politik extrem erweitert, von der Teilnahmemöglichkeit am Streben nach Glück hin zur Garantie auf Glück. Sowohl der Exekutive als auch der Legislative wohnt die Dynamik inne – und hat es immer getan – dass sie ihre diversen Aufgaben umso besser unter Kontrolle hat, je mehr Geld sie ausgeben kann. Für die Garantie auf Glück gilt dieselbe Dynamik – das einzige wirksame Tool der Regierung, um alle glücklich oder gesund oder sicher zu machen, ist Geld.

Nehmen wir mal an, Überwachung wäre so billig, dass sie keinen Budgetierungsprozess mehr durchlaufen müsste. Verringert das dann die Macht der Exekutive, oder die Macht der Legislative? Ich denke, immer billigere Überwachung verschiebt das Machtverhältnis zu Gunsten der Exekutive. Etwas, das keines Bereitstellungsprozesses bedarf, befindet sich außerhalb des Systems von Kontrolle und Balance. Trägt die zunehmende Installation von Sensoren im Namen der IT-Sicherheit zu unserem Schutz bei? Oder zerstört sie unseren Schutz, indem sie ihn bewahren will?

Es gibt im Internet viel mehr Traffic, als wir im Moment die Hand drauf legen können. John Quarterman von [dem Internetrisiko-Monitoring-Unternehmen] Internet Perils gab mir gegenüber die Einschätzung ab, dass rund zehn Prozent des Internet-Backbone-Traffics hinsichtlich seines Protokolls unidentifizierbar ist. Die amerikanische Netzwerksicherheitsfirma Arber Networks schätzt weiterhin, dass rund zwei Prozent des Traffics, der identifizierbar ist, „unbehandeltes Abwasser“ ist (Abbildung 1, [4]).

Von solchen Schätzungen gibt es natürlich noch mehr. So wie ich es verstehe, rufen sie uns immer wieder ins Gedächtnis, das das Ende-zu-Ende-Design des Internet kein intellektuelles Versagen war [5]. Sondern es vermied brilliant, dass man sich zwischen einem komplett schützendem, aber wenig Spaß machendem Internet und einem Internet entscheiden musste, das einem Staat ultimative Kontrolle gewährt. Nirgends passt besser als hier zu sagen: Du hast drei Optionen – Freiheit, Sicherheit, Bequemlichkeit. Such dir zwei davon aus.

Was Realpolitik bedeutet

Realpolitik bedeutet laut dem britischen Historiker Edward Hallett Carr (1892 - 1982), dass das Erfolgreiche das Richtige ist, und das Erfolglose das Falsche. Die Welt funktioniere nicht nach moralischen Grundsätzen, sodass prinzipiengeleitetes Regieren scheitert. Realpolitik ist sowohl atheistisch als auch antiutopisch.

Abbildung 1: Nur 90 Prozent des Internettraffics ist identifizierbar. Und zwei Prozent des identifizierbaren Abwassers können als rohes Abwasser gelten.

Ich finde das geschmacklos. In meiner eigenen Lebensführung gebe ich jeden Tag Machtvorteile zu Gunsten von Prinzipien auf. Andererseits gelingt es mir nicht immer, Prinzipien wie *Wer Macht hat, hat noch lange nicht recht* einzuhalten, und ebenso wenig mag das prinzipiengeleiteten Regierungen immer gelingen. IT-Sicherheit, wie wir sie in Blogs, Foren, auf Konferenzen und so weiter beschreiben, steckt voller Prinzipien und utopischer Wünsche. Währenddessen haben wir Widersacher auf allen Ebenen, und werden sie vermutlich immer haben, denn es gibt auch diejenigen, für die Prinzipien wenig und Macht viel gilt.

Der Informatiker und Biologe Thomas Ray hat mal gesagt, dass jedes erfolgreiche System Parasiten anzieht. Auch das Internet und jede seiner populären Anwendungen hat Parasiten. Manche sagen, wo gehobelt wird, fallen eben Späne. Andere sagen, das ist ein Designfehler und muss korrigiert werden. Am Ende bleibt jedoch allein Realismus übrig, wenn alles andere scheitert.

Ein politischer Realismus, wie ich ihn meine, geht von vier Prämissen aus:

- Das internationale System ist anarchisch.
- Staaten sind die wichtigsten Akteure.
- Jeder Staat agiert rational für sich selbst.
- Die erste Sorge eines Staates ist, zu überleben.

Dieser Realismus gilt auch für die Situation der IT-Sicherheit in einem globalen Internet. Es ist anarchisch, und Staaten sind die wichtigsten Handelnden geworden. Was Staaten in die Cyber-Offensive investieren, dient komplett dem Überleben in der Internet-Welt. Die Staaten tun das, weil sie sich zweifach simultan dazu getrieben fühlen: Einmal durch das, was möglich ist, und einmal durch das, wovon ihre Bürger sich abhängig machen.

Wenn man sich nicht mit etwas befasst, kann man es nicht beeinflussen. Ich will daher zu einigen derzeit dringenden politischen Fragen Stellung nehmen.

1. Meldepflicht von Sicherheitsvorfällen? Abgestuftes Ja.

Das amerikanische Seuchenschutzzentrum (*United States Centers for Disease Control*, CDC, Abbildung 2) genießt weltweit hohes Ansehen. Im Grunde sorgen drei Regeln dafür, dass es so gut funktioniert:

(1) Meldepflicht für übertragbare Krankheiten,

(2) Datenbanken und die analytische Fähigkeit, statistische Anomalien von einem Seuchenausbruch zu unterscheiden,

(3) Einsatzteams, die vor Ort die Verantwortung übernehmen, wenn zum Beispiel in Miami Ebola auftritt.

Alles weitere ist Detail. Die wichtigste Regel dieser drei ist die Meldepflicht. Es herrschen strenge Regeln für den medizinischen Datenschutz. Aber wenn du mit Beulenpest, Typhus oder Anthrax im Krankenhaus aufkreuzt, hast du null Privatsphäre, weil dann die Meldepflicht für übertragbare Krankheiten greift.

Ich frage euch: Wenn man eine öffentliche Gesundheit des Internets annimmt, ergibt es dann Sinn, eine Meldepflicht für IT-Sicherheitsversagen zu haben? Ist es euch lieber, Computereinbrüche der Regierung oder einer Nichtregierungsorganisation zu melden? Sollte das Nichtmelden strafbar sein? Wenn du einen IT-Angriff bemerkst, hast du dann eine ethische Pflicht, ihn zu melden? Sollte das Gesetz verfügen, dass du einer solchen Pflicht nachkommst?

Meine Antwort auf diese Fragen wäre, sich an das Vorgehen des CDC zu halten: Per Gesetz Sicherheitsversagen meldepflichtig machen, die schwerer wiegen als ein Schwellwert, der zu verhandeln ist.

Abbildung 2: Die Vorgehensweise des amerikanische Seuchenschutzzentrum CDC eignet sich als Vorbild für ein Meldewesen von IT-Sicherheitsvorfällen. (Foto: Daniel Mayer bei Wikipedia, CC BY SA)

Unterhalb dieses Schwellwerts befürworte ich die Studie von Richard Danzig [6] aus dem Jahr 2014, in der er unter anderem ein Konsortium empfiehlt [7], das Charakter und Schwere von IT-Sicherheitsangriffen auf den privaten Sektor beleuchten soll. Grundlage von deren Arbeit soll nach Danzig das Modell sein, nach dem die Luftfahrt freiwillig Beinaheunfälle meldet:

> Oft genauso informativ wie geschehene Unfälle, gibt es keine Meldepflicht für Beinaheunfälle. Fluggesellschaften würden sich gegen noch mehr Regulation wehren und auch Reputationsschäden fürchten. 2007 schlug man aber einen alternativen Pfad ein, als die [im Auftrag der USA arbeitende, nicht profitorientierte] Forschungseinrichtung *MITRE* das *Aviation Safety Information Analysis and Sharing System* (ASIAS) einführte. Hier sammelt die US-Bundesluftfahrtbehörde Beinaheunfälle und erstellt anonymisierte

> Sicherheitsberichte, Benchmarks und Verbesserungsvorschläge.

Mit Status von heute nehmen 44 Fluggesellschaften freiwillig an diesem Programm teil.

Was ich empfehle, ist die Kombination auf der Meldepflicht nach dem CDC-Modell oberhalb eines Schwellwerts und das freiwillige ASIAS-Modell für Vorkommnisse unterhalb des Schwellwerts. Das auszugestalten, bedeutet immer noch eine Menge Denkarbeit. Es ist ein Irrtum zu glauben, dass dieser Vorschlag einfach oder ohne Nebenwirkungen wäre.

2. [Überholt]

Anm. d. Übers.: Dieser Punkt bezieht sich auf Netzneutralität, die aber erstens in den USA etwas anderes bedeutet als in Deutschland, und die zweitens inzwischen durch neue Rechtsprechungen und Initiativen an der im Text beschriebenen Situation von Anfang 2014 auch in den USA vorbei gezogen ist.

3. Produkthaftung für Quellcode? Wahlmöglichkeit.

Nat Howard hat [laut dem amerikanischen Firewall-Experten Marcus Ranum] gesagt: „Security wird immer exakt so schlecht wie nur möglich sein, solange alles funktionieren soll". Mit jedem Tag, der vergeht, erhöht sich der Standard dieser *Solange*-Klausel. Und wie Ken Thompson in seiner Dankesrede für den *Turing-Award* sich ausdrückt, gibt es vor der Technik kein Entrinnen [8].

Mathematisch gesprochen, kannst du weder einem Programm noch einem Haus vertrauen, das du nicht zu 100 Prozent selbst gebaut hast. Realiter aber vertrauen viele von uns einem Haus, das von hinreichend fachkundigen Menschen erbaut wurde – sogar eher noch mehr, als wenn wir es selbst gebaut hätten. Der Grund dafür ist, dass Pfusch am Bau eine entscheidende *Andernfalls*-Klausel kennt, und zwar seit mehr als 3.700 Jahren (Abbildung 3, [9], [10]):

> Gesetzt, ein Baumeister hat für einen Mann ein Haus gebaut, sein Werk (aber) nicht fest gemacht, und das Haus, das er gemacht hat, ist eingefallen und hat den Eigentümer des Hauses getötet, so wird jener Baumeister getötet.

Abbildung 3: Die Gesetze des Hammurapi, ausgestellt im Louvre: Produkthaftung gab es schon vor rund 4.000 Jahren. (Foto: Mbzt bei Wikipedia, CC BY)

Heute nennt man dieses rechtliche Konzept Produkthaftung, und die zu Grunde liegende Formel lautet: Wenn du was gewerblich etwas verkaufst, dann sieh zu, dass es was taugt, oder du bist für davon verursachte Schäden verantwortlich. Die einzigen beiden Produkte ohne Gewährleistung sind heute Religion und Software. Und für Software soll das nicht mehr lange gelten: Poul-Henning Kamp [FreeBSD-Guru und derzeit von der Linux Foundation bezahlter NTP-Entwickler] und ich haben einen Grobentwurf gemacht, wie eine Produkthaftung für Software aussehen könnte. Es sieht drei Punkte vor:

(0) Konsultiere das Strafgesetzbuch, um zu entscheiden, ob ein verursachter Schaden beabsichtigt oder fahrlässig war.

Wir wollen Produkthaftung nur für unbeabsichtigten Schaden geltend machen, egal ob aus

Schluderei, zu wenig Tests, Kostenersparnis, fehlender Doku oder blanker Inkompetenz. Punkt Null räumt jeden absichtlich verursachten Schaden der Software aus dem Fokus.

(1) Lieferst du deine Software mit vollständigem und baubarem Quellcode aus, sowie mit einer Lizenz, mit der der Lizenznehmer beliebige Funktionen der Software deaktivieren darf, beschränkt sich deine Haftung auf eine Rückerstattung.

Punkt Eins ermöglicht, die Haftung zu beschränken: Ermögliche den Usern, die Software zu untersuchen und Teile rauszulassen, denen sie nicht vertrauen oder die sie nicht wollen. Dazu gehören Herkunftsangaben, die Vertrauen ermöglichen – etwa: *Bibliothek ABC stammt von XYZ* – genauso, wie man das bei Lebensmitteln macht.

Das Wort *deaktivieren* ist sorgfältig gewählt: Es ist nicht nötig, das Recht auf Veränderung einzuräumen. Die Haftung ist beschränkt, auch wenn sich der Lizenznehmer den Code nie wirklich anguckt. Solange er ihn erhält, ist der Hersteller des Codes aus dem Schneider. Alle anderen Rechte bleiben in der Kontrolle des Herstellers, sodass die Situation unverändert bleibt für Hardware-Locking, Vertraulichkeit, Kopierschutz, magische Zahlen und so weiter. *Free and Open Source Software* (FOSS) erfüllt Punkt Eins offensichtlich, weswegen sich hier gar nichts ändert.

(2) In jedem anderen Fall bist du haftbar für den Schaden, den deine Software anrichtet, wenn sie normal verwendet wird.

Wenn du also nicht die in Punkt Eins nötigen Informationen preisgeben willst, fällst du unter Punkt Zwei und bist haftbar zu machen, genauso wie jeder andere Hersteller etwa von Autos, Kettensägen oder heißem Kaffee.

Wie streng die Haftung ausfällt und was unter *normaler Nutzung* zu verstehen ist, ist sache der Juristen. Aber lasst uns ein grobes Beispiel machen. Einen USB-Stick von einem altbekannten Unternehmensvertreter einzustecken und eine Produktinfo-Datei von dort auf deinen Rechner zu kopieren, ist normale Nutzung und sollte niemals dazu führen, dass dein Computer Teil eines Botnetzes wird, deine Kreditkartendaten verschickt oder alle Deine vertraulichen Unterlagen zu ebenjenem Unternehmen überträgt. Tut er es doch, ist dein Betriebssystem gestört.

Wir wollen hiermit ein ernstes Sicherheitsproblem lösen. Entweder liefern Software-Unternehmen Qualität und untermauern das mit Produkthaftung, oder sie lassen ihre User sich selbst beschützen. Die momentane Situation ist unhaltbar, in der User nicht sehen können, ob sie sich schützen müssen, und keinen Ausweg haben (Abbildung 4).

Abbildung 4: Wenn der Zugriff auf den Quelltext versperrt ist, kann der User nicht sehen, wovor er sich eventuell schützen muss. (Foto: Johann Jaritz bei Wikipedia, CC BY SA

Würde das funktionieren? Langfristig: Absolut. Kurzfristig gäbe es ein paar böse Überraschungen, sobald schlechter Quellcode publik wird. Die FOSS-Community müsste für ihre Sorgfalt – oder auch nicht-Sorgfalt – geradestehen, außerdem ihre Build-Umgebungen und Quelltexte für alle Zeit verfügbar machen. Die Software-Unternehmen würden Zeter und Mordio schreien, wenn eine solche Gesetzesregelung in kraft träte. Jeder Experte und Lobbyist, den sie kriegen können, wird voraussagen, dass „so ein Gesetz das Ende des Software-Zeitalters bedeutet, das wir kennen!“

Worauf wir dann wohlüberlegt antworten: „Ja, bitte. Genau das war der Plan.“

4. Zurückschlagen? Eingeschränktes Ja.

Ich nehme an, dass viele von Euch schon mal bei einem Angreifer zum Gegenschlag ausgeholt haben, oder zumindest auf ihn gezielt haben, wenn auch nicht abgedrückt. Ich gehe bei vielen von Euch auch davon aus, dass Ihr ein Ziel sorgfältig genug auskundschaften könnt, sodass Ihr Kollateralschäden minimiert. Aber wovon wir hier reden, ist das digitale Äquivalent der selbststeuernden Bombe. Wie ich schon andeutete, sind digitale selbststeuernde Bomben das, woran die Labo-

ratorien vieler Staaten fieberhaft arbeiten. In diesem Sinne wisst Ihr, was sich hinter den Kulissen abspielt, und Ihr wisst auch, wie schwer Zielen ist, weil Ihr wisst, wie schwer Zurückverfolgung – echte Zurückverfolgung – wirklich ist.

Das Problem liegt in der gemeinsamen Infrastruktur, und dieses Problem werden wir nicht los. Es gibt ein paar Einheiten, die global operieren und effektiv zurückschlagen können, zum Beispiel die Zusammenarbeit von Microsoft und dem FBI bei dem *GameOver*-Trojaner [11]. Aber das ist eine teure und seltene Behandlungsmethode, die nur bei allerschlimmster Schadsoftware greift. Nichtsdestotrotz ist das die, die wir haben.

Kleinere Einheiten können weder global handeln noch ohne behördlichen Segen bestimmte Maßnahmen treffen. Das kann und muss so bleiben, aber ich sehe nicht, wie kleinere Einheiten zurückschlagen könnten. Ich sehe nur, dass Kleinere all ihre Kraft darauf verwenden müssen, sich schnell wieder erholen zu können.

5. Fallbacks und Krisenfestigkeit? Kompliziert.

Es wurde immer schon viel darüber geredet, was zu tun ist, wenn Fehler inakzeptabel und doch unausweichlich sind. Bisher hat alles, was für die Öffentlichkeit als grundlegend angesehen wird, einen Versorgungsmindeststandard aufgedrückt bekommen, Elektrizität zum Beispiel, oder Wasser. Aber lasst uns über Software reden.

Zum Beispiel wird bei kryptografischen Protokollen oft Algorithmus-Agilität gefordert, also die Fähigkeit, von einem Algorithmus zum anderen zu wechseln, wenn der eine unsicher wird. Der Sicherheitsvorteil davon liegt nicht darin, dass man was anschaltet, sondern darin, dass man etwas ausschaltet. Dafür muss ein zweiter Algorithmus verfügbar sein, aber das bedeutet, dass er von vornherein so eingeplant werden muss, dass man an beiden Enden der Verbindung den Wechsel erzwingen kann.

Man kann argumentieren, dass das einfach einen einzigen, komplexeren Algorithmus bedeutet. Oder vielleicht will man zwei Algorithmen, die immer beide verwendet werden, etwa dass der eine den anderen verschlüsselt, sodass es keinen Sicherheitsbruch bedeutet, wenn einer von beiden versagt. Ich will damit nur demonstrieren, dass es nicht immer einfach ist, Fehlerbehandlung vorauszuplanen; dass der Wille allein nicht reicht (Abbildung 5).

Abbildung 5: Man kann nicht alles voraussehen. Vielleicht sind vorausschauende Fallbackpläne generell keine gute Idee.

Vielleicht sind vorausschauende Fallbackpläne deshalb generell keine gute Idee. Vielleicht braucht man eher die Möglichkeit, die Endpunkte zu erreichen und zu aktualisieren, wenn es nötig wird. Aber heute sind die meisten Endpunkte, an denen man solch ein Remote Management Interface bräuchte, eingebettete Hardware.

Also lasst mich euch was fragen: Sollten eingebettete Systeme einen Fernzugang haben müssen, oder nicht?

Wenn sie es nicht haben, kann eine spät entdeckte Lücke nicht behoben werden, ohne vor Ort zu sein – was wahrscheinlich unmöglich ist, denn einige Systeme wird man gar nicht finden, an andere kommt man nicht mehr heran, und in jedem Fall sind es einfach zu viele. Wenn sie es aber haben, wird sich jeder fähige Widersacher genau darauf konzentrieren, und sobald er herankommt, wird er es zu langfristiger Kontrollausübung nutzen, und natürlich dafür, ebendies zu verschleiern.

Vielleicht braucht man also eher den Ansatz, eingebettete Systeme wie Menschen zu betrachten, und ich meine mit Sicherheit nicht künstliche Intelligenz. Mit „wie Menschen betrachten“ meine ich: Eingebettete Systeme ohne Remote Management Interface, die somit unerreichbar sind, sind eine Lebensform, und da ein Leben stets einmal endet, muss ein solches System nach einer bestimmten Zeit sterben. Andersherum muss ein eingebettetes System mit Remote Management Interface über soviel Selbstschutz verfügen, dass es einen Befehl verweigern kann. Unausweichlicher Tod und Befehlsverweigerung sind zwei menschliche Eigenschaften, die wir replizieren müssen, anstatt sich auszumalen, dass sie auszuhebeln die Zukunft sei.

Damit nicht einige von Euch denken, das alles sei nur kleinliches, tendenziöses und akademisches Gepose: Es ist durchaus möglich, möchte ich erinnern, das Internet einem großen Teil der Nutzer zu verweigern. Heimrouter (Abbildung 6) arbeiten mit Treibern und Betriebssystemen, die binäre Blobs sind, bestehend aus Linux-Snapshots und der einfachsten Chip-Massenware, die zur Herstellungszeit erhältlich war. Linux hat sich weiterentwickelt. Treiber haben sich weiterentwickelt. Samba hat sich weiterentwickelt. Chipsets haben sich weiterentwickelt. Aber was bei *Best Buy* oder ähnlichen Läden über den Ladentisch geht, ist bemerkenswert billig und bemerkenswert alt. Mit einer Sicherheit, die in langer Engineering-Erfahrung wurzelt, behaupte ich, dass die Hersteller ihre ausgelieferten Blobs selbst gar nicht mehr aus Quellen bauen können.

Abbildung 6: Heimrouter, egal welche, sind millionenfach im Gebrauch und höchstwahrscheinlich Software-seitig angreifbar, da veraltet. Einen neuen kaufen? Der ist Software-seitig ebenso alt.

Wenn, wie der ehemalige VP Software von *One Laptop per Child* Jim Gettys aufwendig maß und mir erzählte, das durchschnittliche Alter der Codebase solcher Router bei vier bis fünf Jahren liegt, dann kann man sicher sein, dass das CVE-Verzeichnis [12] etliche Methoden auflistet, dieser Betriebssysteme und Treiber von fern zu attackieren. Wenn ich sie von fern kommandieren kann, dann kann ich ein Botnet bauen, das sich außerhalb des Heimnetzwerkes befindet. Es muss kein einziges Paket durch die Firewall bekommen, es muss auf keine Weise erkennbar sein, aber es ist mit Sicherheit eine latente Waffe, die man auf einen beliebigen Verbreitungsgrad anwachsen lassen kann, bevor man sie zu mehr benutzt. Alles, was ich in meinen Exploit einbauen muss, ist ein Weg, um dem Gerät drei Dinge zu signalisieren: Höre auf weiterzugeben, was auch immer du bekommst; flute das Netzwerk mit einem Broadcast-Signal, das andere Peers dazu bringt, dasselbe zu tun; und halte die Firmware davon ab, jemals neu zu booten.

Jetzt ist der einzige Weg, sich zu erholen, sämtliche Geräte auszustecken, sie wegzuschmeißen und neue zu installieren – aber werden die neuen nicht mit einiger Wahrscheinlichkeit ähnliche Schwächen haben, die das Ganze erst möglich machten? Natürlich tun sie das, also lässt sich die Sache nicht mit einem schnellen Trip zum Laden erledigen, sondern eher damit, die komplette Werkstatt und Verkaufsinfrastruktur eines jeden Herstellers von Heimroutern durchzuspülen. Auf der *DefCon* gab es anscheinend ein Event zu genau diesem Thema [13].

Krisenfestigkeit ist ein Bereich, wo keine einzelne Policy ausreichend ist. Also habe ich ein Trio kleiner Schritte vorgeschlagen: Eingebettete Systeme können nicht ewig leben, wenn sie kein Remote Management Interface haben; eingebettete Systeme müssen ein Remote Management Interface haben, wenn sie ewig leben sollen; und Swap-over ist besser als Swap-out, wenn es um Datenintegrität geht.

6. Schwachstellen? Beherrschen.

Schwachstellen zu finden, ist seit rund acht Jahren ein Job. Eine lange Zeit konnte man das als Hobby machen, als Lohn allein die Ehre, aber es ist zu schwer geworden - man musste es als Beruf sehen, und man musste als Berufstätiger bezahlt werden. Das war das Ergebnis harter Arbeit auf Seiten der Software-Hersteller. Aber wie die vierte Wahrheit der Politik sagt: Jede Lösung hat Nebenwirkungen.

Hier ist die Nebenwirkung, dass die Schwachstellenfinder aufhörten, ihre Erkenntnisse zu teilen. Wenn du für Spaß und Ehre Schwachstellen suchst, dann musst du sofort jeden wissen lassen, dass du eine gefunden hast, weil sonst jemand anderes schneller ist. Wenn du es für den Profit machst, dann behältst du sie für dich. Und der Nebeneffekt ist: Wenn bezahlte Schwachstellenfinder ihre Erkenntnisse nicht mehr teilen, dann steigt der Prozentsatz der Zero-Day-Angriffe.

In der Mai-Ausgabe des Magazins *The Atlantic* warf der Sicherheitsexperte Bruce Schneier ei-

ne zwingende Prinzipienfrage auf: Sind Software-Schwachstellen rar oder dicht gesät [14]? Wenn sie rar gesät sind, dann verringert jede, die du findest und stopfst, die Zahl der Angriffswege. Wenn sie dicht gesät sind, dann ist es nicht sicherheitsrelevant und gar Ressourcenverschwendung, eine mehr zu finden und zu stopfen. Eine von sechs ist eine 15-prozentige Verbesserung. Eine von sechstausend hat keinen messbaren Wert.

Wenn ein paar Brüder aus Texas den Weltmarkt für Silber in die Ecke treiben können [15], dann kann zweifelsohne die US-Regierung in aller Öffentlichkeit den Weltmarkt für Schwachstellen in die Ecke treiben, indem sie alle aufkauft und veröffentlicht (Abbildung 7). Sie muss nur bekannt geben: „Mach uns ein vernünftiges Angebot, dann verzehnfachen wir es.“ Klar wird es einige geben, die sagen, „Ich mag Amerika nicht, ich verkaufe nur an die Ukraine“. Aber so jemand weiß auch, dass bald jemand anders die Schwachstelle findet, der dann wohl an Amerika verkauft, wo sie öffentlich wird – somit wird es unausweichlich, so schnell wie möglich zu verkaufen.

Abbildung 7: Interessante Theorie: Die Macht des Geldes nutzen, um den Markt für IT-Sicherheitslücken zu beherrschen, indem man sie alle aufkauft und veröffentlicht.

Die Nützlichkeit dieser Strategie resultiert aus zwei Nebenaspekten: Erstens vergrößert die Überbezahlung den Talentpool der Schwachstellenfinder. Zweitens wird jede Schwachstelle entwertet, die die USA kauft und veröffentlicht. Anders gesagt erhöhen wir mit der Überbezahlung die Zahl der gefundenen Schwachstellen, während wir sie durch Veröffentlichung als Waffe stumpf werden lassen. Wir brauchen keine Erkenntnisse über die Waffen des Widersachers, wenn wir eine nahezu vollständige Liste der Schwachstellen haben und sie mit allen Software-Herstellern teilen.

Aber das rückt wieder Schneiers Frage in den Blick: Sind Schwachstellen rar oder dicht gesät? Sind sie rar oder nicht allzu viele an der Zahl, dann gewinnt in absehbarer Zeit, wer den Markt beherrscht. Sind sie dicht gesät, dann besteht alles, was wir tun, am Ende darin, dass wir die Kosten in die Höhe treiben sowohl für Software-Hersteller, die jetzt jede Menge Lücken stopfen und Armeen an Schwachstellenforschern beschäftigen müssen, als auch für den Steuerzahler.

Ich denke, dass Schwachstellen spärlich genug gesät sind, und daher halte ich es für den billigsten Sieg, den Markt zu beherrschen.

Ich möchte aber anmerken, dass die Kollegen aus der statischen Code-Analyse regelmäßig Webanwendungen melden, die größer als zwei Gigabyte sind und 20.000 Variablen haben. Solche Webanwendungen können nur maschinengeschrieben sein, und somit sind auch ihre Schwachstellen maschinengeschrieben. Maschinengetriebene Schwachstellenproduktion mag meine Analyse ändern, allerdings kann ich nicht sagen, in welche Richtung.

7. Recht auf Vergessenwerden? Ja.

Wir sind ja jetzt alle nachrichtendienstliche Aufklärer – wir sammeln Informationen übereinander im Dienste irgendwelcher Lehnsherren [16]. Es gibt heute so viele Technologien, die Observation und Identifizierung Einzelner auf Distanz ermöglichen. Sie stecken noch nicht in deiner Tasche, in deinem Armaturenbrett oder in deinem Rauchmelder, aber das ist nur eine Frage der Zeit. Deine digitale Spur ist einmalig, also identifiziert sie dich. Alle digitalen Spuren in einem Pool zu versammeln ermöglicht außerdem, Abweichung von der Norm zu messen.

Privatsphäre war bisher proportional zu dem, was nicht observiert werden kann, oder was observiert, aber nicht zugeordnet werden kann. Das gilt nicht mehr. Was heute observierbar und identifizierbar ist, macht das nicht-Observierbare und nicht-Identifzierbare zunichte. Was könnte also die Alternative sein?

Wenn du ein Optimist oder ein Apparatschik bist, dann geht deine Antwort in Richtung von Datenschutzgesetzen, verwaltet von einer Regierung, der du vertraust oder die du kontrollierst. Wenn du ein Pessimist oder ein Hacker/Maker bist, dann geht deine Antwort in Richtung des Operativen, und deine Definition eines Staates der Privatsphäre wird die meine sein: die Möglichkeit, sich selbst zu verzerren [17].

Selbstverzerrung bedeutet, Fehlinformation einzusetzen, um eine Informationssammlung über sich zu durchkreuzen. Einiges kann low-tech erfolgen, etwa einen Therapeuten in bar und unter falschem Namen zu bezahlen. Selbstverzerrung bedeutet, durch ein Arsenal an fehlkonfigurierten Webservern hindurch zu surfen, einen Motorgenerator zwischen dich und das Smart Grid zu stellen, und aus keinem besonderen Grund Tor zu nutzen. Selbstverzerrung bedeutet, sich im hellen Licht zu verstecken, wenn kein Schatten da ist. Selbstverzerrung bedeutet, nicht eine digitale Identität zu haben, die du hochhältst, polierst und beschützt, sondern so viel wie es nur geht.

Damit niemand denkt, dass das nur ein Problem für Paranoide ist, lasst mich anmerken, dass eine Deckidentität im personenbezogenen Geheimdienst [18]. aus demselben Grund immer schwieriger zu erstellen ist: Selbstverzerrung wird immer schwieriger. Wenn ich in einem Einsatz wäre, dann würde ich nicht versuchen dafür eine eigene digitale Identität zu erschaffen, sondern ich würde mir eine geeignete – sozusagen – borgen.

Die Initiative der Obama-Verwaltung für die *National Strategy for Trusted Identities in Cyberspace* (NSITC, [19], [20]) ist ein treffendes Beispiel. Sie „fordert die Entwicklung interoperabler technologischer Standards und Richtlinien – ein Ökosystem der Identitäten – in dem Individuen, Organisationen und die zugrunde liegende Infrastruktur – etwa Router und Server – verbindlich authentifiziert werden können".

Wenn man einer digitalen Identität vertrauen kann, dann deswegen, weil sie fälschungssicher ist. Warum will die Regierung das? Sie will digital Regierungsdienste anbieten und eindeutig zuordnen. Ist eine fälschungssichere digitale Identität es wert, deine letzten Geheimnisse mit der Regierung zu teilen? Gibt es einen echten Unterschied zwischen einem System, das einfache, sichere und identitätsbezogene Dienste anbietet, und einem Überwachungssystem? Vertraust du denjenigen, die zeitlich unbegrenzt Transaktionsdaten zwischen dir und den Regierungsdiensten aufbewahren, wofür du eine unfälschbare Identität bieten musst, um an diesen Transaktionen teilzunehmen?

Angenommen, man macht das auch in anderen Bereichen als im öffentlich-rechtlichen – willst du so etwas überall haben? Wenn du heute Authentifizierungssysteme aufbaust, dann spielst du bereits in dieser Liga. Wenn du heute Authentifizierungssysteme nutzt, dann begibst du dich in die Hände derjenigen, die in dieser Liga spielen und die entscheiden, wie es mit dem System weitergeht.

Langer Rede, kurzer Sinn: Meiner Schlussfolgerung nach ist eine einzigartige, unfälschbare digitale Identität kein gutes Geschäft, und ich will keine.

Abbildung 8: Das Recht, das Bild von sich selbst zu verzerren, das die Daten zeichen: Schwindet es, ist etwas verloren und fast nichts gewonnen. (Foto: Jean Pierre Hintze bei Flickr, CC BY SA)

Ich will mich entscheiden können, ob ich meine Identität verzerren möchte. Ich mache das dann vielleicht nicht oft, aber es ist mein Recht es zu tun (Abbildung 8). Wenn dieses Recht schwindet, verliere ich etwas und gewinne fast nichts.

In dieser Hinsicht, wohl wissend, dass es nur ein kleiner Schritt ist, ist das *Recht auf Vergessenwerden* der EU [21] so sachgemäß wie zweckmäßig, auch wenn es nicht weit genug geht. Vergessen zu werden ist dasselbe, wie in einer neuen Stadt neu anzufangen, seinen Namen zu ändern, wie eine Definition von Privatsphäre, die Selbstverzerrung ermöglicht – ein Recht, wie ich erinnern möchte, das derzeit nur denjenigen vorbe-

halten ist, die der Regierung helfen (als Zeugenschutzprogramm zum Beispiel).

Das Recht, vergessen zu werden, ist die einzige Kontrolle inmitten der Flutwelle an Beobachtbarkeit, die das allgegenwärtige Sensorennetz gerade auslöst. Regierungen, die das Internet durch Registrierungskontrolle balkanisieren, beanspruchen das Recht dazu allein für sich. Die einzige demokratische Bremse bei dieser Reise ohne Wiederkehr ist die Möglichkeit für den Einzelnen, auf seine eigene kleine Weise dasselbe zu tun. Ich finde es bemerkenswert ironisch, dass die Zeitung The Guardian, die sich so für Edward Snowdens Enthüllungen eingesetzt hat, an anderer Stelle kommentiert, dass „niemand ein Recht auf Vergessenwerden hat“ [22]. Au contraire, madames et monsieurs, das haben sie.

8. Internet-Wahlen? Nein.

Es ist ja so, dass eine fundierte Sicherheitsanalyse weniger Aufmerksamkeit erhält als eine saftige Verschwörungstheorie – selbst wenn beide zum selben Ergebnis kommen. Wie ist das zu erklären? Wenn ich es wüsste, würde ich es tun. Aber vielleicht brauchen wir diese Erklärung gar nicht, wenn die Richtigkeit einer Wahl dereinst mal durch Vorkommnisse in Frage gestellt wird. Ich möchte gerne glauben, dass wir kein Massaker brauchen, um umzudenken, aber vielleicht brauchen wir das. Und wenn wir es brauchen, dann möge es eher früher als später passieren.

9. Verwaisung? Klarheit über Konsequenzen.

Wenn ich ein Auto auf der Straße aussetze, kommt irgendwann jemand vorbei, der es beansprucht. Wenn ich meinen Partner undoder meine Kinder verlasse, kann jemand anderes an meine Stelle treten. Wenn ich mein Patent nicht verlängere, wird sein Inhalt frei für alle. Wenn ich die Vertraulichkeit von Informationen nicht gewährleiste, etwa indem ich sie veröffentliche, gehen sie unwiederbringlich in die Hände der Allgemeinheit über. Wenn ich meine Sachen irgendwo liegen lasse, gehen sie mir verloren und landen vielleicht im Reality-TV. Und so weiter und so weiter.

Was für mich eine völlig offensichtliche Herangehensweise wäre: Wenn Firma X eine Code-Base abstößt, dann muss diese Code-Base quelloffen gemacht werden. Abgesehen von Sicherheitsüberlegungen gehen mir oft gern genutzte Programme verloren, weil ihr Hersteller sie vernichtet. Aber hinsichtlich Sicherheitsüberlegungen gibt es genug Leute, die Sicherheits-Updates erstellen würden, wenn Zeit und Not es erfordern. Nutzte es nicht dem Gemeinwohl, wenn verwaiste Programme quelloffen gemacht würden? Ich denke schon.

Aber ist Kauf-Software auf normalen Computern nicht von gestern? Sind automatische aktualisierte Smartphone-Clients mit automatisch aktualisierten Cloud-Services in privatwirtschaftlichen Carrier-Netzen nicht die Zukunft? Vielleicht, vielleicht nicht. Wenn jedenfalls die beiden größten Computer-Hersteller nur die Hälfte der heutigen Desktops aktualisieren - wie viele dann noch morgen?

Wer sagt, „Zwingt sie doch!“, dessen Position ist die regulatorische. Die Bürgerrechtsvereinigung *American Civil Liberties Union* (ACLU) geht bereits diesen Weg. Wenn Auto-Updates für Smartphones aber ein Gewährleistungsrecht werden, und dein Smartphone so ausgestattet ist, dass es gezielt dich als seinen Besitzer ausweist, wie lange dauert es dann, bis ein Gericht mit Verweis auf das Überwachungsgesetz *Foreign Intelligence Surveillance Act* (FISA) ein ganz spezielles Update für dich anordnet, um Beweise zu sammeln?

Eine verwaiste Code-Base quelloffen zu machen, ist die schlechteste Option – außer für alle anderen. Wenn diese Frage zu viel ist für dich vor dem Frühstück, dann fang mit einer PKI-CA an, die bankrott geht und fragt: „Wer bekommt jetzt die Schlüssel?“

10. Konvergenz? Ablehnung per default.

Ich habe eine Frage: Sind die digitale und die physische Welt eine oder zwei? Konvergieren oder divergieren *Cyberspace* und *Meatspace* mit der Zeit? Ich denke, sie konvergieren, aber wenn sie das tun, sieht dann der Cyberspace immer mehr aus wie der Meatspace, oder der Meatspace immer mehr wie der Cyberspace? Ich finde das nicht so klar (Abbildung 9).

Möglichkeit #1 ist, dass der Cyberspace immer mehr wie der Meatspace aussieht, und dann ist darin die Reproduktion geografischer und gesetzlicher Grenzen der nächste Schritt. Möglichkeit #2 ist, dass der Meatspace immer mehr wie der Cyberspace aussieht, und dann werden Gesetzesräume zunehmend irrelevant, und eine globale technokratische Regierung ist mehr oder weniger die Folge. Die erste Möglichkeit ist heterogen, die zweite ist die Monokultur eines Einzelstaates. Wir wir alle wissen, erwachsen Widerstandskraft

und Freiheit allein aus Heterogenität, also ist die Angleichung vom Meatspace an den Cyberspace nicht der Weg der Wahl, aber was können wir dagegen tun?

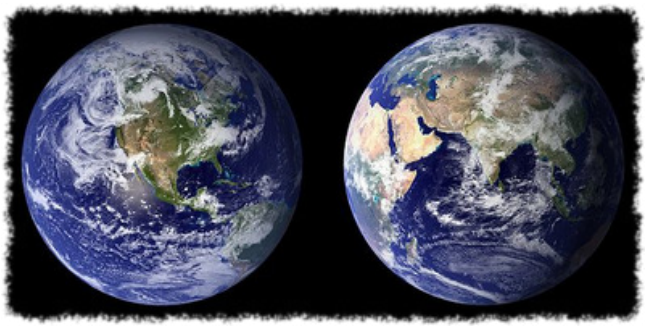


Abbildung 9: Zwei Welten – *Cyberspace* und *Meatspace*: Welche gleicht sich welcher an?

[Mitte] letzten Jahres bat [das amerikanische Meinungsforschungsinstitut] *Pew Research Center* 12.000 so genannte Experten, eine Ja-Nein-Frage zu beantworten: „Wird es im Jahr 2025 gegenüber heute signifikante Verschlechterungen und Hindernisse geben, Inhalte online zu teilen?“ [23] Von den 12.000 Gefragten antworteten um die 1.400. Mal beiseite gelassen, von welchen Vorurteilen die Antwortenden geleitet sein mögen, kristallisierten sich bei der Auswertung vier Leitideen heraus:

(1) Staaten werden mehr blockieren, filtern, segmentieren und das Internet balkanisieren mit dem Ziel, Sicherheit und politische Kontrolle zu gewährleisten.

(2) Im Gefolge des Bekanntwerdens behördlicher und unternehmerischer Überwachung schwindet Vertrauen vollends, was zu noch mehr Überwachung führt.

(3) Kommerzielle Zugzwänge in allen Bereichen des Internets, von der Infrastruktur bis zum Informationsfluss, gefährden die offene Struktur des digitalen Lebens.

(4) Um das Problem der Informationsflut zu lösen, wird man überkompensieren und am Ende Online-Sharing als Ganzes konterkarieren.

In persönlichen Korrespondenzen legte mein Kollege Rob Lemos mal die vier Leitideen von Pew über meine oben genannten zwei Konvergenzmöglichkeiten. Er sagte: „Wenn der Cyberspace sich unser physischen Realität angleicht, haben wir ein balkanisiertes Internet und kommerziell motivierte Informationsmonopole. Wenn sich die physische Welt der digitalen angleicht, dann haben wir mehr Überwachung, Vertrauensschwund, viele Informationslecks und Reaktionen auf diese Lecks.“ Noch folgenschwerer aber ist seine Beobachtung, dass die wachsende Technologie immens die persönliche Macht vergrößert hat:

> Jemand Einzelnes kann heute auf die Gesellschaft einen verheerenden Effekt haben. Die natürliche Reaktion einer Regierung darauf ist, stärker einzugreifen {Möglichkeit #2 von oben}, um die staatliche Monokultur zu schützen, oder mehr zu segmentieren {Möglichkeit #1 von oben}, um Bedrohungen draußen zu halten. Weil Bedrohungen und kinetische Impulse immer schneller durch die digitale Welt wandern, erfordern sie, dass die gesetzlichen Rahmenbedingungen der digitalen und physischen Welt konvergieren.

Mit anderen Worten: Lemos argumentiert, dass Konvergenz eine unvermeidliche Konsequenz des Cyberspace an und für sich ist. Ich zweifle nicht an der Idee, dass zunehmend mächtige, ortsunabhängige Technik in den Händen vieler quasi zwingend eine Machtverschiebung nach sich zieht. Das ist sogar die zentrale Leitidee dieses Essays: Die im Netz wachsende Macht übersteigt zeitnah unsere institutionellen Möglichkeiten, sie zu beeinflussen. Somit muss entweder das Internet in regierungsfähige Teile zerbrochen werden, oder das Netz selbst wird zur Regierung.

Abhängigkeit bedeutet Risiko

Ich habe den Eindruck, dem Cyberspace wird so oft wie blind die Monopolrolle zuerkannt. In den letzten Jahren sind digitale Einreichungen Pflicht geworden bei Institutionen, die ich mehr oder weniger gezwungen bin zu nutzen – etwa meine 401(k)-Verwaltung *[das ist so eine Art Betriebsrente, Anm. d. Übers.]*, die öffentliche Zahlkasse, die von meinem Arbeitgeber outgesourcte Lohnabrechnung. Das bedeutet, dass all diese Institutionen sich in entscheidende Abhängigkeit von einem Internet begeben haben, in dem sich Schwärme von *Men in the middle* aufhalten, und – mehr als das – sie haben zweifelsohne ihre Fähigkeit zu dem Fallback aufgegeben, der jahrhundertelang funktioniert hat.

Dieses Aufgeben aller Alternativen definiert im eigentlichen Sinne, was Konvergenz ist und

macht. Es heißt, Bürgerkriege gehen immer darum, zu wessen Bedingungen Einheit wieder hergestellt wird. Ich würde behaupten, dass wir uns gerade – um einen bekannten Begriff zu verwenden – in einem Kalten Bürgerkrieg befinden, zu welchen Bedingungen Konvergenz passiert. Alle lokalen und managbare Abhängigkeiten, was wir im Meatspace aufgeben, ersetzen wir mit Abhängigkeiten im Cyberspace, die mit Sicherheit nicht lokal und, würde ich sagen, weniger managbar sind, weil viel unsicherer. Ich sage dass, weil die Grundursache für Risiko Abhängigkeit ist, vor allem Abhängigkeit von den Erwartungen an das Staatssystem. Ich sage „viel unsicherer„, denn jemand ist genau dann sicher, wenn er keinen unbeherrschbaren Überraschungen ausgesetzt ist. Je mehr wir ins Internet verlagern, desto breiter und unbeherrschbar werden etwaige Überraschungen.

Langsam setzt sich dieser Gedanke bei einzelnen Leuten durch. Ich möchte etwas aus einem *Bloomberg*-Artikel [von Juli 2014] zitieren [24]:

> Laut einem internen Dokument des Wirtschaftsverbandes *Securities Industry and Financial Markets Association* fordert die größte Handelsgruppe an der Wall Street einen öffentlich-privatwirtschaftlichen *Cyber War Council*, um Terroristenangriffe abzuwehren, die mit vorübergehenden Kontoschwankungen eine Finanzpanik auslösen könnten. Das Dokument findet ungewöhnlich ehrliche und pessimistische Worte für die Lage der Industrie gegenüber terroristischen oder staatlichen Angriffen, die darauf abzielen, ‚Daten und Maschinen' zu zerstören. Es besagt, dass die Sorge ‚von der Abhängigkeit der Finanzinstitute vom Netz', das physikalisch und digital angreifbar ist.

Hier stehen also die größten Finanzunternehmen und sagen, ihre Abhängigkeit sei nicht mehr managbar und das staatliche Gewaltmonopol müsse Anwendung finden (Abbildung 10). Was sie sagen ist, dass sie keine Möglichkeit haben, das Risiko eines Mehrfach-Primärausfalls (*common mode failure*) zu entschärfen.

Ich wiederhole: Risiko ist die Konsequenz von Abhängigkeit. Wegen der miteinander geteilten Abhängigkeit ist die Zusammenschau der gesamtgesellschaftlichen Abhängigkeit nicht abschätzbar. Wenn Abhängigkeiten nicht abschätzbar sind, werden sie unterschätzt. Wenn man sie unterschätzt, wird man sie langfristig nicht absichern, höchstens kurzfristig. Weil das Zutagetreten des Risikos immer unwahrscheinlicher wird, verlängern sich die Zeitabstände zwischen Ereignissen. *[Gemeint sind hier vermutlich 'wahrgenommene' Ereignisse im Unterschied zu Ereignissen, die man eben nicht als einem bestimmten Risiko zugeordnet wahrnimmt. Anm. d. Übers.]* Wenn die Latenz von Ereignissen wächst, wächst auch die Annahme, man habe sich in Sicherheit gebracht, was der Abhängigkeit noch mehr Auftrieb gibt, womit wir in einer wortwörtlichen Feedbackschleife wären.

Abbildung 10: Ungehörte Warnung: Die Wall Street sagt, ihre Abhängigkeit vom Netz sei nicht mehr managbar. (Foto: Vlad Lazarenko bei Wikipedia, CC BY SA)

Hergebrachte Methoden und ein paar mehr Neins zum Internet bewahren alternative, weniger komplexe, aber dauerhaftere Mittel, und setzen somit der Abhängigkeit Grenzen. Abhängigkeit einzugrenzen ist der Kern rationalen Risikomanagements.

Wenn wir die Abhängigkeit nicht begrenzen, leisten wir einem systematischen Mehrfachausfall Vorschub. Im Fachjargon der Statistik kommt der systematische Mehrfachausfall exakt daher, dass man wechselseitige Abhängigkeiten unterschätzt. Das *National Institute of Standards and Technology* (NIST) sagt [25]:

> [R]edundanz ist die Einsatzbereitschaft von Funktionen, die in einem fehlerfreien System unnötig wären. Redundanz ist nötig, aber nicht ausreichend, um Fehlertoleranz zu erreichen. [...] Manchmal passiert es, dass ein Fehler genug redundante Funktionen in Mitleidenschaft zieht, dass es kein fehlerfreies Ergebnis mehr geben

> kann, woraufhin das System einen systematischen Mehrfachausfall erleidet. [...] Computersysteme sind anfällig für systematische Mehrfachausfälle, wenn sie sich auf eine singuläre Stromquelle, Kühlquelle oder Input-Output-Schnittstelle stützen. Eine heimtückischere Quelle für systematische Mehrfachausfälle besteht in einem Designfehler, der redundante Prozesse unter identischen Bedingungen versagen lässt.

Der letzte Satz ist genau das, was von Komplexität unkenntlich gemacht wird, weil Komplexität unterschätzte gegenseitige Abhängigkeit nach sich zieht.

Zusammenfassend: Es muss Richtlinien geben, dass jede offiziell als kritisch einzustufende Infrastruktur unter Beweis stellen muss, dass sie auch ohne das Internet funktioniert. Die Finanzkrise von 2008 beweist, dass wir Systeme haben, die zu komplex sind, als dass wir sie bedienen können, woraufhin sie angewiesen wurden, ein System von Stress-Tests zu haben. Wir brauchen viel mehr solcher Stress-Tests.

Rationaler Handlungsbedarf

Der späte Peter Bernstein (1919 - 2009), der vielleicht vorausschauendste Denker der Welt in dieser Sache, definierte Risiko als *Es kann mehr passieren, als passieren wird* ([26], [27]). Mit voranschreitender Technik bekommt dieser Ausspruch eine ziemlich bedrohliche Qualität, sofern es dein Job ist, das Überleben deiner Bürger in der internationalen Anarchie zu gewährleisten, in der jeden Tag zunehmend mehr passieren kann, als tatsächlich passiert. Realpolitisch würde man sagen, unter diesen Umständen wird Verteidigung irrelevant. Relevant ist nurmehr entweder (1) anzugreifen, oder (2) aus der Schusslinie uz kommen.

Staaten, die ins Angreifen investieren, verhalten sich völlig rational und überleben mit hoher Wahrscheinlichkeit. Diejenigen von uns, die sich der digitalen Welt mehr und mehr entziehen, verhalten sich völlig rational und überleben mit hoher Wahrscheinlichkeit. Die Massen derer, die sich schnell in Abhängigkeit von allem Neuen begeben, suchen das Risiko. Und auch, wenn sie es selbst nicht wissen, so wissen es doch die Staaten, zu denen sie gehören. Das erklärt, warum Staaten sich gegenüber ihren eigenen Bürgern so verhalten, wie sie es vorher nur gegenüber den Oberen konkurrierender Regimes getan haben.

Ihr habt Euch höflich von jemandem, den Ihr nie gewählt habt, ein paar Vorschläge angehört, die helfen mögen, zu Potte zu kommen. Ich danke Euch für Eure Aufmerksamkeit. Noch schöner fände ich aber, wenn welche von Euch das Ausdrucksvermögen fänden, um die herrschende Dynamik in den Griff zu bekommen. Namentlich: Wenn das Erfolgreiche richtig ist und das Erfolglose falsch ist, dann entkoppeln sich wahrnehmbarer Erfolg und Misserfolg komplett von den technischen Fakten der IT-Sicherheit. Am Ende siegt die Wirklichkeit. Und die Wirklichkeit technischer Fakten ist beständiger als Marktanteile oder utopischer Enthusiasmus.

Aber dennoch handelt IT-Sicherheit von Macht, und von nichts anderem. Die Realpolitik sagt, was wir IT-sicherheitstechnisch hinbekommen ist richtig, und was wir nicht hinbekommen ist falsch – daher schwingt Realpolitik im Einklang mit Howards *Security wird immer exakt so schlecht wie nur möglich sein, solange alles funktionieren soll*. Realpolitik sagt, wenn Angriff immer wieder Verteidigung besiegt, dann ist sie richtig, und dann ist es falsch, sich etwas anderes auszumalen. Sie sagt, die siegenden Angreifer sind im Recht, und die verlierenden Verteidiger sind im Unrecht. Die Überlegenheit des Angriffs bedeute, dass Informationen vor Durchsickern schützen zu können eine utopische Fantasie sei, und der einzig richtige Gegenangriff in Desinformation liege. Die Realpolitik sagt, dass Widersacher zum Leben gehören, aber dass sie nie zuvor ortsunabhängig waren und nie zuvor unbezahlte Söldner rekrutierten konnten. Die Realpolitik sagt, Zurückverfolgung ist unmöglich, es sei denn, wir etablieren einen Überwachungsstaat.

Lange habe ich Security-Fachleute bevorzugt, die sich schon mal die Finger verbrannt haben – die also trauriger, aber klüger sind. Sie, und nur sie wissen, dass kommerziell Erfolgreiches meistens nur so lange erfolgreich ist, wie Angreifer es nicht auf dem Schirm haben. Und dass kommerziell Erfolgloses nicht deswegen versagt, weil es nicht funktioniert, sondern weil es nicht billig oder einfach oder sexy genug war, es auszuprobieren. Sie schauen nicht durch eine rosarote Brille, sondern durch eine, die mit Realpolitik bespritzt ist.

Wer gebrannte Kinder bevorzugt, hat allerdings selbst schon mal im eigenen Umfeld tragische Erfahrungen gemacht. Und gebrannte Kinder gibt es nicht im globalen Maßstab – nicht für solch eine Angriffsfläche, die entsteht, wenn man alles mit allem vernetzt und den Moment verpasst, sich selbst

da herauszuziehen. Bis es solche Leute gibt, arbeite ich daran, meine eigene Abhängigkeit von der digitalen Welt zu reduzieren, und damit das Risiko, das ich eingehe. Auch wenn manche das als mürrische Nostalgie missverstehen. Nennt es Selbstverzerrung, wenn Ihr wollt [28].

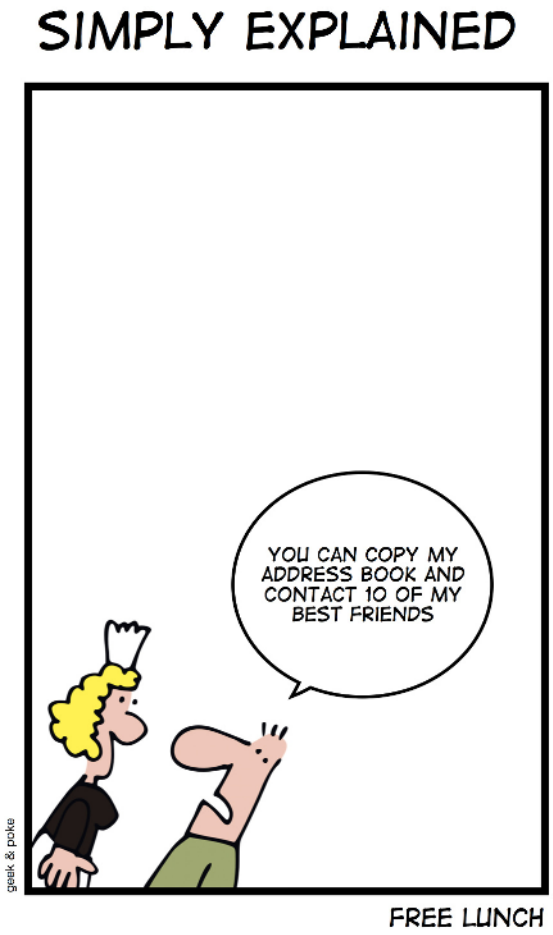
Hinweise und Referenzen

[1] Dan Geer, *Cybersecurity as Realpolitik*: http://geer.tinho.net/geer.blackhat.6viii14.txt
[2] George Santayana, 1863-1953, spanischer Philosoph, Vertreter des kritischen Realismus. Das Zitat stammt aus dem 1923 erschienenen Text *Scepticism and Animal Faith*.
[3] Der Originalsatz lautet: „I will take his comment as confirming at the highest level not only the dual use nature of cybersecurity but also confirming that offense is where the innovations that only States can afford is going on."
[4] Unternehmenstext aus dem Jahr 2008 *2% of Internet Traffic Raw Sewage*:
http://www.arbornetworks.com/asert/2008/03/2-of-internet-traffic-raw-sewage
[5] J.H. Saltzer, D.P. Reed and D.D. Clark: End-to-end arguments in system design. In: ACM Transactions on Computer Systems, Volume 2 Issue 4, Nov. 1984, Pages 277-288. Online erhältlich unter:
http://web.mit.edu/Saltzer/www/publications/endtoend/endtoend.txt
[6] Richard Danzig: http://www.cnas.org/danzigrichard
[7] Richard Danzig, *Surviving on a Diet of Poisoned Fruit; Reducing the National Security Risks of America's Cyber Dependencies*: http://www.cnas.org/surviving-diet-poisoned-fruit
[8] Ken Thompson, *Reflections on Trusting Trust*, Rede zum *Turing Award* 1983:
http://amturing.acm.org/award_winners/thompson_4588371.cfm
[9] *Codex Hammurapi*, Sammlung von Rechtssprüchen des altbabylonischen Königs Hammurapi, 18. Jh. v.Chr.: http://avalon.law.yale.edu/ancient/hamframe.asp
[10] Übersetzung des Codex-Hammurapi-Auszuges nach Gerhard Köbler:
http://www.koeblergerhard.de/Fontes/CodexHammurapi_de.htm
[11] Online-Artikel *Microsoft and FBI team up to take down GameOver Zeus botnet*:
http://www.techradar.com/us/news/internet/web/microsoft-and-fbi-team-up-to-take-down-gameover-zeus-botnet-1251609
Siehe auch in deutscher Sprache: http://www.heise.de/thema/Zeus
[12] CVE: http://cve.mitre.org/cve
[13] DefCon-Aktion *SOHOpelessly Broken*: http://www.sohopelesslybroken.com
[14] Bruce Schneier: *Should U.S. Hackers Fix Cybersecurity Holes or Exploit Them?*
http://www.theatlantic.com/technology/archive/2014/05/should-hackers-fix-cybersecurity-holes-or-exploit-them/371197
[15] Einstiger Online-Artikel *Hunt Brothers Corner Silver Market*:
http://web.archive.org/web/20060118031501/http://www.wallstraits.com/main/viewarticle.php?id=1298
[16] Dan Geer, *We Are All Intelligence Agents Now*: http://geer.tinho.net/geer.rsa.28ii14.txt
[17] Die Originalphrase lautet: „the effective capacity to misrepresent yourself". Die auf die eigene Identität bezogene *Misrepresentation* übersetzt dieser Text im Folgenden stets mit *Selbstverzerrung*.
[18] Der Originalausdruck lautet: „the big-I Intelligence trade".
[19] *National Strategy for Trusted Identities in Cyberspace* (NSTIC): http://www.nist.gov/nstic
[20] Anm. d. Übers. – In Deutschland dürfte der US-NSTIC die *Nationale E-Government Strategie* (NEGS) entsprechen: http://www.it-planungsrat.de/DE/Strategie/negs_node.html
[21] Anm. d. Übers. – Synopse der entsprechenden EuGH-Rechtsprechung vom 13.05.2014, AZ C-131/12:
http://dejure.org/dienste/vernetzung/rechtsprechung?Gericht=EuGH&Datum=2014-05-13&Aktenzeichen=C-131%2F12
[22] Online-Artikel *The Right to Be Forgotten Will Turn the Internet into a Work of Fiction*:
http://www.theguardian.com/commentisfree/2014/jul/06/right-to-be-forgotten-internet-work-of-fiction-david-mitchell-eu-google
[23] Pew-Studie *Bedrohungen aus dem Netz*: http://www.pewinternet.org/2014/07/03/net-threat
[24] Online-Artikel *Banks Dreading Computer Hacks Call for Cyber War Council*:
http://www.bloomberg.com/news/print/2014-07-08/banks-dreading-computer-hacks-call-for-cyber-war-council.html

[25] *High Integrity Software System Assurance*, Abschnitt 4.2. URL, nicht mehr online: http://hissa.nist.gov/chissa/SEI_Framework/framework_16.html
[26] Peter Bernstein: Against the Gods; The Remarkable Story of Risk. Hoboken/New Jersey, John Wiley & Sons 1998.
[27] *Peter Bernstein on risk*, Video von 2008: http://www.mckinsey.com/insights/risk_management/peter_l_bernstein_on_risk
[28] Der Originalsatz lautet: „Call that misrepresentation, if you like."

Über Dan

Dans Biografie ist – lang. Wir erlauben uns, einfach mal auf seine Webseite zu verweisen: http://geer.tinho.net/geer.bio.txt



Weil es so schön ist
Betriebliche IT-Dokumentation in der Praxis (I)

Was man nicht im Kopf hat, muss man in den Beinen haben, heißt ein Sprichwort. Auf das IT-Office gewendet muss es heißen: Was man nicht im Kopf hat, hat jemand anderes hoffentlich aufgeschrieben. Wie das in der Praxis aussieht, hat die UpTimes mit einer Umfrage erhoben.

von **Anika Kehrer**

Eine Investition in Wissen
bringt immer noch die besten Zinsen.

Benjamin Franklin

Verwaiste Wikiseiten, wuchernde Verzeichnisstrukturen und kryptische Dokumente sind nichts, was dem Ratsuchenden dienlich ist. Sie entstehen aber quasi von selbst, wenn keiner dauerhaft ein Auge darauf hat. Genau das passiert aber nicht, weil Admins, Engineers und Systemarchitekten in der Regel etwas anderes zu tun haben, als Schriftstücke zu erstellen oder zu managen. Zum mehr der weniger großen Problem wird das, wenn die Kollegen, die sich auskennen, nicht da sind, wenn neue Mitarbeiter ohne Innenperspektive zeitraubende Erklärungen brauchen, oder wenn Systemzusammenhänge zu komplex sind, als dass sie ein oder auch zwei paar Augen noch ernsthaft überblicken könnten – bei der Einschätzung von Changes etwa.

So weit, so klar. Unklar ist hingegen, was genau in welcher Form und an welchem Ort am besten niedergelegt werden sollte, damit es im Bedarfsfall erreichbar und nutzbar ist. Während es für technische Produktdokumentation Vorschriften und ganze Standards gibt, ist die IT-Abteilung auf sich selbst gestellt, was ihr Wissensmanagement angeht. Im praktischen Alltag ist selten Thema, dass man mal etwas aufschreiben sollte, oder gar, dass das Zeit braucht. Nicht selbstverständlich ist auch Kenntnis davon, dass Aufgeschriebenes nicht zwingend die Information enthält, die aufzuschreiben das Ziel war – nur, was dort steht, kann jemand anderes erfahren, und nicht zusätzlich auch noch das, was der Verfasser beim Schreiben dazu im Hinterkopf hatte.

Diese Herausforderungen laufen mal eben so nebenbei mit. Wie bekommen IT-ler sie in den Griff? Die Umfrage der UpTimes will das herausfinden.

56 Praxis-Snapshots

Auskunft erhielten wir von insgesamt 56 IT-Mitarbeitern. Die allermeisten davon sind sehr erfahren: Über 80 Prozent von allen arbeiten seit mehr als zehn Jahren im IT-Bereich (47 Teilnehmer), gut 60 Prozent von allen seit mehr als 16 Jahren (36 Teilnehmer). Entsprechend konzentriert sich die Altersgruppe auf Menschen zwischen 40 und 50 Lebensjahren (22 Teilnehmer = 40 Prozent), wonach die 30-bis-40-Jährigen den zweitstärksten Anteil bilden (18 Teilnehmer = 33 Prozent) und die 50-bis-60-Jährigen den drittstärksten (10 Teilnehmer = 18 Prozent).

Hinsichtlich der Unternehmensgröße haben vermehrt solche Fachleute an der Umfrage teilgenommen, deren Betrieb insgesamt zwischen 100 und 300 Mitarbeiter (13 Teilnehmer = 23 Prozent) oder aber über 1000 Mitarbeiter zählt (18 Teilnehmer = 32 Prozent). Ein paar Endrücke kommen hinzu aus der IT-Doku-Praxis von Firmen mit 50 bis 100 sowie 300 bis 1000 Mitarbeitern (je 8 Teilnehmende, was rund 13 Prozent entspricht).

Wie man in en Klammern sehen kann, ziehen einige wenige Teilnehmer mehr oder weniger bei der vorliegenden, relativ kleinen Datenbasis Schwankungen im Bereich von mehreren Prozent nach sich. Mit dieser Schwäche müssen wir leider leben. Die Aussagen sind entsprechend mit Vorsicht zu genießen. Dieser Disclaimer ist nötig, auch wenn Tendenzen und Korrelationen innerhalb der vorliegenden Stichprobe dennoch informativ sind. Sie wurden mit entsprechender Vorsicht erstellt und mögen auch so aufgenommen werden. Die Datenbasis zu vergrößern, ist ein Weg, die Situation in Zukunft zu verbessern (siehe Kasten *Appell: Vergrößerung der Datenbasis*).

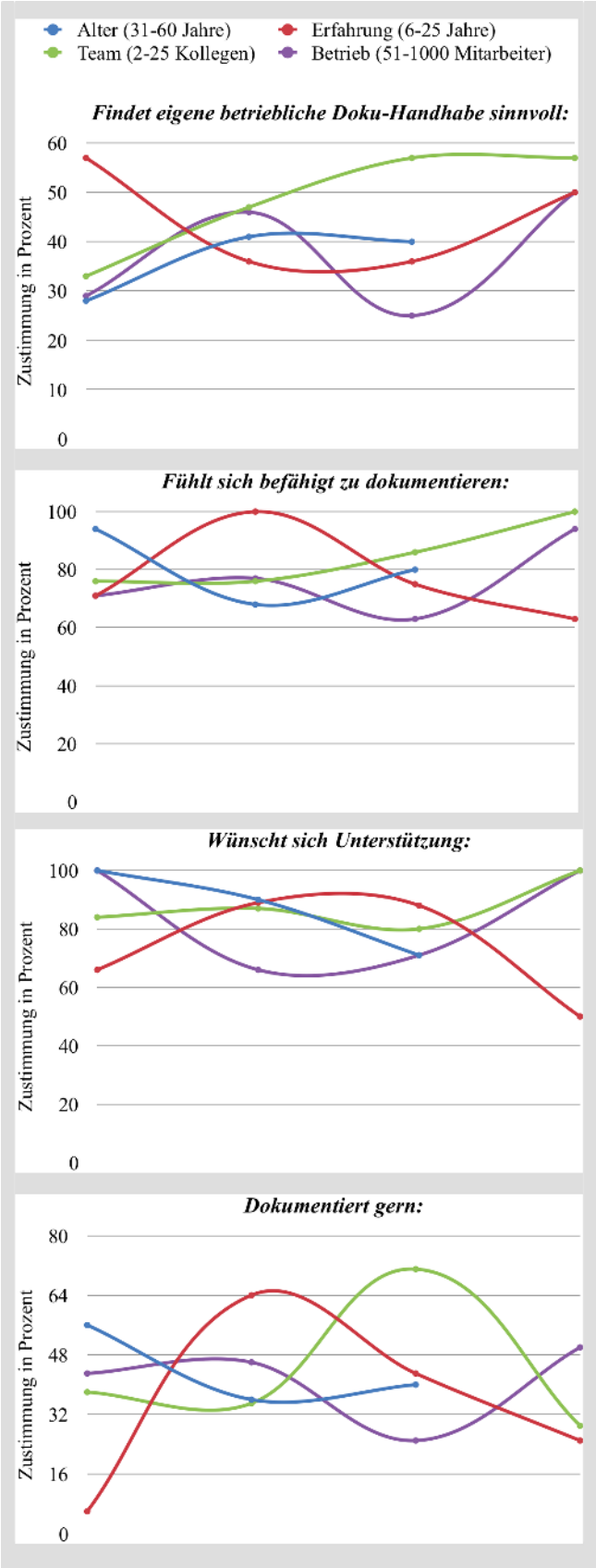


Abbildung 1: Korrelationen individueller Umstände mit verschiedenen Eigenschaften der betrieblichen Dokumentation. Der Nullpunkt auf der X-Achse entspricht jeweils dem kleinsten Wert der Ranges: *Alter* fängt bei 31 an und endet bei 60, *Team* beginnt bei 2 und endet bei 25, und so weiter.

Erhebung: *Wer, wie, was*

Die Umfrage interessiert sich – neben der peniblen Befragung nach Merkmalen des Teilnehmenden zum Zwecke der Umstandsbestimmung (Abbildung 1) – für zwei Bereiche: Wie wird dokumentiert, und was wird dokumentiert. In diesem Teil I der Auswertung kommt nicht alles auf den Tisch, was die Zahlen verraten, denn das hat die Zeit nicht erlaubt. Erst Teil II der Auswertung wird beispielsweise genauer unter die Lupe nehmen, wo die größten Stärken und Schwächen bei den Inhalten der Doku liegen, wie groß der Aufwand ist, und vor allem, ob Zusammenhänge mit dem *Wie* bestehen.

Teil I beantwortet zunächst die Fragen, mit welchen Methoden die Teams operieren, wie zufrieden sie sind, aus welchen Gründen sie etwas aufschreiben, welche Attribute die Dokumentation derer auszeichnen, die extrinsisch motiviert sind gegenüber jenen, die intrinsisch motiviert sind, welche Attribute jene mitbringen, die ihre Dokumentation im Großen und Ganzen sinnvoll beziehungsweise nicht sinnvoll finden – und so weiter.

Git- und SVN-Nutzer am zufriedensten

Eine Frage erhob mittels Mehrfachantwort, welche Medien, Formate und Speicherorte die Teilnehmer nutzen. Für Außenstehende ist das Kuddelmuddel an Tools und Methoden erstaunlich.

Praktisch alle nutzen ein Wiki. Das ist (natürlich) kein Erfolgsgarant: Die Geister der 51 Umfrageteilnehmer, die ein Wiki nutzen und außerdem ihre innerbetriebliche Doku alles in allem sinnvoll finden, scheiden sich ziemlich genau in der Mitte. Die fünf Teilnehmer, die kein Wiki nutzen, schreiben in Text- oder Office-Dateien und tauschen sie via Git oder Netzlaufwerk aus. So richtig sinnvoll finden diese fünf nicht, wie bei ihnen die Doku funktioniert, zum Teil auch deswegen, weil sie erst im Aufbau befindlich ist, oder weil unklar ist, wie eine sinnvolle Doku überhaupt aussehen sollte.

Überraschend ist, dass viele drei Arten nutzen, um zu dokumentieren, zum Beispiel eine Kombination aus Wiki, Git und Office-Programm; oder Office-Programm, Wiki und Inventarisierungs-Software. Die Anzahl der Zufriedenen ist in dieser Gruppe der Dreiwege-Nutzer am höchsten (13 Zufriedene von 18 mit drei Arten = gut 70 Prozent).

Appell: Vergrößerung der Datenbasis

Um die Datenbasis für die Erhebung der praxisnahen betrieblichen IT-Dokumentation zu erhöhen, brauchen wir mehr Datensätze. Das erste Rollout erfolgte binnen drei Wochen und schöpfte aus zwei Kanälen: aus der *Google-Plus*-Blase rund um den GUUG-Account sowie dessen *Twitter*-Stream, und aus der Mailingliste *SAGE@guug.de* mit rund 400 Subskribenten, deren Aktivität aber sehr unterschiedlich ist. Für eine Information mit Appellcharakter, die auf Streuung angewiesen ist, waren das wenig Kanäle in recht kurzer Zeit.

In ihrem ersten Rollout verzeichnete die Umfrage 56 auswertbare Datensätze. Für die genannten Umstände ist das nicht so schlecht. Es genügt aber nicht, um die Realität abzubilden, selbst wenn man nur die unixoide Sparte zu Grunde legt. Um das Bild nicht zusätzlich zu verzerren, sind Einzelgruppen mit weniger als sechs Repräsentanten in manchen Fragen kein Teil der Auswertung. Folgende Gruppen betrifft das: Jüngere zwischen 20 und 30 Jahren, Teamgrößen zwischen 15 und 25 Mitgliedern, Arbeitnehmer in Betrieben mit weniger als 50 Mitarbeitern.

Die UpTimes-Redaktion appelliert an die Leser, die Umfrage zu streuen. Wir beabsichtigen, sie dauerhaft online zu lassen, damit sich im Laufe der Zeit die Datenbasis vergrößert. Jeweils, wenn die Zahl 50 neuer Datensätze erreicht ist, erfolgt eine Aktualisierung der Auswertung.

Darauf möchten wir aber am liebsten nicht 20 Jahre warten. Wer also diese empirische Erhebung zu Lehrzwecken für bessere betriebliche Dokumentation gut findet, streue sie bitte so weit wie möglich im deutschsprachigen Raum (die Umfrage steht zunächst nur in Deutsch zur Verfügung). Die Umfrage ist unter [1] erreichbar.

Auf vier verschiedene Arten zu dokumentieren, macht zwar nicht ganz so zufrieden, ist aber nicht der Knackpunkt. Eindeutig unzufrieden sind vielmehr die neun Teilnehmer, die nur eine Technologie nutzen – das ist dann ein Wiki und nichts sonst – oder die anderen neun Teilnehmer, sich mit fünf oder mehr Technologien wohl doch etwas verzetteln.

Überraschend ist die Aussage, dass drei Wege glücklich machen, deshalb, weil man ja annehmen könnte, wenig Entscheidungsspielraum erleichtert das Leben – also möglichst wenig verschiedene Wege zu dokumentieren. Diese Faustregel scheint nicht zuzutreffen. Womöglich liegt das daran, dass es darum geht, etwas Komplexes wie einen IT-Betrieb zu dokumentieren.

Absolut betrachtet finden diejenigen, die Git oder SVN nutzen, ihre Doku am sinnvollsten (20 Zufriedene von 32 Git/SVN-Nutzern = 63 Prozent). An zweiter Stelle folgen mit 45 Prozent die glücklichen Wiki-Nutzer, denen aber ebenso viele explizit unzufriedene Wiki-Nutzer gegenüberstehen. Insgesamt eher unzufrieden sind diejenigen, die Papier nutzen, die mit einem Office-Programm dokumentieren, oder die eine Software in ihre Doku integrieren (etwa Inventarisierung, Web-Apps, Projektmanagement, ein Ticket- oder Servicemanagement-System).

Doku-QA selten und zufriedenstellend

Auf die Frage, ob sie ihre Doku-Situation im Großen und Ganzen sinnvoll finden, äußerte sich von den 56 Teilnehmenden eine leichte Mehrheit mit Nein (57 Prozent = 32 Teilnehmer), eine kräftige Minderheit mit Ja (43 Prozent = 24 Teilnehmer). Zu den Neinsagern sind in dieser Auswertung auch die vier Teilnehmer gezählt worden, die ausweichend geantwortet haben: Sie wüssten gar nicht, wie eine sinnvolle Doku aussehen könnte. Das ist der Punkt, an dem Standards oder Best Practices fehlen, oder zumindest ein gewisses Monitoring, wie sinnvoll der Doku-Prozess abläuft und eingebunden ist. Sprich: QA.

Qualitätssicherung der Dokumentation erfolgt in den allerwenigsten Teams. Aber sie scheint zu fruchten: Die 11 Teilnehmer, die eine dedizierte oder zumindest eine gewisse Qualitätssicherung bejahten, sind ganz überwiegend auch zufrieden mit ihrer Dokumentation (8 Zufriedene von 11 Teilnehmern mit QA = gut 70 Prozent). Die 45, die keine oder nur in Ausnahmefällen die Qualität ihrer Dokumente sicherstellen, sind mehrheitlich, nämlich zu 60 Prozent, unzufrieden mit ihrer Doku-Situation (entspricht 25 Unzufriedenen von 45 Teilnehmern ohne QA).

Auf der anderen Seite finden damit immerhin 40 Prozent derer, die ohne QA auskommen, ihre Dokumentation ganz sinnvoll so. Die Relevanz einer wie auch immer gearteten QA – angefangen bei Prozessstandardisierung über regelmäßigen Reviews bis hin zu ganzen Redaktionskonferenzen – ist auf der vorliegenden dünnen Datenbasis leider noch nicht verlässlich zu bestimmen.

Attribute der Zufriedenen und Unzufriedenen

Drei der fünf Diagramme zeigen interessante Nuancen. Erstens würden sich unter den Zufriedenen, die keinerlei Unterstützung für ihre Betriebsdoku genießen, fast alle über eine mögliche Unterstützung freuen. Der prozentuale Anteil der Unzufriedenen hingegen, die offen für Unterstützung sind, ist runde 20 Prozent kleiner (75 Prozent statt 95 Prozent). Zweitens arbeiten die Zufriedenen deutlich mehr mit Vorlagen als Hilfsmittel, während sich unter den Unzufriedenen mehr befinden, die keine Vorlagen haben, und sie sich aber wünschen.

Drittens ist der Anteil der rein intrinsisch Motivierten unter den Unzufriedenen höher. Ob der Faktor *externe Unterstützung* – etwa durch den Arbeitgeber – tatsächlich positive Auswirkung auf eine sinnvolle Betriebsdokumentation hat, liegt nahe, insbesondere, wenn Zeit dafür budgetiert wird. Obwohl fünf Teilnehmer von allen aus eigenem Antrieb, also ohne explizite Nachfrage, Zeitmangel für die Doku anprangerten, kann die Datenbasis dennoch nicht die These be- oder widerlegen, dass der Ball beim Arbeitgeber liegt. Dafür ist sie noch zu klein.

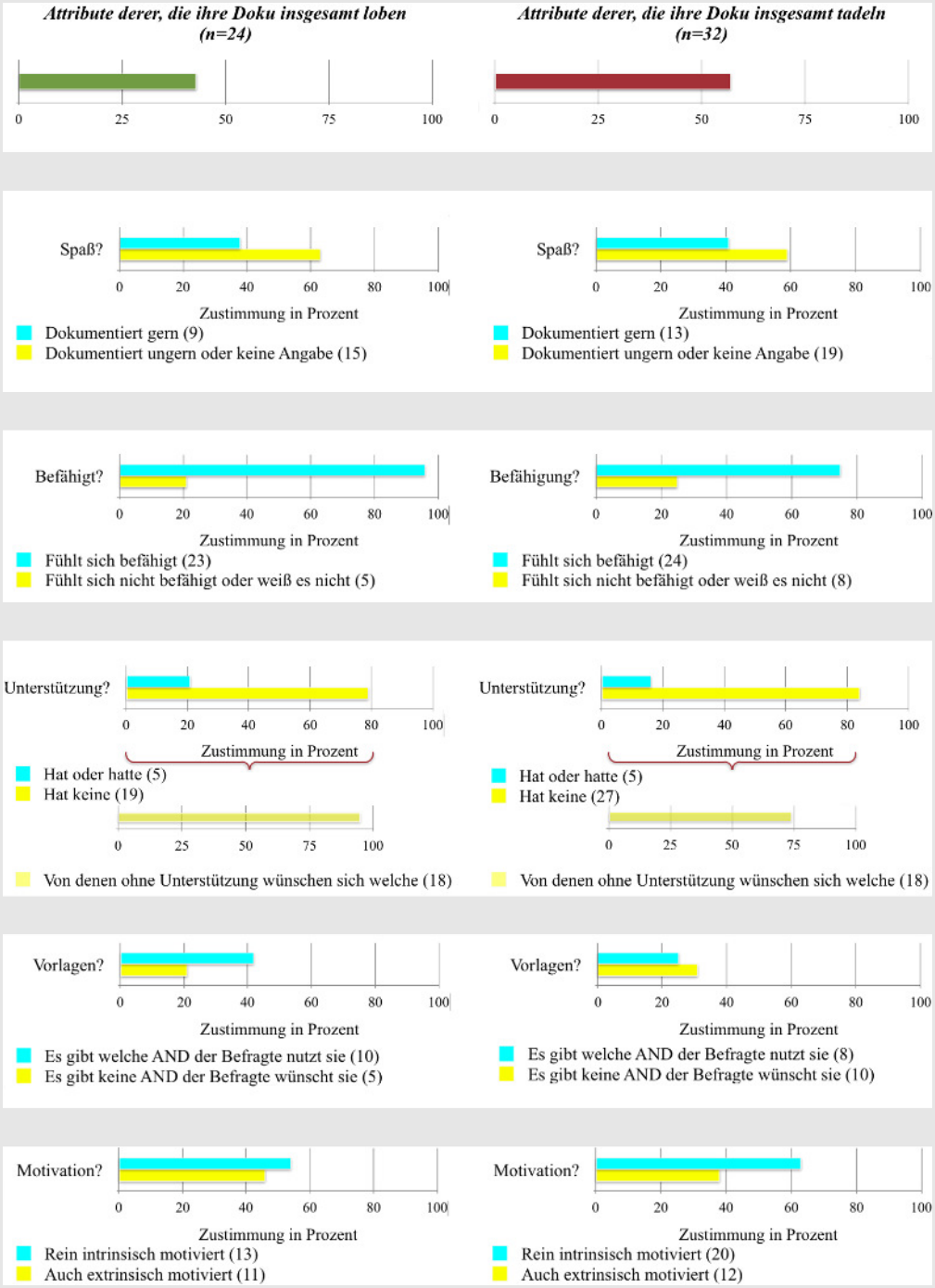


Abbildung 2: Eigenschaften der mit ihrer internen IT-Dokumentation Zufriedenen und Unzufriedenen.

Dass jeweils grob die Hälfte aller Befragten ihre Doku-Situation insgesamt sinnvoll oder nicht sinnvoll finden – egal ob mit oder ohne QA – ist hingegen eine recht deutliche Aussage: Die einen machen was richtig, die anderen machen was falsch. Welche Eigenschaften sie jeweils aufweisen, kann hoffentlich teilweise helfen, die eigene Praxis nachzujustieren.

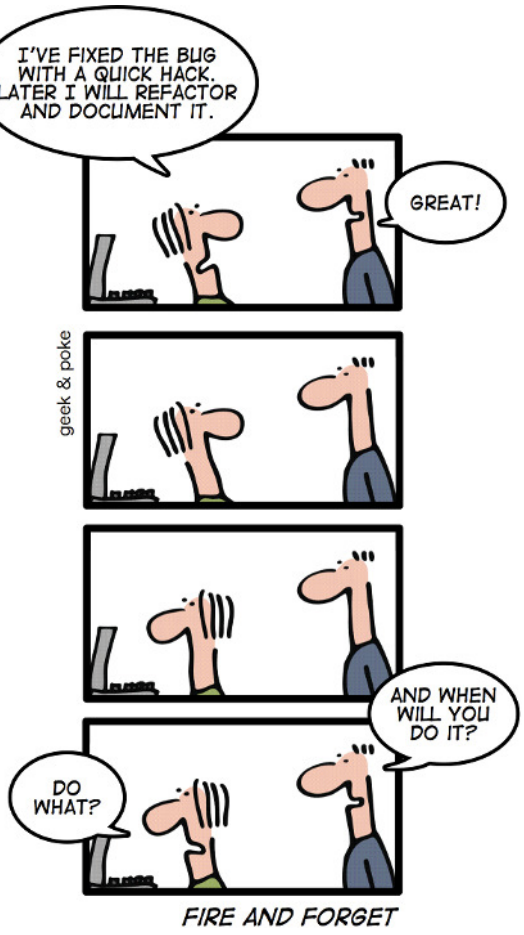
Förderliche und hinderliche Attribute

Korreliert man die Zufriedenheit mit anderen Eigenschaften, lassen sich zwei Typen malen: die Zufriedenen und die Unzufriedenen. Der typische mit seiner betrieblichen Doku zufriedene IT-ler ist nach den vorliegenden Daten zwischen 40 und 50 Jahre alt, hat zwischen sechs und zehn Jahren Erfahrung in der Branche, arbeitet in einem mittelgroßen Team ab sechs Kollegen für eher große Unternehmen mit über 1000 Angestellten. Er hat ein technisches Studium absolviert und bezieht seine Motivation, Dinge aufzuschreiben, überwiegend aus eigenem Antrieb, aber mit Unterstützung durch extrinsische Motive wie Vorgabe durch Arbeitgeber oder Zertifizierungen.

Nach dieser Darstellung scheinen grundlegende Erfahrung, eine große Unternehmensgröße, eine nennenswerte Anzahl an Kollegen und extrinsische Unterstützung zur empfundenen Sinnhaftigkeit der internen Dokumentationspraxis beizutragen.

Der typische mit seiner betrieblichen Doku unzufriedene IT-ler ist älteren Jahrgangs, hat bereits in Dekaden messbare Berufserfahrung und arbeitet in kleineren Teams innerhalb KMU ab 50 Mitarbeitern. Sein fachlicher Hintergrund besteht aus einer technischen Ausbildung, und zu seiner mehrheitlich intrinsischer Motivation tritt weniger Unterstützung von außen, als bei den Zufriedenen. Nach dieser Darstellung scheinen langjährige Erfahrung – möglicherweise Resignation –, eine kleinere Unternehmensgröße, wenig Kollegen und wenig Motivation von außen zur empfundenen Sinnlosigkeit der internen Dokumentationspraxis beizutragen.

Eine genaue Gegenüberstellung einzelner Eigenschaften von Zufriedenen und Unzufriedenen zeigt Kasten *Attribute der Zufriedenen und Unzufriedenen*, in dem es nur um diese zwei Gesamtgruppen geht – also nicht unterschieden nach individuellen Kontexten. Wie die dortige Abbildung 2 zeigt, gibt es bei zwei der fünf verglichenen Eigenschaften kaum Unterschiede zwischen Zufriedenen und Unzufriedenen: Beide Gruppen dokumentieren mehrheitlich ungern, fühlen sich prinzipiell befähigt, Dinge sinnvoll aufzuschreiben, und die wenigsten hatten Unterstützung für ihre Dokumentation. Beide Gruppen schreiben Dinge vor allem deswegen auf, um selbst und im Kollegenkreis besser arbeiten zu können, und nicht etwa, weil es ihnen jemand vorschreibt. Nennenswerte Unterschiede zeigen lediglich die Eigenschaften *Wunsch nach Unterstützung*, *Vorlagennutzung* und *Motivation*.



In der Sommer-Ausgabe 2016 der UpTimes Ende Juni 2016 erscheint Teil II der Auswertung. Die Umfrage wird online blieben: Da die Aussagekraft der Ergebnisse mit der Größe der Datenbasis steigt, bittet Kasten *Appell: Vergrößerung der Datenbasis* herzlich um Streuung des Umfragelinks [1] unter Fachkollegen und Bekannten in anderen Betrieben. Und um Eure eigene Teilnahme, natürlich!

Links

[1] Umfrage *Betriebliche IT-Dokumentation in der Praxis*: http://goo.gl/forms/9E6ev2ICVi

Reflexion
Fachartikel schreiben

Mündlich geht am schnellsten. Wozu sich also die Mühe machen? Eine Antwort: Aus Erkenntnisinteresse – und aus Stolz. Der Autor berichtet aus seiner Erfahrung, indem er sie mit den Vortragsfolien *Fachartikel schreiben* vom Frühjahrsfachgespräch 2015 [1] abgleicht.

von **Mathias Weidner**

Kein Autor sollte als
gescheitert angesehen werden,
bevor er nicht angefangen hat,
anderen das Schreiben beizubringen.

Nassim Nicholas Taleb, Kleines Handbuch für den Umgang mit Unwissen

In etlichen Bereichen hat mündliche Tradition und direkte Überlieferung vom Lehrer zum Schüler einen höheren Nutzen als schriftliche Texte. Wer zum Beispiel in den Urlaub fährt, kann mühsam alles für seine Vertretung aufschreiben, nur um dann doch angerufen zu werden, weil etwas vergessen wurde oder für die Vertretung unklar war. Wer es hingegen vorher erzählt und da dabei zuschaut, wie die Vertretung es testweise selbst umsetzt, erkennt sofort, wo etwas unklar ist.

Denn bei einem geschriebenen Text weiß der Verfasser nicht, wie sein Leser das Geschriebene versteht. Es sei denn natürlich, der Leser macht sich die Mühe, den Autoren anzusprechen und nachzufragen.

Warum also mühsam Fachartikel schreiben? Noch dazu für eine Leserschaft, die ich als Autor nicht kenne! Einen Leser allerdings kenne ich sehr gut: Mich selbst. In der Tat schreibe ich selbst zum Beispiel die meisten meiner Texte in erster Linie für mich, erst in zweiter Linie für andere. Ich schreibe etwa, um ein Thema abzuhaken und den Kopf frei zu bekommen für Neues. Oder ich schlage alte Texte bei Problemen nach, die ich vor Monaten oder Jahren bereits gelöst hatte.

Kollateraleffekte

Bei unveröffentlichten Notizen sitze ich dann allerdings manchmal da und frage mich: Was meinte ich da wohl? Ich profitiere also davon, etwas verständlich aufzuschreiben. Ein Text, den ich zur Veröffentlichung vorsehe, ist für mich ein Ansporn, verständlich zu schreiben.

Dabei stelle ich oft fest, dass ich mich intensiver mit dem Stoff befassen muss, als es für eine schnelle Lösung des ursprünglichen Problems nötig ist. Ich finde dann plötzlich eine Menge weiterer Aspekte zum Thema, die es mir immer vertrauter machen. So lerne ich nebenbei das Thema besser kennen. Und durch das intensive Bearbeiten des Stoffes wird meine Aufmerksamkeit geschärft: Mir fallen Details und Zusammenhänge auf, denen ich sonst keine Beachtung geschenkt hätte.

Das hat allerdings einen negativen Effekt für mein Vorhaben: Der Stoff explodiert (Abbildung 1). Was als eher kleiner Text von drei bis vier Seiten geplant war, wächst auf einmal auf zehn, zwanzig oder gar noch mehr an. An dieser Stelle wird die Frage des Texttyps relevant, was genau ich da schreibe – etwa eine Themendarstellung oder eine Anleitung als Fachartikel, oder doch eher als Buch. Dazu später mehr.

Abbildung 1: Achtung, Explosionsgefahr: Ein kleines Problem führt während der Recherche hierhin und dorthin, und plötzlich explodiert das Thema – und der Seitenumfang – in vielen Farben. (Foto: Sam Churchill bei Flickr, CC BY)

Zunächst hat das Scheiben für die Öffentlichkeit einen weiteren Nebenaspekt: Ich verbessere mein Deutsch. Denn um mich verständlich auszudrücken, muss ich das Thema in klare Sprache fassen. In diesem Punkt unterscheidet sich

das Schreiben übrigens nicht vom Programmieren. Schreibe ich ein neues Programm, lerne ich etwas über die Programmiersprache dazu. Auch als Systemadministrator lerne ich beim Konfigurieren eines komplexen Systems für eine neue Aufgabenstellung das System besser kennen. Beim Schreiben ist es eben die deutsche Sprache. Analog gilt das natürlich genauso, wenn jemand in einer Fremdsprache schreibt.

Und dann ist da das Publizieren. Nach der Veröffentlichung passiert etwas. Manche Leute, die sich in dem Fachgebiet auskennen, lesen den Artikel und lernen mich als Diskussionspartner kennen. Andere sind lediglich interessiert am Thema und nehmen mich als möglichen Berater wahr. Wieder andere lesen den Artikel gar nicht, höchstens die Überschrift, und halten mich dann für einen Experten. Auf die eine oder andere Art werde ich von mehr Leuten wahrgenommen als vorher. Natürlich füttert das mein Ego: der Stolz, etwas geschafft zu haben, etwas vorweisen zu können. Ich bin natürlich nicht ganz klein. Aber wenn ich auf einen veröffentlichten Artikel angesprochen werde, erscheine ich doch gleich etwas größer.

Schließlich kommt das Feedback. Oder auch nicht. Für mich persönlich ist kein Feedback zu einem Artikel schlimmer als negatives Feedback, denn Letzteres trägt für mich zum Lerneffekt bei. Und etwas zu lernen, ist eine meiner persönlichen Triebfedern, überhaupt erst einen Artikel zu schreiben.

Ich musste allerdings erst lernen, mit negativem Feedback umzugehen. Ein sachlicher, konstruktiver Hinweis in freundlichem Ton auf Fehler im Text lässt sich erst erst dann als positives Feedback begreifen, wenn man bereit ist, Fehler zuzugeben. Schlimmer ist direkte Konfrontation in unfreundlichem Ton, womöglich noch unsachlich. Wer kennt das nicht: Alle Klappen gehen runter, und es ist Kampfmodus angesagt. Zu allem Überfluss gerät man früher oder später an jemanden, der bei aller Unfreundlichkeit und Unsachlichkeit auch noch recht hat. Ich persönlich habe mir angewöhnt, solche Kritiken später noch einmal auf sachliche Hinweise abzuklopfen, wenn ich mich abgekühlt habe. Manchmal kommt dann doch noch etwas für mich heraus. Und wenn nicht, dann brauche ich wenigstens kein schlechtes Gewissen zu haben, wenn ich die Kritik ignoriere.

Es gibt es noch weitere Nebeneffekte des Publizierens, zum Beispiel Geld. In der Tat kompensiert das aber in den wenigsten Fällen den eingebrachten Aufwand. Wer vom Schreiben von Fachartikeln oder Büchern leben kann, braucht diesen Text hier nicht zu lesen und kann getrost weiterblättern.

Wer kann Fachartikel schreiben?

Ich denke, dass jeder, der bis hierhin dabei geblieben ist, selbst Fachartikel schreiben kann. Ich würde sogar sagen: Er sollte. Selbst wenn der Artikel am Ende nicht veröffentlicht wird, macht die Erfahrung des Schreibens reicher. Man schaut dann mit anderen Augen auf das, was man so liest.

Zwei Dinge vor allem sind es, die durch das eigene Schreiben meinen Blick auf andere Texte verändert hat: Zum einen setze ich mich mit einem Thema, über das ich schreiben möchte, so intensiv auseinander, dass ich in anderen Texten viel mehr Details dazu erkenne. Zum anderen setze ich mich durch das Schreiben so viel mit Rechtschreibung, Grammatik und Stil auseinander, dass ich unwillkürlich andere Texte danach beurteile, wie lesbar sie geschrieben sind (Abbildung 2).

Abbildung 2: Wer selbst daran arbeitet, verständlich zu schreiben, schärft den Blick dafür, wie lesbar andere Artikel geschrieben sind. (Foto: Anika Kehrer, CC BY SA)

Anika Kehrer gibt auf ihren Folien zur Frage des Wer eine Reihe Gegenfragen, von denen eine lautet: „Hast du etwas zu sagen?“Was man zu sagen haben könnte, wurzelt ihrer Darstellung nach in drei Punkten: Interesse, Kompetenz, oder Perspektive.

Interesse setze ich voraus. Alles andere wäre Zwang, daher hätte ich das nicht extra erwähnt. Ich kann mir im Moment auch nicht vorstellen, dass jemand, der vorher kaum als Autor hervorgetreten ist, zu einem Thema verpflichtet werden könnte, das ihn nicht interessiert.

Ich halte Kompetenz für die wichtigste Voraussetzung zum Schreiben. Darunter verstehe ich eigene Erfahrungen mit dem Thema. Natürlich kann man sich auch durch viel Lesen viel Wissen aneignen und damit in vielen Situationen Fragen

beantworten – auch solche, die gar nicht gestellt wurden. Aber das ist für mich keine Kompetenz. Viel Lesen halte ich zwar für wichtig, wenn ich über etwas schreiben will. Aber ich selbst verstehe Sachverhalte meistens erst dann, wenn ich sie selbst ausprobiert, mir die Hände schmutzig gemacht habe. Vorher glaubte ich nur, sie zu verstehen.

Daher würde ich beim Schreiben eher auf Erfahrung als auf Perspektive setzen. Eine Perspektive kann ich mir erlesen, eine Erfahrung nur erleben. Natürlich gibt es auch Werke, die Erfahrungswissen aus anderen Texten zusammenfassen, etwa um es für den Leser besser aufzubereiten. Aber ich persönlich würde mich auch hier wohler fühlen, wenn der Autor tatsächlich weiß, was er da zusammenfasst – und nicht alles nur gelesen hat.

In Anikas Folien kommt als weitere Gegenfrage auf das Wer die Frage: „Willst du interagieren?“Diese Frage kommt hier erst an dritter Stelle (an zweiter Stelle fragt sie: „Kannst du schreiben?“).

Ich halte die Interaktionsbereitschaft zunächst mal für wichtiger als die Schreibfertigkeit bei jemanden, der erwägt, eigene Fachartikel zu schreiben. Möglicherweise sollte er sich Fragen wie diese sogar als allererste stellen: Will ich Dinge hinterfragen? Will ich Antworten geben? Will ich auch Kritik aushalten und gegebenenfalls meine Aussagen überdenken?

Ich wiederhole: Der Umgang mit Kritik ist nicht immer einfach. Gehe ich mit einem Fachartikel an die Öffentlichkeit, muss ich aber damit rechnen, dass Kritik kommt. Und ich muss ebenso damit leben, wenn es scheinbar gar keine Reaktion gibt. So oder so: Eine Veröffentlichung ist wie eine Wortmeldung in einer Diskussion. Sie zieht mehr oder weniger offensichtliche Reaktionen nach sich, mit denen ich umgehen können muss.

Erst an dritter Stelle steht für mich die Frage, ob ich schreiben kann. Denn so, wie ich persönlich Programmieren am besten durch programmieren gelernt habe, Systemadministration durch konfigurieren und Fehlersuche, genauso lerne ich Schreiben am besten, indem ich schreibe.

Natürlich ist es wichtig, das ein Fachartikel eine Struktur hat, dass die Sätze verständlich formuliert sind, dass ich etwas zu erzählen habe und nicht einfach nur Fakten aneinanderreihe. Das sind jedoch Techniken, die sich durch Anleitung und Übung verbessern lassen. Schlimmstenfalls kann man sich am Ende immer noch entscheiden, den Artikel doch nicht zu veröffentlichen, und lieber einen anderen zu schreiben.

Worüber kann man schreiben?

Drei Dinge sind laut der Folien für Fachartikel gefragt: „Relevantes“, „Kompetentes“, oder „Soziales“ (Abbildung 3). Dem stimme ich zu. Und relevant ist auch für mich „Neues“, etwa ein junges Projekt, eine neue und stark geänderte Softwareversion oder ein jüngst bekannt gewordenes Sicherheitsproblem. Solche Themen eignen sich auch für kurze Darstellungen: Der Artikel kann dann schneller erscheinen, sodass das Thema nicht veraltet. Ebenso halte ich „Vertracktes“ für relevant, bei dem man sich womöglich schnell mal in die Nesseln setzt, wenn bestimmte Dinge keine Berücksichtigung finden.

Abbildung 3: Themen tarnen sich oft im Alltag. Doch hinein zu zoomen und Details zu erkennen, ergibt ein überraschend anderes Bild.

Möchte ich etwas Vertracktes beschreiben, hole ich persönlich hingegen weiter aus, um das Thema von verschiedenen Seiten beleuchten und die Vor- und Nachteile verschiedener Varianten abzuwägen. So ein Artikel braucht etwas Zeit. Aber er wird dafür im Ergebnis eventuell zeitlos, wenn das, was ich schreibe, auch in ein paar Jahren noch

Bestand hat (bei Neuem ist das unwahrscheinlicher). Beispiel: Du bist dessen müde, immer wieder mit fremden Administratoren zu streiten, die mit ihren Paketfilterregeln den normalen Netzbetrieb stören (Stichwort: Sperren von ICMP)? Dann schreib einen Artikel darüber, der das für diejenigen Administratoren aufbereitet, die die entsprechenden RFCs nicht lesen.

Als drittes Beispiel für Relevantes diente im Vortrag „Denkwürdiges“. Dahinter steckt für mich eine andere Betrachtungsweise, eine neue Kombination von bekannten Dingen, eine andere Herangehensweise, oder gar eine Übertragung von Methoden oder Erkenntnissen aus einem anderen Fachgebiet. Beispiel: Du weißt, wie man in der Shell Prozesse parallel und synchronisiert startet, indem man eine Kette von Pipes zweckentfremdet? Mach einen Artikel draus, der das erläutert und auf die Vor- und Nachteile eingeht.

Damit sind wir – auch auf den Folien – wieder bei „Kompetenz“ angelangt, das zweite Beispiel dafür, was man in Fachartikeln beschreiben kann. Als kompetent ordnen die Folien ein Fallbeispiel ein. Das sehe ich auch so. Fragen, die sich dann stellen, wären: Was habe ich beobachtet? Was ist anders als beim üblichen Vorgehen? Wie kann man es besser machen?

Das dritte Beispiel für Fachartikel-Aufhänger ist „Soziales“. Als Beispiele sind genannt eine Glosse, ein Erlebnis oder eine Meinungsäußerung. Hier stehen dann nicht die technischen Aspekte im Vordergrund, sondern ich als Subjekt. Wie wirkt ein Sachverhalt auf mich? Welche Wirkungen auf andere habe ich beobachtet? Wenn etwas Witziges passiert ist, entsteht vielleicht eine Glosse. Wenn meiner Meinung nach etwas schief oder auch sehr richtig läuft, gehört das in einen Meinungsbeitrag.

Das Wo kommt vor dem Wie

Ich weiß, ich weiß: Inzwischen sind diejenigen, die bis hierher dabei geblieben seid, überzeugt und möchten wissen, wie man denn nun anfängt. Aber Geduld. Ich hatte überlegt, anders als in den Folien das Wie vor das Wo zu setzen. Bei näherem Hinsehen hat aber die Frage großen Einfluss auf den Typ meines Textes, wo ich ihn veröffentlichen will. Der Texttyp bestimmt zwar nur teilweise, was ich schreibe, aber auf jeden Fall, wie ich es aufbereite. Daher bleibt es bei der Reihenfolge, in der als nächstes die Frage ansteht, bei welchem Medium ich etwas veröffentlichen möchte.

„Das ist mir egal, ich probiere es an mehreren Stellen“, mag der eine oder andere denken. Das finde ich legitim: Ich habe auch Texte mehrfach verwertet. Sind die rechtlichen Fragen geklärt, ist das kein Problem. Es geht aber darum, dass verschiedene Medien unterschiedliche Anforderungen an einen Text stellen.

Es gibt die zwei Möglichkeiten, in einem externen Medium zu veröffentlichen, oder alles selbst zu machen. Externe Medien, sagen die Folien, bieten Qualitätssicherung in Form einer Redaktion, die die Qualität der Artikel hoch hält. Das heißt, sie kann einen nicht passenden Artikel auch ablehnen. Insofern ergibt es Sinn, sich schon vorher über Themenspektrum und Zielpublikum des angestrebten Mediums zu informieren.

Habe ich schon Eigenwerbung angebracht (Abbildung 4)? Die *UpTimes* als Mitgliederzeitschrift der GUUG, bei der der Autor dieser Zeilen als Techniker, Redakteur und Autor mitwirke, ist nämlich genau ein solches externes Medium. Die Redaktion nimmt unter <redaktion@uptimes.de> gespannt Artikelideen entgegen, hilft, das Thema festzuklopfen, diskutiert das Ergebnis in Redaktionsschleifen mit dem Autor und zahlt bei Veröffentlichung ein (kleines) Honorar. Das ganze Programm also.

Abbildung 4: Heft im Heft: Darf’s ein wenig Eigenwerbung sein? Fachartikel kann man natürlich auch in der *UpTimes* schreiben. :-)

Für umfangreiche Themen ist statt eines Artikels ein Fachbuch das Medium der Wahl. Für eine Buchidee wendet man sich entweder an einen Verlag, der das Thema im Programm hat. Einige Verlage sind beispielsweise beim Frühjahrsfachgesprächen der GUUG und auf anderen Fachkonferenzen vor Ort, sodass sich dort persönlich Ansprechpartner oder Themen besprechen lassen. Ansonsten dienen Verlagswebseiten als Informationsquelle.

In Eigenregie

Bei selbst veröffentlichten Texten hingegen – egal ob Artikel oder Buch – kümmert sich der Autor selbst um Vermarktung und Qualitätssicherung. In den wenigsten Fällen ist mit einem Honorar zu rechnen. Als Medien bieten sich Blogs an, entweder auf eigenen oder fremden Servern. Auf einer eigenen Website lässt sich besser mit Formaten experimentieren. Auf Blog-Portalen ist die Infrastruktur bereits vorhanden - da kann es gleich losgehen. Über Serverstatistiken und – für Mutige – über die Kommentarfunktion lässt sich auch bereits der Umgang mit Feedback ausprobieren.

Schließlich kann ich längere Texte in Buchform auch bei einem Selfpublishing-Verlag herausgeben. In Frage kommen entweder E-Books als PDF, Epub oder im Mobi-Format für den Kindle-Reader, oder ein gedrucktes Buch. Einige Selfpublishing-Verlage bieten sogar an, für ein Buchprojekt Artikel aus einem Blog zu importieren. Das empfehle ich allerdings nicht, wenn das Buch nicht gerade ein Almanach werden soll oder die Blog-Artikel eigens für das Buch entstehen. Zum Beispiel ein Buchprojekt namens „XYZ Hacks“, das eine sortierte Folge von Kochrezepten darstellt, ließe sich aus bereits vorhandenen Blog-Artikel importieren, wenn sie zum Thema passen.

In anderen Fällen besteht das Problem darin, dass bei der Verbindung von Blogartikeln zu einem Buch nicht automatisch ein roter Faden entsteht, der den Leser von einem Kapitel zum nächsten führt. Diesen roten Faden nachträglich in einen umfangreichen Textkorpus hinein zu friemeln ist in etwa so aufwendig, wie von Anfang an ein Buch zu schreiben. Die andere Richtung, nämlich Kapitel aus einem Buchprojekt für Blog-Artikel zu verwenden, ist übrigens einfacher: Nur einen relativ kleiner Text ist an das andere Medium anzupassen.

Bei einem selbst veröffentlichten Buch winkt sogar ein Honorar. Jedoch steht dieses in den meisten Fällen in keinem Verhältnis zum Aufwand, den ich für eine akzeptable Qualität hineinstecken muss. Und über das Marketing muss ich mir selbst Gedanken machen. Eine Rezension in einer Fachzeitschrift kann einen Sprung in den Verkaufszahlen bedeuten. (Nein, auf diese Idee bin ich nicht von allein gekommen. Aber ich gebe sie gern weiter.)

Egal, ob fremdes Medium oder eigenes, Artikel oder Buch: Während ich überlege, wo ich veröffentliche, denke ich bereits an die Leser. Wen erreiche ich, und was will ich bei ihnen bewirken? Bei einem externen Medium wie einer Zeitschrift hilft, ältere Exemplare mit ähnlichen Artikeln zu lesen, um eine Vorstellung vom Zielpublikum zu bekommen. Was schreiben andere Autoren dort? Wie sehen die Artikel aus? Wie ist das Niveau der Artikel? Passt meiner dazu? Kann ich ihn passend machen? Bei einem Buch erfüllt diese Funktion das Verlagsprogramm an. In Fachbuchhandlungen lässt sich in das eine oder andere Buch hineinschauen, bei den Messeständen der Verlage auf Fachkonferenzen ebenfalls.

Fallstudie: Wie ich Artikel schreibe

Jetzt geht es ans Eingemachte: Wie schreibt man einen Fachartikel? Bei mir beginnt es fast immer mit einer Idee, die ich während der Entstehung ähnlich wie bei der Snowflake-Methode [2] immer weiter auswalze, bis alles beschrieben ist, was beschrieben werden muss (Abbildung 5). Ein Überarbeiten am Ende entfernt Überflüssiges.

Idealerweise formuliere ich anfangs die Idee in einem Satz, der zusammenfasst, worum es in dem Text gehen soll. Wenn mich jemand zum Artikel befragt, kann ich mit diesem Satz antworten. Will ich den Text in einem externen Medium veröffentlichen, kann ich den Redakteur so ansprechen: „Ich habe hier einen Artikel, in dem ...“, und bringe hier den Satz an. Das passiert in einer E-Mail, einem Telefon oder auf einer Konferenz.

Abbildung 5: Die Schreibstube des Autoren.

Diesen einen Satz, der den Text zusammenfasst, arbeite ich dann zu einem Absatz aus, der

alles Wesentliche enthält, worum es im Text gehen wird. Dieser Absatz stellt den Abstract dar, der in manchen Medien dem Artikel vorangestellt wird. Vielleicht stelle ich dabei fest, dass der eine, ursprüngliche Satz gar nicht mehr passt. Kein Problem: Wenn ich mir mit dem Abstract sicher bin, ändere ich den Zusammenfassungssatz.

Spätestens jetzt sollte ich an die Leser denken. Idealerweise habe ich das bereits getan, als ich mich für ein Medium entschieden habe. Denn wie ich die Leser einschätze, beantwortet die Frage, was ich bei meinen Lesern voraussetzen kann, und was ich gegebenenfalls ausführlicher erkläre. Bei einem externen Medium wird es nun auch Zeit, Kontakt zur Redaktion aufzunehmen und meine Idee vorzustellen. Dafür habe ich Zusammenfassung in einem Satz und Abstract parat. Wird der Vorschlag angenommen, gibt es Absprachen mit der Redaktion über Termine, Umfang, Artikeltyp und Dateiformat, in dem ich liefern soll. Bei selbst veröffentlichten Artikeln setze ich mir selbst einen Zieltermin.

Die inhaltliche Arbeit beginnt jetzt, falls nicht bereits geschehen: Ich recherchiere Fakten. Üblicherweise verlasse ich mich dabei nicht auf das, was ich lese, sondern probiere es selbst aus – Artikel, deren Autor unreflektiert von anderen abschreiben und lediglich umformulieren, gibt es zur Genüge. Allenfalls bei einer Übersetzung spare ich mir die Mühe. alles selbst auszuprobieren. Code, den ich dabei schreibe, hebe ich auf, um ihn als Supplement dem Text beizugeben oder zur Illustration zu verwenden. Taucht Code im Text auf, sollte ich ihn erläutern. Das hängt aber vom Publikum ab, für das ich schreibe, und von der Komplexität des Codes.

Aus dem Abstract erzeuge ich dann ein Gerüst für den Text. Ich rolle ihn aus, wie Teig für Weihnachtsplätzchen. Dabei nehme ich aber nicht den ganzen Abstract auf einmal, sondern immer nur einen Satz, und wenn zu diesem alles gesagt ist, dann den nächsten. So ist das Expandieren des Abstracts zum Artikel nicht schwieriger als das Expandieren der Zusammenfassung zum Abstract. Ich muss es nur etwas häufiger machen – bis ich am Ende alles zum Thema gesagt habe.

Hier mache ich persönlich mir noch keine Gedanken über Rechtschreibung, Grammatik oder Stil. Es geht nur darum, die Gedankenkette nicht abreißen zu lassen. Ich schreibe sogar am liebsten mit Bleistift auf Papier. Ein Diktiergerät ist eine andere Möglichkeit. Aber bei Papier kann ich schneller zurückblättern, falls der Faden doch mal reißt. Am Ende tippe ich es für die weitere Verarbeitung ein. Dabei bevorzuge ich simplen Text. Es geht bis hierher ausschließlich um den Inhalt.

Die erste Version speichere ich ab und wende mich anderen Dingen zu. Zum Beispiel suche oder erstelle ich Diagramme und Bilder, die den Text unterstützen. Will ich Code zur Illustration einsetzen, dann kann ich diesen jetzt für das Zielmedium aufbereiten. Auf jeden Fall lasse ich den Text an sich aber liegen, um Abstand zu gewinnen, bevor ich zum Text zurückkehre.

Dann rückt der Abgabetermin heran. Ich gehe dabei so vor: Das, was ich bis jetzt habe, gebe ich so auf keinen Fall heraus. Das muss noch überarbeitet werden. Ich hole mir also den Rohtext hervor, denke: Meine Güte, was hab ich da nur wieder fabuliert; und bringe den Text in eine kohärente(re) Form. Ich frage ihn dafür ab: Ist der Satzbau verständlich? Stimmt der Ideenfluss? Ist das nachvollziehbar? Weitere Punkte, die ich bei der Überarbeitung beachte finden sich in diversen Stilfibeln (zum Beispiel [3], [4], [5]).

Warum Artikelschreiben Arbeit macht

Das ist richtig schwere Arbeit. Ließ ich bei der ersten Rohversion die Zügel schießen, bin ich nun mein erster Kritiker. Und genau dafür brauche ich den zeitlichen Abstand: um den Text mit anderen Augen zu sehen. Umschalten vom freien Fabulieren zum disziplinierten Prüfen und Überarbeiten desselben Textes geht nicht in ein paar Minuten. Zumindest nicht bei mir. Ich habe auch noch von niemandem gehört, der das kann. Zum Einstimmen lese ich den Abstract, um zu überprüfen, ob der Text noch dahin führt. Gut möglich, dass ich feststelle, ihn lieber noch einmal umschreiben zu wollen.

Je nachdem, ob ich den Text an eine Redaktion gebe oder vollständig selbst entwickle, überarbeite ich ihn einmal oder mehrmals. Spätestens bei der letzten Überarbeitung entferne ich die Grammatik- und Rechtschreibfehler. Ich nutze Hilfsmittel wie Checklisten, oder auch der TÜV von Andreas Eschbach [6]: Er hilft, Stellen im Text zu finden, die ich wahrscheinlich überarbeiten will.

Arbeite ich mit einer Redaktion zusammen, bekomme von dieser oft weitere Hinweise, was noch der Klärung bedarf. Mein Text wird immer verändert werden, bevor er veröffentlicht wird: Darauf muss ich mich einstellen und damit umgehen können. Der Text ist zwar mein Baby, das kann man ruhig so sagen, und ich möchte so viel Einfluss wie möglich haben, wie es am Ende aussieht. Aber der

Text muss sich in den Stil des Mediums einfügen, damit er nicht zum Fremdkörper wird. Dafür sorgt normalerweise die Redaktion. Vor der Veröffentlichung erhält der Autor oft einen Probeabzug, an Hand dessen sich Fehler noch korrigieren lassen.

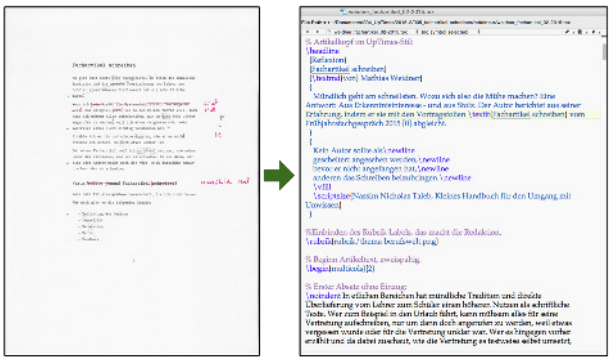


Abbildung 6: Zwischen Entwurf und Veröffentlichung liegt ein langer Weg. Links: Ein handschriftlich bearbeiteter Ausdruck vor Lieferung. Rechts: Der Text im Editor einer Redaktion.

Am Ende ist der Text reif für die Veröffentlichung (Abbildung 6). Wieder darf man es ruhig so sagen: Es ist dann Zeit, ihn ziehen zu lassen und zu schauen, wie es ihm in der Welt da draußen ergeht.

Wenn Feedback kommt und das gewählte Medium es erlaubt, dann ändere ich persönlich auch bereits veröffentlichte Texte. In elektronischen Medien ist das technisch kein Problem. Es kann allerdings zum Problem werden, wenn der ursprüngliche Text bereits zitiert worden ist. Daher mache ich die Änderungen stets kenntlich. Im Extremfall kann ich auch beide Versionen vorhalten, wenn das Medium es erlaubt.

Berühmte letzte Worte

Hoffentlich hat dieser Artikel dem einen oder anderen den Mund wässrig gemacht. Ich möchte aber noch auf einige wichtige Punkte hinweisen. Die eingangs erwähnten Folien erwähnen es, und ich unterschreibe: Publizieren ist nicht trivial. Das heißt: Technisch mittlerweile schon. Ein Blog zum Beispiel ist ruck, zuck eingerichtet und kostet im einfachsten Fall nichts zusätzlich zu den Kosten des eigenen Internetzugangs. Und um ein Buch bei einem Selfpublishing-Verlag zu verlegen, muss ich ebenfalls kein Geld, sondern nur Zeit investieren. Das meine ich nicht. Sondern es geht darum, ob ich mit meinem Artikel vor allem, sagen wir mal: meine Eitelkeit befriedigen will, oder ob ich vor allem Nutzen für den Leser erzielen möchte. Letzteres braucht harte Arbeit.

Jeder Text führt ein „Eigenleben“, wie die Vortragsfolien es formulieren. Ich beobachte selbst, dass es von den Ideen und Gedanken in meinem Kopf zum Text ein weiter Weg ist. Es kommt zum Beispiel vor, dass ein Text nicht genau das darstellt, was ich mir ursprünglich gedacht habe, wenn ich ihn später betrachte. Und wenn ein Leser den Text liest, interpretiert er ihn anhand seiner Erfahrungen auf seine eigene Weise. Was dabei herauskommt, unterscheidet sich dann ebenfalls nicht nur vom Text, sondern auch von meinen Gedanken sowie von den Gedanken aller anderen Leser.

Darum empfehle ich, die Hauptaussagen so klar und vollständig wie möglich herausarbeiten und alle möglichen Tricks anwenden, um die verschiedenen Stärken meines Gehirns zu nutzen. Daher beginne ich damit, im Rahmen des Themas frei zu fabulieren und meine Gedanken möglichst vollständig, wenn auch noch nicht geordnet, zu Papier zu bringen. Mit einem Satz anzufangen, ihn zu einem Absatz zu expandieren und von diesem immer weiter bis zum fertigen Artikel zu gelangen, ist aus demselben Grund eine Methode, die ich mir angeeignet habe. Ich breche damit das Problem, einen kohärenten Artikel oder ein Buch zu schreiben, auf kleinere, handhabbare Probleme herunter. Und ich bestimme sehr früh die Hauptaussagen, sodass ich mich später stärker auf die Formulierung konzentrieren kann.

Auch wenn es scheint, dass es mit Internet und Selfpublishing-Verlagen keiner Redaktion und keines sonstigen Wasserkopfes mehr bedarf, erscheint es mir sinnvoll, sich die Aufgaben einer Redaktion bewusst zu machen. Diese Aufgabe besteht nicht darin, wie die Vortragsfolien zuspitzen, den Autor zu ärgern oder seine Mühen abzulehnen, sondern durch Qualitätssicherung und Bereitstellen der Infrastruktur für eine optimale Verbreitung die Wirkung des Textes zu erhöhen.

Sicher gibt es auch Probleme im Umgang mit Redaktionen. Bei einem meiner ersten Artikel zum Beispiel, so um 1990 herum, bekam ich von der Redaktion einen Brief mit dem Text eines Reviewers, der davon abriet, den Artikel zu veröffentlichen. Meine erster Gedanke war: Was fällt dem ein! Ich nahm tatsächlich den Review-Text und ältere Ausgaben der Zeitschrift unter die Lupe, um aufzuspüren, wer der Ablehner denn gewesen sein könnte. Am Ende habe ich eine gepfefferte Widerlegung des Reviews an die Redaktion geschrieben und den Artikel zurückgezogen.

Soviel Aufwand, um verletzten Stolz zu besänftigen... Aus heutiger Sicht wäre es wohl besser ge-

wesen, die Kritik ein paar Tage liegen zu lassen, dann zu schauen, was in sachlicher Hinsicht berechtigt war und ob der Artikel anzupassen gewesen wäre. Aber ob ich das heute so souverän hinbekommen würde, weiß ich auch erst, wenn es das nächste Mal passiert.

Literatur und Links

[1] Anika Kehrer, Vortragsfolien *Fachartikel schreiben*: https://www.torial.com/anika.kehrer/portfolio/78266
[2] Randy Ingermansson, *The Snowflake Method For Designing A Novel*:
http://www.advancedfictionwriting.com/articles/snowflake-method/
[3] Ludwig Reiners: Stilfibel; Der sichere Weg zu gutem Deutsch. München, dtv 2015.
[4] Christoph Prevezanos: Technisches Schreiben; für Informatiker, Akademiker, Techniker und den Berufsalltag. München, Carl Hanser 2013.
[5] Wolf Schneider: Deutsch für Profis; Wege zu gutem Stil. München, Goldmann 2001.
[6] Andreas Eschbachs 10-Punkte-Text-TÜV:
http://www.andreaseschbach.de/schreiben/10punkte/10punkte.html

Über Mathias

Mathias Weidner studierte Ende der 1980-er Jahre Automatisierungstechnik in Leipzig. Nach verschiedenen Stellen in der Software-Entwicklung landete er bei einem kleinen Rechenzentrum in Wittenberg als Administrator für Unix/Linux und Netzwerke. Seit einiger Zeit schreibt er hin und wieder Bücher zum Thema, die sowohl gedruckt als auch unter http://buecher.mamawe.net als PDF oder ePUB erhältlich sind. Mathias ist Mitglied der UpTimes-Redaktion.

Mind Management
Interview zum Job des Scrum Masters

Der ehemalige Sysadmin Florian Groß begleitet seit vier Jahren als selbständiger *Scrum Master* Teams beim Arbeiten. Nicht immer sind es technische Teams, doch seine Funktion ist stets dieselbe: wahrnehmen, was mit dem Team geschieht.

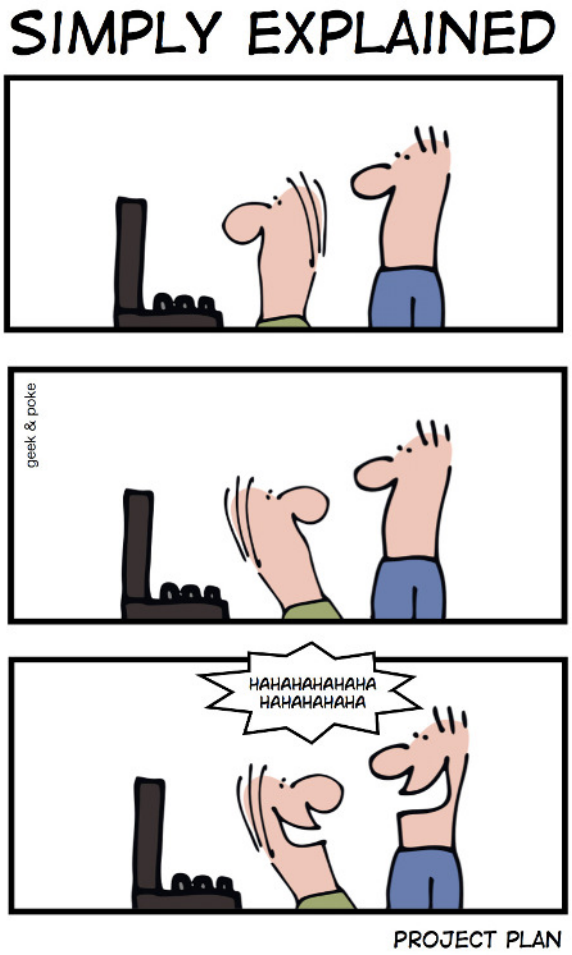
Interview: **Anika Kehrer**

Wer auf andere nicht mehr
angewiesen zu sein glaubt,
wird unerträglich.

Luc de Clapiers, Marquis de Vauvenargues

Florian, ist Scrum Master ein einfacher Job?

Florian: Gegenfrage: Ist Systemadministrator ein einfacher Job? Was ich damit meine: Mir machen die Facetten des Jobs großen Spaß und sie liegen mir, wie das Coaching und die Facilitation *[also einer Gruppe dabei zu helfen, ihr Ziel zu erreichen; Anm. d. Red.]*. Deshalb ist der Job für mich einfach, entspannt und ich genieße es sehr, jeden Tag mehr über Menschen und Teams zu lernen. Inwieweit sich das auf andere übertragen lässt, ist eine andere Frage.



Was, meinst Du, sagen Deine Teammitglieder über Deinen Job? Schätzen sie Deiner Meinung nach, was Du tust?

Florian: Durch die Aufteilung der Verantwortung in Produkt (*Product Owner*) und Prozess (*Scrum Master*) kann ich oft eine Perspektive einnehmen, die es in vielen Firmen mit Linien- oder Matrixorganisation vorher so nicht gab. Das Feedback, das ich von meinen Teammitgliedern dazu bekomme, ist für mich extrem wertvoll. Ich würde den Job nicht mehr machen, wenn es nicht hauptsächlich sehr positiv wäre.

Welche Qualifikationen fallen Dir auf, die Du in Deiner beruflichen Rolle am meisten brauchst?

Florian: Am wichtigsten ist für mich die Fähigkeit, im Außen zu sein, also wahrzunehmen, was bei einzelnen Teammitgliedern und dem gesamten Team gerade geschieht. Das ist für mich die Grundlage, um als dienende Führungskraft ohne disziplinarische Befugnisse zu agieren. Teams vertrauen und folgen mir, weil meine Vorschläge und Unterstützung Sinn ergeben und ihnen helfen.

Dienende Führungskraft

Welchen Weg kann man einschlagen, wenn man sich für *Scrum* und vielleicht speziell die Rolle des Scrum Masters interessiert?

Florian: Für Podcast-Liebhaber habe ich zwei Empfehlungen: In Deutsch und auch für Einsteiger geeignet ist *Agiles Produktmanagement* [1]. In Englisch und fortgeschrittener ist *Agile for Humans* [2]. Wer Videos mag, kann zum Beispiel eine Viertelstunde mit Henrik Knibergs *Product Ownership in a Nutshell* auf Youtube verbringen [3]. Danach gibt es viel kostenloses Material bei den einschlägigen Konferenzen, oder auch gut struk-

turierte, zahlungspflichtige Einführungen [4]. Als Buch empfehle ich gern *Essential Scrum* (gleicher Titel in Deutsch wie in Englisch) von Kenneth Rubin. Danach dann für die Rolle des Scrum Masters *Scrum Mastery* von Geoff Watts, und für Product Owner *The Lean Product Playbook* von Dan Olsen.

Kann jeder Scrum Master sein? Oder sind bestimmte Zertifikate o.Ä. ratsam?

Florian: Als Scrum Master darf man grundsätzlich Spaß an der Arbeit mit Menschen haben, denn daraus bestehen weite Teile jeden Tages. Programmieren und Administration sind zumindest bei mir stark in den Hintergrund gerückt. Zertifizierungen werden im agilen Bereich genauso kritisch gesehen wie in anderen IT-Berufen. Auf der einen Seite sichern sie ein gewisses Grundwissen, auf der anderen liegt viel mehr Wert in praktischer Erfahrung. Ich glaube, eine Schulung ist am Anfang sinnvoll, und danach zählt bei vielen Firmeninterviews inzwischen nur noch die Praxis. Es gibt zwei große Zertifizierungsorganisationen: *Scrum Alliance* [5] und *Scrum.org* [6].

Welche Qualifikationen hättest Du anders herum gern auf Seiten Deiner Scrum-Teammitglieder?

Florian: Hinter den konkreten Fähigkeiten stehen für mich die agilen Prinzipien und Werte. Mit der gemeinsamen Wertebasis werden Qualifikationen sowieso recht bald vom Team selbst gefördert und gefordert, etwa in der Testautomatisierung. Außer Offenheit und Neugier brauche ich für den Start nichts weiter. Toll ist es, wenn das Team gute Erfahrungen mit *Extreme-Programming*-Praktiken hat. Das macht vieles einfacher.

Kannst Du Dir vorstellen, dass agile Teamarbeit auch in anderen Bereichen als in der Software-Entwicklung nützlich wäre? Zum Beispiel in der Systemadministration?

Florian: Ich begleite aktuell zwei Teams, die aus Einkauf und Vertrieb kommen. Und das Feedback sagt: Ja – die agile Teamarbeit ist auch in diesen Bereichen sehr nützlich. Dort machen wir allerdings kein reines Scrum, sondern eher *Kanban*. Außerdem geisterte gerade diese Woche eine Projektanfrage über die Vermittlungsplattformen, die einen Scrum Master in einem Infrastrukturprojekt suchte, nämlich für die Einführung von *Windows 10*. Es gibt also auch andere Firmen, die inzwischen überzeugt sind, dass ein agiler Ansatz Sinn ergibt.

Must-have: Feedbackschleifen und Transparenz

In was für Projekten würden sich agile Methoden gar nicht eignen?

Florian: Mir fallen dazu zwei Perspektiven ein: Für wirklich agiles Arbeiten brauchen die Teams möglichst regelmäßigen, auch informellen Kontakt zum Kunden und die Möglichkeit, Anpassungen vorzunehmen. Denn das Überprüfen und Anpassen findet nicht nur auf Prozess-, sondern auch auf Inhaltsebene statt. Ohne einfache Feedbackschleifen zum Kunden kann ich zum Beispiel meinen Umsetzungsplan nicht anpassen, wenn ich auf Grundlage der bisherigen Arbeit etwas gelernt habe. In klassischen Projekten kann ich das ignorieren. Aber in agilen Projekt herrscht oft so viel Transparenz, dass allen klar ist, wenn nur noch stur an einem veralteten Plan festgehalten wird. Dadurch entsteht mehr sichtbarer Frust als beim klassischen Projekt.

Außerdem gibt es manchmal Standardprojekte, die keine großen Risiken oder Unbekannten bergen, dafür möglichst effizient umgesetzt werden sollen. Hier würde ich mich auch wieder am agilen Werkzeugkasten bedienen und zum Beispiel die Arbeit visualisieren, aber sicher keinen Scrum Prozess aufsetzen.

Stichwort DevOps: Inwiefern sind agile Methoden da nützlich oder hinderlich?

Florian: Ein wesentliches agiles Ziel ist die frühe und kontinuierliche Lieferung von funktionierender Software an Kunden. Dazu gehört in vielen Firmen das Deployment auf eigene Server, und damit braucht das Team auch Wissen in der Systemadministration. Außerdem ist es unglaublich wertvoll, schon während der Entwicklung Feedback und die Perspektive aus dem Betrieb einfließen zu lassen. Deshalb habe ich genauso gern DevOps-Teammitglieder an Board, wie auch Test-Spezialisten. Die Teams sollen ja eben selbstorganisierend und interdisziplinär sein.

Ein zusätzlicher Aspekt: vielen Entwicklerteams tut es sehr gut, auch bei der Automatisierung der eigenen Entwicklungsumgebung Unterstützung zu bekommen. Auch dafür ist die engere Verbindung von Entwicklung und Betrieb sinnvoll.

Was hilft generell einem agilen Team, und was ist hinderlich?

Florian: Generell hilfreich ist, wenn im Unternehmen viel Vertrauen herrscht und offen über Kon-

flikte gesprochen wird, um diese zu lösen. Wenn dann von vorneherein ein Bewusstsein dafür da ist, dass ein agil arbeitendes Team auch Auswirkungen auf den Rest der Organisation haben wird – zum Beispiel was Transparenz in Lieferungen oder Einbindung in Entscheidungen angeht – dann ist erst mal alles am richtigen Platz. In fast jedem meiner Scrum-Trainings kommt die Frage auf, inwieweit *Agil* einfach Methode ist, und inwieweit eine Kultur. Spätestens am zweiten Tag antworten die Fragesteller dann selbst, dass es um den Kulturwandel geht. Damit ist auch klar, dass agile Teams in ihrer Organisation Unterstützung brauchen für eine moderne Art der Wissensarbeit.

Ein Product Backlog namens Ponyhof

Geschichten aus dem Scrum Alltag! Passiert da auch mal was Lustiges?

Florian: Hoffentlich jeden Tag! [7] Eins meiner aktuellen Teams beendet jedes *Daily* mit einem Eintrag *Unnützes Wissen*, was oft zu Lachern am Ende des Meetings führt. Ein anderes Team hat mal einen DNS-Alias für unseren Bugtracker eingerichtet, *gorleben*. Darauf habe ich das Product Backlog auch unter *ponyhof* erreichbar gemacht. Keine zwei Wochen später hatten wir auf unserem physischen Board lauter *My-Little-Pony*-Aufkleber hängen. Und in wieder einem anderen Team hatten wir als Redestab für das Daily einen 30 Zentimeter großen Plastikdinosaurier. Nach einer Weile wurde damit auf das Board gedeutet und wild gestikuliert.

Nochmal zur Systemadministration. Mal angenommen, so richtig will man als Admin nicht scrummen, würde aber trotzdem die stützende Funktion eines Scrum Masters schätzen. Kann man sich einen auch so ins Haus holen, ohne von vorn bis hinten Scrum zu machen? Lässt sich also die Rolle quasi einer guten Seele des Teams nicht auch außerhalb von Scrum oder Agilität generell gewinnbringend nutzen?

Florian: Ich habe länger über die Formulierung nachgedacht, ob der Scrum Master wirklich die „gute Seele des Teams“ ist. Oft bin ich auch das schlechte Gewissen oder der professionelle Anspruch. Am Anfang habe ich als Coach mehr zu tun, als nach ein paar Monaten. Ich möchte mich nämlich weitestgehend überflüssig machen, damit die Teammitglieder selbst volle Verantwortung für ihren Prozess und die Lösungsfindung in die Hand nehmen. Dann kann ich als wirklicher Facilitator dort arbeiten und bei Bedarf noch Impulse auf Augenhöhe geben.

Wenn Teams am Anfang an ihren Werten und Zielen arbeiten, also auch an der Teamkultur, ist ein Coach aus meiner Sicht sehr wertvoll. Oft heißt meine Rolle dann *Agile Coach*, und neben der „guten Seele“ ist ein Teil davon die Beratung, welche Methoden wir aus dem agilen Werkzeugkasten im konkreten Kontext möglichst sinnvoll einsetzen können.

Links

[1] Podcast *Agiles Produktmanagement*: http://www.agilesproduktmanagement.de
[2] Podcast *Agile for Humans*: http://www.stitcher.com/podcast/agile-for-humans
[3] Video *Product Ownership in a Nutshell*: https://www.youtube.com/watch?v=502ILHjX9EE
[4] Kostenpflichtige Online-Kurse: https://www.frontrowagile.com
[5] Zertifizierungsorganisation *Scrum Alliance*: https://www.scrumalliance.org
[6] Zertifizierungsorganisation *Scrum.org*: https://www.scrum.org
[7] Richard Sheridan: Joy, Inc.; How We Built a Workplace People Love. London, Penguin Publishing Group 2013.

Über Florian

Florian Groß lebt in der Nähe von Düsseldorf und arbeitet seit sechs Jahren im agilen Umfeld, inzwischen selbständig als Scrum Master und Agile Coach. Vorher war er Product Owner bei der *genua mbh* und kommt ursprünglich aus der Systemadministration und dem Unix-Support. Vor vier Jahren hat er den Wechsel von der Product-Owner- zur Scrum-Master-Rolle gewagt und fühlt sich auf der menschlichen Seite der IT sehr wohl.

Randnotizen
Nix Neues auf der *LinuxCon Europe* 2015

Die hauseigene Konferenz des Linux-Projekts hatte weder große Neuigkeiten, noch einen Kommunikations-Knigge in petto.

von **Nils Magnus**

Es ist schwer, jemanden so zu achten,
wie er geachtet werden will.

Luc de Clapiers, Marquis de Vauvenargues

Bei der *LinuxCon Europe* im irischen Dublin ging es dieses Jahr zwar nutzwertig, aber ansonsten etwas unentschlossen zu. Große Neuigkeiten fehlten, jeder Sponsor stellte seine Beiträge zum unausweichlichen Container-Thema vor. Da wundert es nicht, wenn ein weiches Thema die Diskussionen auf den Fluren beherrschte, nämlich der Umgangston.

Den hatte *Intel*-Entwicklerin Sarah Sharp zum Anlass genommen, öffentlichkeitswirksam ihren Rücktritt von Linux-Kernel-Angelegenheiten zu verkünden. Ebenfalls unzufrieden mit der Gesamtsituation hatte sich *UEFI*-Querdenker Matthew Garrett ihr angeschlossen und gar einen Fork des Kernels in Aussicht gestellt.

Das Aufregerthema der Konferenz war damit perfekt. Fortan diskutierten die Teilnehmer darüber, wie zuträglich der Kommunikationsstil auf der Linux-Kernel-Mailingliste (LKML, [1]) für die nachhaltige Stabilität der langfristigen Kernel-Entwicklung sei. Weder vom Chef selbst, der gewohnt lässig auf der Couch mit Intimus Dirk Hohndel kleine Neckereien austauschte, noch von einem auffällig stark mit Frauen besetzten Keynote-Panel von Kernentwicklern gab es schlüssige Vorschläge, wie mit dem Höflichkeitsthema umzugehen sei.

Eine Fraktion befürwortet eine klare Sprache, wenn bisweilen unsinnige Vorschläge geäußert würden. Dem halten Gegner entgegen, dass manche Protagonisten die Grenzen der Eignung mancher Idee sehr großzügig im eigenen Sinn interpretierten. Auch der formelle Dienstvorgesetzter von Linus Torvalds hat das Patt nicht aufgelöst. Im Gespräch mit der *UpTimes* verwies Jim Zemlin lediglich auf den etwas dürren *Code of Conflict* [2], den das *Technical Advisory Board* (TAB, [3]) der *Linux Foundation* Anfang 2015 beigesteuert hatte. Das TAB wiederum bezeichnen einige Entwickler, die namentlich nicht genannt werden wollen, auch nur als weiteren zahnlosen Tiger.

Mit seinen mehr als 1.000 aktiven Entwicklern und regelmäßig mehr als 10.000 Commits pro Minor-Release hat die Kernel-Entwicklung heute mit deutlich mehr als 20 Millionen Zeilen Code [4] eine Größenordnung erreicht, dass sich Darwin'sche Abläufe auf das Projekt anwenden lassen: Solange eine Mehrheit dem durch LKML und Torvalds organisierten Kern die Treue hält, überlebt dieser Zweig. Irgendwann mag einmal eine Abzweigung die Entwicklung anführen – immerhin ist in gewisser Weise auch Linux selbst als eine Art geistiger Fork entstanden, nannte Torvalds doch *Minix* und *GNU Hurd* als Vorbilder [5]. Das Verflixte an der Evolution ist nur, dass man nie weiß, wann sie zuschlägt.

Links

[1] Linux Kernel Mailing List (LKML): https://lkml.org/
[2] Linux' *Code of Conflict*:
https://git.kernel.org/cgit/linux/kernel/git/torvalds/linux.git/tree/Documentation/CodeOfConflict
[3] Linux' *Technical Advisory Board*: http://www.linuxfoundation.org/programs/advisory-councils/tab
[4] Online-Artikel: Thorsten Leemhuis, *Linux-Kernel durchbricht die 20-Millionen-Zeilen-Marke*:
http://heise.de/-2730780.html
[5] Linux-Ankündigung von Torvalds 1991:
https://groups.google.com/forum/#!original/comp.os.minix/dlNtH7RRrGA/SwRavCzVE7gJ

Hilfreiches für alle Beteiligten
Autorenrichtlinien

Selbst etwas für die UpTimes schreiben? Aber ja! Als Thema ist willkommen, was ein GUUG-Mitglied interessiert und im Themenbereich der GUUG liegt. Was sonst noch zu beachten ist, steht in diesen Autorenrichtlinien.

Der Schriftsteller ragt zu den Sternen empor,
Mit ausgefranstem T-Shirt.
Er raunt seiner Zeit ihre Wonnen ins Ohr,
Mit ausgefranstem T-Shirt.

Frei nach Frank Wedekind, Die Schriftstellerhymne

Wir sind an Beiträgen interessiert. Wir, das ist diejenige Gruppe innerhalb der GUUG, die dafür sorgt, dass die UpTimes entsteht. Dieser Prozess steht jedem GUUG-Mitglied offen. Der Ort dafür ist die Mailingliste <redaktion@uptimes.de>.

Welche Themen und Beitragsarten kann ich einsenden?

Die UpTimes richtet sich als Vereinszeitschrift der GUUG an Leser, die sich meistens beruflich mit Computernetzwerken, IT-Sicherheit, Unix-Systemadministration und artverwandten Themen auseinandersetzen. Technologische Diskussionen, Methodenbeschreibungen und Einführungen in neue Themen sind für dieses Zielpublikum interessant, Basiswissen im Stil von *Einführung in die Bourne Shell* hingegen eher nicht. Wer sich nicht sicher ist, ob sein Thema für die UpTimes von Interesse ist, kann uns gern eine E-Mail an <redaktion@uptimes.de> schicken.

Neben Fachbeiträgen sind Berichte aus dem Vereinsleben, Buchrezensionen, Konferenzberichte, humoristische Formen und natürlich Leserbriefe interessant. Wer nicht gleich mehrseitige Artikel schreiben möchte, beginnt also mit einem kleineren Beitrag.

Fachbeiträge sind sachbezogen, verwenden fachsprachliches Vokabular und anspruchsvolle Erläuterungen, besitzen technische Tiefe und ggf. auch Exkurse. Berichte aus dem Vereinsleben greifen aktuelle Themen auf oder legen Gedankengänge rund um die GUUG und ihre Community dar. Konferenzberichte zeigen, welche Veranstaltungen jemand besucht hat, was er/sie dort erfahren hat und ob die Veranstaltung nach Meinung des Autoren beachtenswert oder verzichtbar war. Unterhaltsame Formen können ein Essay oder eine Glosse sein, aber auch Mischformen mit Fachartikeln (Beispiel: der „Winter-Krimi“ in Ausgabe 2013-3). Auch unterhaltsame Formen besitzen jedoch inhaltlichen Anspruch. Denn die UpTimes ist und bleibt die Mitgliederzeitschrift eines Fachvereines.

In der UpTimes legen wir daher auch Wert auf professionelle publizistische Gepflogenheiten und einheitliche Schreibweisen. Dafür sorgt zum Beispiel ein einheitliches Layout der Artikel, oder etwa die grundsätzliche Vermeidung von Worten in Großbuchstaben (entspricht typografisches Schreien) oder von Worten in Anführungsstrichen zum Zeichen der Uneigentlichkeit (entspricht Distanzierung von den eigenen Worten). Wichtig sind außerdem beispielsweise Quellenangaben bei Zitaten, Kenntlichmachung fremder Gedanken, Nachvollziehbarkeit der Argumentation sowie Informationen zum Autor nach dem Artikel.

In welchem Format soll ich meinen Artikel einsenden?

ASCII: Am liebsten blanke UTF8-Texte. Gern mit beschreibenden Anmerkungen oder Hinweisen (zum Beispiel mit Prozentzeichen zum Kenntlichmachen der Meta-Ebene).

LaTeX: Wir setzen die UpTimes mit LaTeX. Weil wir – wie es sich beim Publizieren gehört – mehrspaltig setzen und ein homogenes Erscheinungsbild anstreben, verwenden wir für die UpTimes bestimmte Formatierungen. Es ist nicht erwünscht, eigene Layoutanweisungen einzusenden. Wir behalten uns vor, Texte für die Veröffentlichung in der UpTimes umzuformatieren. Eine Vorlage mit den von uns verwendeten Auszeichnungen für Tabellen, Kästen und Abbildungen gibt es unter http://www.guug.de/uptimes/artikelvorlage.tex.

Listings: Der mehrspaltige Druck erlaubt maximal 45 Zeichen Breite für Code-Beispiele, inklusive 1 Leerzeichen und einem Zeichen für den Zeilenumbruch innerhalb einer Code-Zeile (Backslash). Breitere Listings formatieren wir um, verkleinern die Schriftgröße oder setzen sie als separate Abbildung.

Bilder: Wir verarbeiten gängige Bildformate, soweit ImageMagick sie verdaut und sie hochauflösend sind. Am besten eignen sich PNG- oder PDF-Bilddateien. Plant bei längeren Artikeln mit 1 Abbildung pro 3000 Zeichen. Das müssen nicht Bilder sein, sondern auch Tabellen, Listings oder ein Exkurskasten sind möglich. Verseht Eure Bilder nicht mit Rahmen oder Verzierungen, weil die Redaktion diese im UpTimes-Stil selbst vornimmt.

Wie lang kann mein Artikel sein?

Ein einseitiger Artikel hat mit zwei Zwischentiteln um die 2.700 Anschläge. Mit etwa 15.000 Anschlägen – inklusive 3 Abbildungen – landet man auf rund vier Seiten. Wir nehmen gern auch achtseitige Artikel, achten dabei aber darauf, dass der Zusammenhang erhalten bleibt und dass es genug Bilder gibt, damit keine Textwüsten enstehen.

Wer Interesse hat, für die UpTimes zu schreiben, macht sich am besten um die Zeichenzahl nicht so viele Gedanken – auch für kurze oder lange Formate finden wir einen Platz. Die Redaktion ist bei der konkreten Ideenentwicklung gern behilflich. Für eine Artikelidee an <redaktion@uptimes.de> reicht es, wenn Ihr ein bestimmtes Thema behandeln wollt.

Wohin mit meinem Manuskript?

Am einfachsten per E-Mail an <redaktion@uptimes.de> schicken. Das ist jederzeit möglich, spätestens jedoch vier Wochen vor dem Erscheinen der nächsten UpTimes. Zum Manuskript ist ein kleiner Infotext zum Autor wichtig, ein Bild wünschenswert.

Nützlich ist, wenn der Text vor Einsendung durch eine Rechtschreibkorrektur gelaufen ist. `aspell`, `ispell` oder `flyspell` für Textdateien sowie die von LibreOffice bieten sich an. Wenn Ihr Euren Text an die Redaktion schickt, solltet Ihr also weitestmöglich bereits auf die Rechtschreibung geachtet haben: Nach der Einschickung ist Rechtschreibung und Typo-Korrektur Aufgabe der Redaktion. Die Texte in der UpTimes folgen der neuen deutschen Rechtschreibung.

Wie verlaufen Redaktion und Satz?

Wir behalten uns vor, Texte für die Veröffentlichung in der UpTimes zu kürzen und zu redigieren. Das bedeutet, dafür zu sorgen, dass der Artikel nicht ausufert, versehentliche Leeraussagen wegfallen, Syntax und Satzanschlüsse geglättet werden, dass Passiva und Substantivierungen verringert und Unklarheiten beseitigt werden (die zum Beispiel Fragen offen lassen oder aus Passivkonstruktionen resultieren, ohne dass der Schreibende das merkt). Manchmal ist dieser Prozess mit Nachfragen an den Autoren verbunden.

Die endgültige Textversion geht jedem Autoren am Ende zur Kontrolle zu. Dabei geht es um die inhaltliche Kontrolle, ob sich durch den Redaktionsprozess Missverständnisse oder Falschaussagen entstanden sind. Danach setzt die Redaktion die Artikel. Wenn der Satz weitgehend gediehen ist – also ein *Release Candidate* als PDF vorliegt – erhalten die Autoren als erste diesen RC. Danach wird die UpTimes dann veröffentlicht.

Gibt es Rechtliches zu beachten?

Die Inhalte der UpTimes stehen ab Veröffentlichung unter der CC-BY-SA-Lizenz, damit jeder Leser die Artikel und Bilder bei Nennung der Quelle weiterverbreiten und auch weiterverarbeiten darf. Bei allen eingereichten Manuskripten gehen wir davon aus, dass der Autor sie selbst geschrieben hat und der UpTimes ein nichtexklusives, aber zeitlich und räumlich unbegrenztes Nutzungs- und Bearbeitungsrecht unter der CC-BY-SA einräumt.

Bei Fotos oder Abbildungen Dritter ist es rechtlich unabdingbar, dass der Autor sich bei dem Urheber die Erlaubnis zu dieser Nutzung einholt, und fragt, wie die Quelle genannt zu werden wünscht. Die Frage nach der CC-BY-SA ist hierbei besonders wichtig.

An Exklusivrechten, wie sie bei kommerziellen Fachzeitschriften üblich sind, hat die UpTimes kein Interesse. Es ist den Autoren freigestellt, ihre Artikel noch anderweitig nach Belieben zu veröffentlichen.

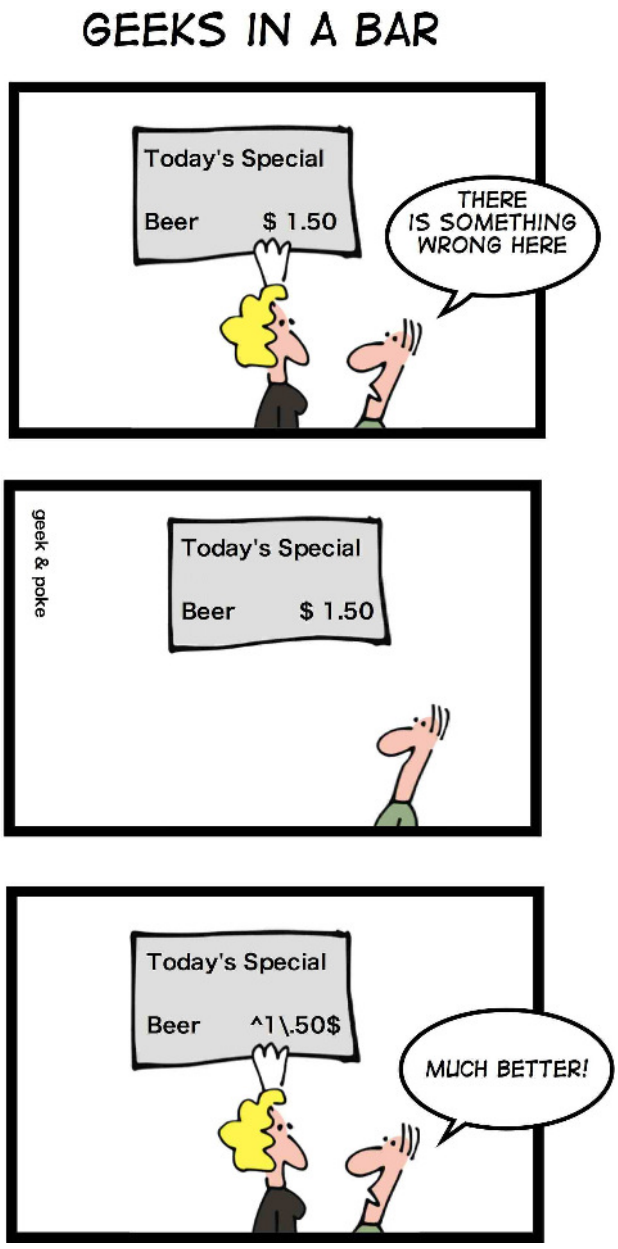
Bekomme ich ein Autorenhonorar?

Für Fach- und literarische Beiträge zahlt die GUUG dem Autor nach Aufforderung durch die Redaktion und Rechnungstellung durch den Autor pro Seite 50 € zuzüglich eventuell anfallender USt. Beiträge für die Rubrik „Vereinsleben“,

Buchrezensionen und Artikel bezahlter Redakteure sind davon ausgenommen. Gleiches gilt für Paper, wenn die UpTimes die Proceedings der Konferenz enthält.

Nächste redaktionelle Ausgabe:
UpTimes 2016-1, Sommer-Ausgabe

- Redaktionsschluss: Sonntag, 22. Mai 2016.
- Erscheinung: Sonntag, 26. Juni 2016.
- Gesuchte Inhalte: Fachbeiträge über Unix und verwandte Themen, Veranstaltungsberichte, Rezensionen, Beiträge aus dem Vereinsleben.
- Manuskript-Template: http://www.guug.de/uptimes/artikel-vorlage.tex
- Fragen, Artikelideen und Manuskripte an: <kehrer@guug.de> oder an die Redaktionsmailingliste <redaktion@uptimes.de>



Über die GUUG
German Unix User Group e.V.

Vereinigung deutscher Unix-Benutzer

Die Vereinigung Deutscher Unix-Benutzer hat gegenwärtig rund 700 Mitglieder, davon etwa 90 Firmen und Institutionen.

Im Mittelpunkt der Aktivitäten der GUUG stehen Konferenzen. Ein großes viertägiges Event der GUUG hat eine besondere Tradition und fachliche Bedeutung: In der ersten Jahreshälfte treffen sich diejenigen, die ihren beruflichen Schwerpunkt im Bereich der IT-Sicherheit, der System- oder Netzwerkadministration haben, beim *GUUG-Frühjahrsfachgespräch* (FFG).

Seit Oktober 2002 erscheint mit der *UpTimes* – die Sie gerade lesen – eine Vereinszeitung. Seit 2012 erscheint die UpTimes einerseits zu jedem FFG in Form einer gedruckten Proceedings-Ausgabe (ISBN), und andererseits im Rest des Jahres als digitale Redaktionsausgabe (ISSN). Daneben erhalten GUUG-Mitglieder zur Zeit die Zeitschrift *LANline* aus dem Konradin-Verlag kostenlos im Rahmen ihrer Mitgliedschaft.

Schließlich gibt es noch eine Reihe regionaler Treffen (http://www.guug.de/lokal): im Rhein-Ruhr- und im Rhein-Main-Gebiet sowie in Berlin, Hamburg, Karlsruhe und München.

Warum GUUG-Mitglied werden?

Die GUUG setzt sich für eine lebendige und professionelle Weiterentwicklung im Open Source-Bereich und für alle Belange der System-, Netzwerkadministration und IT-Sicherheit ein. Wir freuen uns besonders über diejenigen, die bereit sind, sich aktiv in der GUUG zu engagieren. Da die Mitgliedschaft mit jährlichen Kosten

Fördermitglied	350 €
persönliches Mitglied	90 €
in der Ausbildung	30 €

verbunden ist, stellt sich die Frage, welche Vorteile damit verbunden sind?

Neben der Unterstützung der erwähnten Ziele der GUUG profitieren Mitglieder auch finanziell davon, insbesondere durch die ermäßigten Gebühren bei den Konferenzen der GUUG und denen anderer europäischer UUGs. Mitglieder bekommen außerdem *c't* und *iX* zum reduzierten Abopreis.

Wie GUUG-Mitglied werden?

Füllen Sie einfach das Anmeldeformular unter https://www.guug.de/verein/mitglied/ aus und schicken Sie es per Fax oder Post an die unten auf dem Formular angegebene Adresse.

Impressum

Uptimes – Mitgliederzeitschrift der
German Unix User Group (GUUG) e.V.
Herausgeber: GUUG e.V.
Grube-Nassau-Straße 3
D-56462 Höhn
E-Mail: <redaktion@uptimes.de>
Internet: http://www.guug.de/uptimes/

Autoren dieser Ausgabe: Anika Kehrer, Nils Magnus, Patrick Ben Koetter, Mathias Weidner
V.i.S.d.P: Anika Kehrer
Oslostr. 9
D-81829 München
Chefredaktion: Anika Kehrer
Redaktion: Mathias Weidner, Wolfgang Stief
LaTeX-Layout (PDF): Robin Schröder
XHTML-Layout (ePub): Mathias Weidner
Titelgestaltung: Hella Breitkopf
Bildnachweis: Titelbild *Schneegestöber* von Hella Breitkopf. Icon zum Gedenkkasten *Hannes Kuhnert Kreuz* von Amit6 bei Wikimedia Commons, CC BY SA. Comicreihe *geek & poke* von Oliver Widder, CC BY SA, mit zusätzlicher freundlicher Genehmigung von Oliver Widder. Andere Quellennachweise am Bild.
Verlag: Lehmanns Media GmbH, Hardenbergstraße 5, 10623 Berlin
ISSN: 2195-0016

Wenn Sie Interesse an Anzeigen in der UpTimes haben,
wenden Sie sich bitte an <werbung@guug.de>.