# Sicherheit in einer digital vernetzten Welt

Florian Walther

GIWK-Tagung 2014

27.-29. März 2014 in Bielefeld

# Über mich

- Florian Walther, Baujahr `77, selbständiger IT-Sicherheitsberater
- Seit Ende der 90er Jahre beschäftige ich mich beruflich mit dem Thema IT-Sicherheit.
- Über 12 Jahre Erfahrung als Penetrationstester.
- Zahlreiche praktische Sicherheitsüberprüfungen in verschiedenen Branchen, darunter Softwarehersteller, soziale Netzwerke, Pharma- und Medizintechnik, Automobilindustrie, Maschinenbau, Banken, Versicherungen, Tourismus, Verkehr sowie staatliche Einrichtungen.
- Sachverständiger in IT-Sicherheitsfragen für den Innenausschuss des EU Parlament.
- Vorträge auf Konferenzen wie u.a. Chaos Communication Congress, SigInt, CyCon, Re:publica, alternativer Polizeikongress und viele weitere.
- Schulungen für Firmen und Organisationen wie z.B. Sichere Softwarenetwicklung, Incident- und Threat- und Penetrationstestmanagement, Operative Sicherheit für Mitarbeiter.

# Kenne dein Publikum!

- Nachdem ich nun ein paar Worte zu meiner Person erzählt habe möchte ich auch auch etwas über Sie erfahren.

# Frage 1

- Wer von ihnen hat eine Anti-Virus Software auf dem eigenen Rechner?
- Gegenprobe: Wer von ihnen hat keine Anti-Viren Software?

# Frage 2

- Wer von ihnen arbeitet üblicherweise mit administrativen Rechten auf dem eigenen Rechner? (Das ist wenn sie neue Software installieren können ohne extra ein Passwort eingeben zu müssen)

- Gegenprobe: Wer arbeitet mit einem nicht privilegierten Benutzer?

# Frage 3

- Wer von ihnen hat die Festplatte des eigenen Rechners verschlüsselt? (So dass man vor dem Start des Systems ein Passwort eingeben muss)
- Gegenprobe: Wer hat keine verschlüsselte Festplatte?

# Frage 4

- Wer von ihnen benutzt ein Passwort für mehrere Dienste oder Zugänge?
- Gegenprobe: Wer von ihnen hat für jeden Zugang und jeden Dienst ein eigenes Passwort?

# Sicherheit - ein weites Feld

- Fragt man 3 verschiedene Leute was *Sicherheit* ist, bekommt man 5 verschiedene Antworten.
  - Rechtsstaatlichkeit (Sicherheit vor Willkür)
  - persönliche Sicherheit (Erpressung/Raubüberfälle/ Einbrüche/Entführung/…)
  - Arbeitssicherheit, IT-Sicherheit, Flugsicherheit, militärische Sicherheit, Rechts- und Investitionssicherheit (Investoren und Wirtschaftsvertreter)
  - …

# Sicherheit - ein weites Feld

- Ich möchte mich heute vor allem mit den folgenden Themen beschäftigen:
  - IT-Sicherheit
  - Informationssicherheit
  - Datensicherheit
  - Computersicherheit

# Begriffsklärung

**IT-Sicherheit**

IT-Sicherheit bezeichnet die Sicherheit von soziotechnischen Systemen. IT oder auch ITK-Systeme sind Teil der soziotechnischen Systeme. Zu den Aufgaben der IT-Sicherheit gehört der Schutz von Organisationen (zum Beispiel Unternehmen) und deren Werte gegen Bedrohungen. Gleichzeitig soll wirtschaftlicher Schaden verhindert werden

Quelle: http://de.wikipedia.org/wiki/Informationssicherheit

# Begriffsklärung

**Informationssicherheit**

Der Begriff Informationssicherheit bezieht sich oft auf eine globale Informationssicherheit, bei der die Zahl der möglichen schädlichen Szenarien summarisch reduziert ist oder der Aufwand zur Kompromittierung für den Betreiber in einem ungünstigen Verhältnis zum erwarteten Informationsgewinn steht. In dieser Sichtweise ist die Informationssicherheit eine ökonomische Größe, mit der zum Beispiel in Betrieben und Organisationen gerechnet werden muss.

Quelle: http://de.wikipedia.org/wiki/Informationssicherheit

# Begriffsklärung

**Informationssicherheit**

Abgrenzung zur IT-Sicherheit: Die Informationssicherheit umfasst neben der Sicherheit der IT-Systeme und der darin gespeicherten Daten auch die Sicherheit von nicht elektronisch verarbeiteten Informationen. Beispiel: Die Prinzipien der Informationssicherheit können auch auf per Hand auf Papier notierte Rezepte eines Restaurants angewendet werden (da Vertraulichkeit, Integrität und Verfügbarkeit der Rezepte für das Restaurant extrem wichtig sein können, selbst wenn dieses Restaurant 100 % ohne Einsatz irgendeines IT-Systems betrieben wird).

Quelle: http://de.wikipedia.org/wiki/Informationssicherheit

# Begriffsklärung

**Datensicherheit**

Datensicherheit ist ein häufig mit dem Datenschutz verknüpfter Begriff, der von diesem zu unterscheiden ist. Datensicherheit hat das technische Ziel, Daten jeglicher Art in ausreichendem Maße gegen Verlust, Manipulationen und andere Bedrohungen zu sichern. Hinreichende Datensicherheit ist eine Voraussetzung für effektiven Datenschutz.

Quelle: http://de.wikipedia.org/wiki/Informationssicherheit

# Begriffsklärung

**Computersicherheit**

Die Sicherheit eines Computersystems vor Ausfall und Manipulation sowie vor unerlaubtem Zugriff (virtuell als auch physikalisch).

# Wie entsteht Sicherheit in einer digital vernetzten Welt?

- **Vertraulichkeit** - Nur berechtigte Personen sollen Informationen einsehen und/oder verändern können.
- **Integrität** - Daten dürfen nicht unbemerkt verändert werden. Alle Änderungen müssen nachvollziehbar sein.
- **Verfügbarkeit** - Verhinderung von Systemausfällen; der Zugriff auf Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet sein.
- **Authentizität** - bezeichnet die Eigenschaften der Echtheit, Überprüfbarkeit und Vertrauenswürdigkeit eines Objekts.
- **Verbindlichkeit/Nichtabstreitbarkeit** - „kein unzulässiges Abstreiten durchgeführter Handlungen“
- **Zurechenbarkeit** - „Eine durchgeführte Handlung kann einem Kommunikationspartner eindeutig zugeordnet werden.“ oder kommuniziere ich wirklich mit demjenigen mit dem ich kommunizieren möchte.

# Wie entsteht Sicherheit in einer digital vernetzten Welt?

- Sicherheit in einer digital vernetzten Welt braucht allerdings auch **Anonymität und Abstreitbarkeit**

- Unter anderen für Journalisten, Aktivisten, Menschenrechtler, Angehörige von verfolgten Minderheiten oder Religionsgemeinschaften sowie Whistleblower und viele andere

# Gegensätzliche Ziele

- Wer bei den letzten beiden Folien aufgepasst hat, dem wird aufgefallen sein, dass manche Ziele zur Erreichung von Sicherheit (in einer digital vernetzten Welt) gegensätzlich sind.

- Zurechenbarkeit / Nichabstreitbarkeit sind mit Abstreitbarkeit und Anonymität nicht in Einklang zu bringen!

- Wir brauchen aber - je nach Szenario - beides.

# (Nicht)Abstreitbarkeit

- Für - über das Internet - geschlossene Verträge brauchen wir Nichtabstreitbarkeit.
- Um die rechtswidrigen Aktivitäten meines Arbeitgeber als Whistleblower an die Öffentlichkeit zu bringen brauche ich plausible Abstreitbarkeit und Anonymität.

# Anonymität

- In einer digital vernetzten Welt, in welcher immer mehr Aspekte des täglichen Lebens im Internet stattfinden brauchen Bürger Anonymität um für Staat und Industrie nicht zum gläsernen Menschen zu werden.

- Es gibt zahlreiche weitere Beispiele für die man Anonymität braucht. Beratungsstellen, Ermittlungen, Recherchen,….

# Herausforderungen

- strategische Vorteile der Angreifer
- banana software
- multi-stage, multi-step und multi-jurisdiction
- attribution problem
- Aberglaube

# Strategischer Vorteil für Angreifer

- Ein Angreifer muss nur eine Lücke im System finden, ein Verteidiger muss alle finden (und beheben - können)

# Banana Software

- Bananen werden unreif (noch grün) zum Kunden geschickt und reifen auf dem Weg zum oder beim Kunden.
- Als Banana Software bezeichnet man Software die - wie Bananen - beim Kunden reift.
- Unfertige, nicht ausreichend getestete Software wird zum Kunden ausgeliefert und dann (möglicherweise, wenn man Glück hat) nachträglich geflickt.
- Oft werden Sicherheitskisiken bei Planung, Entwurf und Entwicklung von Software nicht oder nur unzureichend betrachtet. SDL ist immer noch die Ausnahme.

# Multi-Stage Angriffe

- Multi Stage - Als Multi-Stage Angriff bezeichnet man einen Angriff im Internet welcher über mehrere Stationen geführt wird.

- Ein Täter greift System A an, um von dort System B zu kompromittieren und von System B wiederum System C, und so weiter.

# Multi-Step Angriffe

- Als Multi-Step Angriff bezeichnet man einen Angriff der in mehreren zeitlich mitunter weit auseinander liegenden Schritten ausgeführt wird.
- Beispiel: Im **Mai** wird ein Rechner einer Bank kompromittiert (und bleibt unentdeckt), im **Oktober** werden über diesen Rechner (Multi-Stage) die Kreditkartendaten der Kunden - von einem anderen Rechner - kopiert. Im **Februar** des Folgejahres fallen Unregelmäßigkeiten bei den Kreditkartenabrechnungen auf.

# Multi-Jurisdiction

- Unsere Justiz und Strafverfolgungssysteme sind auf Nationalstaaten ausgerichtet, das Internet ist aber global und kennt keine Nationen, Territorien und Grenzen.
- Multi-Stage Angriffe werden so auch schnell zu einem Problem vieler beteiligter Jurisdiktionen.
- Wenn die Ermittler den Durchsuchungsbefehl im letzten Land bekommen haben, ist der aus dem ersten Land nicht mehr gültig. Durchsucht man nicht zeitgleich werden Täter möglicherweise gewarnt und dadurch nicht ermittelt oder gefasst.

# Attribution Problem

- Als Attributions Problem bezeichnet man das Problem dass man im Internet nicht weiß welche Person etwas getan hat, sondern nur welche Maschine. In Kombination mit den schon zuvor Erklärten Multi-Stage, Multi-Step und Multi-Jurisdiction Problemen entsteht das sogenannte Attribution Problem.

- Nur weil ich weiß das der Angreifer von einem Rechner in China kommt, heißt das noch lange nicht das ein Chinese hinter dem Angriff steckt. Es könnte genauso gut ein 14jähriger Brasilianer sein.

# Warum ist das Attributionsproblem so schwierig zu lösen?

- Siehe Multi-Stage, Multi-Step und Multi-Jurisdiction.
- Das Attributionsproblem kann nicht mit technischen Mitteln alleine gelöst werden.
- Das Attributionsproblem braucht internationale Kooperation und gemeinsame Standrads auf die sich die Verantwortlichen anscheinend nicht einigen können oder wollen.

# Konzepte

- Haftungsrisiken für Softwarehersteller würden die ökomimische Gleichung der Hersteller verändern, so dass Sicherheit für die Hersteller wichtiger würde.

- Abgestufter Schutz: für gut administrierte Systeme wird hoher - rechtlicher - Schutz garantiert, für schlecht administrierte Systeme könnte ein niedrigeres Schutzniveau gelten um Ermittlungen und Gegenmaßnahmen zu vereinfachen.

# Kategorie: Aberglaube

- Aberglaube: Glaubenssätze und Praktiken, die wissenschaftlich unbegründet sind und nicht dem erreichten Kenntnisstand einer Gesellschaft entsprechen.

# Aberglaube: Kopierschutz

- Computer sind Maschinen zum Kopieren von Daten. Die meisten Leute glauben Computer seien in erster Linie Maschinen zum Rechnen ( heißt ja auch *Rechner*). In der Realität kopieren Computer aber zu ca. 75% und Rechnen nur zu ca. 25%.

- Maschinen zum Kopieren von Daten wird man das kopieren von Daten nicht abgewöhnen können. Leider versucht die Inhalte-Industrie immer wieder genau das zu erreichen.

# Aberglaube: PLPII

- PLPII steht für Packet Level Personal Identifiable Information. Die Idee dahinter ist das Attributionsproblem zu lösen indem man jedes Datenpaket mit persönlichen Informationen des Absenders versieht, um so bei einem IT-Angriff die Identität des Angreifers erkennen zu können.

- Die wenigsten Menschen bauen ihre Datenpakete von Hand zusammen und *morsen* diese dann ins Kabel. Es sind Maschinen zum Kopieren von Daten die das tun.

- Also müsste man die Informationen zur eigenen Identität erst einer Maschine übergeben, die dann für mich alle von mir erzeugten Datenpaket vor dem Versand damit versieht.

- Was kann da schon schief gehen?

# Aberglaube: Zensur

Cencorship is telling a man he can't have a steak just because a baby can't cheew it. - *Mark Twain*

—

Die Zensur ist das lebendige Geständnis der Großen, daß sie nur verdummte Sklaven treten, aber keine freien Völker regieren können. - *Johan Nepomuk Nestroy*

# Aberglaube: AntiVirus

- Wir kaufen uns eine AV Software und eine Firewall, dann sind wir sicher. - Falsch!
- Ein Anti-Virus Program birgt allerhand Probleme:
  - Parsing - ist komplex und fehleranfällig.
  - AV parst alles was ein Angreifer so schickt.
  - AV läuft (zumindest teilweise) mit Systemrechten  - muss ja überall reinschauen dürfen, vor allen anderen Prozessen.
  - Für Network Intrusion und - Prevention Systeme gilt das genauso.

# Verbessern sie ihre IT-Sicherheit

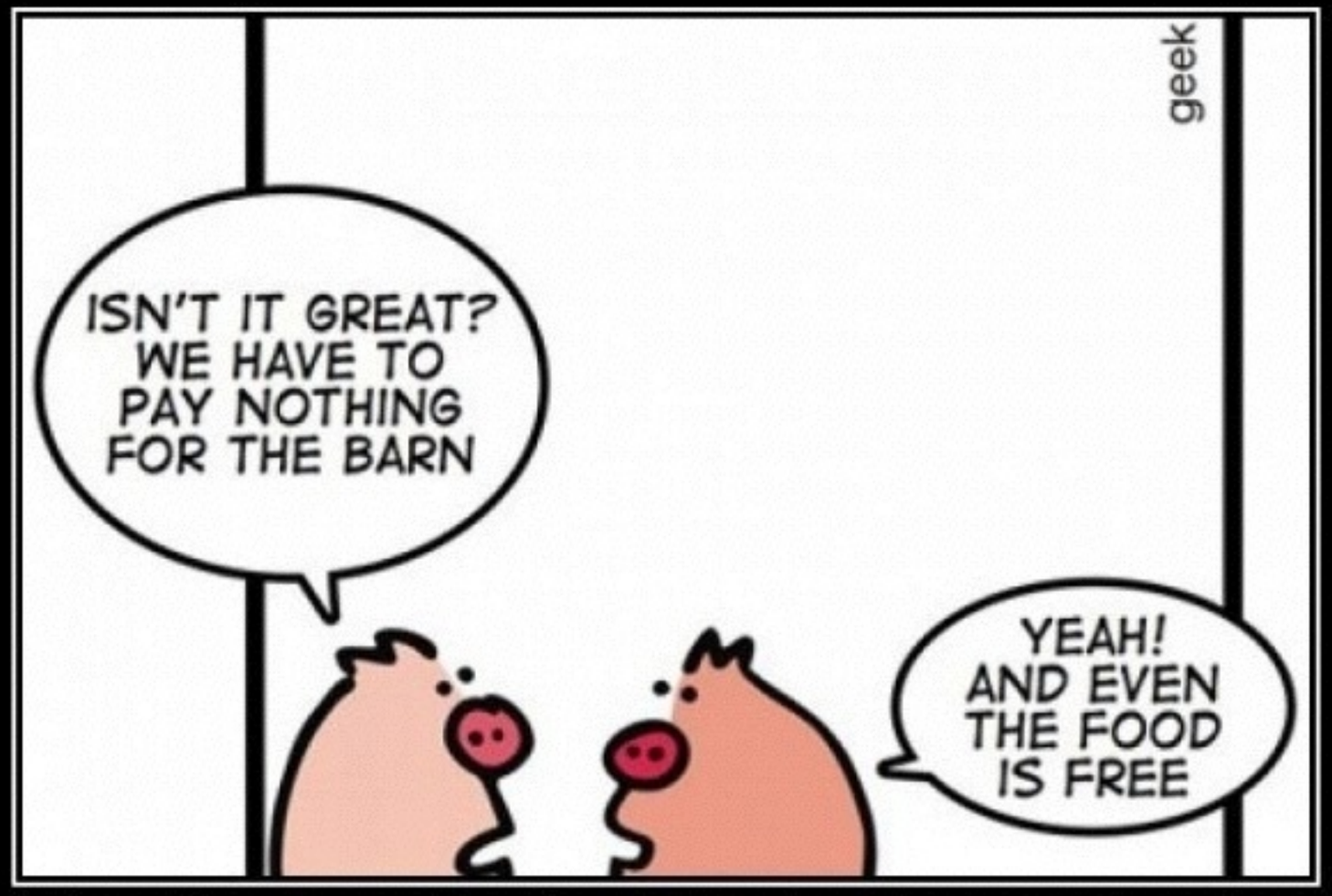
- Benutzen sie ein aktuelles Betriebssystem (Windows XP ist keines!)
- Installieren sie Sicherheitsaktualisierungen für ihr System (Betriebssystem, Treiber, Anwendungen)
- Nutzen sie einen guten Passwortmanager oder ein Passwortschema um für jeden Dienst und Zugang ein individuelles Passwort zu verwenden.

# Verbessern sie ihre IT-Sicherheit

- TrueCrypt ist toll!
- verschlüsseln Sie ihre Festplatte(n), und Speichermedien, alle, immer.
- Zeigen Sie ihren Freunden, Bekannten und Arbeitskollegen wie das geht.
- …oder lassen sich das mal zeigen.

# Verbessern sie ihre Datensicherheit!

- Wer nicht zum gläsernen Bürger/Konsument/ Kunde/Antragsteller/Vertragspartner/Patienten/ … werden will, sollte das folgende klar sein:




# FACEBOOK AND YOU

If you're not paying for it, you're not the customer. You're the product being sold.

# Bist du schon Kunde, oder noch Produkt?

- Für alle kostenlose Angebote im Internet (die nicht von einer do-it-yourself community getragen werden) gilt:

- Wer für einen Dienst nichts bezahlt, ist nicht der Kunde, sondern das Produkt welches verkauft wird!

# Verschlüsselung muss sein!

- Internetdienste ohne Verschlüsselung sind untragbar. `https://` o.ä. muss sein wenn persönliche Daten übertragen werden.

# Vielen Dank…

…für ihre Zeit und Aufmerksamkeit.

Sie erreichen mich per Email unter:
florian.walther@posteo.de
PGP-ID: 0x74A5D6EA

Fingerprint:
3434 E348 C15A 069D D2A6
11FB AC62 9AC8 74A5 D6EA

# Fragen?

- Fragen sie jetzt!