„10 things I wished they'd told me!“

IT Analyse. Software Test. Better Results.

„10 things I wished they'd told me!“

Julia Kremsl
Marketing

Darum SEQIS...

SEQIS „10 things“ Programm 2017

16.03.2017	Agile Testing Strategie für die effiziente Continuous Delivery von Microservices
01.06.2017	Die EU Datenschutz-Grundverordnung – Auswirkungen auf den Test
21.09.2017	Auf dem Weg zur innovativen Lösung – Kreativität in der IT Analyse
16.11.2017	**Sind Sie (sich) wirklich sicher? – IT Security im Fokus**

Sind Sie (sich) wirklich sicher? – IT Security im Fokus

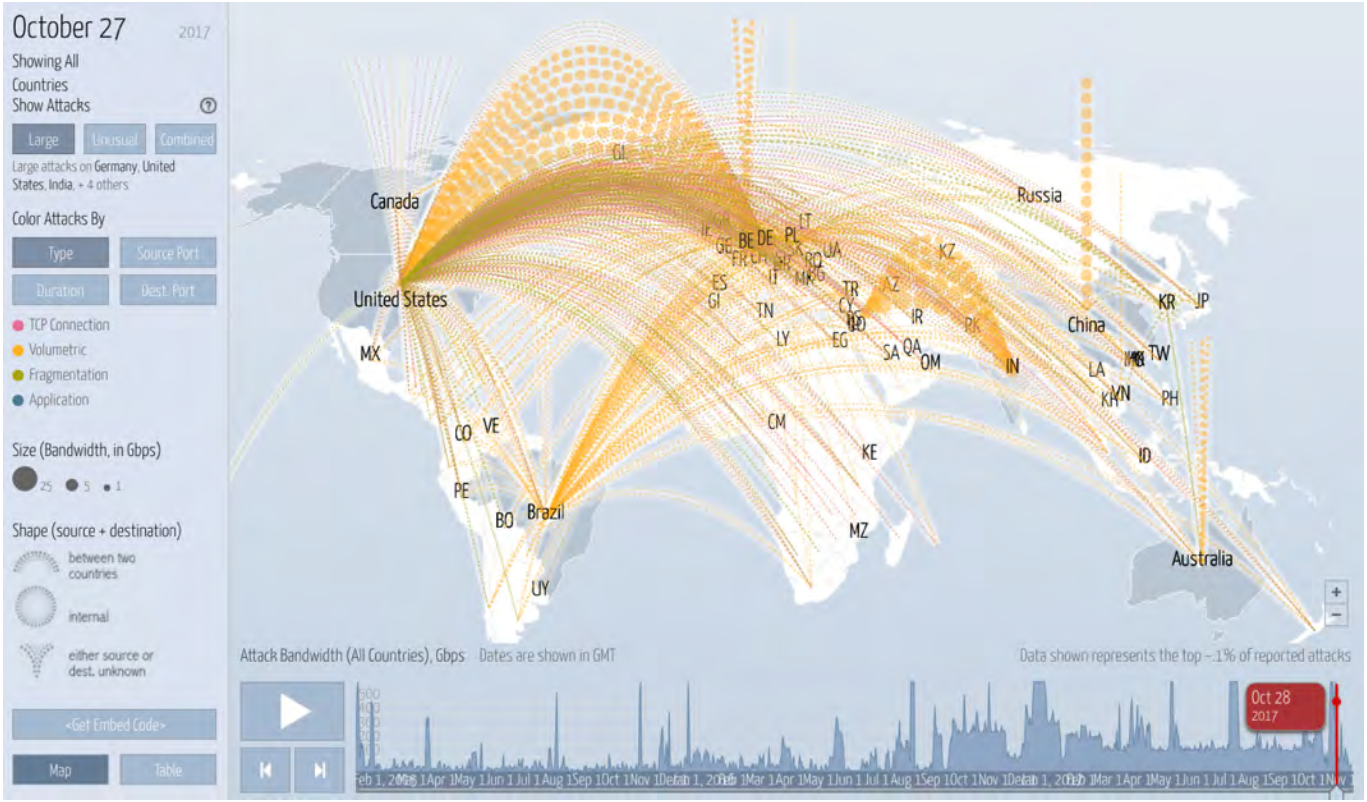
Klemens Loschy

Principal Consultant, Teamlead

- „[... Bedrohungslage nach wie vor als ansteigend einzustufen.
- Neue Geschäftsmodelle
  - Randsomware-as-a-Service
  - Crime-as-a-Service
- Cyber Kriminalität hat sich rasch entwickelt.]“

Cyber Sicherheit Steuerungsgruppe, Mai 2017

Die Frage ist...



http://www.digitalattackmap.com/

Die Frage ist...

... nicht OB sondern

WANN zuletzt und WANN wieder?

Und WIE davor schützen?

http://www.digitalattackmap.com/

Software Development Life Cycle

Secure Software Development Life Cycle

10 things
I wished they'd told me!

7. Social Engineering Richtlinien

A & D	DEV	TST	OPS
2. Analyse der Security-requirements	4. Secure Coding Guidelines	5. White – Black Box Testing	
3. Architektur & Design Vorgaben		6. Verletzbarkeit und Patchmanagement	

1. Security Richtlinie, Compliance Guidelines & Standards/Normen

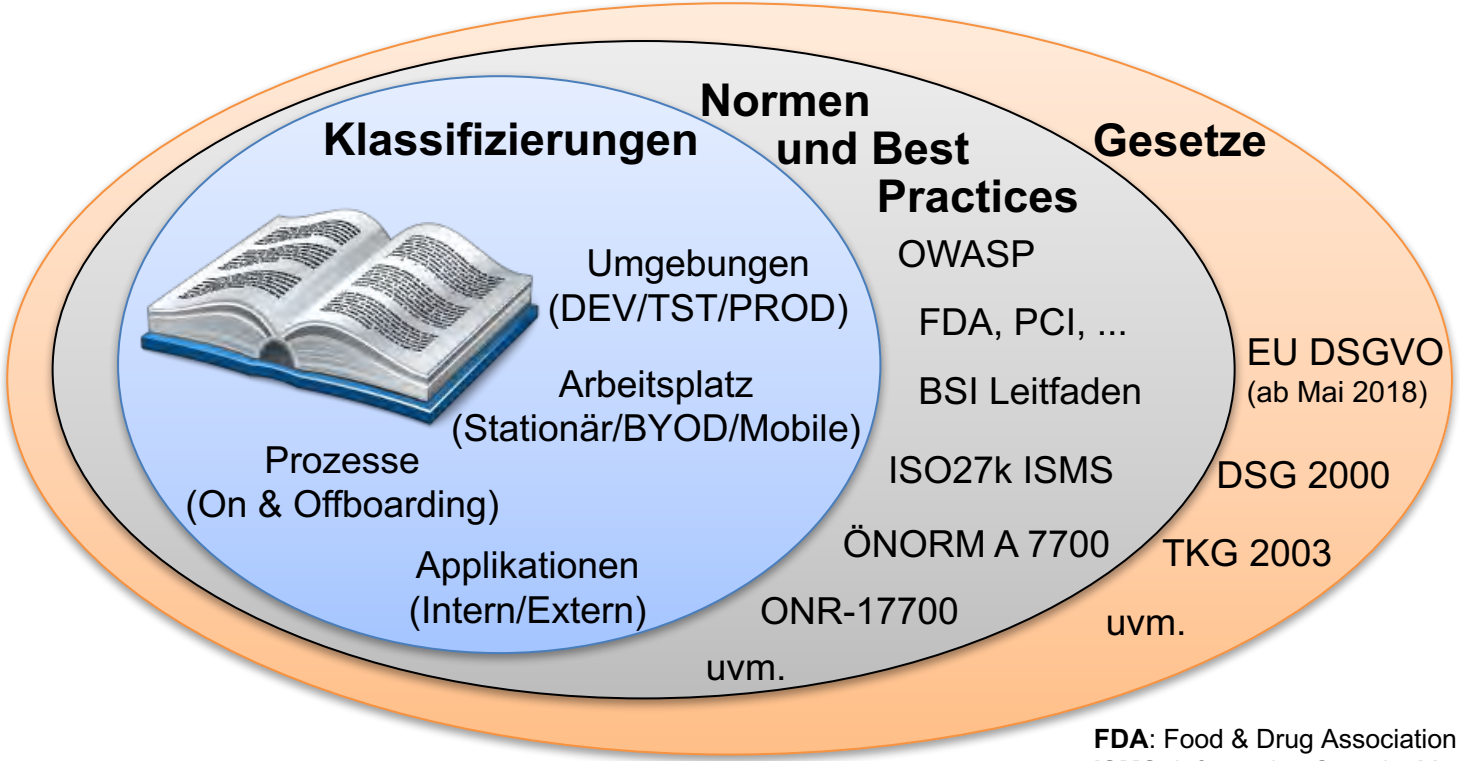
Secure Software Development Life Cycle

10 things I wished they'd told me!

A & D	DEV	TST	OPS

1. Security Richtlinie, Compliance Guidelines & Standards/Normen

Unternehmensweite Sicherheitsrichtlinien



BSI: Bundesamt f. Sicherheit i.d. IT
DSG: Datenschutzgesetz
EU DSGVO: EU Datenschutz-Grundverordnung

FDA: Food & Drug Association
ISMS: Information Security Management Systems
OWASP: Open Web Application Security Project
PCI: Payment Card Industry
TKG: Telekommunikationsgesetz

Persönlicher Komfort exponiert Sicherheit

10 things
I wished they'd told me!

Persönlicher Komfort exponiert Sicherheit

Persönlicher Komfort exponiert Sicherheit

Persönlicher Komfort exponiert Sicherheit

Nur ausgewählte Daten!

Persönlicher Komfort exponiert Sicherheit

Nur ausgewählte Daten!

Persönlicher Komfort exponiert Sicherheit

Persönlicher Komfort exponiert Sicherheit

10 things
I wished they'd told me!

Nur ausgewählte Daten!

Passcode erweitern!

Daten wieder löschen!

Persönlicher Komfort exponiert Sicherheit

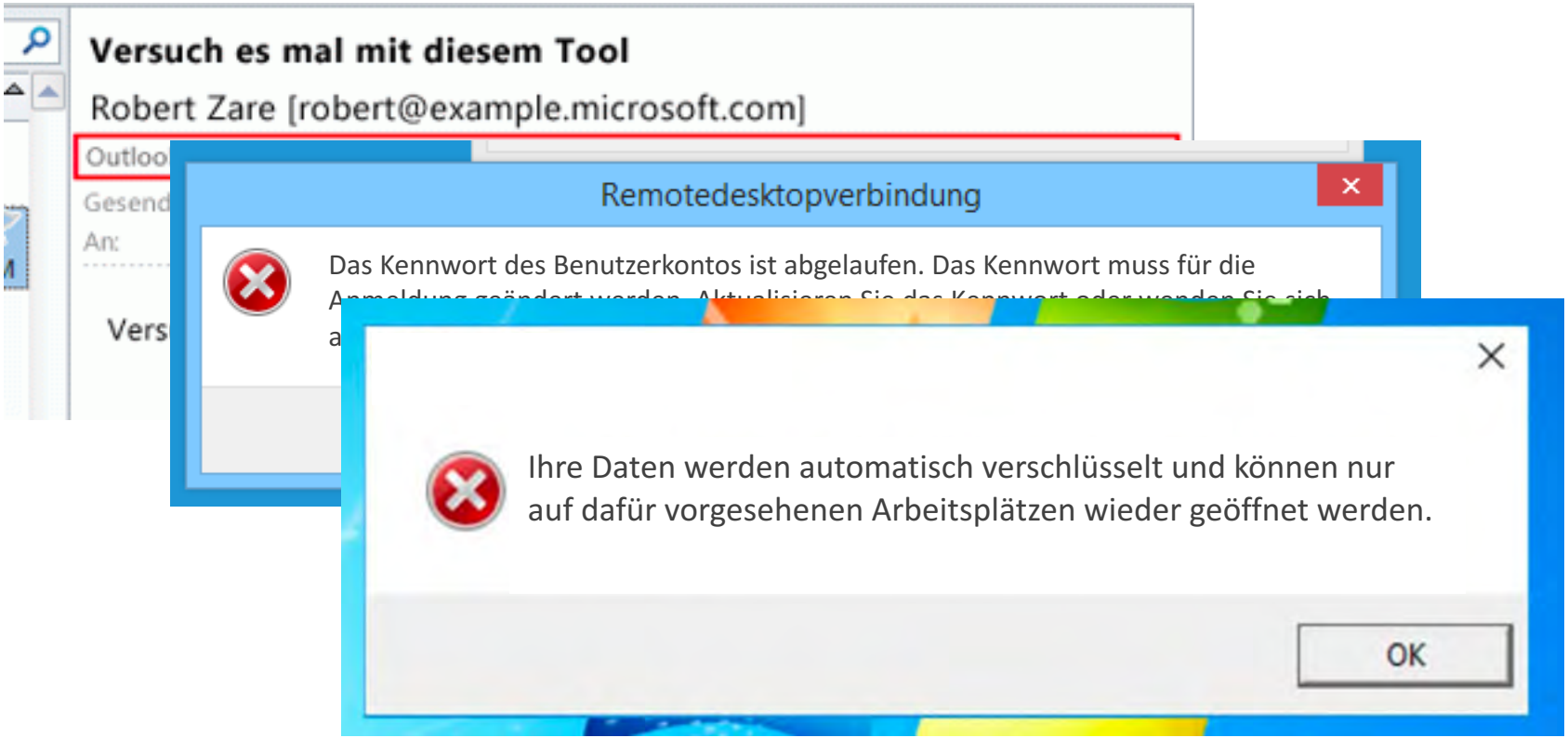
Security First!

10 things
I wished they'd told me!

1. **Definieren Sie eine unternehmensweite Sicherheitsrichtlinie!**

- Normen, Standards, Gesetze und Best Practices
- Detaillierungsgrad (gering → hoch)
- Persönliche Maßnahmen setzen

Unterstützung oder Hürde?



10 things
I wished they'd told me!

2. Unterstützen Sie Ihre Mitarbeiter mit sinnvollen Einschränkungen!

- Hürden werden kreativ (und unsicherer) umgangen
- Weniger ist mehr

Secure Software Development Life Cycle

10 things I wished they'd told me!

A & D	DEV	TST	OPS

2. Analyse der Security-requirements

1. Security Richtlinie, Compliance Guidelines & Standards/Normen

Der sichere Blickwinkel

- **Klemens**
- Männlich
- 30-40
- HTL-Matura
- IT-Branche
- Verheiratet

Interessen

- Hausautomation, Sport

Sicherheitsbewusstsein

- **legt Wert auf hohe und zeitgemäße Standards**

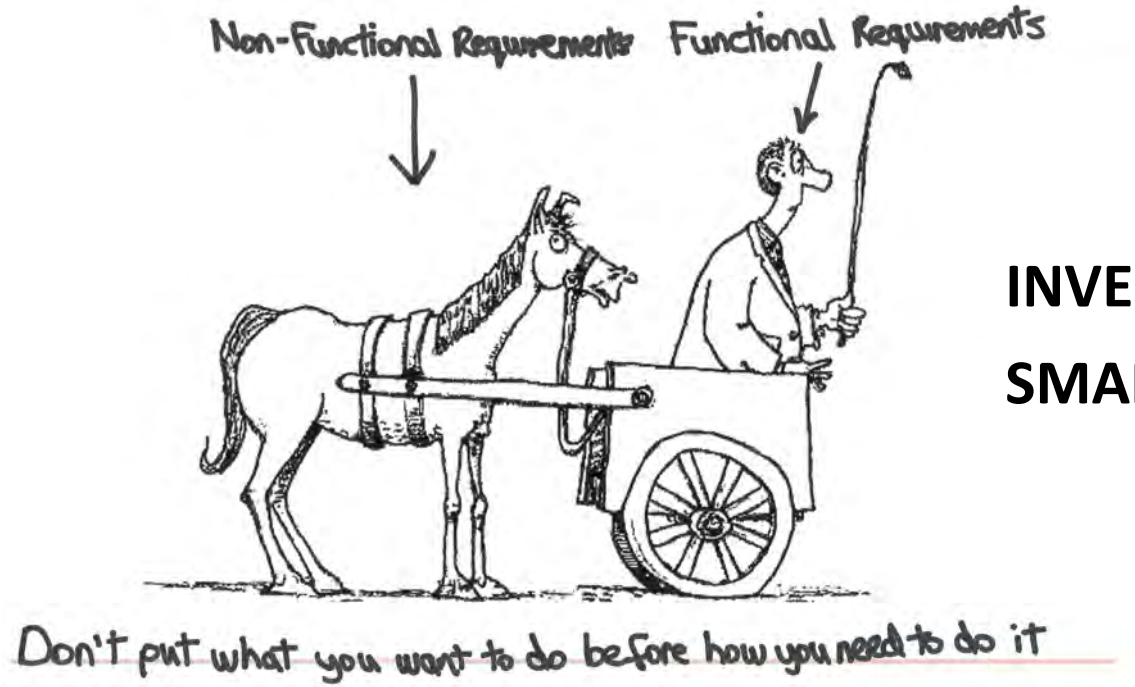
...

„Personas“ mit definiertem Sicherheitsbezug

Zusätzlicher mit Security Fokus

http://www.furnitureandfurnishing.com/images/sep15/business-issues-beyond-innovation-the-wholistic-advantage-02.jpg

Nicht funktional? Nicht so wichtig?



INVEST
SMART
!

INVEST: Independent, Negotiable, Valuable, Estimable, Small
SMART: Specific, Measurable, Achievable, Relevant, TimeBoxed

https://stevenwilliamalexander.files.wordpress.com/2015/07/nfr-non-functional-cart-before-horse.png

Nicht funktional? Nicht so wichtig?

NFAs sind das Fundament einer Applikation!

INVEST: Independent, Negotiable, Valuable, Estimable, Small
SMART: Specific, Measurable, Achievable, Relevant, TimeBoxed

https://stevenwilliamalexander.files.wordpress.com/2015/07/nfr-non-functional-cart-before-horse.png

Secure Software Development Life Cycle

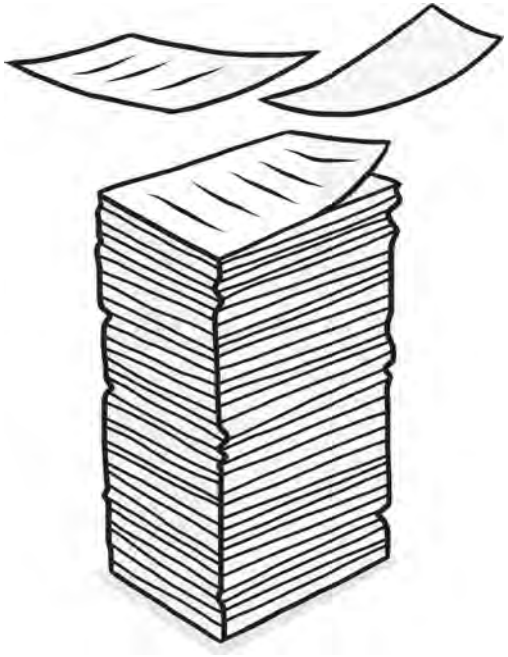
A & D	DEV	TST	OPS

2. Analyse der Security-requirements

3. Architektur & Design Vorgaben

1. Security Richtlinie, Compliance Guidelines & Standards/Normen

Spätestens jetzt...



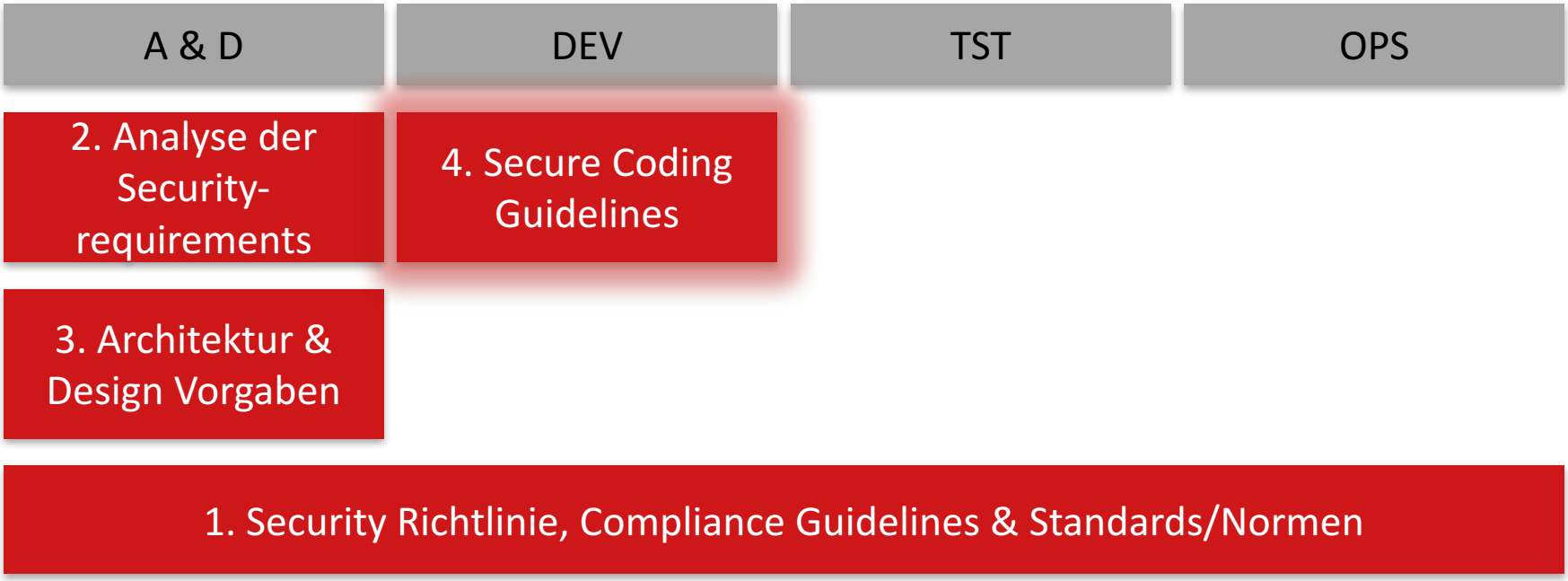
1. Security Richtlinie, Compliance Guidelines & Standards/Normen

10 things
I wished they'd told me!

3. Security muss von Anfang an berücksichtigt werden!

- Security nachträglich zu integrieren ist aufwändig bis unmöglich
- Anforderungen speziell mit Blick auf Security definieren und prüfen

Secure Software Development Life Cycle



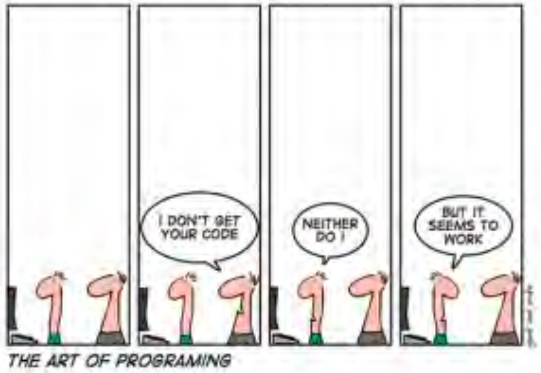
Wieso Coding Guidelines?

10 things I wished they'd told me!

Code must be read- and understandable

Keep it small and simple

Least necessary privilege



Minimize the attack surface area

Obscurity is not security

Validate input and verify consistency

Don‘t trust (services, dependencies, ...)

Don‘t develop custom authentication and session management

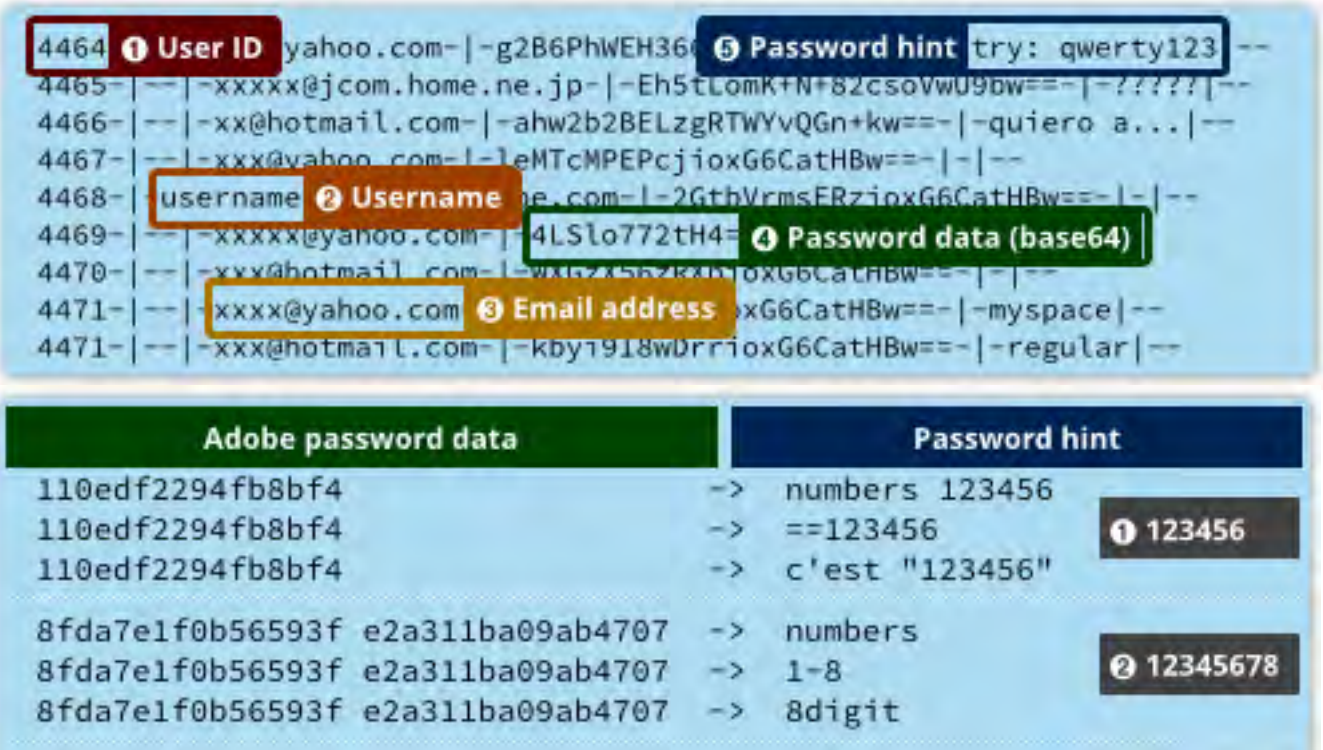
http://blog.castsoftware.com/wp-content/uploads/2011/04/Poor-Software-Quality.jpg

10 things
I wished they'd told me!

4. Definieren Sie Coding Guidelines und halten Sie diese ein!

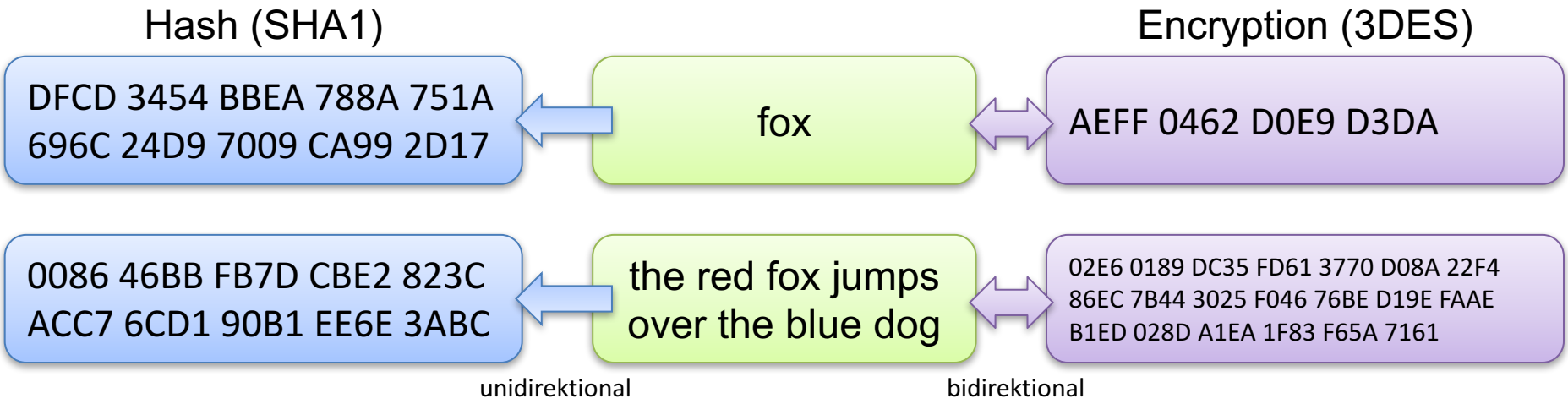
- Disziplin und Commitment notwendig (besonders vor Deadlines/Milestones/...)
- Kaum technische Herausforderungen

Das größte Kreuzworträtsel der Welt

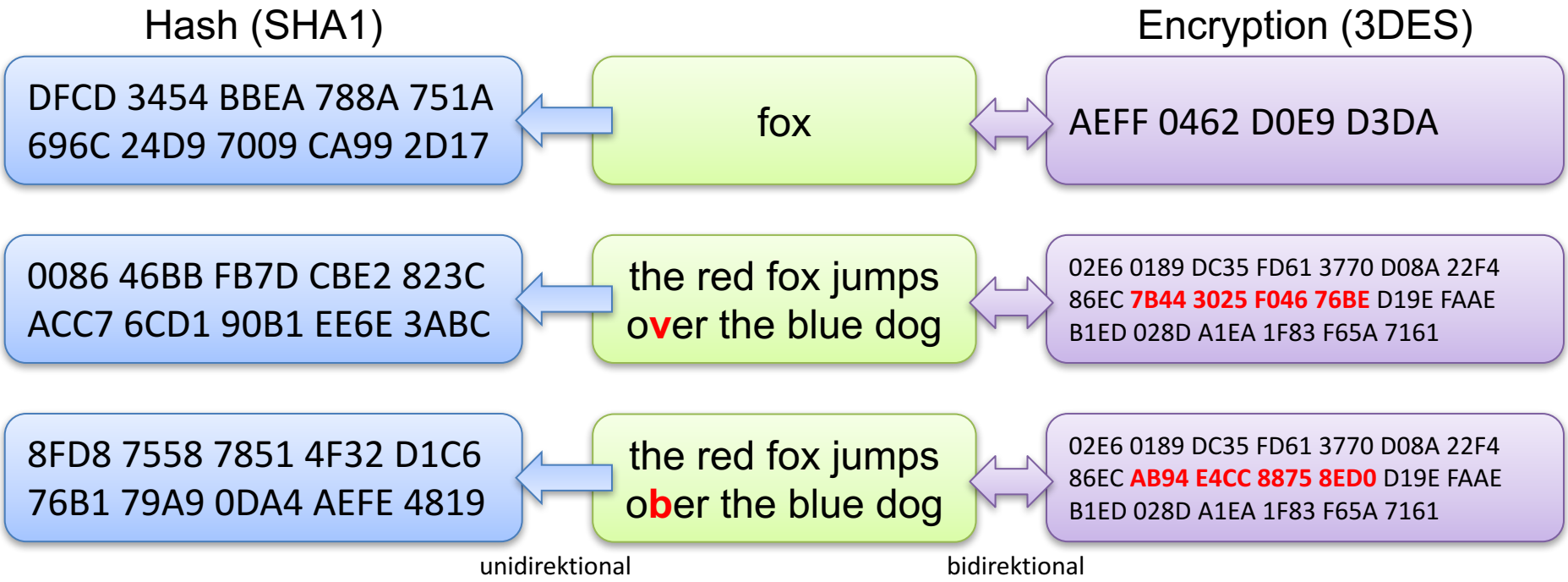


https://nakedsecurity.sophos.com/2013/11/04/anatomy-of-a-password-disaster-adobes-giant-sized-cryptographic-blunder/

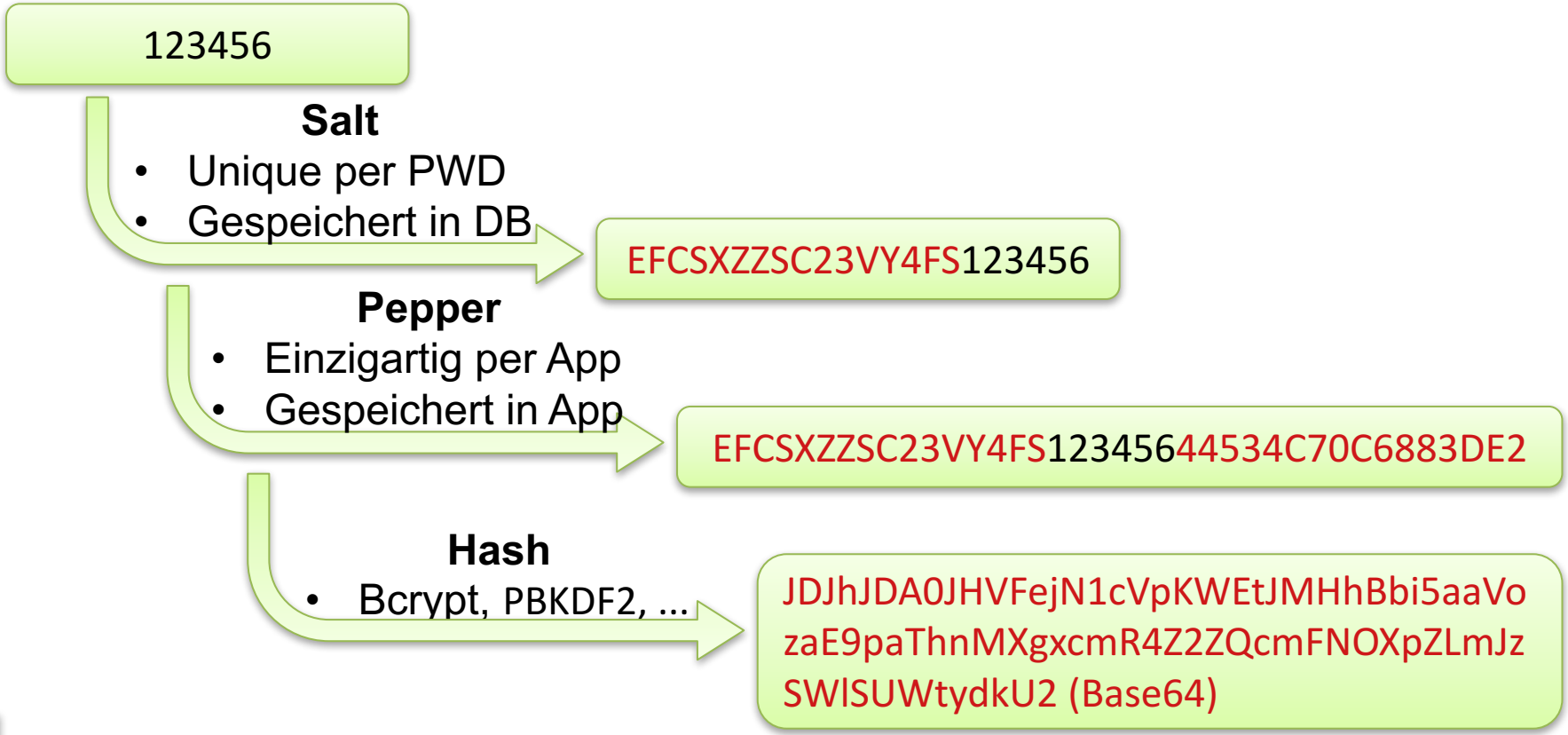
(crypto) Hashing vs. Encryption



(crypto) Hashing vs. Encryption



Hashing mit Salt and Pepper



10 things
I wished they'd told me!

5. Gehen Sie sorgsam mit Benutzerdaten um!

- Verwendung von (aus heutiger Sicht) als sicher geltende Algorithmen
- Passworte hashen, andere personenbezogene Daten (Sicherheitsfragen, Passwort Hinweise, ...) verschlüsseln

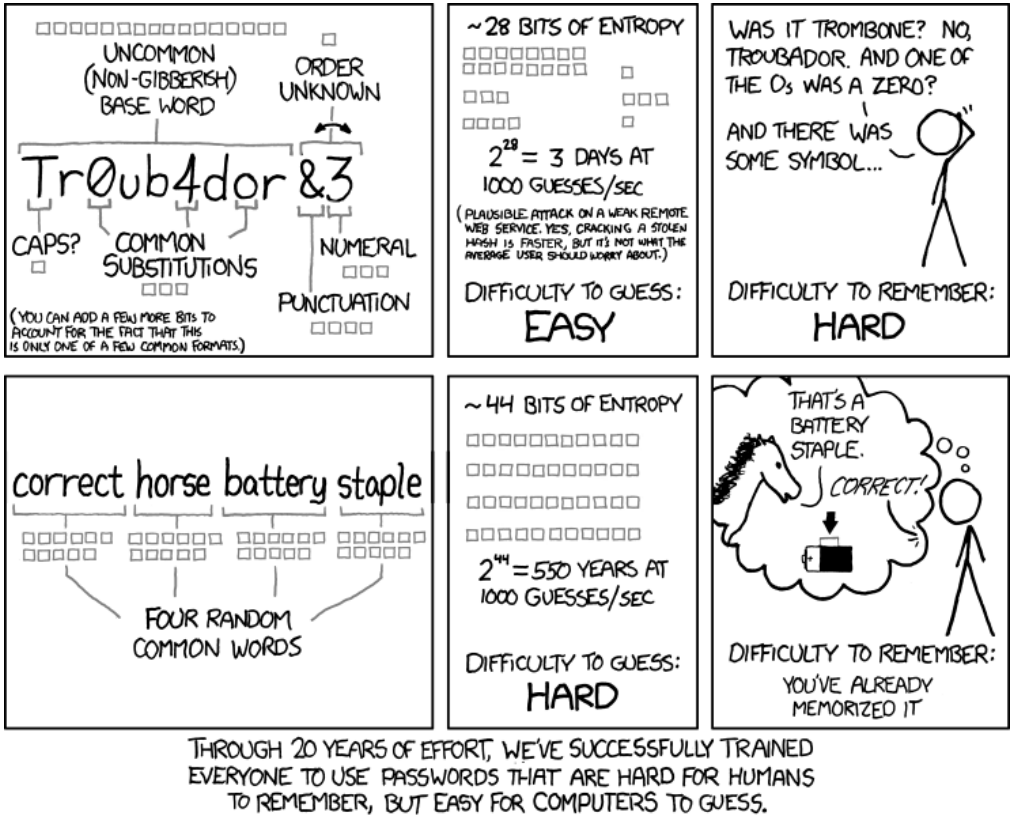
Das sichere Passwort

10 things
I wished they'd told me!

„Mindestens eine Zahl, mindestens ein Sonderzeichen und ab und zu einfach mal ein neues Passwort“

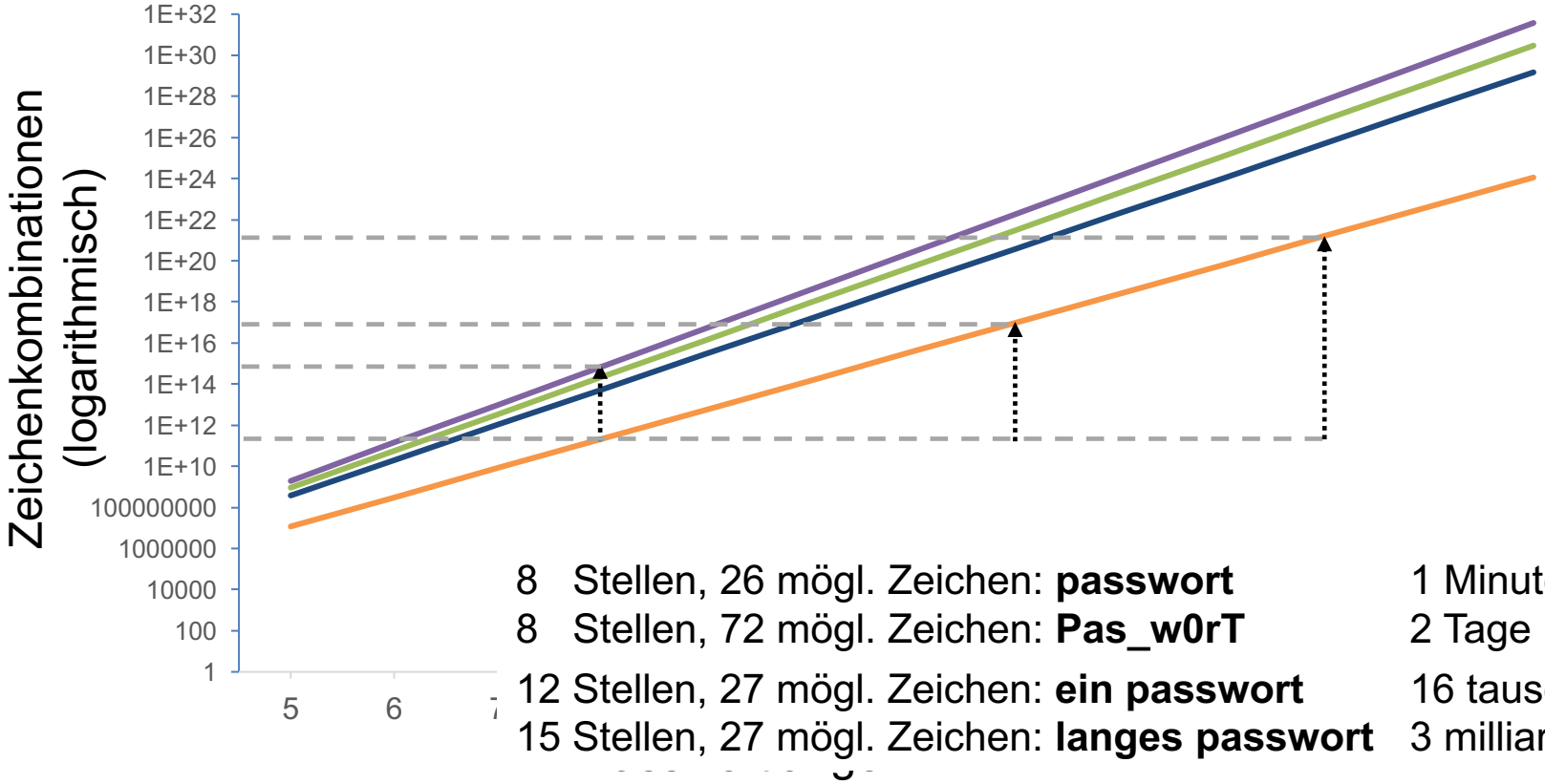
Bill Burr, 2003, National Institute for Standards and Technology (NIST)

Komplexität vs. Länge



https://xkcd.com/936/

Komplexität vs. Länge



8 Stellen, 26 mögl. Zeichen: **passwort**		1 Minute
8 Stellen, 72 mögl. Zeichen: **Pas_w0rT**		2 Tage
12 Stellen, 27 mögl. Zeichen: **ein passwort**		16 tausend Jahre
15 Stellen, 27 mögl. Zeichen: **langes passwort**		3 milliarden Jahre

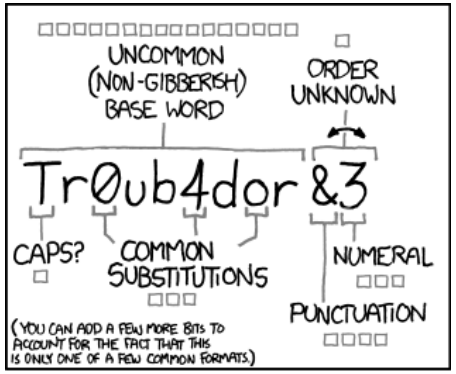
Komplexität vs. Länge vs. Verbreitung

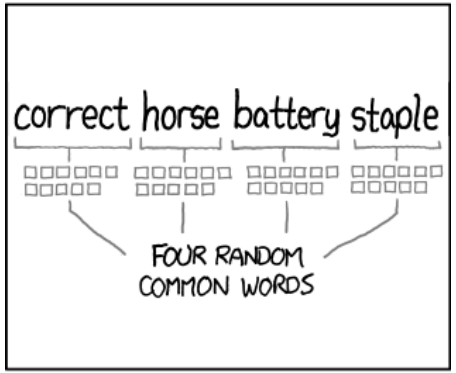
10 things
I wished they'd told me!

https://wpengine.com/unmasked/

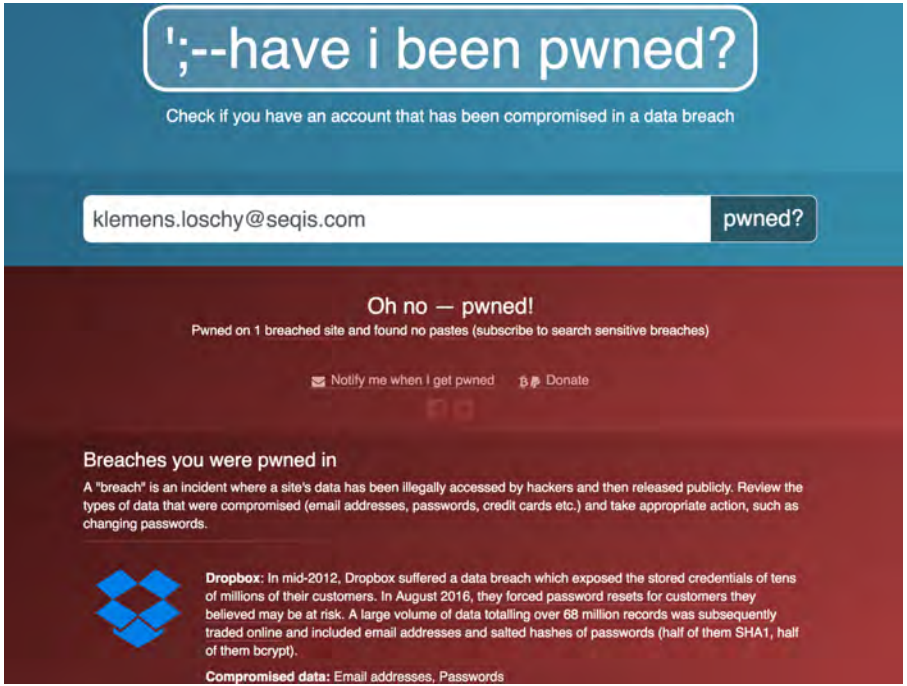
https://wpengine.com/unmasked/assets/images/5-most-used-passwords.png

Das eigentliche Problem



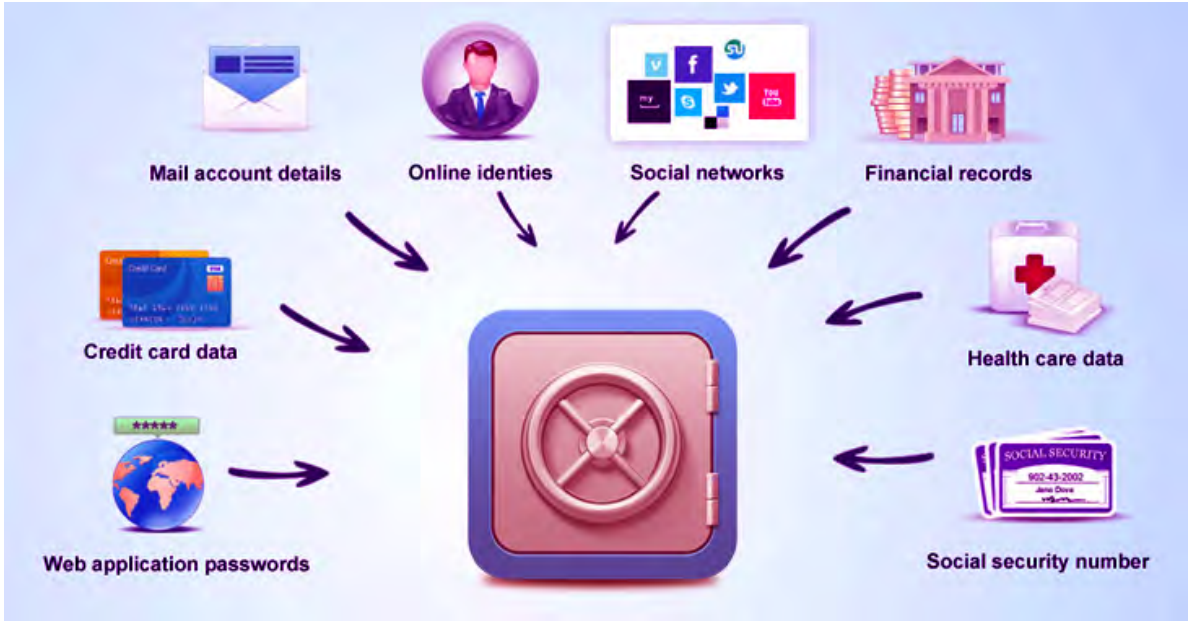


Das eigentliche Problem



https://haveibeenpwned.com/

Eine (einfache) Lösung: Passwort Manager



1 Passwort merken (entsprechend stark)
X Passwörter (automatisch) verwenden

 https://1.bp.blogspot.com/-LY7pI45tMq0/V5r_XV083RI/AAAAAAAAo6M/MivILg0_4Vs7UgLKZJqM5vhvYujQCCcpgCLcB/s1600/best-password-manager-software.png

Password 2.0: two factor authentication

https://lifehacker.com/5932700/please-turn-on-two-factor-authentication

Die Zukunft: biometrische Merkmale?

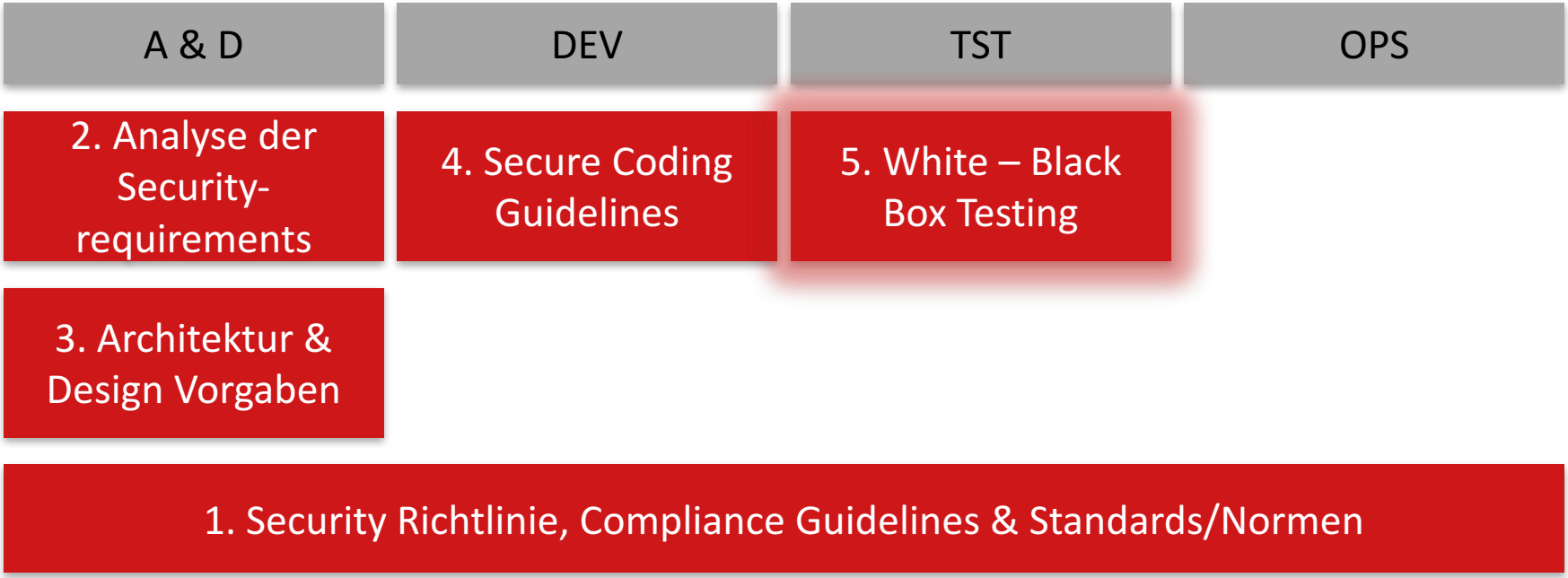
https://www.troyhunt.com/content/images/2017/09/Face-ID.png

10 things
I wished they'd told me!

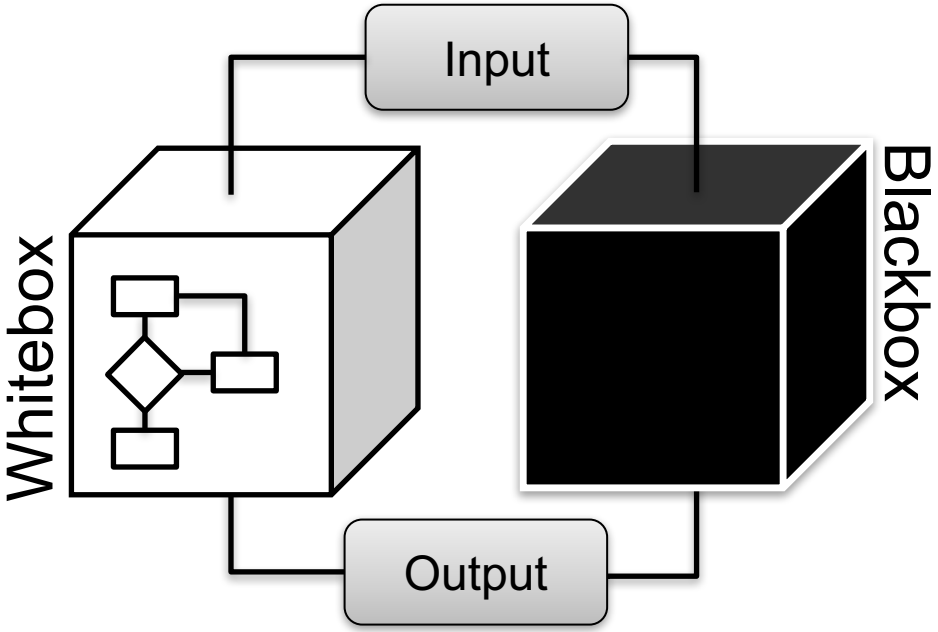
6. Forcieren Sie Länge und Eindeutigkeit bei Passwörtern!

- Komplexität allein hilft nicht
- Benutzung von Passwort Managern ermöglichen
- Optionale two factor authentication erhöht zusätzlich die Sicherheit

Secure Software Development Life Cycle



Test Techniken



Statisch

Dynamisch

Testinhalte: Fokus auf Security

Authentication and session management

Password brute force prevention

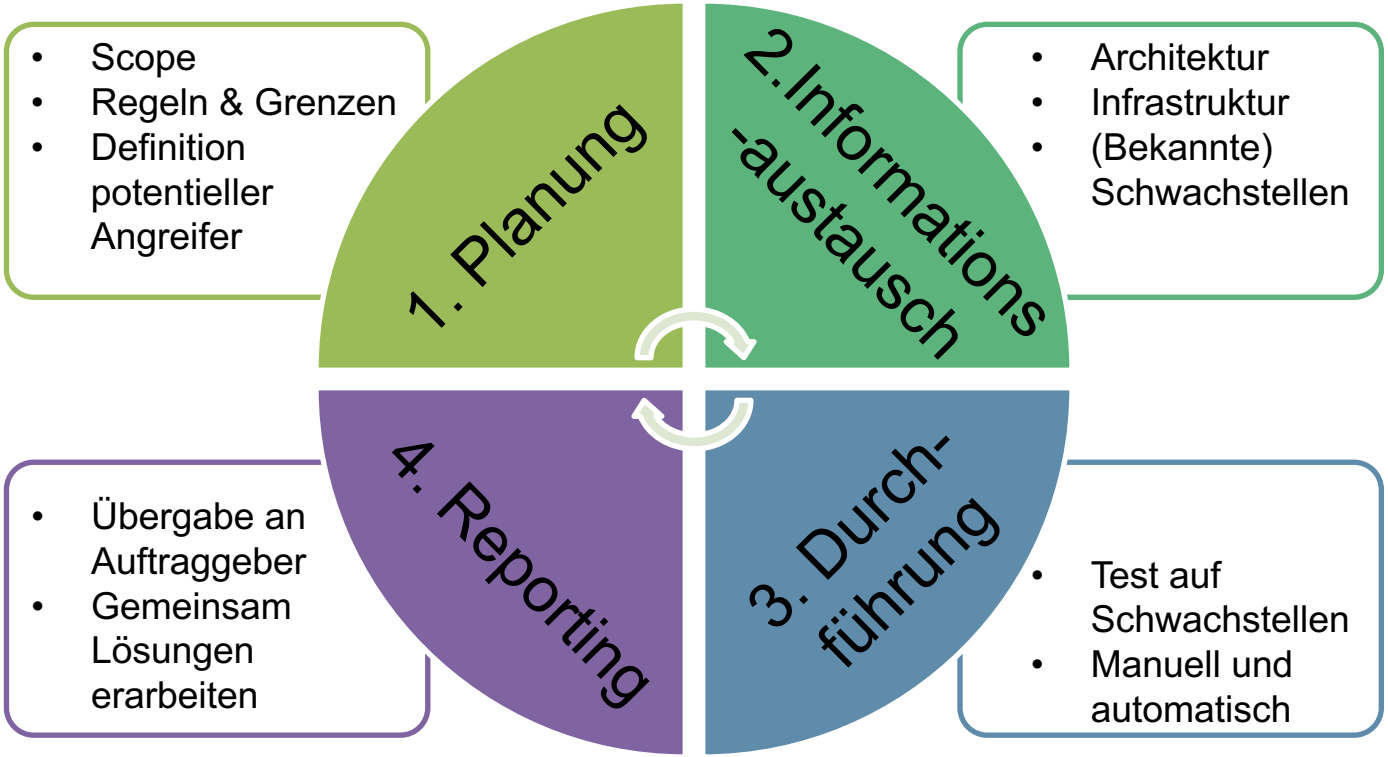
XSS and SQL Injection prevention

Server side input validation

File upload and handling

Minimal error messages and return codes

Schwachstellen finden: PEN Testing!

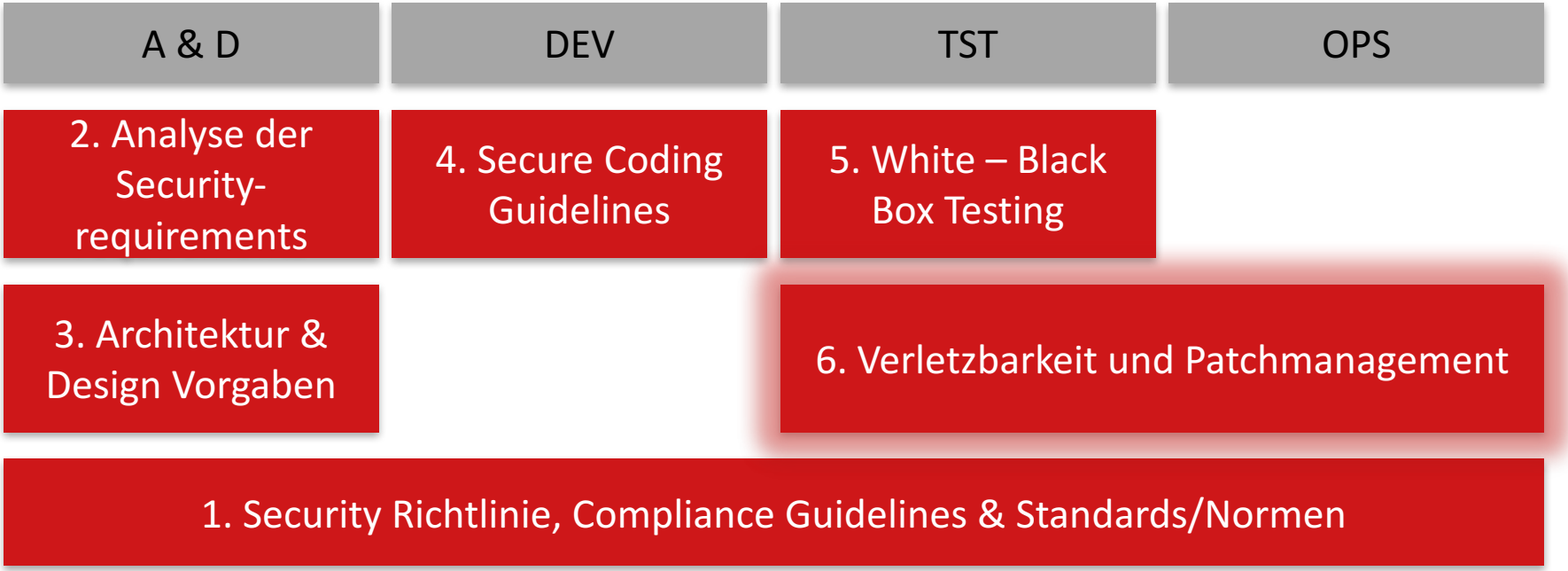


10 things
I wished they'd told me!

7. Security Issues findet man nicht nebenbei!

- Nur mit gezielten Tests und der Tester-Expertise ist das möglich
- Security-Status zyklisch mittels PEN Tests feststellen und Schwachstellen schließen

Secure Software Development Life Cycle



Secure Operations

10 things
I wished they'd told me!

IPS

IDS

Firewall

UTM

NSM

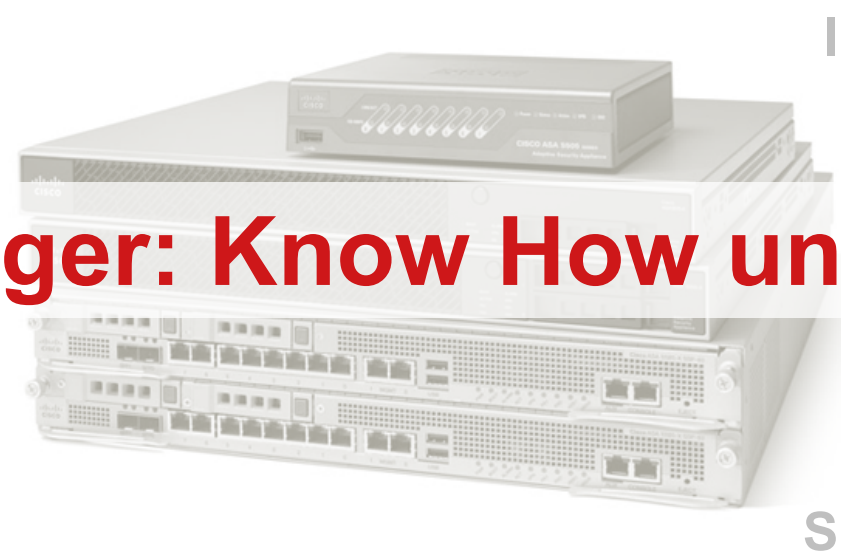
SIEM

IPS: Intrusion Protection System
NSM: Network Security Manager

IDS: Intrusion Detection System
UTM: Unified Threat Manager
SIEM: Security Information and Event Management

https://www.cisco.com/content/dam/assets/swa/img/600/security-appliance-asa-software-600x400.jpg

Secure Operations



Wichtiger: Know How und Zeit!

IPS: Intrusion Protection System
NSM: Network Security Manager

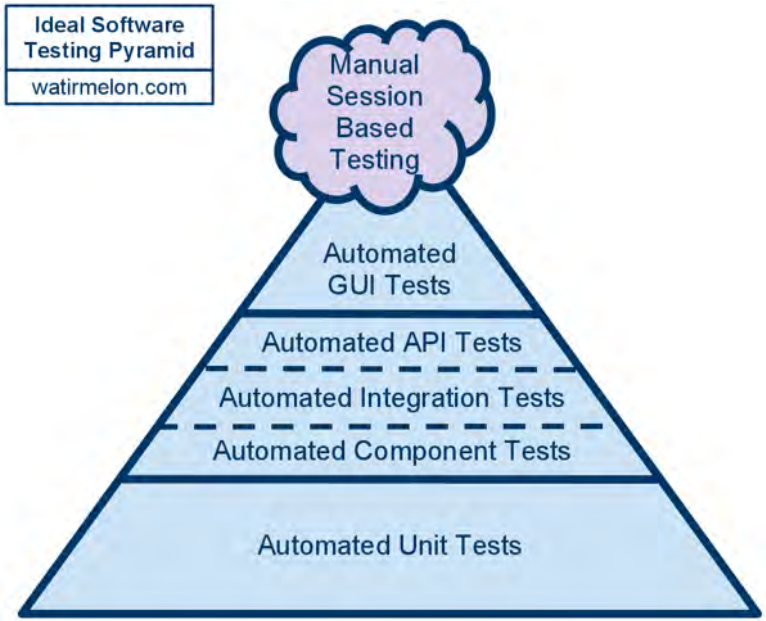
IDS: Intrusion Detection System
UTM: Unified Threat Manager
SIEM: Security Information and Event Management

Auf Exploits schnell reagieren

Auf Exploits schnell reagieren

up2date halten und Änderungen testen!

Auf Exploits schnell reagieren



https://watirmelon.files.wordpress.com/2012/01/automatedtestingpyramid.png

10 things
I wished they'd told me!

8. Sichern Sie Ihre Systeme durch etablierte Appliances (IDS, IPS, UTM, usw.)!

- Test aller Updates auf (nicht) funktionale Sideeffects
- Fast Feedback durch gezielten Einsatz von Testautomation

Simulierte Realität: RED Team Assessment

https://vignette.wikia.nocookie.net/rvb/images/7/77/Red_Team_Jersey.jpg/revision/latest?cb=20140709011924

Data Breach Plan

10 things
I wished they'd told me!

1. **Vorbereitet** sein
2. Erste Stunden entscheiden (**30 min**)
3. **Fakten** töten Mythen
4. Transparenz: **völlig**
5. Wer spricht? **Nur einer**
6. **100% korrekte** Aussagen
7. Sofort und durchgängig **ansprechbar**
8. Zugang zu Informationen **kontrollieren**
9. **Interne** Kommunikation
10. **Mitgefühl** zeigen

10 things
I wished they'd told me!

9. Erstellen und testen Sie Ihren Data Breach Plan!

- Der Ernstfall muss gut vorbereitet sein und geprobt werden (RED Team)

Secure Software Development Life Cycle

10 things
I wished they'd told me!

7. Social Engineering Richtlinien

A & D	DEV	TST	OPS
2. Analyse der Security-requirements	4. Secure Coding Guidelines	5. White – Black Box Testing	
3. Architektur & Design Vorgaben		6. Verletzbarkeit und Patchmanagement	

1. Security Richtlinie, Compliance Guidelines & Standards/Normen

Nicht zielgerichtetes Social Engineering

https://itsecurity.blog.fordham.edu/wp-content/uploads/2017/09/phishing03_web.png
https://www.cablebahamas.com/wp-content/uploads/2017/01/slack-imgs.com_.jpeg

Gezieltes Ausnutzen

Bequemlichkeit

Vertrauen

Hilfsbereitschaft

Autoritätshörigkeit

„wie du mir, so ich dir“

Unwissenheit

Schlechtes Multitasking

https://cdn.davidwolfe.com/wp-content/uploads/2016/03/manipulation-FI02.jpg

10 things
I wished they'd told me!

Wie lautet Ihr Windows Benutzername & Passwort?

Don‘t trust anymore?

10 things
I wished they'd told me!

29,8%

http://orbilu.uni.lu/handle/10993/26214

Don‘t trust anymore?

10 things
I wished they‘d told me!

39,9%

http://orbilu.uni.lu/handle/10993/26214

Don‘t trust anymore?

10 things
I wished they'd told me!

47,9%

http://orbilu.uni.lu/handle/10993/26214

Don‘t trust anymore?

10 things
I wished they‘d told me!

48,3%

http://orbilu.uni.lu/handle/10993/26214

Don‘t trust anymore?

10 things
I wished they'd told me!

48,3%

Trust, but verify!

http://orbilu.uni.lu/handle/10993/26214

10 things
I wished they'd told me!

10. Nehmen Sie Social Engineering ernst!

- Awareness schaffen durch Aufklärung, Workshops und Trainings aller Mitarbeiter

Secure Software Development Life Cycle

10 things
I wished they'd told me!

7. Social Engineering Richtlinien

A & D	DEV	TST	OPS
2. Analyse der Security-requirements	4. Secure Coding Guidelines	5. White – Black Box Testing	
3. Architektur & Design Vorgaben		6. Verletzbarkeit und Patchmanagement	

1. Security Richtlinie, Compliance Guidelines & Standards/Normen

10 things
I wished they'd told me!

11. Security muss aktiv betrieben werden!

- Nur darüber reden allein macht es nicht sicherer

SEQIS „10 things“ Programm 2018

15.03.2018	Early Access - Lassen wir den Kunden testen?!
14.06.2018	Der Output der IT-Analyse oder Das Frankenstein-Prinzip
20.09.2018	Automate your mobile - 10 instruktive Tipps zur Testautomation
15.11.2018	Agile PM

„10 things I wished they'd told me!“

IT Analyse. Software Test. Better Results.