GFU Cyrus AG

anderScore
trust in competence

Sicherheitsrisiko Mensch - Social Engineering

25.07.17, J.Lühr

Inhalt

1. Vorstellung & Einleitung 2

2. Usable Privacy & Security: Fallbeispiele & Motivation 8

3. Social Engineering 18

4. Wie entwickeln wir sichere Software? 19

Unser Unternehmen: Zahlen & Fakten

anderScore trust in competence

Unser Fokus:

- Individual-Entwicklung, Projekte kompletter SW life-cycle
- pragmatisches, agiles Vorgehen, auch bei Auftragsarbeiten/ Festpreis, kurze Zyklen, zielorientierte, brauchbare Ergebnisse
- komponentenbasierte web-Anwendungen
- stabile, zweckorientierte Architekturen, performance-tuning
- technisch: Java-Umgebungen
- Optimierungen/ Migrationen unwartbar gewordender Altanwendungen
- Prozessgestaltung (BPM)
- Service-Orientierung, SOA, Integrationsarchitekturen
- mobileApps & Plattformen
- security checks (in SW-Entwicklung, im Betrieb)
- trainings, Schulungen

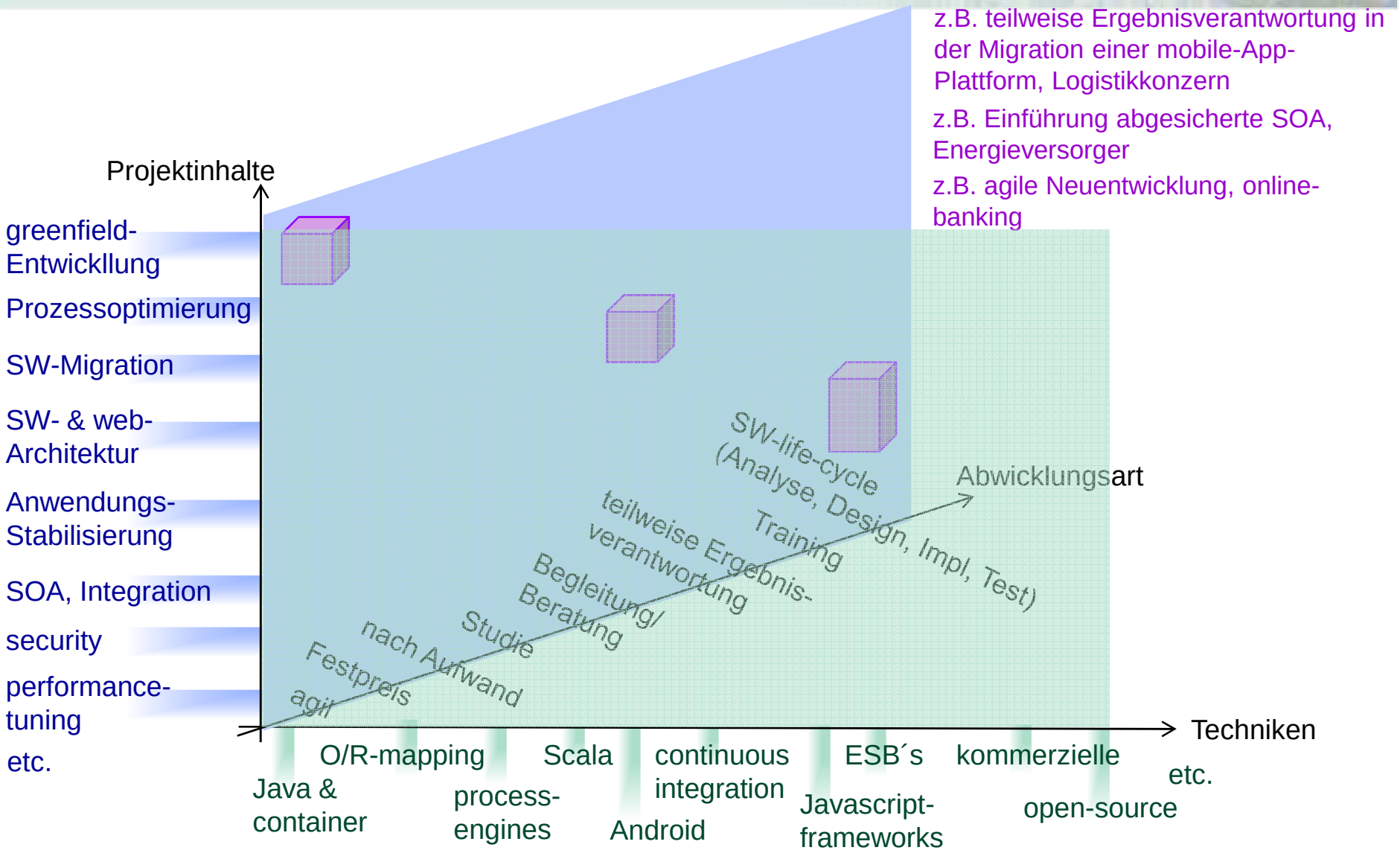
- Gründung Ende 2005 Inhaber-geführte GmbH
- Firmenhauptsitz: Köln
- Über 20 Großkunden
- ~10 Partnerunternehmen
- Goldschmiede anderScore
- Projekt-Staffing auch aus unserem Netzwerk (~70 aus gemeinsamen Projekteinsätzen erprobten Spezialisten)

Mitgliedschaften/ Angliederungen

- IuK-Ausschuss IHK Köln, Digital Cologne
- eco Verband der deutschen internet-Wirtschaft
- BVMW (Bundesverband Mittelständische Wirtschaft)
- JUGC (Java User Group Cologne)
- Kanban Gruppe Köln "limited WIP society"
- Scrumtisch Köln
- VATM (Sitz im selben Gebäude)

Projekt-Leistungsangebot

anderScore trust in competence



1. Vorstellung Jan Lühr
Senior Entwickler, Architekt

anderScore trust in competence

Jan Lühr

Bachelor of Science, Computer Science

- Senior Software Engineer, Architect
- Seit 2007 bei anderScore
- Schwerpunkte
  - Trainer für
    - Security
    - Java (Spring, Wicket ..)
    - JavaScript (jQuery,..)
  - Entwicklung von pragmatischen Architekturen
  - Build- und Deploymentkonzepte
  - Netz- und Sicherheitstechniken
  - Datenbanken & Datenhaltung
- Java, JavaScript, Ruby

1. Einleitung
'Supersichere' Techniken

anderScore trust in competence

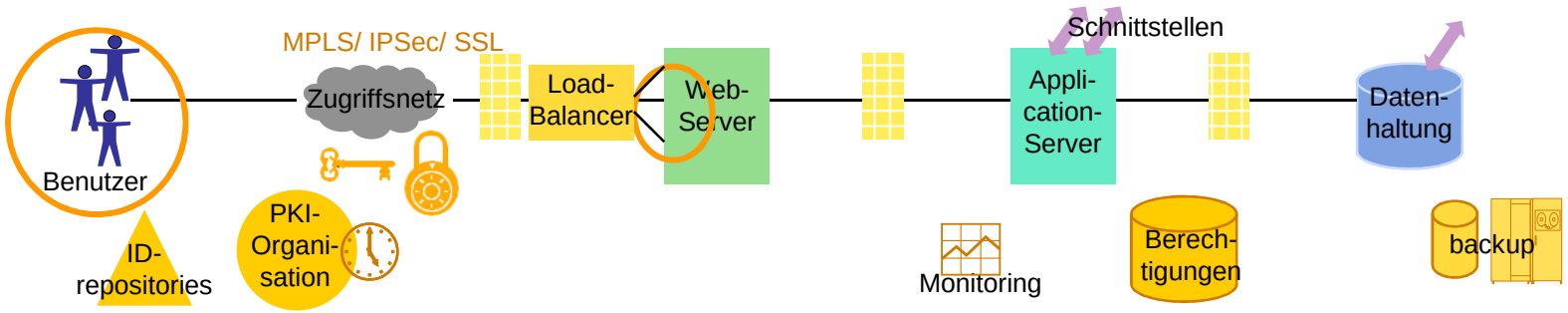
Vielfalt sicherheitsrelevanter Themen:

- ? Signaturen, Zertifikate, PKI
- ? IAM, Benutzerverwaltung, Authentifizierung/ PKI, Autorisierung
- ? Verschlüsselung beim Transfer/ PKI
- ? Zeitstempel/ PKI
- ? VPN´s
- ? Zugriff von außen/ reverse-proxy-Gestaltung/ FW´s/ Zonen (DMZ´s)/ intrusion-detection/ prevention
- ? Ausfallsicherheit (HW-Redundanz mit automatischem failover, LB, backup & restore, monitoring)
- ? Bauliche, organisatorische, personelle Sicherheits-Ebenen

➔ **infrastrukturelle Prägung**

Sicherheitsziele (nach BSI GS):

- **Verfügbarkeit**
- **Integrität**
- **Vertraulichkeit**



Usable Security & Privacy:
Herausforderungen und Motivation

2. FALLBEISPIELE

SICHERE TECHNIK – UNSICHERE BENUTZUNG

2. Fallbeispiel 1
Mirai Botnet

SPIEGEL ONLINE DER SPIEGEL SPIEGEL TV Mein SPIEGEL

NETZWELT

Schlagzeilen | Wetter | DAX 10.662,08 | TV-Programm | Abo

Nachrichten > Netzwelt > Web > Internetkriminalität > DDoS-Attacke: Angriff mit der IP-Cam

Neue Bedrohung

Angriff aus dem Internet der Dinge

Die Website des US-Sicherheitsexperten Brian Krebs ist Opfer eines heftigen Angriffs aus dem Internet geworden. Die schiere Größe der Attacke wirft Licht auf ein neues Phänomen, das Sicherheitsexperten beunruhigt.

Von Andreas Albert

DPA

27.9.2016 , http://www.spiegel.de/netzwelt/web/ddos-attacke-angriff-mit-der-ip-cam-a-1113993.html

2. Fallbeispiel 1
Mirai Botnet

2. Fallbeispiel 1
Mirai Botnet

anderScore trust in competence

KrebsonSecurity
In-depth security news and investigation

03 Who Makes the IoT Things Under Attack?

OCT 16

As KrebsOnSecurity observed over the weekend, the source code that powers the "Internet of Things" (IoT) botnet responsible for launching the historically large distributed denial-of-service (DDoS) attack against KrebsOnSecurity last month has been publicly released. Here's a look at which devices are being targeted by this malware.

The malware, dubbed "**Mirai**," spreads to vulnerable devices by continuously scanning the Internet for IoT systems protected by factory default usernames and passwords. Many readers have asked for more information about which devices and hardware makers were being targeted. As it happens, this is fairly easy to tell just from looking at the list of usernames and passwords included in the Mirai source code.

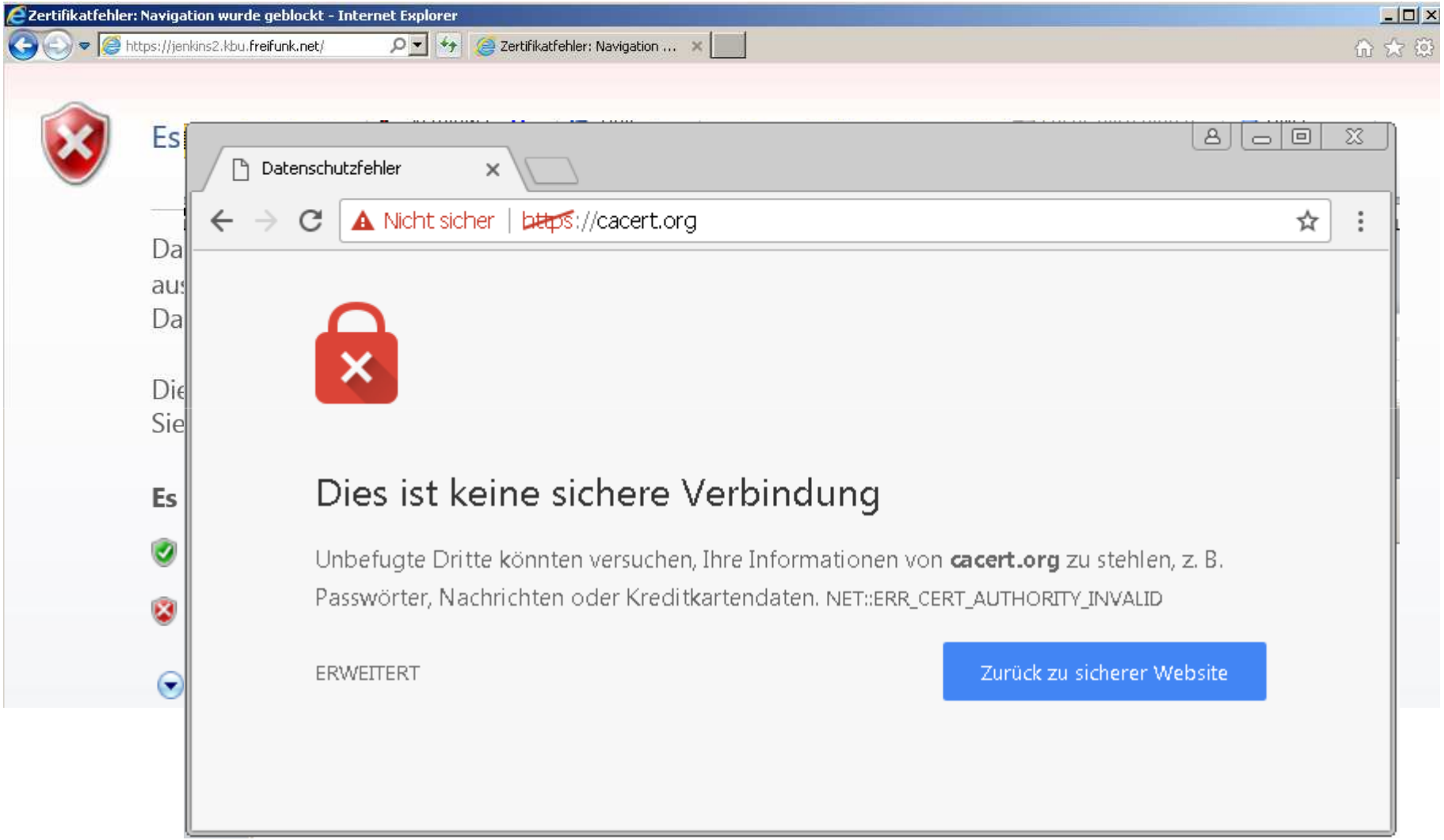
2. Fallbeispiel 1
Mirai Botnet

anderScore trust in competence

Username/Password	Manufacturer	Link to supporting evidence
admin/123456	ACTi IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/anko	ANKO Products DVR	http://www.cctvforum.com/viewtopic.php?f=3&t=44250
root/pass	Axis IP Camera, et. al	http://www.cleancss.com/router-default/Axis/0543-001
root/vizxv	Dahua Camera	http://www.cam-it.org/index.php?topic=5192.0
root/888888	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/666666	Dahua DVR	http://www.cam-it.org/index.php?topic=5035.0
root/7ujMko0vizxv	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
root/7ujMko0admin	Dahua IP Camera	http://www.cam-it.org/index.php?topic=9396.0
666666/666666	Dahua IP Camera	http://www.cleancss.com/router-default/Dahua/DH-IPC-HDW4300C
root/dreambox	Dreambox TV receiver	https://www.satellites.co.uk/forums/threads/reset-root-password-plugin.101146/
root/zlxx	EV ZLX Two-way Speaker?	?
root/juantech	Guangzhou Juan Optical	https://news.ycombinator.com/item?id=11114012
root/xc3511	H.264 - Chinese DVR	http://www.cctvforum.com/viewtopic.php?f=56&t=34930&start=15
root/hi3518	HiSilicon IP Camera	https://acassis.wordpress.com/2014/08/10/i-got-a-new-hi3518-ip-camera-modules/
root/klv123	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/klv1234	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/jvbzd	HiSilicon IP Camera	https://gist.github.com/gabonator/74cdd6ab4f733ff047356198c781f27d
root/admin	IPX-DDK Network Camera	http://www.ipxinc.com/products/cameras-and-video-servers/network-cameras/
root/system	IQinVision Cameras, et. al	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/meinsm	Mobotix Network Camera	http://www.forum.use-ip.co.uk/threads/mobotix-default-password.76/
root/54321	Packet8 VOIP Phone, et. al	http://webcache.googleusercontent.com/search?q=cache:W1phozQZURUJ:community.freepbx.org/t/packet8-atas-phones/411
root/00000000	Panasonic Printer	https://www.experts-exchange.com/questions/26194395/Default-User-Password-for-Panasonic-DP-C405-Web-Interface.html
root/realtek	RealTek Routers	
admin/1111111	Samsung IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/xmhdipc	Shenzhen Anran Security Camera	https://www.amazon.com/MegaPixel-Wireless-Network-Surveillance-Camera/product-reviews/B00EB6FNDI
admin/smcadmin	SMC Routers	http://www.cleancss.com/router-default/SMC/ROUTER
root/ikwb	Toshiba Network Camera	http://faq.surveillixdvrsupport.com/index.php?action=artikel&cat=4&id=8&artlang=en
ubnt/ubnt	Ubiquiti AirOS Router	http://setuprouter.com/router/ubiquiti/airos-airgrid-m5hp/login.htm
supervisor/supervisor	VideoIQ	https://ipvm.com/reports/ip-cameras-default-passwords-directory
root/<none>	Vivotek IP Camera	https://ipvm.com/reports/ip-cameras-default-passwords-directory
admin/1111	Xerox printers, et. al	https://atyourservice.blogs.xerox.com/2012/08/28/logging-in-as-system-administrator-on-your-xerox-printer/
root/Zte521	ZTE Router	http://www.ironbugs.com/2016/02/hack-and-patch-your-zte-f660-routers.html

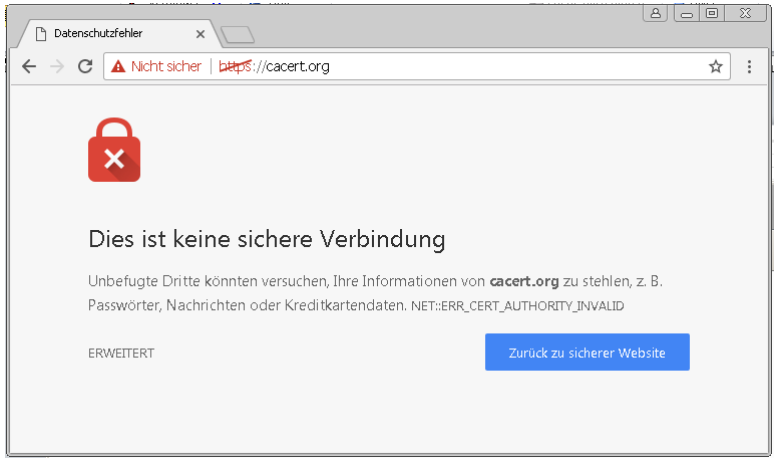
2. Fallbeispiel 2
TLS-Fehler im Browser

anderScore trust in competence



2. Fallbeispiel 2
TLS-Fehler im Browser

- Ist das Problem sicherheitsrelevant?
- Findet ein Angriff statt?
- Was bedeuten die Meldungen genau?
- Hintergrund:
  tv,



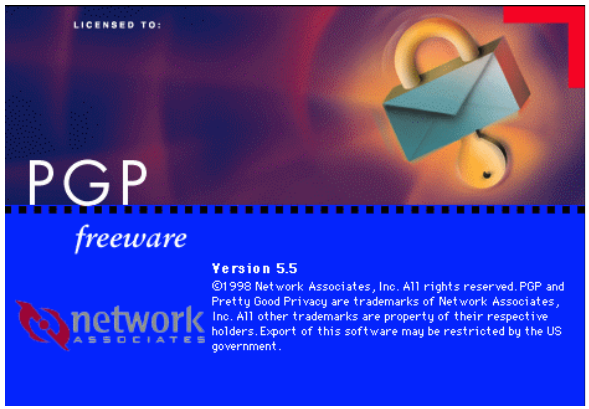
"(...) a better approach may be to minimize the use of SSL warnings altogether by blocking users from making unsafe connections and eliminating warnings in benign situations".

Sunshine, Egelman, Almuhimedi, Atri, Cranor,
SSYM'09, Proceedings of the 18th conference on USENIX security symposium

2. Fallbeispiel 3
E-Mail Encryption

anderScore trust in competence

- A. Whitten, J.D. Tygar *Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0,*
  SSYM'99 Proceedings of the 8th conference on
  USENIX Security Symposium



- PGP 5.0 Handbuch:
  "significantly improved graphical user interface makes complex mathematical cryptography accessible for novice computer users"

- Laborstudie: 12 Teilnehmer – Szenario: Freiwillige einer politischen Kampagne
  - Entschlüsseln / Verschlüsseln / Signieren
  - Ergebnis:
    - Nachrichten u.a. korrekt verschlüsselt, entschlüsselt, signiert **33%**
    - Fehler: Geheimnis unverschlüsselt übertragen: **25%**
    - Fehler: Keine Nachricht verschlüsselt oder entschlüsselt: **8%**

2. Fallbeispiele Zusammenfassung

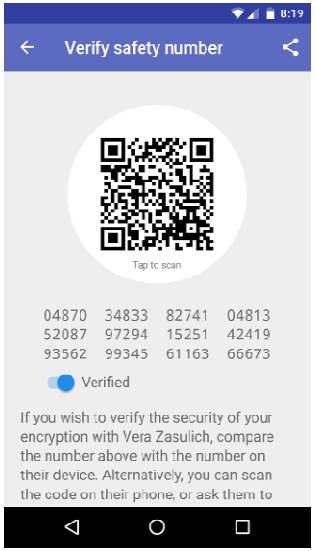
anderScore trust in competence

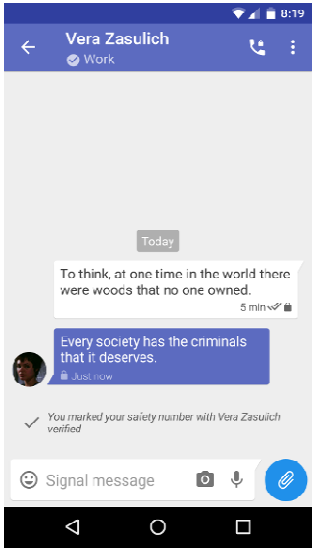
Einfache Fehler in Entwicklung / Design

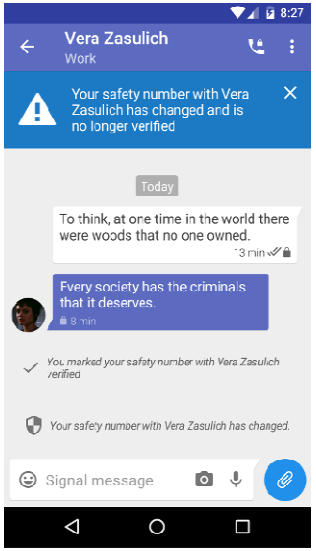
- WLAN-Richtfunk
  - Betrieb mit Standard-Passwort möglich
- TLS Browser-Fehler
  - Einfaches weg-klicken erlaubt
- PGP (E-Mail Verschlüsselung)
  - Unverschlüsseltes Senden möglich
  - Kein Weg guter Weg zur Schlüssel-Verifikation

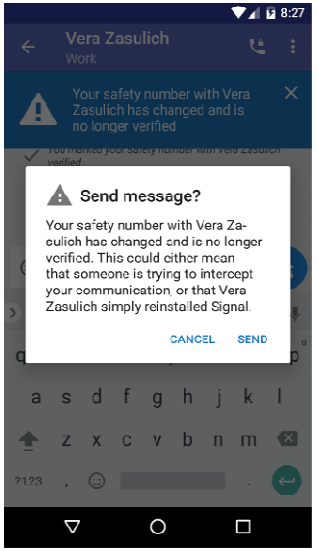
Strategie: Vermeiden und erkennen?

- Erfahrene Entwickler(in)
- Wichtig:
  - Häufig keine funktionale Anforderung („Es muss sicher sein!“)
  - Fehler finden:
    Strukturiert testen und evaluieren









Quelle: Open Whisper System Blog - Safety number Updates
https://whispersystems.org/blog/verified-safety-number-updates/

Der Mensch als Ziel

3. SOCIAL ENGINEERING

HTTPS://WWW.YOUTUBE.COM/WATCH?V=LC7SCXVKQOO

3. Social Engineering

- Mensch wird zur Kooperation **überzeugt**
  - Stress, Hilfsbereitschaft, Erpressung, Rhetorik (Ethos, Pathos, Logos) …

- Zusammenhang Usable Security:
  - **Falsches Verständnis** von Ausgaben (E-Mail-Adresse o. Telefonnr. gefälscht, …)
  - **Warnung / Fehler / Bugs** sind normal (TLS-Fehler, „Ja klicken“,..)
  - **Umgehen** von Hürden / Schranken ist **Gewohnheit**
  - Benutzer **überfordert** – Falsche Entscheidung
    (Wieviel Bit Schlüssellänge? Fingerprint akzeptieren?)

- Ziel: Widerstandsfähige Software
  - **Strukturiert**, **einheitlich** & **vorhersehbar**
  - **Entscheidungen** sind zumutbar
  - **Keine Fehler erwartet**; Benutzung macht Spaß
  - Auch **unter Stress** gut & einfach benutzbar
  - Keine **illegalen Abkürzungen** möglich
  - Konsistentes **Gesamtbild**: Zusammenspiel
    in Geschäftsprozessen
    (3. Systeme, Anwendungen, etc.)

Wie entwickeln wir sichere Software?

4. USABLE SECURITY

4. Usable Security
Worauf ist zu achten?

anderScore trust in competence

Benutzer müssen

1. Sicherheits-Funktionen zuverlässig erkennen
2. Sicherheits-Funktionen erfolgreich nutzen
3. Keine gefährlichen Fehler machen
4. Sich wohlfühlen und die Software weiter verwenden

Hindernisse

1. Benutzer unmotiviert
2. Security-Policies abstrakt
3. Feedback: Security-Status häufig zu komplex für Zusammenfassung
4. Schwächstes Glied der Kette versagt
5. Stalltür-Eigenschaft: Geheimnis für immer verloren

Nach: A. Whitten, J.D. Tygar, *Why Johnny Can't Encrypt:*
A Usability Evaluation of PGP 5.0, SSYM'99 Proceedings of the 8th, conference on USENIX Security Symposium

4. Usable Security
... und wie gehen wir damit um?

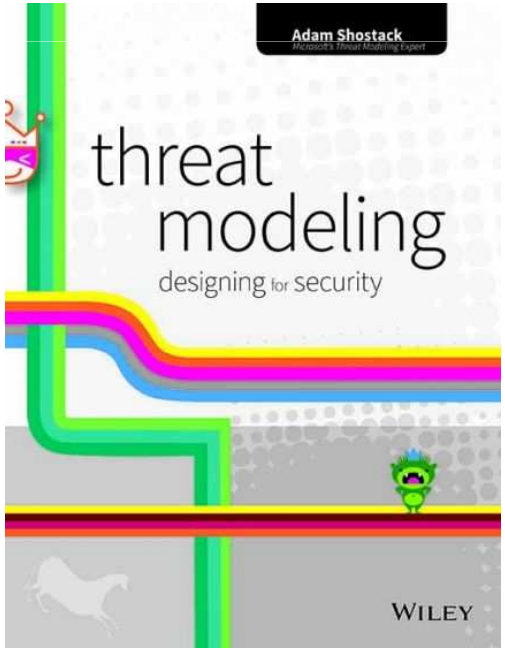
anderScore trust in competence

1. Usability als Designziel – z.B.
   - Design Persona (threat modelling)
   - Motivation via
     Nudging, Gamemification

2. Product Discovery Phase einplanen
   - Walkthrough & Think-Aloud:
     Security Experte:
     Stimmt die Wahrnehmung?

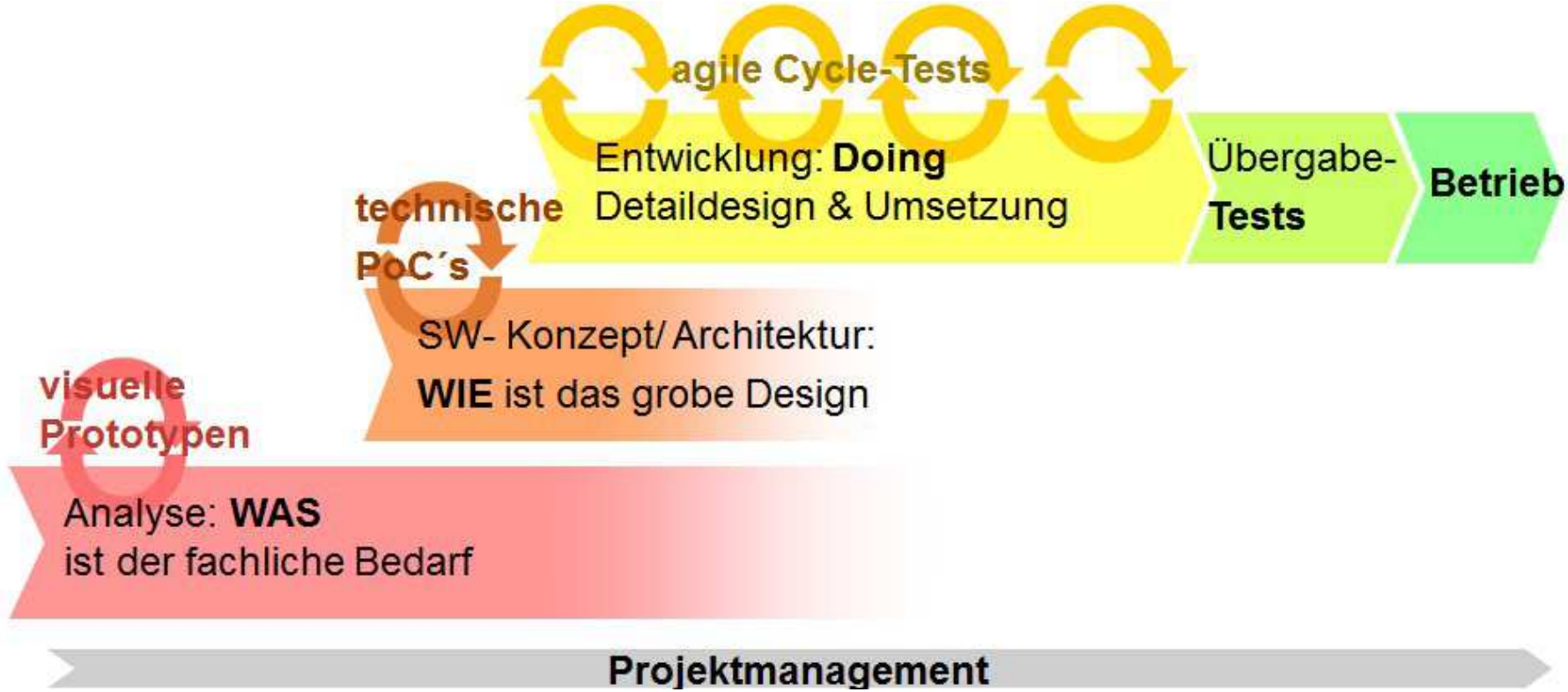
3. Usability Ist Test - / Abnahmekriterium
   - Im User-Acceptance-Test (UAT) einplanen
   - Nicht nur Funktion testen – auch Usability evaluieren
   - Welche Hürden werden umgangen?

4. Projekt Vorgehen u.a. agile Verfahren/ Cycle Meetings
   - Fehler beachten
   - Usability: Nutzerakzeptanz einfordern!



4. Usable Security
Unser Vorgehen beim Entwickeln

- Cycles – Fehler finden und erkennen

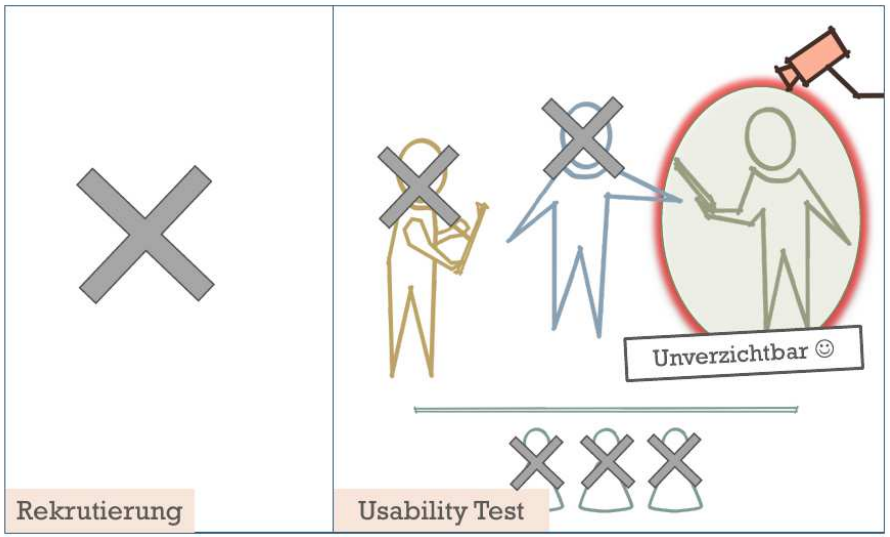


4. Usable Security
Option „Lean Usability Testing“

1. Lean Usability Testing: Nur Nutzer, Testleiter
   (kein Labor, Rekrutierer, Protokollant, …)

2. Optionen (u.a.)
   - „Guerillia Testing“: Direkt ansprechen (z.B. Kantine, Stand)
   - Remote (moderiert vs. nicht-moderiert)

3. Ziel: Direktes Feedback,
   einfache Fragen



Quelle: Hans-Joachim Belz, UX & lean usability testing, Goldschmiede 18.11.2016, https://www.anderscore.com/partner/goldschmiede/

4. Usable Security
Option „Lean Usability Testing“

Steve Krug

Autor und Usability Pragmatiker

- **1 Nutzer** ist 100% besser als gar keiner
- **3 Nutzer** sind meist ausreichend
- Je **öfter und früher** desto wirksamer
- Nicht immer ist es notwendig **repräsentative Benutzer** zu befragen; z. B. bei einem frühen ersten Test

Quantitative Studien ab 20 Testpersonen.
Für eine differenzierte kritische Betrachtung des gesamten Themas
http://alandix.com/blog/2011/06/04/are-five-users-enough/

Jakob Nielsen über Usability Tests

Urgestein der Usability

„Elaborate usability tests are a waste of resources. The best results come from testing **no more than 5 users** and running **as many small tests** as you can afford.“

(Nielsen Norman Group, 2000)

Quelle: Hans-Joachim Belz, UX & lean usability testing, Goldschmiede 18.11.2016, https://www.anderscore.com/partner/goldschmiede/

Zusammenfassung

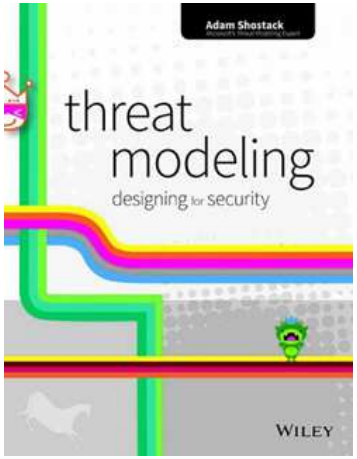
anderScore trust in competence

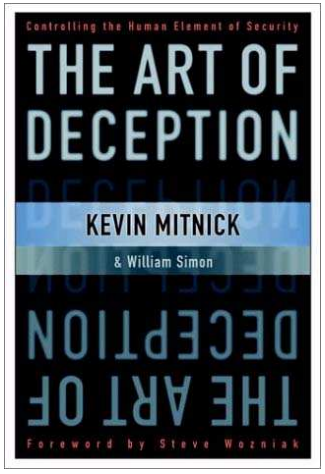
1. Security Software häufig schwer benutzbar
   - ✓ Inhärente Eigenschaften
2. Privacy & Security gehören zur Usability
   - ✓ In Anforderungen & Testfälle aufnehmen
   - ✓ Usability wesentlich für sichere Software
   - ✓ **Social Engineering: Begünstigt durch schlechte Usability**
3. Entwicklung: agiles Vorgehen existentiell
   - ✓ Evaluationsergebnisse → Änderung von Anforderungen
   - ✓ Kurze Entwicklungszyklen
   - ✓ agiles Projektmangement als Kernkompetenz unverzichtbar

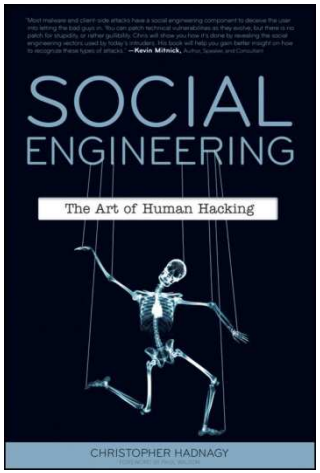
Abschluss

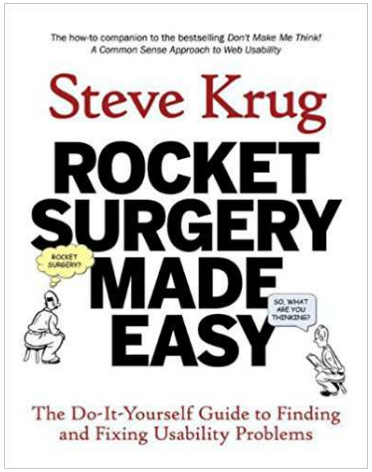
Vielen Dank für Ihre Aufmerksamkeit

jan.luehr@anderscore.com









Tony Wills - CC-BY 2.5 - https://en.wikipedia.org/wiki/Childproofing#/media/File:Child_proof_fence.jpg