REQU-IS: Requirements for IT Security

hope for the best, but prepare for the worst

Dr. Gabriele Haller, Tanja Hanauer

gt-muenchen GmbH

Speakers

- Dr. Gabriele Haller (Dipl.-Phys., Freiburg, Berlin)

  Software Engineering, Requirements Engineering,
  Prozess-Beratung, Projekt Management

- Tanja Hanauer (CISSP, M. A. Computerlinguistik, München)

  IT Security Management, Storage Consultant, Logfile-Management,
  Datenanalyse

gtmuenchen


Schließfach
Locker
Mobile
Schließfächer
mieten – kaufen – leasen
Tel.

Agenda

- Sicherheitsvorfälle
- Bedeutung von IT Security
- REQU-IS
    - Security Requirements
    - REQU-IS Leitmotive
    - REQU-IS Methodik
    - REQU-IS Angriffstypen / Angreifertypen
    - Analyse / Priorisierung
- Ausblick

gtmuenchen

BKA-Warnung vor Locky enthält Virus

heise Security 02.03.2016 15:59 Uhr – Ronald Eikenberg

Betreff: Offizielle Warnung vor Computervirus Locky

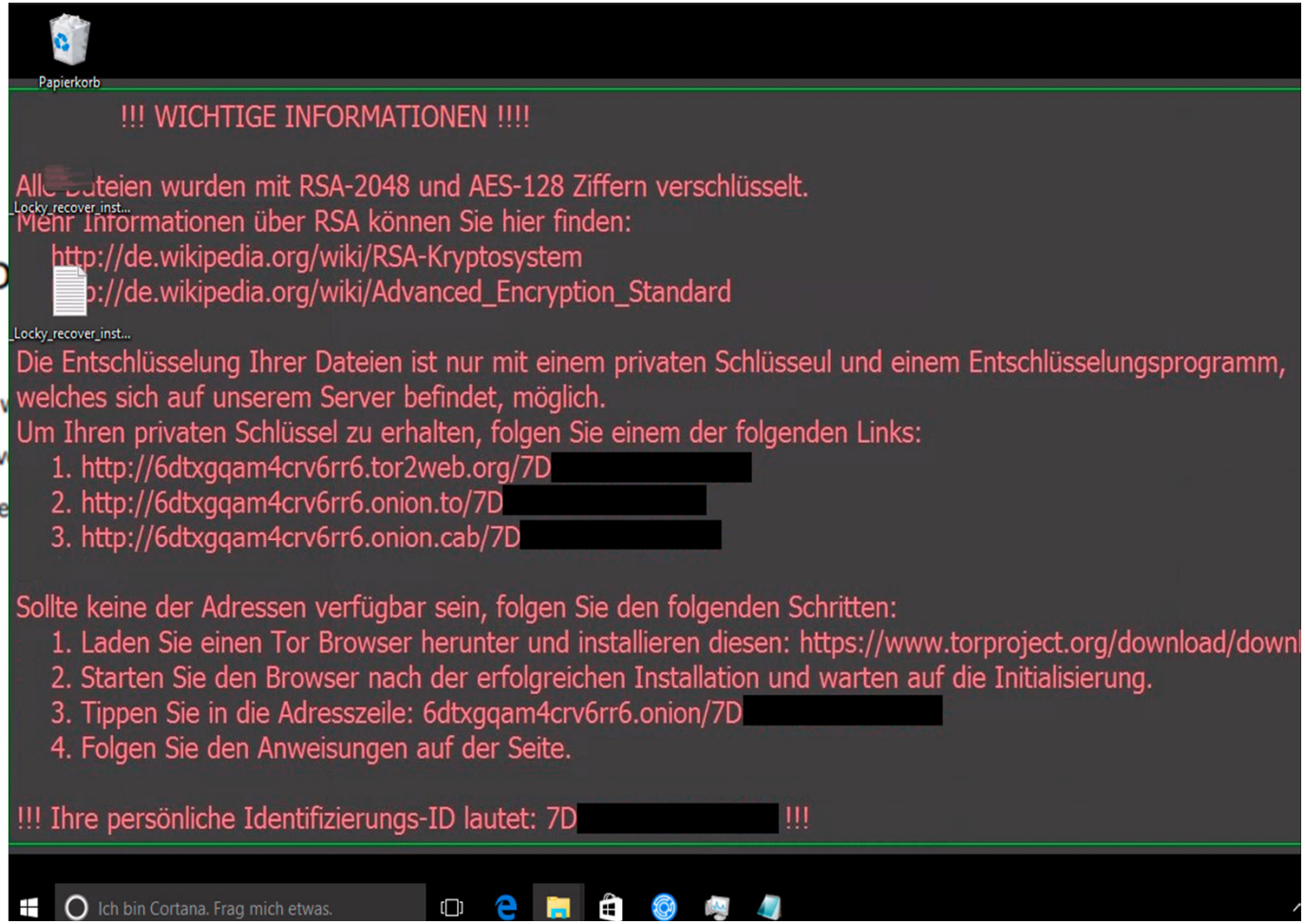
Bundeskriminalamt

Offizielle Warnung vo

Aufgrund wiederholter Email mit Nachfragen v

Infektion mit dem Computervirus "Locky" zu v

mit Anti Virensoftware Herstellern einen Siche



IT-Sicherheitsvorfälle

Angriff im OP: Hacker könnten Narkosegeräte manipulieren

DPA

Patienten in Narkose (Symbolbild): Hacker könnten Medizinapparate beeinflussen

Patienten droht eine neue Gefahr: Hacker könnten medizinische Apparate kapern und deren Funktionen verändern. Nach Informationen des SPIEGEL ist das bereits einmal gelungen.

Testfall, von einem Krankenhaus beauftragt / in Heidelberg / Gerätehersteller nicht bekannt gegeben / keine Informationen über Vorgang des Hackings

Nach Fernsteuerungs-Hack ruft Fiat Chrysler 1,4 Millionen Autos zurück

heise online 24.07.2015 18:20 Uhr – Raimund Schesswendter vorlesen

Während ein Journalist im Wagen saß, konnten die Angreifer das Fahrzeug steuern.
(Bild: Screenshot)

Fiat Chrysler ruft diverse Fahrzeuge der Marken Jeep, Chrysler und Dodge zum Software-Update zurück. Zuvor war ein Jeep Cherokee gehackt und ferngesteuert worden. Das Update soll solche Einbrüche verhindern.

https://www.youtube.com/watch?v=-FqsW5IodkM

Nichts ist verschlossen genug, nichts zu hoch,
nichts zu dunkel für Diebe und Räuber.

Francesco Petrarca (1304 - 1374), italienischer humanistischer Gelehrter

Industrie 4.0

Karikatur Industrie 4.0
Foto: Reinhard Alff

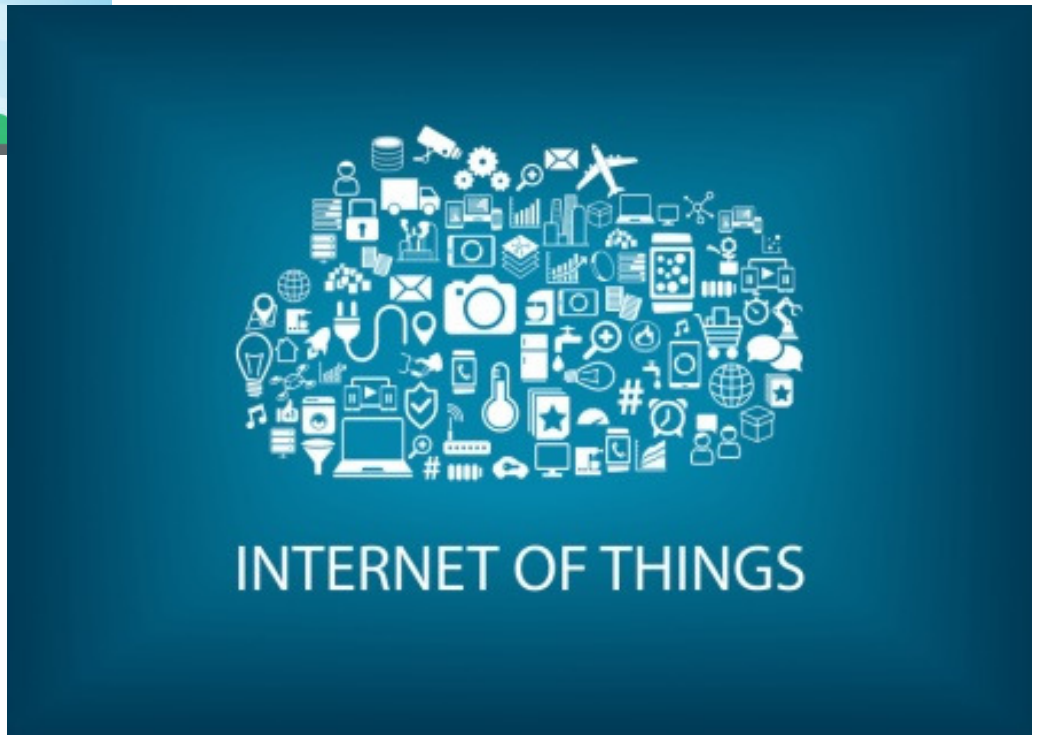
Warum jetzt IT Security?

Big Data **Cloud** **Smart Home**

Warum jetzt IT Security?

Smart City

IoT



SAE
SmartAnythingEverywhere

https://smartanythingeverywhere.eu/

Was ist ein Requirement?

gemäß DIN 69901-5:2009-01:

„Beschaffenheit, Fähigkeit oder Leistung, die ein Produkt, Prozess oder die am Prozess beteiligte Person erfüllen oder besitzen muss, um einen Vertrag, eine Norm, eine Spezifikation oder andere formell vorgegebene Dokumente zu erfüllen."

gemäß IEEE Standard 830 (1998):

„Eine Anforderung ist eine Bedingung oder eine Fähigkeit, die ein Benutzer benötigt, um ein Problem zu lösen oder um sein Ziel zu erreichen."

Aussage über eine Funktion oder Eigenschaft eines Produktes

gemäß Rupp:

„Aussagen über eine Eigenschaft oder Leistung eines Produktes, eines Prozesses oder der am Prozess beteiligten Personen."

gemäß Robertson:

„Something that the product must do, or a property that the product must have, and that is needed or wanted by the stakeholders."

gemäß Wiegers

„A statement of a customer need or objective, or of a condition or capability that a product must possess to satisfy such a need or objective."

Kategorien von Requirements

funktional

beschreibt
die Funktion
von
Produkten,
Systemen,
Applikationen,
Services, …

nicht- funktional

beschreibt
das Verhalten,
die Eigenschaften,
das Aussehen

Randbedingungen

Gegebenheiten
oder Bedingungen,
an die sich das Produkt
anpassen muss

Kategorien von Requirements

funktional

nicht- funktional

- Performance, Leistung, Zeitliches Verhalten,
- Fehlerverhalten
- Usability, GUI, Look&Feel
- Safety
- **Security**
- Cultural, Polit…
- Maintenance / Wartbarkeit
- Technologie, Hardware, …
- Daten, Schnittstellen, …
- …

Randbedingungen

Security Requirements in der Fachliteratur - Auswahl

- Common Criteria ISO/IEC 15408 (2012)
- SQUARE **S**ecurity **Qua**lity **R**equirements **E**ngineering (SEI) (2005)
- SAMM Project (OWASP)
- CLASP Project (OWASP)
- „A comparison of security requirements engineering methods“ (2010) Fabian et al.
- „Core Security Requirements Artefacts“ (2004) ; Moffet et al.

…
…

- „Cyber Security Requirement Engineering“ Christof Ebert; RE-Magazin 4/2015
- IEC 62443 ”Industrial communication networks – Network and system security”

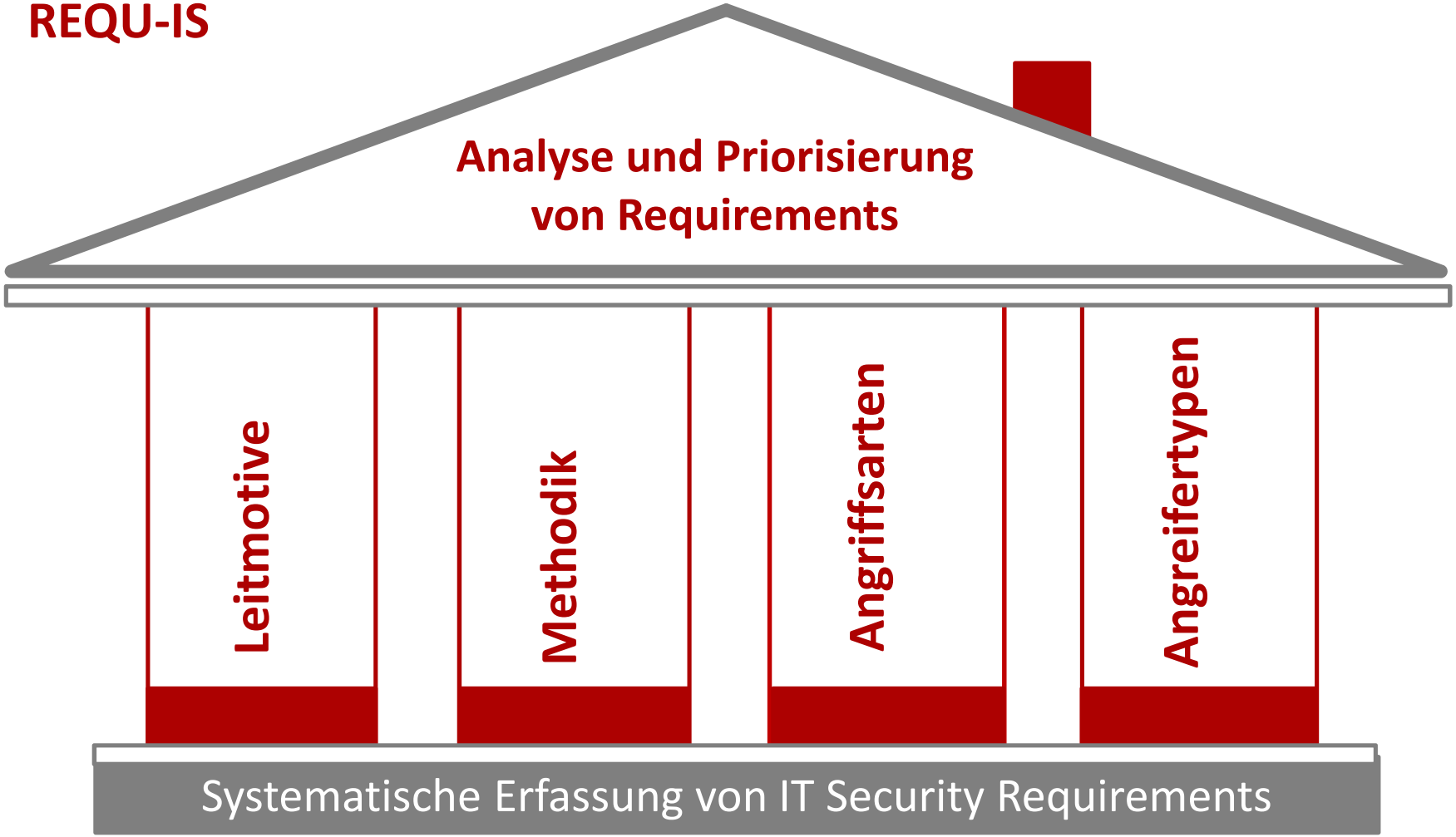
REQU-IS

- Framework **REQU-IS** = REQUirements for IT Security
- erhebt Security Requirements wegen ihrer Wichtigkeit zur eigenen Kategorie
  (Security Requirements können sowohl funktional als auch nicht-fktn sein)
- bietet Unterstützung bei der systematischen und strukturierten Erhebung von Security Requirements
- schafft Bewusstsein für Security Requirements (Awareness)
- berücksichtigt Aspekte der IT-Sicherheit zu einem frühen Zeitpunkt

Kategorien von Requirements

funktional nicht- funktional **security related** Randbedingungen

REQU-IS


Analyse und Priorisierung
von Requirements
Leitmotive
Methodik
Angriffsarten
Angreifertypen
Systematische Erfassung von IT Security Requirements

REQU-IS Leitmotive

Schutzziele der IT-Sicherheit als Leitmotive für Erhebung von Security Requirements

- Confidentiality / Vertraulichkeit
- Integrity / Integrität
- Availability / Verfügbarkeit
- Accountability / Zurechenbarkeit
- Authenticity / Authentizität, Echtheit, Glaubwürdigkeit
- Non-Repudiation / Verbindlichkeit, Zuordenbarkeit, Nichtabstreitbarkeit
- Privacy / Privatsphäre
- …

Confidentiality - Vertraulichkeit

Information ist für einen autorisierten Empfängerkreis bestimmt,
keine Veröffentlichung / Weitergabe
sowohl für Zugriff auf gespeicherte Daten, als auch bei Datenübertragung

Mögliche Security Requirements zum Leitmotiv Vertraulichkeit:

- unberechtigte Personen haben keinen Zugriff auf Daten
- strenge Regeln für Zugriffsvergabe
- streng reglementierte Weitergabe von Daten und Überprüfung
- verschlüsselte Datenablage
- …

Grafik: http://www.pracht-mediation.de/SymbolBibliothek

Integrity - Integrität

Korrektheit/Unversehrtheit von Daten und korrekte Funktion von Systemen
Daten dürfen nicht unbemerkbar verändert werden;
alle Änderungen müssen erkennbar sein

Mögliche Security Requirements zum Leitmotiv Integrität:

- Daten dürfen nicht durch die Art der Übertragung beeinflusst werden
- Konsistenzverletzung
- (unautorisierte) Veränderungen müssen automatisch angezeigt werden
- Inhalt der Webseite muss unverändert angezeigt werden
- …

Availability - Verfügbarkeit

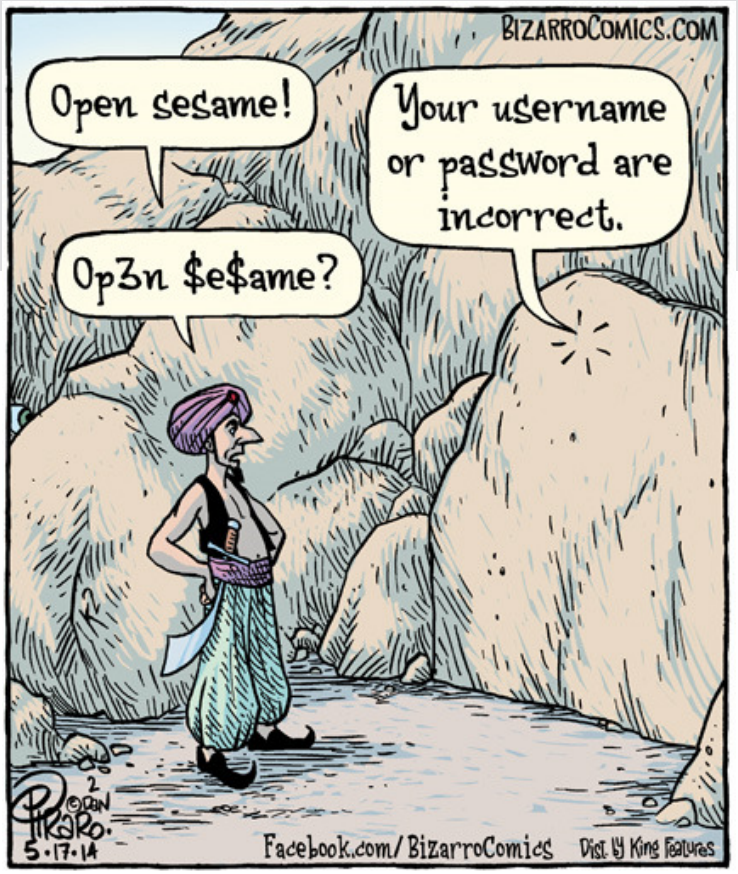
Applikation ist funktionsbereit. Daten und Systeme sind verfügbar.
Verhindern von Systemausfällen
Zugriff auf Daten muss innerhalb eines vereinbarten Zeitrahmens gewährleistet sein

Mögliche Security Requirements zum Leitmotiv Verfügbarkeit:

- Die Applikation muss rund um die Uhr zur Verfügung stehen
- Die Funktionalität der Applikation ist nicht durch Stoßzeiten beeinträchtigt
- Wartungsintervalle sind 4 Wochen im Voraus einzuplanen und anzukündigen
- Der Ausfall eines Servers in einer Niederlassung, darf die Verfügbarkeit der Gesamtanwendung nicht beeinflussen.
- …

Authenticity – Authentizität (Echtheit, Glaubwürdigkeit)

Die Eigenschaft einer Entität, das zu sein, was sie vorgibt zu sein. Zum Beispiel wird in der Benutzerverwaltung ein Nutzer zweifelsfrei mit einer digitalen ID verbunden.



Quelle:
Blog:
bizzarocomics.com
vom 16.05.2014

Privacy - Privatsphäre

Die Kontrolle der betroffenen Personen über ihre Daten (informationelle Selbstbestimmung) und die Einhaltung von Gesetzen und Regelungen zum Schutz der Privatsphäre.

Besonders wichtig bei personenbezogenen Daten.

Accountability - Zurechenbarkeit

Verantwortlichkeit einer Entität für ihre Aktionen und Entscheidungen.
Aktionen können den Personen zugeordnet werden, die sie durchgeführt haben.

Non-Repudiation – Nichtabstreitbarkeit, Verbindlichkeit

Der Eintritt eines Ereignisses oder einer Aktion sowie die verursachende Entität kann zweifelsfrei belegt werden.

REQU-IS Methodik

Problem:

Der Hauptzweck von Security Requirements ist,
sicherzustellen, dass etwas **NICHT** passiert.

Beispiele:

- „Vertrauliche Daten dürfen nicht an die Öffentlichkeit gelangen.“
- „Die Integrität der Daten darf nicht verletzt werden“
- „Die Verfügbarkeit des Systems soll zu keinem Zeitpunkt gefährdet sein.“

Was bedeutet das konkret?

Wie kann man die Abwesenheit eines Merkmals nachweisen?

REQU-IS Misuse Cases

Misuse Cases als Methode zum Auffinden von Security Requirements

- Use Cases mit „böser“ Absicht, Missbrauch-Anwendungsfälle
- Use Cases mit Akteuren, die keinen Zugriff haben sollen
- Use Cases bei denen sich die Umgebung nicht wie erwartet verhält (z.B. Systemausfall)
- Methode erstmals ca. 1990 in Fachkreisen erwähnt;
  bisher in der Industrie wenig verbreitet

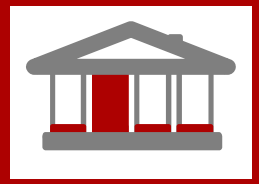
REQU-IS Misuse Cases

Titel	**…**
Autor	…
Erstellungsdatum	…
Misuser	die Rolle, von der die Funktion ausgelöst wird
Vorbedingung	z.B. der Zustand des System zum Zeitpunkt eines Angriffs befindet
Funktionsablauf	z.B. die Schritte eines Angriffs
Alternativer Funktionsablauf	evtl. Verzweigungsmöglichkeiten im Vorgehen bei einem Angriff (z.B. weitere points of entry)
Nachbedingung oder Erfolgskriterium	z.B. woran man erkennt, dass ein Angriff gelungen ist
Bemerkung	jegliche Art der ergänzenden Beschreibung oder zusätzliche Information zum Verständnis

REQU-IS Misuse Cases

Beispiele:

- bewusste Fehlbedienung von Systemen
  (z.B Ausschalten ohne Logout; falsche Tastenkombinationen eingeben, …)
- sich unbefugt Zugang zu einem System verschaffen
- Fehlkonfiguration von Systemen
- Eingabe falscher Datensätze
- Datenausgabe herbeiführen (z.B. Personaldaten, Stücklisten, Kalkulationen)
- Daten manipulieren, Webseite manipulieren (z.B. Preise ändern)
- geheime Daten einsehen
- Information aus Kombination verschiedener Daten erschliessen
- Abschaltung von Systemkomponenten
- …



REQU-IS - Test Driven Security Requirements Elicitation

Im Vorfeld einer Systemerstellung! → sogenanntes „Paper Testing“

NICHT Penetration Testing!!!

REQU-IS - Test Driven Security Requirements

Im Vorfeld einer Systemerstellung! → sogenanntes „Paper Testing“

NICHT Penetration Testing!!!

Beispiel:

- „Die Verfügbarkeit des Systems soll zu keinem Zeitpunkt gefährdet sein.“

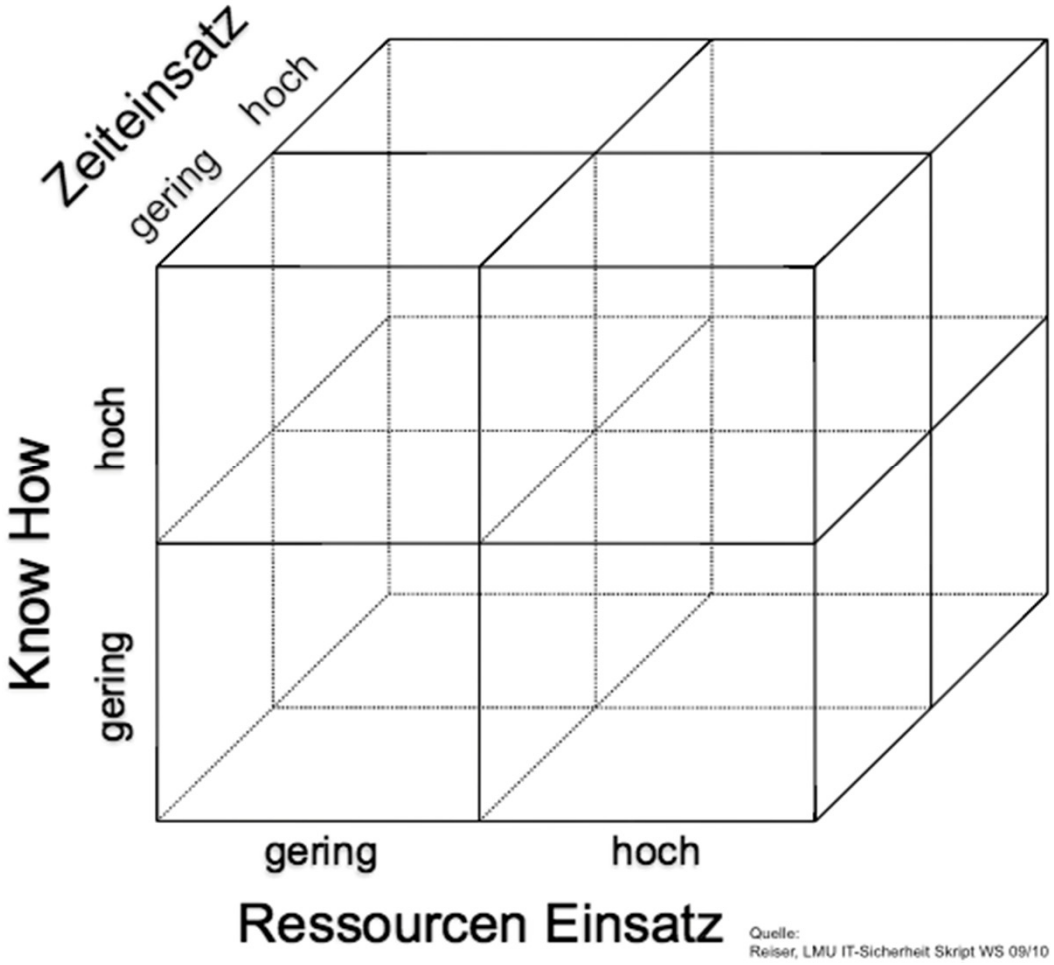
Testfälle:

> …
> …

REQU-IS - Angriffsarten

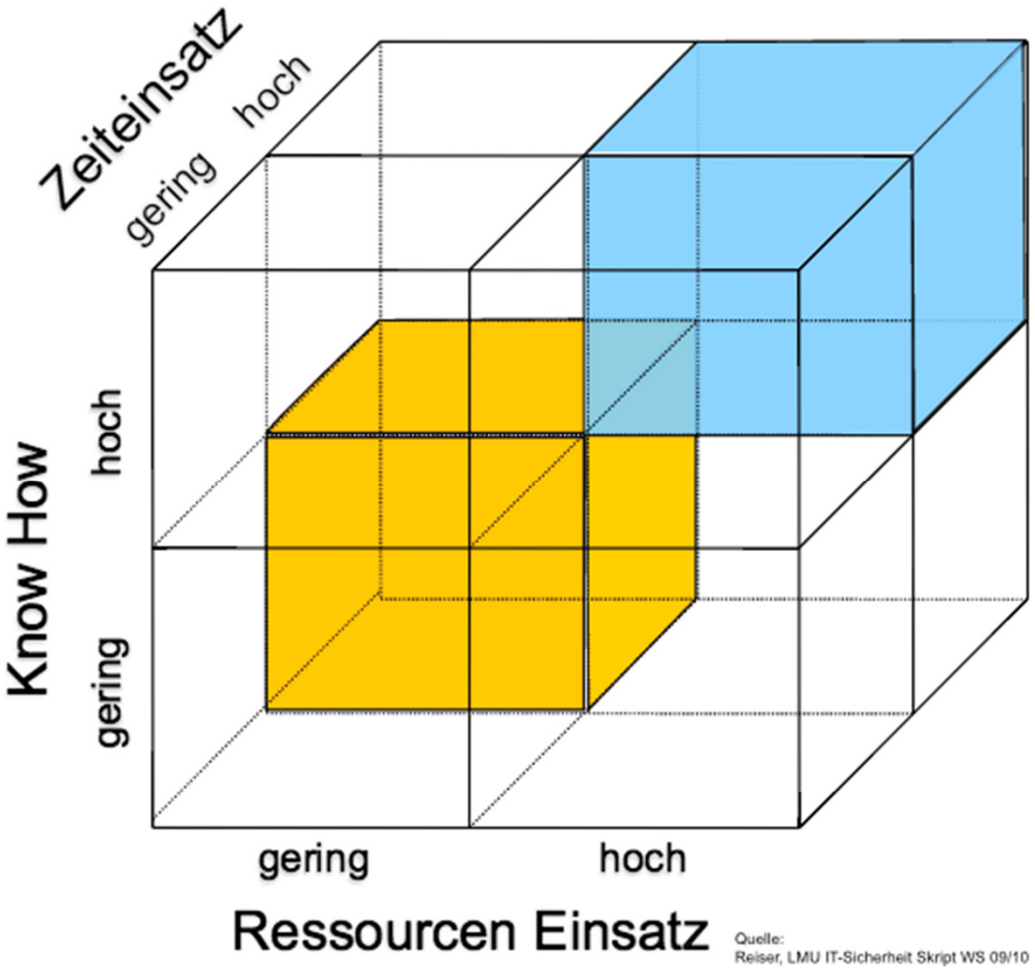
	„gestreute Angriffe“	**„zielgerichtete Angriffe“**
Ziel	• wertvolle Daten erbeuten (z.B. Kreditkartendaten, Logins) • persönlichen Vorteil verschaffen • Ausprobieren, Zeitvertreib (Script-Kiddie)	• bestimmte Daten erbeuten • Informationen für Entscheidungen erlangen • Informationsvorsprung sichern • Wettbewerber schwächen
Vorgehen	• auf den raschen Erfolg aus • viele unspezifische Zielsysteme • automatisiertes Vorgehen • technisch eher „billig“ und „einfach“	• sorgfältig und langfristig geplant • konkretes Zielsystem • „Handarbeit“ • hohe Komplexität, hohes Fachwissen, finanzielle Ressourcen

REQU-IS - Angreifer Klassifikation



Quelle:
Reiser, LMU IT-Sicherheit Skript WS 09/10

REQU-IS - Angreifer Klassifikation



Quelle:
Reiser, LMU IT-Sicherheit Skript WS 09/10

Die Security-Requirements sind erfasst – eine Analyse/Priorisierung ist notwendig

Priorisierung - Risiko / Kosten

- Gewichtung der identifizierten Bedrohungs-Szenarien
  im Bezug auf Risiko für die Business-Ziele (eines Unternehmens, einer Anwendung, etc.)
- Bezifferung des Risikos in Kosten
- Entscheidung über die Höhe der Kosten, die für die Behandlung eines Risikos
  in Kauf genommen werden
- Rückschluss auf die Security Requirements, die zur Umsetzung kommen müssen

▶ **das Schützenswerteste zuerst**

Ausblick

- zunehmende Vernetzung weltweit
  ist gewünscht und nicht aufzuhalten
- Auswirkungen und Gefahren bisher nur zu erahnen
  (Fokus auf Spaß und Nutzen)
- Vorausdenken zwingend erforderlich
- neue Systeme müssen diesem Bedarf
  gerecht werden (und darüber hinausgehen)
- physische Sicherheit alleine reicht nicht mehr

siehe z.B.:
- Digitales Deutschland 2020 (Bundesministerium des Inneren, Referat IT)
- Mission Zukunft: ICT 2032 - Thesen für den Weg ins Morgen (Detecon)

gtmuenchen

Ausblick


Selbstverwirklichung
Wertschätzung
Sozial Bedürfnisse
(z.B. Liebe, Zuwendung)
Sicherheitsbedürfnisse
(z.B. Geborgenheit und Schutz der Person)
Physiologische Bedürfnisse
(z.B. Hunger, Durst, Schlaf)
WLAN
AKKU

Take home message

- Security Requirements sind eine eigene,
  sehr wichtige Kategorie von Requirements

- Sie müssen zwingend im Vorfeld einer System- oder Produktentwicklung
  berücksichtigt werden

- Es ist nahezu unmöglich, Sicherheit nachträglich hinzuzufügen

gtmuenchen

… zum Weiterlesen …

IT-Sicherheit: Richtlinien, Standards, Allgemeines:

- Bundesamt für Sicherheit in der Informationstechnik BSI, www.bsi.bund.de;
- Computer Security Division – NIST, http://csrc.nist.gov
- ISO 15408 Common Criteria, www.commoncriteriaportal.org
- Praxisbuch ISO/IEC 27001, Hanser Verlag, 2011, M. Brenner, N. Gentschen Felde, W. Hommel, S. Metzer, H. Reiser, T. Schaaf
- Basiswissen Sichere Software, dpunkt Verlag, 2011, S. Paulus
- Open Web Application Security Project OWASP, www.owasp.org;
- IoT spezifisch: https://www.owasp.org/index.php/OWASP_Internet_of_Things_Project
- Allianz für Cybersicherheit: www.allianz-fuer-cybersicherheit.de
- SANS Critical Security Controls, www.sans.org/critical-security-controls/
- IEC 62443 Industrial communication networks – Network and system security
- BSI: ICS Security Kompendium: https://www.bsi.bund.de/DE/Themen/Industrie_KRITIS/Empfehlungen/ICS/empfehlungen_node.html
- ISIS12 Informationssicherheit für den Mittelstand: http://www.it-sicherheit-bayern.de/produkte-dienstleistungen/isis12.html

IT Sicherheitsvorfälle / Security Breaches / Stand der Dinge:

- 2015 Data Breach Investigations Report: http://www.verizonenterprise.com/DBIR/2015/
- Heise Security Report: http://www.heise.de/security/news/
- Symantec Internet Security Threat Report 2015: https://know.elq.symantec.com/LP=1542
- BSI: Die Lage der IT-Sicherheit in Deutschland 2015 https://www.bsi.bund.de/DE/Publikationen/Lageberichte/bsi-lageberichte.html

… zum Weiterlesen …

Security Requirements:

- Capturing Security Requirements through Misuse Cases (2001); Guttorm Sindre, Andreas L. Opdahl, http://folk.uio.no/nik/2001/21-sindre.pdf
- Misuse cases: use cases with hostile intent (2003); I.Alexander, *Software, IEEE* , vol.20, no.1, pp.58,66, Jan/Feb 2003 http://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=1159030&isnumber=25969
- SQUARE Security Quality Requirements Engineering (2005); N. Mead; E. Hough; T. Stehney ; 2005 Techn. Report, CMU/SEI-2005-TR-009 http://resources.sei.cmu.edu/asset_files/TechnicalReport/2005_005_001_14594.pdf
- OWASP SAMM http://www.opensamm.org
- OWASP CLASP
  BP3: Capture Security Requirements; https://www.owasp.org/index.php/Category:BP3_Capture_security_requirements
  Activity: Detail Misuse Cases; https://www.owasp.org/index.php/Detail_misuse_cases
  Activity: Document Security Relevant Requirements; https://www.owasp.org/index.php/Document_security-relevant_requirements
- Core Security Requirements Artefacts; J. Moffet; C. Haley; B.Nusheibe; Technical Report 2004/23; The OpenUniversity, Milton Keynes
- „A comparison of security requirements engineering methods“ ; 2010; Fabian et al.; Sec. Requ. Eng. 15:7-40
- RE Wissen – das Portal für Anforderungsmanagement http://www.re-wissen.de/opencms/Wissen/Techniken/Erhebung_von_MisUse_Cases.html

Ausblick:

- Plattform Industrie 4.0: http://www.plattform-i40.de
- Auf dem Weg zur smarten Fabrik http://www.zvei.org/Publikationen/Industrie-40-Auf-dem-Weg-zur-smarten-Fabrik-aktuell.pdf
- Digitales Deutschland 2020 (Bundesministerium des Inneren, Referat IT) https://www.bmi.bund.de/SharedDocs/Downloads/)
- Mission Zukunft: ICT 2032 - Thesen für den Weg ins Morgen (Detecon) http://www.detecon.com/sites/default/files/2014_Buch_ICT_2032.pdf

… zum Weiterdiskutieren …

www.it-sa.de vom 18. – 20.10.2016 in Nürnberg

Sicherheitsnetzwerk München

http://www.it-sicherheit-muenchen.net/

ITSECURITY
Bavarian IT Security & Safety Cluster

http://www.it-sicherheit-bayern.de/

acm German Chapter - IT Security live

Startseite | Call for Participation | Bisherige Veranstaltungen

http://www.it-security-live.org (21.4.2016 München)

OWASP German Chapter Stammtisch Initiative/München

Willkommen beim OWASP-Stammtisch München

... wir freuen uns über neue Teilnehmer und 'Stammgäste' ...

https://www.owasp.org/index.php/OWASP_German_Chapter_Stammtisch_Initiative/München

etc.

Workshop:

„Security Requirements für Embedded Systeme definieren“

am Di 31.5.2016, 9-17h, bei NewTec GmbH, Pfaffenhofen (bei Neu-Ulm)
(Anmeldung über www. newtec.de)

Tanja Hanauer

0152/53 45 77 94

tanja.hanauer@gt-muenchen.de

Dr. Gabriele Haller

0160/844 65 69

haller@gt-muenchen.de

gt-muenchen GmbH

Josef-Beiser-Str. 28

81737 München

Tel. 089/67905107