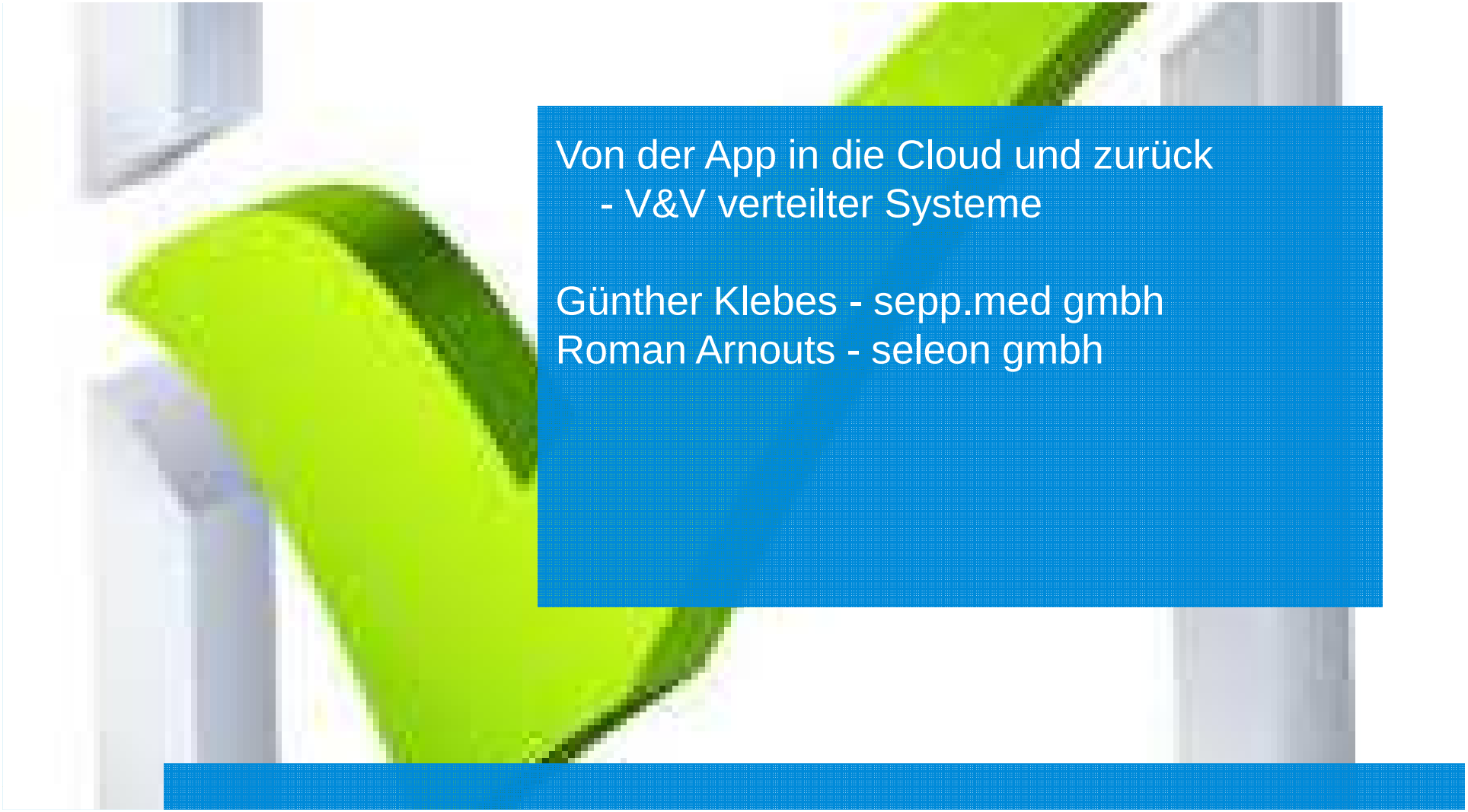
Umsetzung der Standards in die Praxis



Von der App in die Cloud und zurück
- V&V verteilter Systeme

Günther Klebes - sepp.med gmbh
Roman Arnouts - seleon gmbh

Von der App in die Cloud und zurück
- V&V verteilter Systeme

Über uns

Günther Klebes

- Leiter Qualitätssicherung und Prozessoptimierung

sepp.med gmbh

- > 30 Jahre Erfahrung in der Medizintechnik
- ca. 20 Jahre Erfahrung in QS und Prozessoptimierung

Roman Arnouts

- Senior Consultant und Projektleiter

seleon gmbh

- > 7 Jahre Erfahrung in der Medizintechnik
- Ca. 3 Jahre Projektmanagement, 4 Jahre QM&RA

Agenda

- Grundanforderungen für die Verifizierung und Validierung verteilter Systeme
- Verifizierung der Security verteilter Systeme in der Praxis
- Infrastrukturaufwände und Provideranforderungen von Cloud Lösungen
- Testautomatisierung zur Durchführung von Verifikationen und Validierungen verteilter Systeme

Themenraum dieses Vortrags

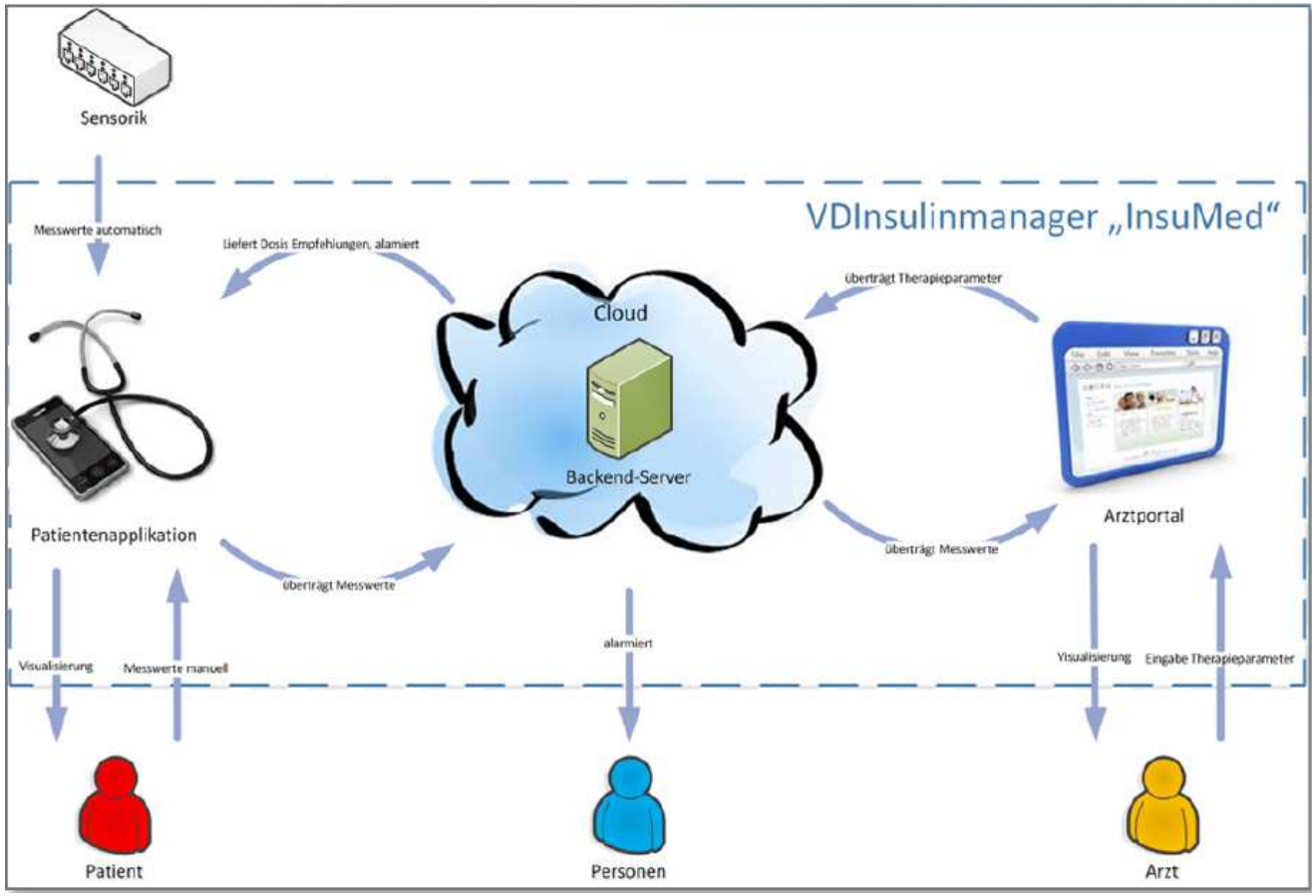
Wird betrachtet...

- Besonderheiten bei dem V&V verteilter Systeme
- Nachweis von Security

Wird nicht betrachtet...

- V&V von Web-Browser-basierten Systemen
- Validierung von Stand-alone Software
- Implementierung von Security
- Usability Validierung

Ausgangslage – Wo stehen wir im Projekt VDInsulinmanager?



Begrifflichkeiten

IEC 62304:2006 Kap. 3.31

SOFTWARE SYSTEM

integrierte Sammlung von SOFTWARE-KOMPONENTEN, die so organisiert sind, dass eine spezifische Funktion oder ein Satz von Funktionen ausgeführt werden kann

Beispiel:

- Software eines Controllers,
- Gesamte Software eines Medizinproduktes,

Begrifflichkeiten

IEC 60601-1:2006 Kap. 3.64

MEDIZINISCHES ELEKTRISCHES SYSTEM

Kombination von einzelnen Geräten, von denen mindestens eines ein MEGERÄT sein muss

Beispiel:

- Fahrbarer Gerätewagen mit mind. einem Medizinprodukt
- IT Netzwerk (zur Verwendung in einer Gesundheitseinrichtung)

Begrifflichkeiten

IEC 60601-1-8:2006 Kap. 3.17

VERTEILTES ALARMSYSTEM

ALARMSYSTEM, das mehr als ein Gerät eines ME-SYSTEMS betrifft

Beispiel:

- Bettseitige Patientenmonitore mit Überwachungszentrale.

Begrifflichkeiten

IEC 60601-1-10:2008 Kap. 3.8

VERTEILTES PCLCS

PCLCS, das mehr als ein Gerät eines ME-SYSTEMS umfasst.

PCLC= Physiologisches geschlossenes Regelsystem

Beispiel:

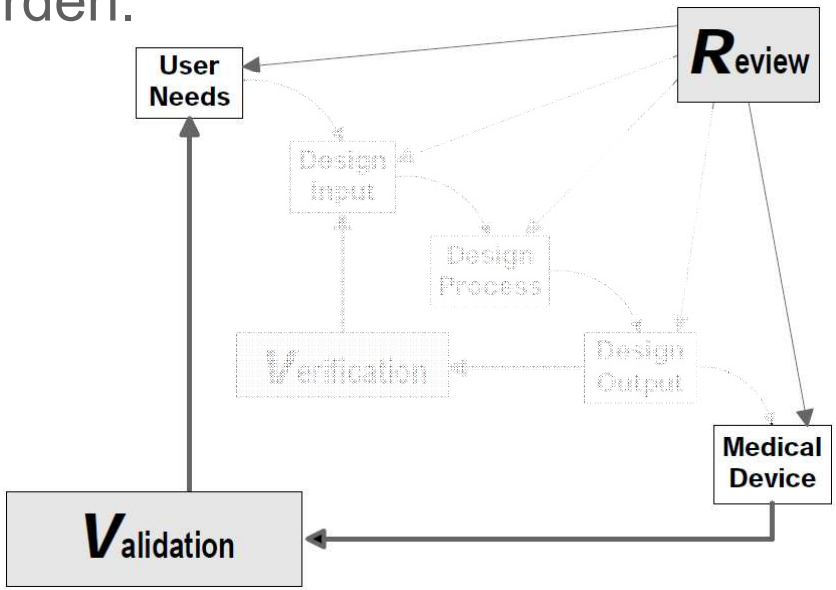
- Medikamentenpumpe mit Kopplung an ein Messgerät

Begrifflichkeiten

FDA Design Control Guidance

Design Validierung

Bewertungsverfahren, ob die an das fertige Medizinprodukt gerichteten Nutzeranforderungen und Zweckbestimmung erfüllt werden.



Begrifflichkeiten

IEC 62366:2007 Kap. 5.9

Gebrauchstauglichkeits-Validierung

Nachweis, dass die Benutzerschnittstellen des Medizinproduktes eine hohe Gebrauchstauglichkeit bereitstellen.

Begrifflichkeiten

FDA Software Validation Guidance

Software Validierung

Nachweis, dass es im bestimmungsgemäßen Gebrauch des Medizinproduktes zu keinen Beeinträchtigungen der Zweckbestimmung durch Software-Komponenten kommt.

Begrifflichkeiten

IEC 62304:2006 Kap. 3.22

Datensicherheit

Schutz von Informationen und Daten derart, dass nicht autorisierte Personen oder SYSTEME sie nicht lesen oder verändern können und dass autorisierten Personen und SYSTEMEN der Zugang zu ihnen nicht verweigert wird

95/46/EG

Datenschutz

Schutz zur Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten.

Grundanforderungen für die Verifizierung und Validierung verteilter Systeme

	IEC 62304	IEC 82304-1	IEC 60601-1	IEC 60601-1-8	IEC 60601-1-10	IEC 60601-1-11
Behandelt verteilte Systeme	Nein	JA	JA	JA	JA	JA
Liefert Design Input für verteilte Systeme	Nein	(JA)	Nein	JA	JA	(JA)
Liefert Verifikationsvorgaben für verteilte Systeme	Nein	Nein	Nein	Nein	Nein	Nein
Liefert Validierungsvorgaben für verteilte Systeme	Nein	(JA)	Nein	Nein	Nein	Nein

Grundanforderungen für die Verifizierung und Validierung verteilter Systeme

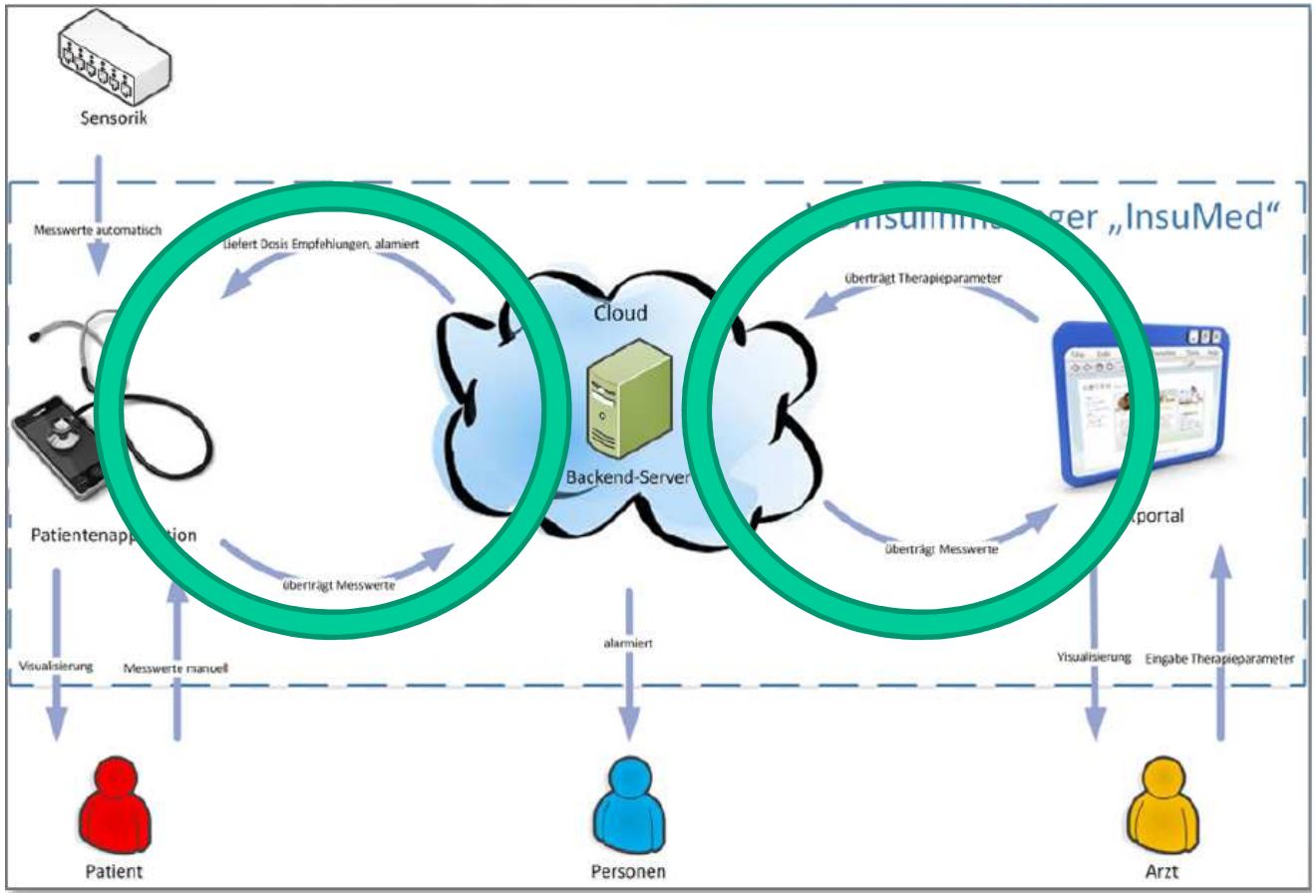
Verifikations- & Validierungsvorgaben für verteilte Systeme:

- Harmonisierte Normen liefern keinen expliziten Vorgaben, nach welchen Kriterien verteilte Systeme geprüft werden sollen
- Allgemein wird auf das Risikomanagement zur Identifikation von Risiken und Schutzmaßnahmen verwiesen, die durch die Verteilung der Systeme resultiert
- Keine expliziten Kriterien, wie die Sicherheitsintegrität eines verteilten Systems gewährleistet werden kann

Frage: Gibt es andere Industriestandards für mehr Sicherheit?

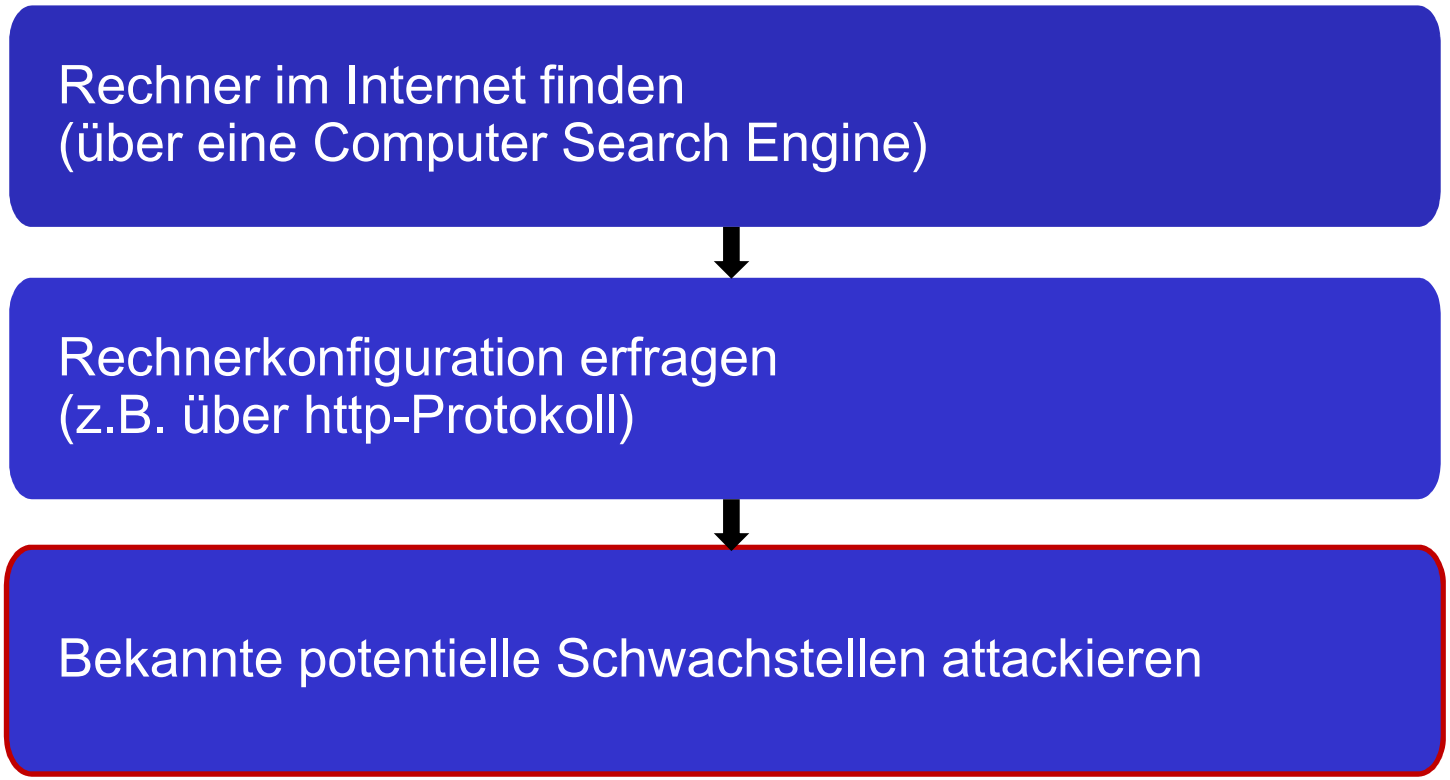
Antwort: JA! Department of Defense!

Ausgangslage – Wo stehen wir im Projekt VDInsulinmanager?



Verifizierung der Security verteilter Systeme in der Praxis

- Wie attackiere ich einen Rechner?



Verifizierung der Security verteilter Systeme in der Praxis

Anforderungen des Department of Defense (DoD)

- Warum denn das??? Wir machen doch ein Medizinprodukt!
- Die Anforderungen des DoD gelten AUCH für Medizinprodukte!
- Wenn Sie also Medizinprodukte an das DoD liefern wollen … ☺
- Sind auch als „Best Practices“ für Medizinprodukte verwendbar (auch wenn Sie nicht an das DoD liefern)

Verifizierung der Security verteilter Systeme in der Praxis

Anforderungen des DoD

Das DoD sagt, WIE etwas gemacht werden soll

- Sehr konkret und damit ungewohnt für die Medizintechnik ☺

via sog. Security Technical Implementation Guidelines (STIGs)

- zur Zeit ca. 400, Anzahl steigend
- Produkthersteller muss ein eigenes Sicherheitskonzept erstellen
- Produkthersteller muss sein System selbst klassifizieren
- STIGs werden regelmäßig (derzeit monatlich) aktualisiert
- DoD testet mit der aktuell geltenden Suite
- Einmal Testen reicht nicht!
- Hat massiven Einfluss auf den Entwicklungsprozess

Windows 7 Security Technical Implementation Guide

Overview

Version	Date	Finding Count (278)			Downloads		
1	2015-06-24	CAT I (High): 21	CAT II (Med): 196	CAT III (Low): 61	Excel	JSON	XML

STIG Description

The Windows 7 Security Technical Implementation Guide (STIG) is published as a tool to improve the security of Department of Defense (DoD) information systems. The requirements were developed from DoD consensus, as well as the Windows 7 Security Guide and security templates published by Microsoft Corporation. Comments or proposed revisions to this document should be sent via e-mail to the following address: disa.stig_spt@mail.mil.

Available Profiles

Jump to comments on this STIG

Findings (MAC I - Mission Critical Classified)

Finding ID	Severity	Title	Description
V-1073	High	Systems must be at supported service pack (SP) or release levels.	Systems at unsupported service packs or releases will not receive security updates for new vulnerabilities and leaves them subject to exploitation. Systems must be maintained at a service pack level ...
V-34974	High	The Windows Installer Always install with elevated privileges must be disabled.	Standard user accounts must not be granted elevated privileges. Enabling Windows Installer to elevate privileges when installing applications can allow malicious persons and applications to gain ...
V-39137	High	The Enhanced Mitigation Experience Toolkit (EMET) v5.x or later must be installed on the system.	Attackers are constantly looking for vulnerabilities in systems and applications. The Enhanced Mitigation Experience Toolkit can enable several mechanisms, such as Data Execution Prevention (DEP), ...

The Windows Installer Always install with elevated privileges must be disabled.

Overview

Finding ID	Version	Rule ID	IA Controls	Severity
V-34974	WINCC-000001	SV-46219r1_rule	ECLP-1	High

Description

Standard user accounts must not be granted elevated privileges. Enabling Windows Installer to elevate privileges when installing applications can allow malicious persons and applications to gain full control of a system.

STIG	Date
Windows 7 Security Technical Implementation Guide	2015-06-24

Details

Check Text (None)

None

Fix Text (F-39548r1_fix)

Configure the policy value for Computer Configuration -> Administrative Templates -> Windows Components -> Windows Installer -> "Always install with elevated privileges" to "Disabled".

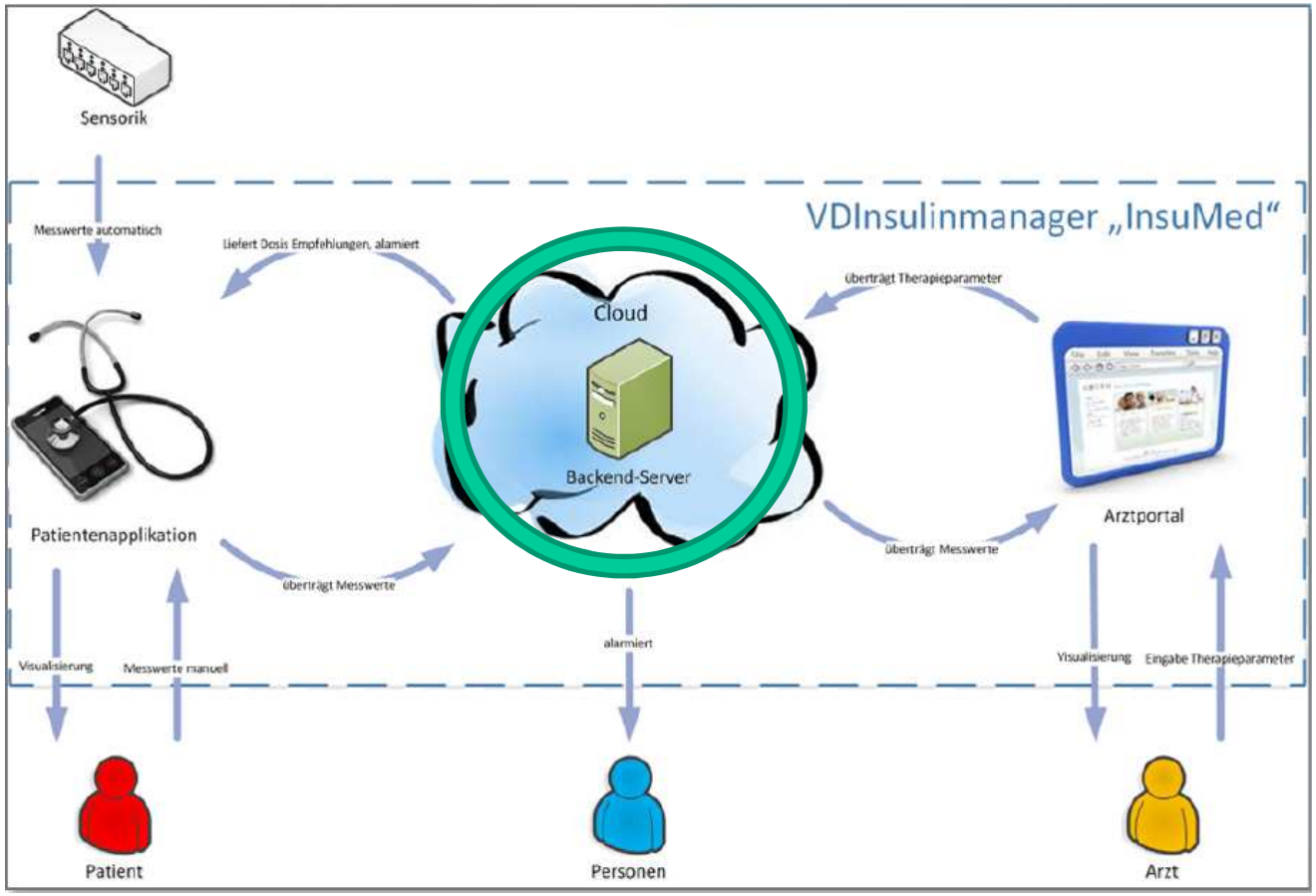
- Zeigt, wie man Sicherheitslücken beseitigt
- … aber auch, wo welche sind, die für Angriffe genutzt werden können!

Verifizierung der Security verteilter Systeme in der Praxis

Solche STIGs gibt es u.a. auch für

- Mobile Apps
- Web-Server
- Browser
- Datenbanksysteme
- Netzwerkdrucker
- MS PowerPoint
- …

Ausgangslage – Wo stehen wir im Projekt VDInsulinmanager?



Verifizierung der Security verteilter Systeme in der Praxis

Und für die Cloud:

DoD CLOUD COMPUTING SECURITY REQUIREMENTS GUIDE (SRG)

Auszug aus dem Inhaltsverzeichnis:

- 4 RISK ASSESSMENT OF CLOUD SERVICE OFFERINGS
- 5 SECURITY REQUIREMENTS
- 6 COMPUTER NETWORK DEFENSE AND INCIDENT RESPONSE

Infrastrukturaufwände und Provideranforderungen von Cloud Lösungen

Infrastrukturaufwände von Cloud Lösungen

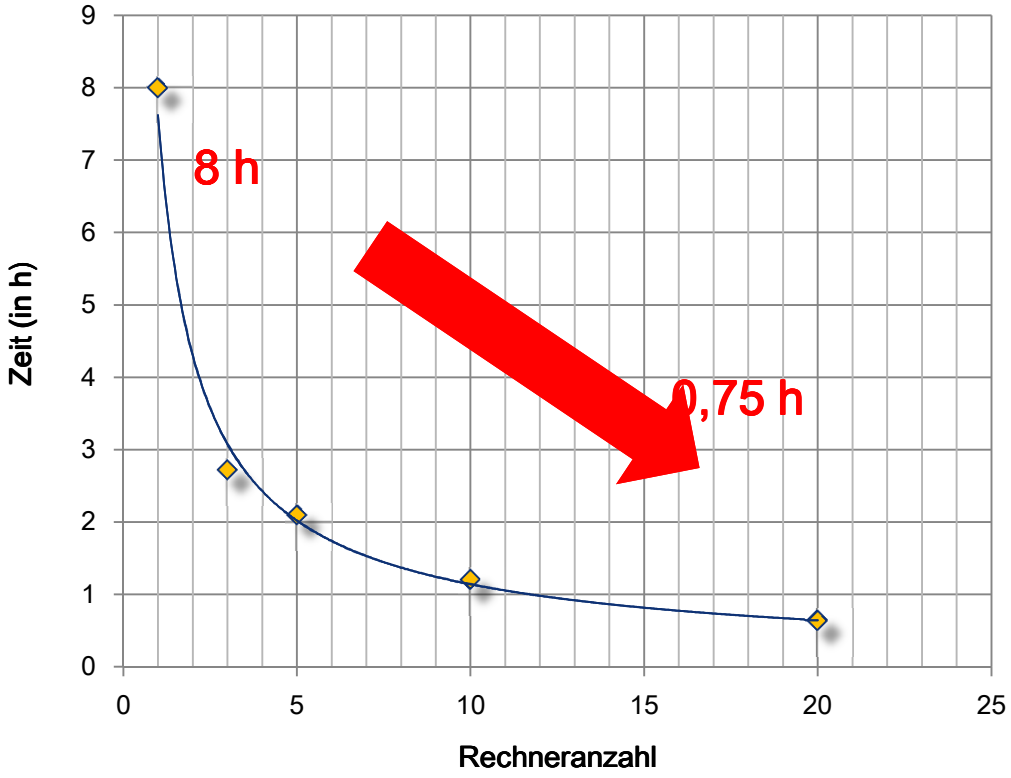
- Initialkosten für Virtualisierung
- Deutlich geringere Kapitalbindung in der Infrastruktur
  - z.B. Rechnerbeschaffung und Administration
  - ggf. Lizenzkosten
  - Pay-as-you-use

Verifizieren in der Cloud

- Testinfrastruktur ist stark skalierbar
- Testdurchführung nahezu beliebig verkürzbar
  - Abhängig von gemieteter Cloud-Performance und Testfall mit längster Durchführungszeit

Infrastrukturaufwände und Provideranforderungen von Cloud Lösungen

Testdurchführung in der Cloud



1296 Testfälle

Infrastrukturaufwände und Provideranforderungen von Cloud Lösungen

Verifizieren in der Cloud

- Bei Testfallgenerierung: Aufwandsreduktion
  - Zusätzliche Testabdeckung leicht generierbar
- Produktperformance
  - Aussagen hierüber nur bedingt möglich
- Security:
  - Eigene Cloud (mit Verlust einiger Vorteile) oder
  - Empfehlung: Cloud-Provider mit auditierbarem Sicherheitskonzept auswählen

Infrastrukturaufwände und Provideranforderungen von Cloud Lösungen

Validierung

in der Cloud

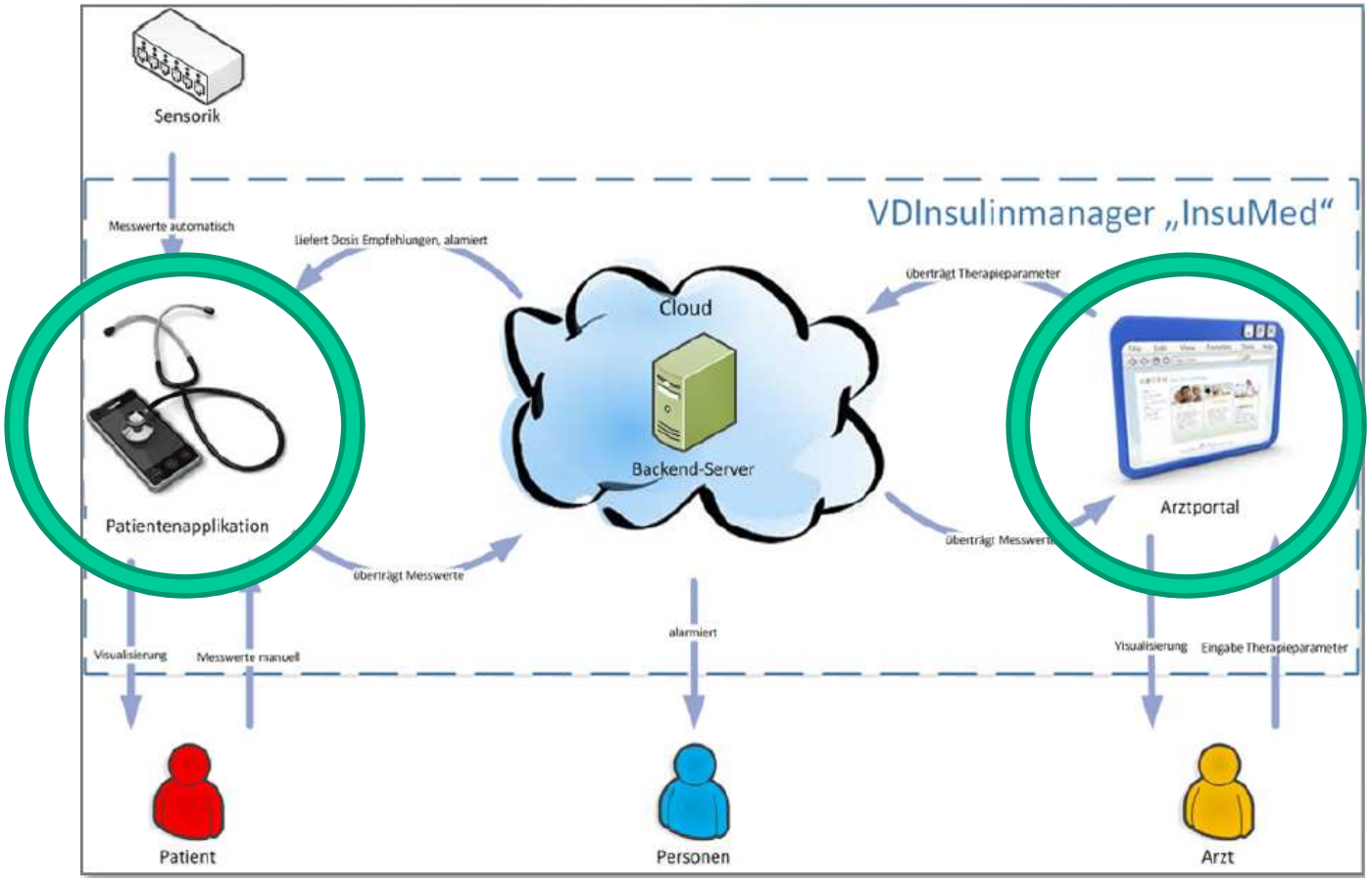
- SUT in der Cloud ist nicht das Endprodukt
- Also (eher) nicht

der Cloud-Infrastruktur

- als Produktbestandteil
- als Bestandteil von Entwicklungswerkzeugen

notwendig

Ausgangslage – Wo stehen wir im Projekt VDInsulinmanager?



Testautomatisierung zur Verifikation verteilter Systeme

Verifikation von Medical Apps

- Benötigt/erwünscht:
  - Testautomatisierungswerkzeug, das verschiedene (Mobil-) Plattformen unterstützt
- Erfahrungen:
  - Unterstützung für White-Box-Tests (instrumentierter Code) ist gut
  - Unterstützung für Black-Box-Tests verbesserungswürdig (unabhängig von einem bestimmten Tool)
  - Unterstützung für verschiedene Plattformen verbesserungswürdig (unabhängig von einem bestimmten Tool)
- Lösung:
  - Testautomatisierungsschnittstelle, die vom konkreten Tool abstrahiert
  - Für eine bestimmte Mobilplattform: Best-of-Breed-Ansatz (d.h. unterschiedliche Werkzeuge für verschiedene Plattformen)

Literaturhinweise

- Gesetzentwurf der Bundesregierung, Drucksache 18/5293, Entwurf eines Gesetzes für sichere digitale Kommunikation und Anwendungen im Gesundheitswesen, 22.06.2015
- BSI-Standard 100-3, Risikoanalyse auf der Basis von IT-Grundschutz, Version 2.5, 2008
- NIST STIG's Security Technical Implementation Guide
- DoD CLOUD COMPUTING SECURITY REQUIREMENTS GUIDE (SRG), Version 1, Release 1, 12 January 2015

Von der App in die Cloud und zurück
- V&V verteilter Systeme

Fragen?

guenther.klebes@seppmed.de
roman.arnouts@seleon.de