

Ihr Hacker im Unternehmen

Penetrationstests als ITIL basierender Prozess innerhalb
des IT-Security Managements

Falk Husemann

Sommersemester 2011

Für die Vorlesung IT-Management
Lehrstuhl 13, TU-Dortmund

Inhalt

- Motivation
- ITIL Security Management Prozess
 - Prozessanforderungen
 - Taktische Ebene
 - Operative Ebene
- Penetrationstest mit ITIL
 - Voraussetzungen
 - Prozessdefinition
 - Zusammenfassung

Motivation

- Was ist ein Hacker?

Ein Hacker ist eine *”Person, die aus technischem Interesse sich detailliert mit der Funktionalität von Hard- und Software auseinandersetzt und dadurch das Notwendige Know-How besitzt, Sicherheitsvorkehrungen in Hard- oder Software zu umgehen.”* (Bundesamt für Sicherheit in der Informationstechnik)

- ITIL konformes Security Management mit externen Security-Auditoren/Penetrationstestern

- Nachteile

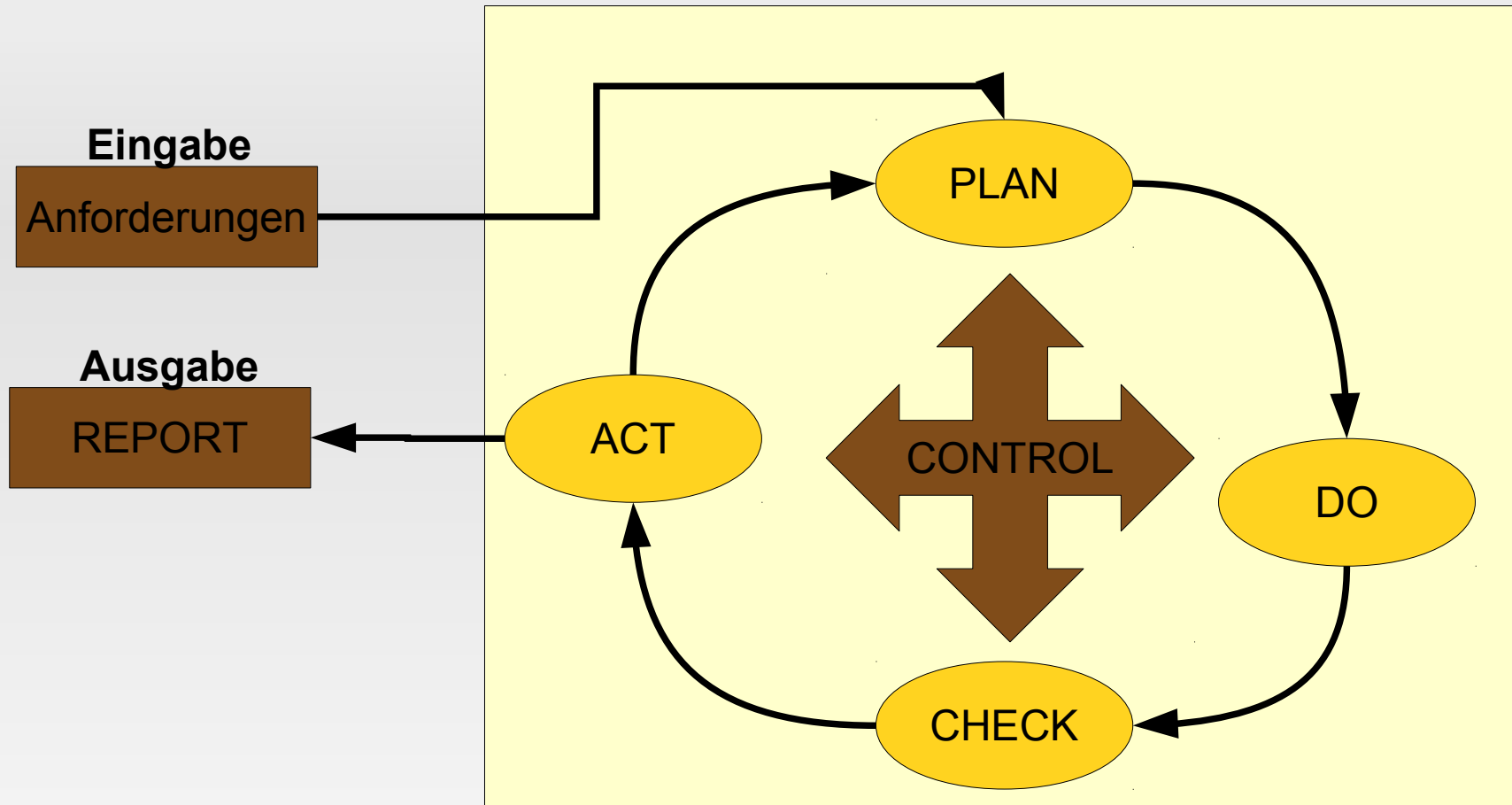
- Test muss manuell ausgelöst werden
- Informationsfluss während des Tests sporadisch
- Einflussnahme während der Durchführung begrenzt
- Relevanz der Ergebnisse für Unternehmensziele?

Motivation

- Vorteile eines eigenen Prozesses
 - Direkte Kommunikation mit zuständigen Unternehmensstellen
 - Kosteneinsparung gegenüber externen Beratern
 - Aktuelle Entwicklungen schneller miteinbeziehen
 - Kürzere Durchlaufzeiten
- Für wen sind bei erfolgreicher Penetration Geschäftsgeheimnisse und Unternehmensdaten sichtbar?
- Neue Bedrohungslagen ("Cyberwarfare") erfordern bessere Prävention und schnellere Reaktion
- Direkte Einbindung des Penetrationstestings in das IT-Security Management als Unterprozess

ITIL Security Management

Prozessanforderungen



- ITIL Definition des Security Management Prozesses
- Basiert auf ISO/IEC 17799 *Leitfaden für das Informationssicherheits-Management*

ITIL Security Management

Anforderungen

- Außerhalb ITSM-Prozess vorhanden
- Müssen zusammengetragen werden
- Grundlagen für Anforderungen nach ITIL
 - Sicherheitsziele für Dienste allgemein
 - Service Level Agreements (SLA)
 - Vereinbarungen mit Kunden
 - Operational Level Agreements (OLA)
 - Vereinbarungen mit internen Leistungserbringern
 - Underpinning Contracts (UC)
 - Externe Partner zur Leistungserbringung

ITIL Security Management

PLAN

- Sicherheitsziele aus SLAs in OLAs konvertieren
- OLAs enthalten
 - Maßnahmen zur Realisierung der Sicherheitsziele
 - Durch Risikoanalyse ermitteln
 - Security Pläne sind operative Maßnahmen
- Informationssicherheits-Policy erstellen
 - Ziel und Umfang des Informationssicherheitsmanagementsystems (ISMS)

ITIL Security Management

DO

- Implementierung der Security Pläne

ITIL Security Management

CHECK

- Qualitätssicherungsphase
- Self Assessment
 - Selbstbewertung anhand von Fragebögen
- Interne Prüfung
 - IT-Revision
 - Wurde dem Unternehmen durch die IT Schaden zugefügt?
 - IT-Security Manager
 - Werden Sicherheitsziele eingehalten?
- Externe Prüfung
 - Audit oder **Penetrationstest**

ITIL Security Management

ACT

- Gefundene Schwachstellen abstellen
- Optimierungspotenziale umsetzen
- Entschiedene Maßnahmen einhalten
- Informationssicherheit halten oder übertreffen
 - Änderungen der IT auf Einfluss der IT-Sicherheit analysieren
 - Regelmäßige Risikobewertung
 - Anpassung der Sicherheitsziele
 - Eingabe für PLAN Phase

ITIL Security Management

CONTROL

- Macht PDCA-Modell ITIL kompatibel
- Security Management Rahmenwerk
 - Definition von Security Plänen
 - Implementierungsrichtlinien
 - Berichtswesen
 - Definition der Prozessorganisation
 - Rollen
 - Verantwortlichkeit
 - Eskalationswege
- Schnittstellendefinition zu anderen Prozessen

ITIL Security Management

REPORT

- Nicht Teil des klassischen PDCA-Modells
- Externes Berichtswesen für ITIL Konformität
- Vermittelt Ergebnisse und Status Dritten
 - Unternehmensleitung
 - Andere Prozesse (Incident Management ,...)
- Kennzahlen ermöglichen Unternehmensleitung Trends zu erkennen
- Basis für zukünftige Entscheidungen

ITIL Security Management

- Wie ist der Security Management Prozess mit anderen Prozessen verbunden?
 - Auf der Taktischen Ebene
 - Auf der Operativen Ebene

ITIL Security Management

Taktische Ebene 1/2

- Beschreibung durch Service Delivery
- Prozesse für Planung und Controlling



- Taktische Prozesse

Service Level Management

Availability Management

Capacity Management

Finance Management für IT-Services

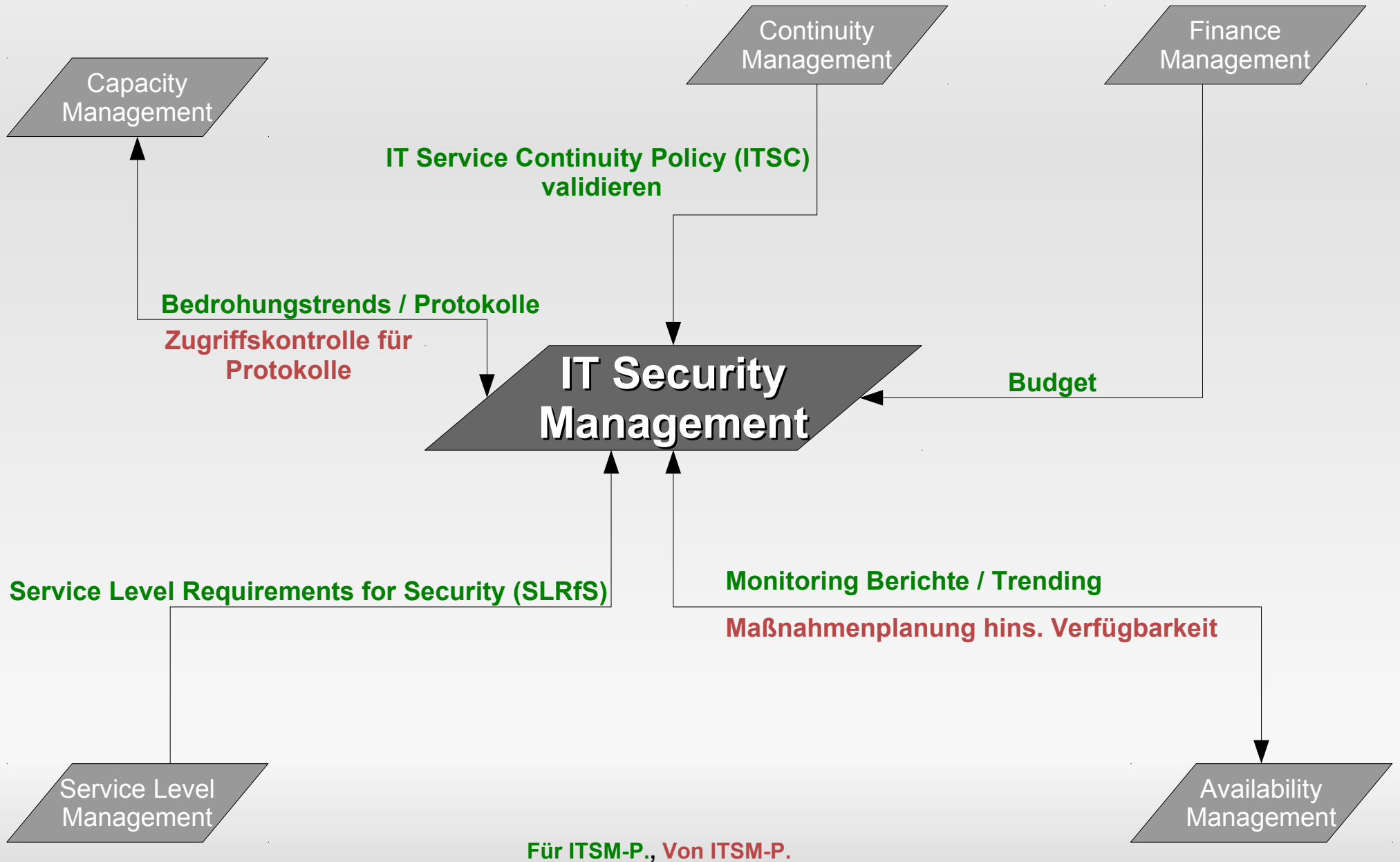
IT Service Continuity Management

IT Security Management

- Wie interagieren die Prozesse?

ITIL Security Management

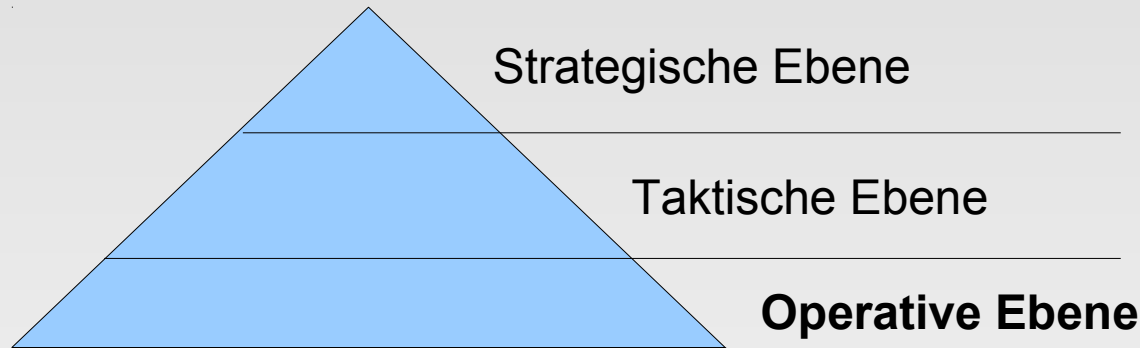
Taktische Ebene 2/2



ITIL Security Management

Operative Ebene 1/2

- Beschreibung durch Service Support
- Prozesse für direkte Leistungserbringung



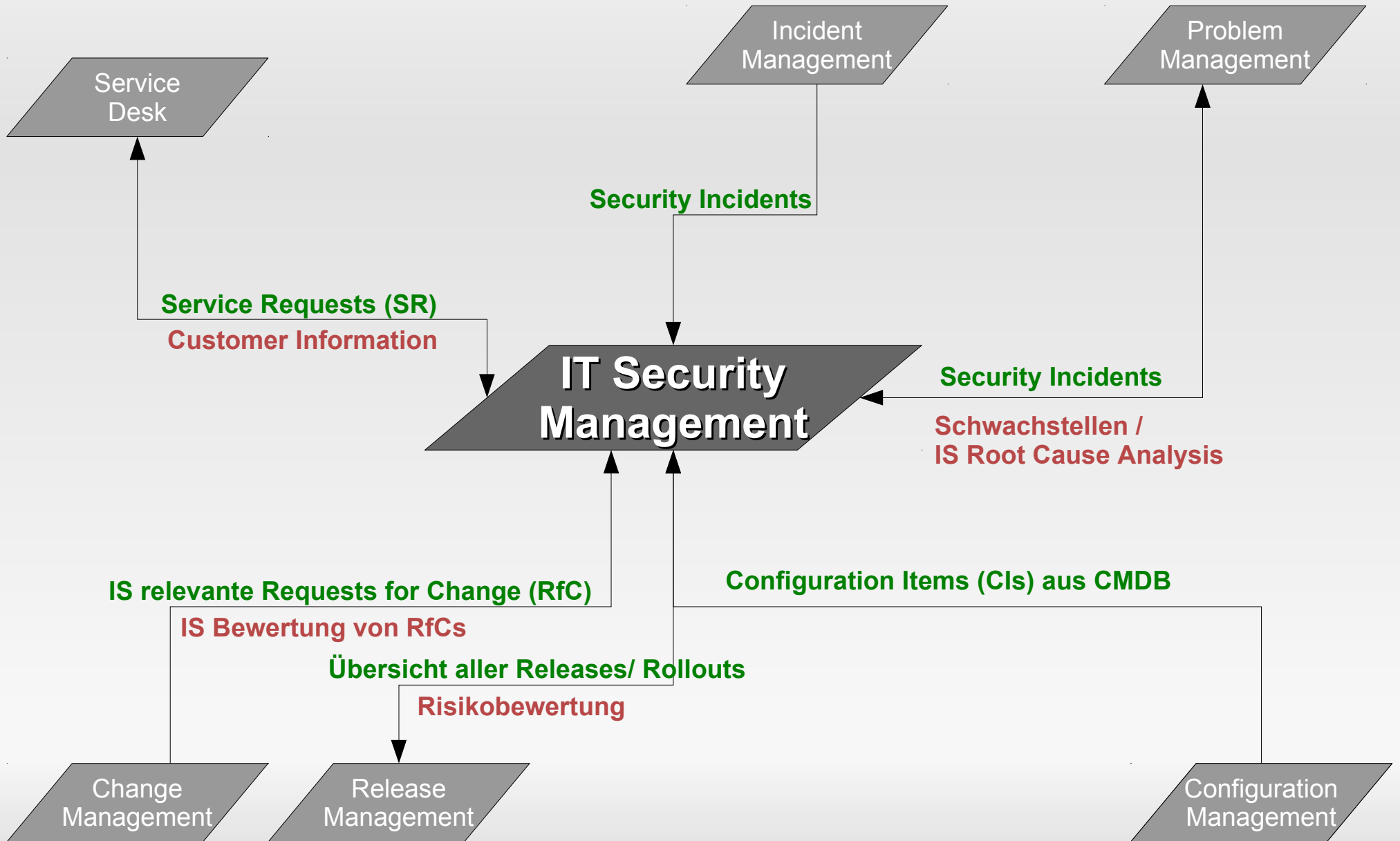
- Operative Prozesse

Service Desk	Incident Management
Problem Management	Change Management
Configuration Management	Release Management

- Wie interagieren die Prozesse?

ITIL Security Management

Operative Ebene 2/2



Für ITSM-P., Von ITSM-P.

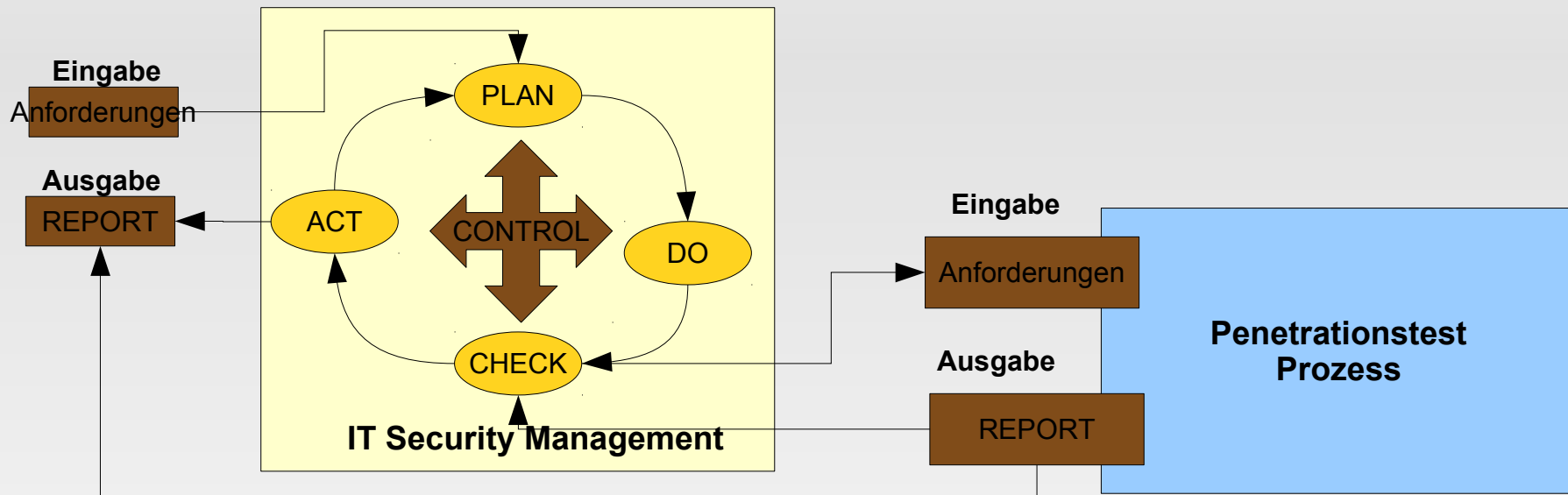
Penetrationstests nach ITIL

- Penetrationstest mit ITIL
 - Voraussetzungen
 - Prozessdefinition
 - Anforderungen
 - PLAN
 - DO
 - CHECK
 - ACT
 - CONTROL
 - REPORT
 - Zusammenfassung

Penetrationstests nach ITIL

Voraussetzungen 1/2

- Idee: Penetrationstest Prozess ersetzt externe Tests

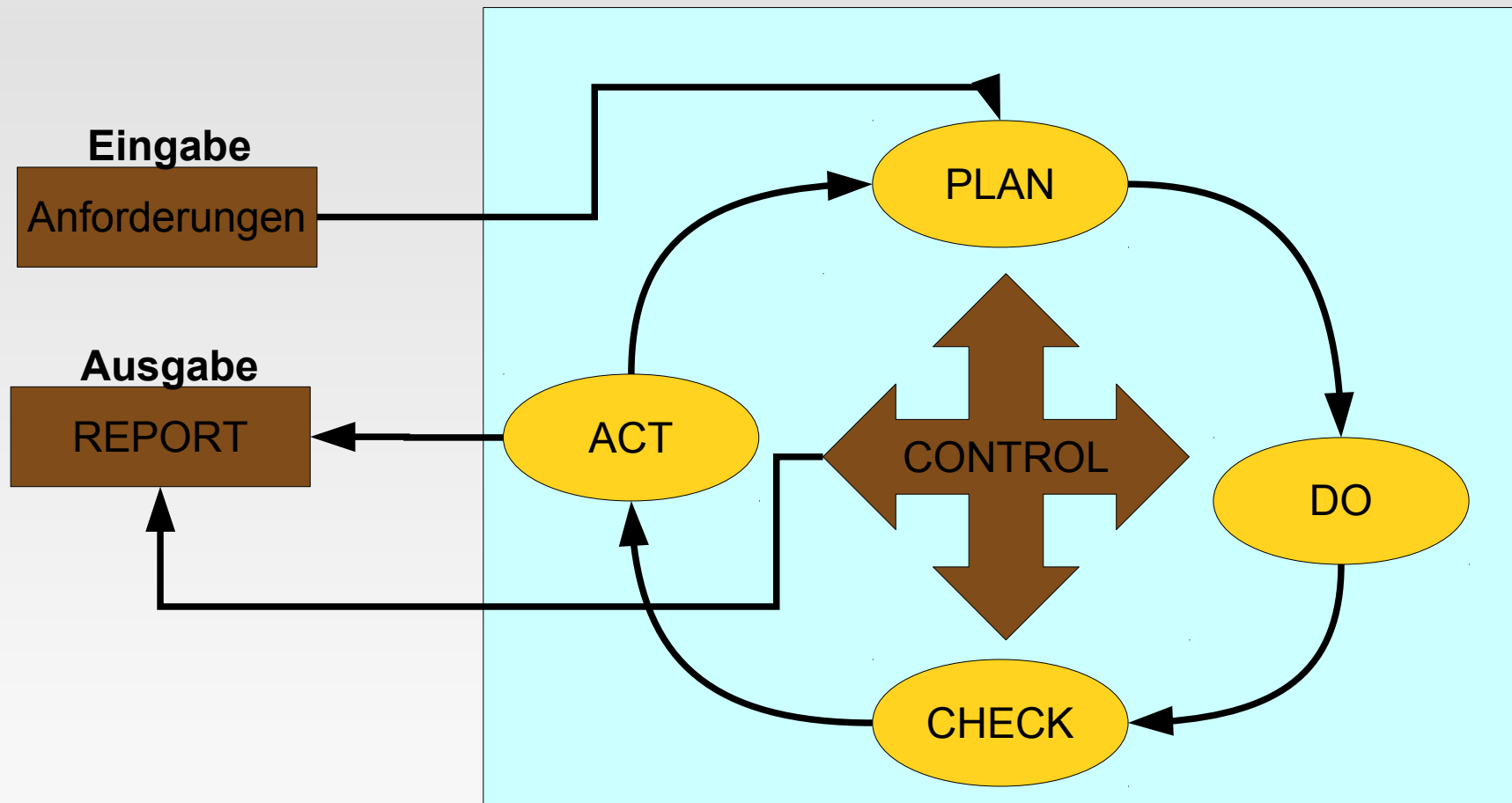


- Nahtlose Anbindung an taktische und operative Prozesse über IS Management
- Direkte Einbindung in CHECK Phase
- Statt Beauftragung externer Penetrationstests

Penetrationstests nach ITIL

Voraussetzungen 2/2

- Wie Penetrationstest Prozess (PtP) aufbauen?



Penetrationstests nach ITIL

Anforderungen

- **Zu prüfende Dienste**

Ein Dienst ist ein System, das aus einer oder mehreren logischen Einheiten besteht und dessen Zweck die Erbringung einer eingrenzbaeren Leistung ist.

- Netzwerkdienst SMTP (ein Server)
- Webshop im Clusterbetrieb (viele Server)

- **Bedingungen an Prozess**

- SLAs/OLAs die nicht gebrochen werden dürfen
- Datenschutzrichtlinie
- Nicht auszulösende Notfallprozeduren

Penetrationstests nach ITIL

PLAN 1/3

- Kriterien des Tests auswählen
- **Informationsbasis**
 - Black-Box
 - White-Box
- **Aggressivität**
 - Passiv-scannend
 - Vorsichtig
 - Abwägend
 - Aggressiv
- **Umfang**
 - Vollständig
 - Begrenzt
 - Fokussiert
- **Vorgehensweise**
 - Verdeckt
 - Offensichtlich
- **Technik**
 - Netzwerkzugang
 - Sonstige Kommunikation
 - Physischer Zugang
 - Social-Engineering
- **Ausgangspunkt**
 - Von außen
 - Von Innen

Penetrationstests nach ITIL

PLAN 2/3

- Rechtliche Rahmenbedingungen
 - Bei Diensten mit Underpinning Contracts (UC)
 - §202a Abs. 1 (1) StGB *Ausspähen von Daten*
 - §263a StGB *Computerbetrug*
 - §303b StGB *Computersabotage*
- Ethische Rahmenbedingungen
 - Social Engineering und Arbeitsklima
- Organisatorische Rahmenbedingungen
 - Vorbereitung und Information des Notfall Managements

Penetrationstests nach ITIL

PLAN 3/3

- Einzelschritte nach OSSTMM und BSI-Studie aus Modulkatalog wählen
- I-Module *Informationsbeschaffung*
 - I12: Recherche nach Schwachstellen
- E-Module *Eindringversuche*
 - E11: Abhören von Passwörtern
- Module sind Eingabe für DO-Phase

Penetrationstests nach ITIL

DO 1/2

- **Ausführen des Penetrationstests**

1. **Phase I-Module** ausführen

2. **Phase** Bedrohungen analysieren und Prioritäten definieren

3. **Phase E-Module** ausführen

- **Systematische Dokumentation der Eingabe und Ausgabe der Module**

- **BSI-Studie liefert Vorlagen**

- Anpassung an Unternehmensumfeld

- Erweiterung der Incident Reports des Incident Managements

Penetrationstests nach ITIL

DO 2/2

- Software für systematische unternehmensweite Penetrationstests



- Linux Distribution für Penetrationstests



- Python Framework mit > 600 Exploits
 - Leicht automatisier- und parallelisierbar (SQL-Backend)

Penetrationstests nach ITIL

CHECK

- Dokumentation aus DO-Phase analysieren
- Einzelergebnisse kategorisieren
 - Incident
 - Problem
 - Emergency
- Zustand des geprüften Dienstes erarbeiten
- Erfolgreiche Angriffspfade dokumentieren

Penetrationstests nach ITIL

ACT

- Kategorisierte Einzelergebnisse an zuständige Prozesse weitergeben

Penetrationstests nach ITIL

CONTROL

- Vetofunktion während aller Phasen
- Operativer Vorteil gegenüber externem Penetrationstest
 - Feingranulare Prozesssteuerung
- Prozess stoppen
 - Wenn SLA oder OLA gefährdet
 - Rechtsverletzung
 - Prozessziel ist kein Unternehmensziel

Penetrationstests nach ITIL

REPORT

- Aufbereitung der Ergebnisse
- Vermittlung an Unternehmensleitung
- Key Performance Indicators (KPI)
 - Anzahl durchgeführter Tests
 - Anzahl erfolgreicher Tests (Kompromittierung)
 - Durchschnittliche Testdauer pro Dienst?
 - Aufschlüsselung nach Dienstgröße
 - Anzahl gefundener Schwachstellen
 - Anzahl behobener Schwachstellen mit Auslöser PtP

Zusammenfassung

- Exemplarischen Prozess entwickelt
- Anbindung an vorhandene Prozesse
- Weitgehend nach ITIL
- Konkrete Implementierung
 - Rollen definieren
 - Berichtswesen an Unternehmen anpassen
 - Produktiver Einsatz?

Quellen

- J. Brunnstein: ITIL Security Management realisieren (2006)
ISBN: 3834801658
- BSI: Durchführungskonzept für Penetrationstests (2005)
<https://www.bsi.bund.de/ContentBSI/Publikationen/Studien/pentest>
- C. McNab: Network Security Assessment (2007)
ISBN: 9780596510305

Fragen