

# Ihr Hacker im Unternehmen

## Penetrationstests als ITIL basierender Prozess innerhalb des IT-Security Managements

Falk Husemann

Lehrstuhl für Dienstleistungsinformatik  
Technische Universität Dortmund

**Zusammenfassung** Die IT Infrastructure Library hilft Unternehmen und öffentlichen Einrichtungen, Prozesse in der IT zu konzipieren und zu betreiben. Im Rahmen dieser Übungsarbeit stelle ich die Konzepte des Security Managements nach ITIL vor. Die Arbeit basiert auf dem Buch *ITIL Security Management realisieren*. Im Anschluss wird prototypisch ein neuer Unterprozess in das Security Management integriert: Das Penetrationstesting.

# Inhaltsverzeichnis

1	Einleitung .....	III
2	Sicherheit .....	III
3	ITIL .....	IV
4	Security Management .....	V
4.1	Anbindung taktische Ebene.....	VII
	Service Level Management.....	VII
	Availability Management .....	VII
	Capacity Management .....	VIII
	IT Service Continuity Management .....	IX
	Finance Management for IT-Services .....	IX
4.2	Operative Ebene .....	IX
	Service Desk.....	IX
	Incident Management .....	IX
	Problem Management.....	X
	Change Management .....	X
	Configuration Management .....	XI
	Release Management.....	XI
5	Fallstudie: Penetrationstest Prozess .....	XI
5.1	Grundlagen.....	XII
5.2	Prozess .....	XII
5.3	Fazit.....	XIV

## 1 Einleitung

Die Informationstechnik prägt den Unternehmensalltag immer mehr. Kaum ein Unternehmen kommt ohne Personalcomputer oder andere Geräte zur digitalen Datenverarbeitung aus. Die durch die IT angebotenen Dienstleistungen sind oft erfolgskritisch für das Unternehmen. Aber wie wird sichergestellt, dass die Lohnkostenberechnung oder der Webshop des Unternehmens fortwährend so verfügbar sind, wie beabsichtigt? Der Security Management Prozess aus ITIL beantwortet diese Frage und bindet die Sicherheit in die Unternehmens IT ein.

## 2 Sicherheit

Es gibt viele Arten von Sicherheit, zwischen denen es nicht immer leicht ist, zu unterscheiden. So ist die Garantie, dass ein Dienst immer zur Verfügung steht eine andere Art der Sicherheit als die Garantie, dass dieser Dienst auch das tut, wofür er konzipiert wurde. Im ersten Fall wird von Verfügbarkeit gesprochen, im zweiten von Funktionssicherheit. Um den Umfang des Security Managements nach ITIL zu überblicken, müssen die Schutzziele<sup>[5]</sup> für informationstechnische Systeme definiert werden.

### Funktionssicherheit

Unter Funktionssicherheit wird der Zustand verstanden, bei dem die Soll-Funktionalität eines Dienstes oder Systems der Ist-Funktionalität entspricht. Gebräuchlich ist auch der Begriff Safety. Ein Webshop, der keinen Warenkorb bereitstellt, dies aber sollte, ist ein Beispiel für nicht gegebene Funktionssicherheit.

### Informationssicherheit

Hier ist der Zustand gemeint, bei dem keine unautorisierte Informationsveränderung stattfinden kann. Auch unter Informationssicherheit fällt der Zustand, bei dem nicht unautorisiert Informationen gewonnen werden können. Könnte jeder Kunde in einem Webshop die Preise selbst ändern und Einkaufspreise einsehen, wäre Informationssicherheit nicht gegeben.

### Datensicherheit

Datensicherheit ist der Zustand, bei dem kein unautorisierter Zugriff auf Ressourcen des Systems (und die dort enthaltenen Daten) genommen werden kann. Könnte über eine SQL-Injection jeder Kunde eines Webshops die komplette Kundendatenbank lesen, wäre Datensicherheit nicht gegeben.

### Datenschutz

Wenn eine natürliche Person die Erhebung und Verarbeitung ihrer Daten selbst bestimmen kann, wird von Datenschutz gesprochen. Würden alle Kontaktdaten eines Kunden ohne sein Einverständnis an andere Unternehmen verkauft, wäre Datenschutz nicht gegeben.

**Vertraulichkeit**

Vertraulichkeit bezeichnet den Zustand, bei dem keine unautorisierte Kenntnisnahme von Daten oder Informationen möglich ist. Wenn alle Kontodaten aller Kunden eines Webshops offen für jeden Besucher zugänglich wären, ist Vertraulichkeit nicht gegeben.

**Integrität**

Hier wird ein Zustand beschrieben, in dem keine unbemerkte Manipulation von Daten möglich ist. Könnten Artikel im Warenkorb eines anderen Kunden vor der Bestellung manipuliert werden, wäre Integrität nicht gegeben.

**Verfügbarkeit**

Mit einer Autorisierung ausgestattete Zugriffe können ohne Beeinträchtigung durch unautorisierte Zugriffe ihre Berechtigungen nutzen. Sind Angreifer in der Lage, den Webshop durch einen Denial of Service Angriff<sup>1</sup> lahm zu legen, ist Verfügbarkeit nicht gegeben.

**Zurechenbarkeit**

Für die IT-Sicherheit wichtige Aktionen sind eindeutig dem ausführenden Subjekt zurechenbar. Könnte jeder Kunde eines Webshops völlig anonym Bestellungen ohne Adresse und Namen aufgeben, wäre die Zurechenbarkeit nicht gegeben.

**3 ITIL**

Die IT Infrastructure Library[1] an sich ist eine Entwicklung des OGC<sup>2</sup> in Großbritannien und dient dem Zweck, die Unternehmensprozesse hinsichtlich IT zu definieren und so eine Sammlung an Best-Practise Vorgehensweisen zur Verfügung zu stellen. Dabei wurde besonderer Wert darauf gelegt, die praktische Relevanz von ITIL sicherzustellen. Vorgänge nach ITIL werden als Prozess definiert, die eine feste Eingabe und eine feste Ausgabe haben.

Das IT-Management nach ITIL ordnet die Prozesse drei Ebenen zu. Die Prozesse werden hier kurz schemenhaft eingeführt, um die Anbindung des IT-Security Managements an die anderen Unternehmensprozesse verständlicher zu machen.

**Strategische Ebene**

Die strategische Ebene ist für das Management der IT-Dienstleistungen zuständig und spielt für das IT Security Management eine untergeordnete Rolle.

---

<sup>1</sup> Angriff mit Ziel der Überlastung eines Dienstes. Folge ist der Ausfall des Dienstes.

<sup>2</sup> Office of Government Commerce

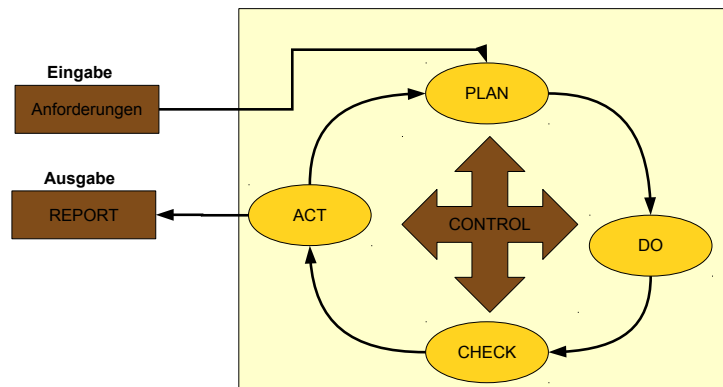
### Taktische Ebene

Die taktische Ebene ist für die Planung und Steuerung von IT-Dienstleistungen zuständig. Diese Ebene wird durch das Service Delivery beschrieben. Auf der taktischen Ebene befinden sich neben dem IT Security Management noch weitere Prozesse.

### Operative Ebene

Die Operative Ebene ist für die Ausführung der geplanten Aufgaben zuständig und erfüllt einen Großteil der Aufgaben in praktischer Hinsicht.

## 4 Security Management



**Abbildung 1.** Der IT-Security Management Prozess

Das Security Management ist ein neuer Prozess der IT Infrastructure Library, dessen Aufgabe die Entwicklung und Einhaltung der IT-Sicherheitsrichtlinie für das Unternehmen ist. Der Prozess ist dabei sehr stark in alle anderen Prozesse eingebunden, um Einschätzungen hinsichtlich Sicherheit anzubieten. Der Prozess selbst ist in sieben Phasen aufgeteilt, die zusammen einen zyklischen Ablauf ermöglichen. Der in Abbildung 1 dargestellte Informationsfluss zwischen den Phasen ermöglicht die Einbindung in das IT Management und die anderen Prozesse sowohl auf der taktischen, wie auch auf der operativen Ebene. Dieser

Prozess basiert auf ISO/EIC 1779 <sup>3</sup> und wird als erweiterter Demingkreis <sup>4</sup> dargestellt.

*Anforderungen* sind bereits außerhalb des ITSM-Prozesses vorhanden und müssen zusammengetragen werden. Grundlagen für die Anforderungen nach ITIL sind unter anderem die Sicherheitsziele allgemein, sowie die Service Level Agreements (SLA) mit Endkunden. Außerdem zu betrachten sind die Operational Level Agreements (OLA) sowie die Underpinning Contract (UC).

*In der Plan-Phase* wird die Informationssicherheits-Policy definiert. Die Service Level Agreements mit Kunden werden in Operational Level Agreements mit internen Leistungserbringern konvertiert. Die Sicherheitsziele die aus den Operational Level Agreements hervorgehen, werden geprüft. Aus dieser Prüfung müssen dann Maßnahmen zur Realisierung der Sicherheitsziele erarbeitet werden, diese Maßnahmen werden in Security Plänen beschrieben. Security Pläne enthalten die operativen Maßnahmen zur Realisierung der Sicherheitsziele.

*In der Do-Phase* werden die Security Pläne ausgeführt.

*Die Check-Phase* ist die Qualitätssicherungsphase im erweiterten Demingkreis. Die Qualitätssicherung kann nach ITIL auf drei verschiedenen Arten durchgeführt werden. Die erste Art ist das Self Assessment, bei dem eine Selbstbewertung anhand von Fragebögen stattfindet. Die zweite Art ist die interne Prüfung. Hier wird zwischen zwei Unterarten unterschieden. Die erste Unterart zur Qualitätssicherung ist die IT-Revision, die unter dem Gesichtspunkt des möglichen Unternehmensschadens die IT untersucht. Die zweite Unterart zur Qualitätssicherung ist die IT-Revision durch den IT Security Manager. Diese findet unter dem Gesichtspunkt der Einhaltung der Sicherheitsziele statt. Beide Unterarten der internen Prüfung folgen verschiedenen Zielen und können sich gegenseitig ergänzen oder unterstützen. Die dritte Art der Qualitätssicherung ist die externe Prüfung durch einen Audit oder einen Penetrationstest. Dabei werden die Sicherheitsrichtlinie und die Security Pläne mit dem Ist-Zustand abgeglichen (Audit) oder versucht, Abdeckungsprobleme der Security Plänen auf die Sicherheitsrichtlinie zu finden (Penetrationstest).

*In der Act-Phase* müssen die gefundenen Schwachstellen abgestellt werden. In der Regel geschieht dies durch die Erweiterung der Security Pläne. Außerdem müssen gefundene Optimierungspotenziale genutzt werden und die unterschiedlichen Maßnahmen eingehalten werden. Ziel der Act-Phase ist also, den erreichten Grad der Informationssicherheit zu halten oder zu übertreffen. Weiter muss die Act-Phase den Einfluss der IT-Sicherheit auf Änderungen der IT prüfen und regelmäßige Risikobewertungen erstellen. Diese Risikobewertungen können wieder als Eingabe für die Plan-Phase dienen, wodurch der Prozess zyklisch wird.

---

<sup>3</sup> ISO/EIC 1779: *Leitfaden für das Informationssicherheits-Management*

<sup>4</sup> Demingkreis: Auch PDCA-Zyklus, vierphasiger iterativer Problemlösungsprozess

*Die Report-Phase* ist nicht Teil des klassischen Demingkreis, wird aber für ITIL Konformität gefordert. Aufgabe der Phase ist es, ein externes Berichtswesen zur Verfügung zu stellen. Dieses Berichtswesen dient dem Zweck, die Prozessergebnisse an externe Dritte zu vermitteln. Dazu gehört die Unternehmensleitung, wie auch andere Prozesse (zum Beispiel das Incident Management). Eine weitere Aufgabe des externen Berichtswesens ist die Ermittlung der Key Performance Indicators (KPI), die eine wichtige Grundlage für das Erkennen von Trends und fällen zukünftiger Entscheidungen sind.

*Durch die Control-Phase* wird das Security Management Rahmenwerk definiert. Dazu gehört das Erarbeiten von Security Plänen, Implementierungsrichtlinien und das Einrichten des Berichtswesens. Außerdem muss die Prozessorganisation definiert werden, zu der die Definition der Rollen, Verantwortlichkeiten und Eskalationswege gehört. Auch die Schnittstellendefinition zu anderen Prozessen wird durch die Control-Phase bestimmt.

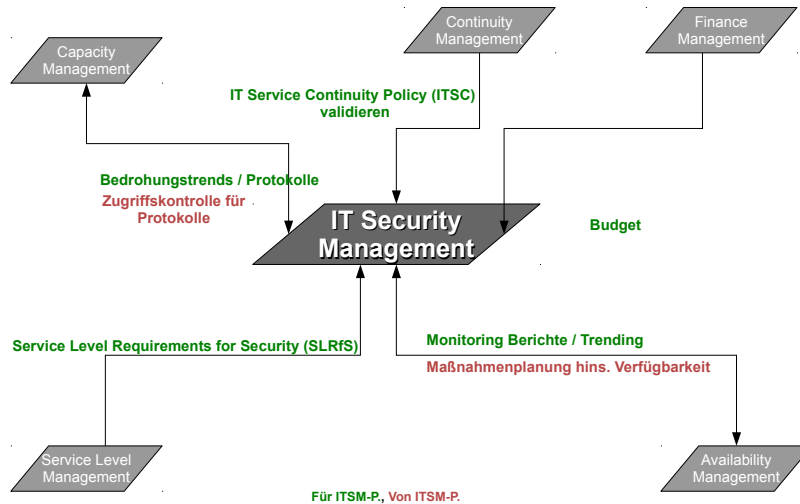
#### 4.1 Anbindung taktische Ebene

Wie aber ist das Security Management an die anderen Prozesse angebunden? Auf der taktischen Ebene ist die Anbindung schemenhaft Abbildung 3 dargestellt. Zu unterscheiden ist dabei zwischen Eingaben für andere Prozesse (rot gekennzeichnet) und Eingaben aus anderen Prozessen (grün gekennzeichnet).

**Service Level Management** Das Service Level Management soll sicherstellen, dass verbindliche Absprachen mit dem Kunden über Umfang und Güte des zu erbringenden IT-Services getroffen werden und Nebenabsprachen vermieden werden. Ziel in Bezug auf das Security Management ist, dass alle zu erbringenden Dienstleistungen dokumentiert sind. Sonst wäre unklar, ob eine Dienstleistung nur nicht in ein Service Level Agreement aufgenommen wurde, weil sie zu teuer ist, oder weil sie nicht die Informationssicherheitsrichtlinie erfüllen kann.

*SLA und OLA* Ein Service Level Agreement (SLA) ist eine Vereinbarung über Dienstleistungen mit dem Kunden. Diese Vereinbarung wird in Operational Level Agreements (OLA) aufgebrochen. OLAs sind Vereinbarungen mit den internen Leistungserbringern. Ein SLA besteht also aus mehreren OLAs. Kann eine Dienstleistung nicht intern erbracht werden, muss ein Underpinning Contract (UC) mit einem externen Leistungserbringer abgeschlossen werden.

**Availability Management** Die Aufgabe des Availability Managements ist es, die Verfügbarkeit der angebotenen IT-Dienstleistung anhand mehrerer Kriterien sicherzustellen. Dabei unterstützt das Availability Management das Security Management durch Analysen und Maßnahmenplanungen hinsichtlich der Verfügbarkeit der Dienste.



**Abbildung 2.** Anbindung des ITSM auf taktischer Ebene

*Zuverlässigkeit* beschreibt die Eigenschaft einer IT-Dienstleistung, zu vereinbarten Zeiten die festgelegten Funktionen vollständig zur Verfügung zu stellen. Eine Aussage über die Einflussnahme unautorisierter Benutzer (siehe Funktionssicherheit) wird hier nicht getätigt.

*Wartbarkeit* trifft Aussagen darüber, wie gut ein System gewartet werden kann und ob es Auswirkungen bei der Wartung auf andere Systeme gibt. Eine Wartung ist eine Erweiterung, Reparatur, Update, Upgrade oder Patch einer Software- oder Hardware-Komponente.

*Servicefähigkeit* gibt an, wie gut eine IT-Dienstleistung durch dritte (siehe Underpinning Contracts) hinsichtlich Verfügbarkeit gewartet werden kann.

**Capacity Management** Die Aufgabe des Capacity Managements ist es, die wirtschaftliche Verwendung aller IT-Ressourcen sicherzustellen. Der wesentliche Aspekt des Capacity Managements ist also die Planung. Im Capacity Management wird sowohl die IT-Strategie geplant, als auch Abschnittsziele erarbeitet. Eine weitere wichtige Dienstleistung, insbesondere für das Security Management, ist die Erarbeitung von Bedrohungstrends. Diese Trends helfen dem Security Management, konkrete zukünftige Bedrohungen für das Unternehmen zu ermitteln.

**IT Service Continuity Management** Um in Notfallsituationen die IT-Dienstleistungen schnell wieder in Betrieb zu nehmen, muss vor einem Notfall ein Notfallplan vorliegen. Um die Erarbeitung dieser Pläne kümmert sich das Service and Continuity Management. Ein Notfall liegt genau dann vor, wenn ein IT-Service nicht innerhalb der durch ein Service Level Agreement festgelegten Zeit wieder in den Normalbetrieb übergehen kann. In diesem Fall muss ein Notfallplan ausgeführt und der Dienst in den Notfallbetrieb überführt werden. Dabei ist es nicht nur Aufgabe des IT Service Continuity Managements, diese Pläne zu erarbeiten, sondern auch die Analyse von Auswirkungen der Notfälle, sowie die Definition von Mindestwiederherstellzeiten. Das Security Management unterstützt das IT Service Continuity Management durch Sicherheitsprüfung der Notfallpläne gegen die Sicherheitsrichtlinien und die Beratung für die Sicherung der Notfallpläne.

**Finance Management for IT-Services** Aufgabe des Finance Management for IT-Services ist es, das Budgeting, Accounting und Charging für alle IT-Dienstleistungen abzuwickeln. Budgeting beschreibt dabei die Zuordnung von Mitteln zu IT-Services und Projekten. Accounting beschreibt die Ermittlung der Kosten eines IT-Services und Charging die Abrechnung der in Anspruch genommenen Leistungen. Da das Security Management ein Teil des Unternehmens ist, wird das Budget des Prozesses durch das Finance Management for IT-Services abgewickelt.

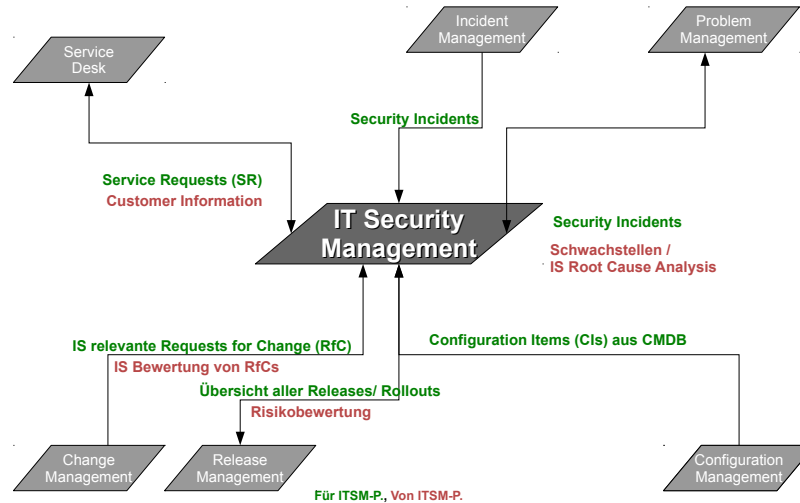
## 4.2 Operative Ebene

Die operative Ebene ist für die Unterstützung von IT-Dienstleistungen zuständig. Auf Abbildung 3 ist die Anbindung des Security Management Prozesses an die anderen Prozesse der operativen Ebene schemenhaft dargestellt. Zu unterscheiden ist hierbei zwischen Eingaben für andere Prozesse (rot gekennzeichnet) und Eingaben aus anderen Prozessen (grün gekennzeichnet).

**Service Desk** Der Service Desk ist der Prozess mit direktem Kundenkontakt. Aufgabe des Service Desk ist die Aufnahme und Weiterleitung von Anfragen. Dazu zählen Störungen, Informationsanfragen, Wünsche, Aufträge und Service Requests. Die Aufgaben des Service Desks werden in vielen Unternehmen durch das Incident Management wahrgenommen.

**Incident Management** Aufgabe des Incident Management ist die komplette Verwaltung und Bearbeitung von Störungen. Eine Aufnahme und Klassifizierung von Störungen erleichtert die Weiterleitung an die zuständigen internen Stellen der IT-Organisation. Zwei wichtige Kriterien werden durch das Incident Management für jede Störung festgelegt. Das Resultat dieser Klassifizierung ist die Priorität einer Störung.

Die Schadensauswirkung beschreibt die möglichen Auswirkungen einer Störung auf die IT-Dienstleistungen und muss im Rahmen einer Risikoanalyse ermittelt



**Abbildung 3.** Anbindung des ITSM auf operativer Ebene

werden. Die Dringlichkeit wird als Maß verwendet, bis zu dem die Verfügbarkeit und die Sicherheitsziele eines IT-Dienstes wieder erreicht werden müssen. Sollte es sich um einen Notfall handeln, beschreibt die Dringlichkeit die maximale Wiederanlaufzeit eines IT-Dienstes.

An das Security Management gibt das Incident Management Störungen der Informationssicherheit weiter. Dies sind Störungen, die eins der Schutzziele Funktionssicherheit, Informationssicherheit, Datensicherheit, Datenschutz, Vertraulichkeit, Integrität, Verfügbarkeit oder Zurechenbarkeit verletzen.

**Problem Management** Das Problem Management ist eine Fortsetzung des Incident Managements mit anderem Aufgabenbereich. Das Incident Management hat zum Ziel eine möglichst schnelle Wiederherstellung des betroffenen IT-Dienstes zu erreichen. Dazu gehört keine Analyse der Ursachen für die Störung (auch Root Cause Analysis). Diese Aufgabe nimmt das Problem Management wahr. Ziel des Problem Managements ist also eine umfassende Identifizierung und Ausschaltung der Ursachen einer Störung.

**Change Management** Die zentrale Instanz für die Verwaltung aller Änderungen der IT-Dienste ist das Change Management. Dabei ist die wichtigste Aufgabe des Change Managements, den Überblick über durchgeführte Änderungen nicht zu verlieren. Zentrale Eingabe für den Change Management Prozess

sind Requests for Change (RfC), die durch das Security Management geprüft werden müssen. Das Change Management kontrolliert alle Änderungen sowohl unter Kostenaspekten wie auch unter technischen Aspekten. Das Change Management steuert also direkt die Rollouts, die eine Änderung durchführen, sowie die Prozesse zur Qualitätssicherung. Ein Rollout ist die Einführung eines neuen oder geänderten Releases einer Software oder Hardware in die IT-Infrastruktur.

**Configuration Management** Das Configuration Management ist für die ganzheitliche Erfassung aller Konfigurationen aller Entitäten der IT zuständig. Die Configuration Items (CI) erfassen dabei nicht nur die Konfiguration der IT-Dienste und einzelnen Netzwerkkomponenten, sondern auch die zuständigen Administratoren. Die CIs werden in der zentralen Configuration Management Database (CMDB) verwaltet. Aufgabe des Configuration Managements ist auch, die CMDB auf einem aktuellen Stand zu halten, sodass die Datenbank immer die Realität repräsentiert. CIs werden nach bestimmten Kriterien klassifiziert, wie zum Beispiel hinsichtlich der notwendigen Vertraulichkeit oder der notwendigen Verfügbarkeit.

**Release Management** Das Release Management steuert die tatsächliche Umsetzung von Änderungen, die zuvor durch das Change Management genehmigt wurden. Die Eingabe für den Release Management Prozess ist also ein genehmigter RfC.

## 5 Fallstudie: Penetrationstest Prozess

Wie bereits in der Check-Phase des Security Management Prozesses beschrieben, bindet das IT Security Management nach ITIL auch externe Dienstleister für Audits und Sicherheitsprüfungen ein. Exemplarisch soll ein neuer Unterprozess des Security Managements entwickelt werden, der den Penetrationstest in das Security Management einbindet. Die beschriebenen externen Tests müssen manuell ausgelöst werden, bieten möglicherweise nicht die Informationsdichte wie vom Unternehmen gewünscht und sind während der Ausführung schwer beeinflussbar. Ein eigener Prozess bietet dagegen eine direkt Kommunikation mit den zuständigen Unternehmensstellen, kann aktuelle Entwicklungen der Sicherheitslage schneller mit einbeziehen und hat kürzere Durchlaufzeiten. Diese Vorteile sollen im Unternehmen genutzt und durch einen Prozess für das Penetrationstesting abgebildet werden.

*Ein Penetrationstest* ist die Überprüfung der Anfälligkeit eines Dienstes gegen Angriffe. Ein Dienst ist ein informationstechnisches System, das aus mehreren logischen Einheiten besteht und dessen Zweck die Erbringung einer eingrenzbar Leistung ist.

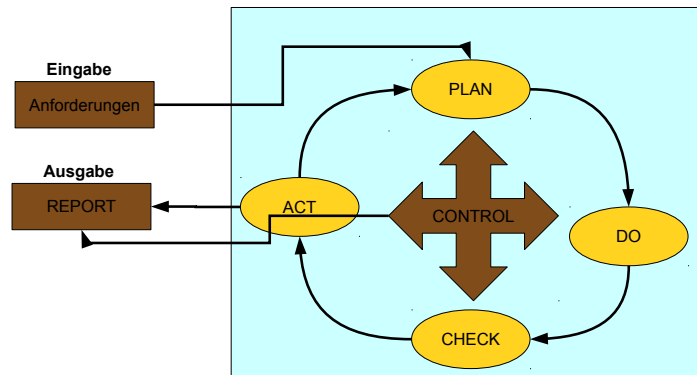


Abbildung 4. Penetrationstests als ITIL Prozess

## 5.1 Grundlagen

Dass Penetrationstests die Informationssicherheit von Unternehmen deutlich stärken können, da eine praktische Validierung der Sicherheitsmaßnahmen stattfindet, ist nicht abstreitbar [6]. Fraglich ist, wie die einzelnen Schritte eines Penetrationstests so in einen Unternehmensprozess eingebunden werden können, dass eine effiziente Abarbeitung möglich ist. Die Studie *Durchführungskonzept für Penetrationstests* [3] des BSI<sup>5</sup> gliedert den Penetrationstest in mehrere Phasen und definiert einzelne Tests. Dabei wird zwischen Informationsbeschaffung und Eindringversuchen unterschieden. Jedes Modul ist eigenständig bearbeitbar, vergleichbar zu den Modulen der Open Source Security Testing Methodology [4]. Dieser modulare Aufbau eignet sich gut, um ihn als Kernstück für den Penetrationstesting Prozess zu verwenden und in einen erweiterten Demingkreis einzubetten.

## 5.2 Prozess

Wie in Abbildung 4 dargestellt, wird der Demingkreis für den Penetrationstest lediglich um eine weitere Kante aus der Control-Phase in die Report-Phase erweitert<sup>6</sup>. Der Prozess bearbeitet einen Penetrationstest wie folgt.

<sup>5</sup> Bundesamt für Sicherheit in der Informationstechnik

<sup>6</sup> Verofunktion der Control-Phase, siehe Control-Phase.

*Anforderungen* sind Bedingungen an den Penetrationstest Prozess. Dazu gehören SLAs und OLAs, die im Rahmen des Tests nicht gebrochen werden dürfen. Außerdem ist die Datenschutzrichtlinie zu beachten. Es kann erforderlich sein, nicht auszulösende Notfallprozeduren zu definieren. Dies dient dem Zweck, mögliche Kosten durch Notfalldienste<sup>7</sup> abzuwenden. Die Anforderungen müssen dokumentiert werden.

*In der Plan-Phase* müssen die Kriterien, nach denen der Test durchgeführt wird, ausgewählt werden. Hier wird nach BSI-Studie [3] ein Maß für die sechs wichtigsten Kriterien festgelegt:

- Informationsbasis (*Wieviele Daten dürfen als bekannt angenommen werden?*)
- Aggressivität (*Welche Schäden sind akzeptabel?*)
- Umfang (*Welche Dienste werden geprüft?*)
- Vorgehensweise (*Wie erkennbar ist der Test?*)
- Technik (*Welche nicht-technischen Methoden werden angewendet?*)
- Ausgangspunkt (*Von wo wird getestet?*)

Dabei sind natürlich die rechtlichen Rahmenbedingungen zu beachten, insbesondere bei Diensten mit Underpinning Contracts, also externen Dienstleistern. Außerdem sind die ethischen Rahmenbedingungen zu beachten, um eine Beeinträchtigung des Arbeitsklimas durch zu aggressives Vorgehen zu vermeiden. In der Plan-Phase muss außerdem der Eskalationsweg zum Notfall Management definiert werden, um möglicherweise auftretende Systemfehler schnell lösen zu können. Es werden außerdem die konkreten Module[3] für den Penetrationstest ausgewählt.

*Die Do-Phase* führt den in der Plan-Phase definierten Penetrationstest aus und ist in drei Schritte unterteilt. Im ersten Schritt werden die Informationsbeschaffungsmodule ausgeführt. Im zweiten Schritt werden die gewonnen Erkenntnisse hinsichtlich Bedrohungen gegen das Unternehmen analysiert und entsprechend einer Risikoanalyse priorisiert. Daraufhin werden in der dritten Phase die Eindringversuche ausgeführt. Die Eingabe in die Module und deren Ausgabe muss ausführlich dokumentiert werden. Die BSI-Studie[3] liefert hierfür Vorlagen. Diese können an das Unternehmensumfeld angepasst, oder deren wichtige Aspekte in die vorhandenen Incident Reports eingebaut werden.

*In der Check-Phase* wird die Dokumentation aus der Do-Phase analysiert. Die Einzelergebnisse müssen kategorisiert werden in die Klassen Incident, Problem und Emergency. Aus diesen Ergebnissen muss der aktuelle Stand des Dienstes erarbeitet werden und die erfolgreichen Angriffspfade dokumentiert werden. Dies dient dem Zweck eine ganzheitliche Sicht auf den Zustand des Dienstes im Unternehmensumfeld zu gewinnen.

---

<sup>7</sup> Beispiel: Im Rahmen eines Penetrationstests soll kein Feuernotfall ausgelöst werden.

*Die Act-Phase* gibt die in der Check-Phase erstellten Incident-, Problem- und Emergency-Reports an die zuständigen Prozesse weiter.

*Die Control-Phase* hat während des kompletten Durchlaufs des Penetrationstest Prozess eine Vetofunktion und kann den Prozesslauf stoppen, wenn eine SLA oder OLA die in den Anforderungen nicht beschrieben wurde gefährdet wird. Außerdem kann so eine Rechtsverletzung verhindert werden, oder der Prozess gestoppt werden, sollte das Prozessziel nicht mehr ein Unternehmensziel sein. Diese Phase stellt den größten taktischen Vorteil gegenüber externen Penetrationstests dar, denn hier kann eine feingranulare Prozesssteuerung erfolgen. Außerdem können dringende Erkenntnisse direkt in die Report-Phase eingegeben werden.

*In der Report-Phase* werden die Ergebnisse aufbereitet und an die Unternehmensleitung vermittelt. Key Performance Indicators für den Penetrationstest Prozess sind die Anzahl der durchgeführten Tests, die Anzahl der erfolgreichen Tests (mit Kompromittierung), die Anzahl der gefundenen Schwachstellen und die Anzahl der behobenen Schwachstellen, die durch den Prozess aufgedeckt wurden.

### **5.3 Fazit**

Der exemplarisch im Rahmen der Fallstudie entwickelte Prozess kann direkt in das Security Management nach ITIL eingebunden werden und ist weitgehend nach ITIL konstruiert. Für eine konkrete Implementierung bleibt nur die Rollen zu definieren, das Berichtswesen an das Unternehmen anzupassen und geeignete Software für die einzelnen Module der Do-Phase festzulegen.

## Abbildungsverzeichnis

1	Der IT-Security Management Prozess . . . . .	V
2	Anbindung des ITSM auf taktischer Ebene . . . . .	VIII
3	Anbindung des ITSM auf operativer Ebene . . . . .	X
4	Penetrationstests als ITIL Prozess . . . . .	XII

## Literatur

1. Rob Addy. *Effective IT service management - to ITIL and beyond*. Springer, 2007.
2. J. Brunstein. *ITIL Security Management realisieren: It-service Security Management nach ITIL- so gehen sie vor*. Edition kes. Vieweg, 2006.
3. Bundesamt für Sicherheit in der Informationstechnik. *Studie: Durchführungskonzept für Penetrationstests*. BSI, 2003.
4. C.P. Herzog, R.E. Lee, R. Tucker, N. Hedges, C. Clark, A. Barisani, M. Ivaldi, R. Chiesa, K. Supporters, D. Lavigne, et al. *Osstmm 2.1.-the open source security testing methodology manual*. 2003.
5. Dr. Michael Meier. *Präventive sicherheit*. 2009.
6. E. Rey, M. Thumann, and D. Baier. *Mehr IT-Sicherheit durch Pen-Tests*. Vieweg+Teubner, 2005.