IT-SERVICEMANAGEMENT UND GESCHÄFTSPROZESSMANAGEMENT SICHERN DIE EFFIZIENZ VON CLOUD-SERVICES

Daniele Fiebig
IT Beratung
Papitzer Str.25 , D-04435 Schkeuditz, Deutschland
E-mail: daniele.fiebig@yahoo.de

Keywords:
ITIL, Security Management, Geschäftsprozesse, Geschäftsprozessvisualisierung, Cloud Computing

Abstrakt:
Um den sich immer schneller ändernden Geschäftsanforderungen gerecht werden zu können, müssen Unternehmen ihre Geschäftsprozesse und ihre Ressourcen flexibel anpassen können. Gleichzeitig sollte dies bei sinkenden oder gleich bleibenden Kosten umgesetzt werden. Abhilfe könnte im IT-Bereich die Nutzung von Cloud Computing Services bringen. Um die Potentiale von Cloud-Services wie z. B. hohe Flexibilität, Effizienz, Skalierbarkeit oder planbare Kosten nutzen zu können, müssen die Cloud-Angebote zu den Geschäftsprozessen des Unternehmens passen. Eine möglichst hohe Passgenauigkeit der Cloud-Services wird nur erreicht, wenn die Unterstützung der Kernprozesse und die durchgängige Bereitstellung ausgereifter IT-Service-Management-Prozesse gewährleistet sind.
Die Anwendung und Kombination neuer Technologien zur Automatisierung von IT-Prozessen und ihres Customizings können helfen, die Effizienz von IT-Services in der Cloud zu erhöhen. Um ihren Nutzen für die Unternehmenssicherheit zu optimieren, müssen die Security-Prozesse ebenfalls auf den neuesten Technologien beruhen. Die Verantwortung für den Datenschutz obliegt dem Cloud-Anwenderunternehmen als Auftraggeber. IT-Sicherheit ist eine Managementaufgabe, die nicht ausschließlich von den technischen Möglichkeiten sondern ebenso vom Sicherheitsbewußtsein, von der Prozessbeherrschung und vom Sicherheitsbudget abhängt. In diesem Kontext werden die Auswirkungen die Industrialisierung der IT auf das Service Management und hier besonders auf das IT Security Management untersucht werden. Betrachtet werden die zusätzlichen Risiken für die IT-Sicherheit in der Cloud. Welche Veränderungen ergeben sich für das Service Management und die Service Management Prozesse durch Cloud Computing? Welche Technologien können zeitgemäße Services sichern? Wie kann eine integrierte Sicherheitsinfrastruktur erstellt werden?

Inhalt

Geschäftsprozessmanagement

„Nur was ich kenne, kann ich ändern.“ Unternehmen verfügen oft nicht über eine durchgängige Dokumentation ihrer Geschäftsprozesse und sind so nicht in der Lage, angemessen auf Änderungen zu reagieren. Gemäß der Studie der Fa. PwC schätzten 2011 nur ca. 27% der befragten Firmen ein, dass ihr Geschäftsprozessmanagement weit oder sehr weit entwickelt ist und entscheidend zu Erhöhung der Flexibilität und Entscheidungssicherheit beiträgt. [Müller - PwC, 2011]
Ausgangsbasis für transparente Steuerungssysteme kann neben dem Businessplan die Prozesslandkarte sein.

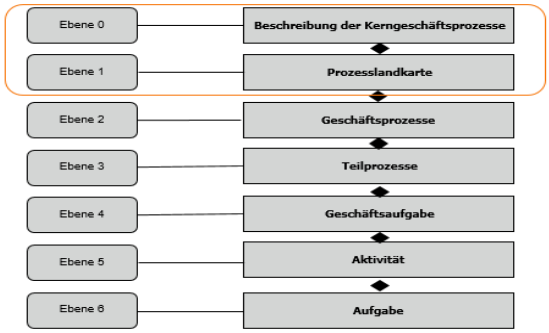

Abbildung 1: Abstraktionsgrade der Prozessarchitektur

Geschäftsprozessmanagement ist kein Projekt, sondern ein Konzept der permanenten Organisationsgestaltung und -veränderung.
Unter Geschäftsprozess wird eine Folge von Aktivitäten verstanden, die in einem logischen Zusammenhang stehen, inhaltlich abgeschlossen sind und unter Zuhilfenahme von Ressourcen und eingehenden Informationen durch Menschen und/oder Maschinen auf ein Unternehmensziel hin ausgeführt werden. [Schmelzer, 2006]
Eine Geschäftsprozessvisualisierung erleichtert das Verständnis für die Prozesse im Unternehmen. Die Unternehmenslandkarte gibt einen Überblick über alle Prozesse. Dabei lassen sich im Bezug zum Geschäftsmodell drei Prozesstypen erkennen. Die **Kernprozesse** sind wertschöpfende Prozesse in Bezug

auf das Geschäftsmodell. Die **Führungsprozesse** beinhalten alle planenden und steuernden Geschäftsprozesse. Während die Aufgabe der **Unterstützungsprozesse** in der Bereitstellung von Infrastruktur, Informationen, Sachmitteln, Ressourcen und Materialien besteht. Sie sind die wertsichernden Prozesse.
Während die Prozesslandkarte häufig unstrukturiert und graphisch frei gestaltet wird, werden die Prozessabläufe in verschiedenen Notationen einheitlich und standardisiert dargestellt. Häufig verwendete Notationen sind die ereignisgesteuerte Prozesskette (EPK), die Business Process Model and Notation (BPMN 2.0), die Business Process Execution Language (BPEL) oder die Unified Markup Language (UML). Ergänzt werden die graphischen Modelle i.d.R. durch tabellarische Darstellung, Prozess-Datenblätter, Prozesslisten, Tätigkeitslisten oder Aufgabenblätter. [copargo, 2010].

Prozess-Datenblatt: <*Bezeichnung des Prozesses*>

1. Allgemein/organisatorische Prozessbeschreibung

Zweck und Ziel: <*Kurzdarstellung*>

Einordnung: Kern- ( ) Führungs- ( ) Unterstützungs- (x) Prozess

Kritikalität: Normal (x) Kritisch ( ) sehr kritisch ( )

Daten:

IT-Komponenten:

IT-Services:

Abhängigkeiten: *z. B. Patch-Management*

2. Risikobetrachtung

Datenklassifikation: Gering ( ) Normal (x) Kritisch ( ) sehr kritisch ( )

Mögliche Bedrohungen:

Schwachstellen:

3. Messgrößen / KPIs

KPI	Beschreibung	Datenherkunft
Security-Incidents	*Anzahl der Sicherheits-Vorkommnisse*	*z. b. Incident-Management*
Lösungs-zeiten	*Zeiten bis zur Entdeckung, zur Reaktion und zur Behebung*	*z. b. Incident-Management*
Patch-zeiten	*Zeit vom Verfügbarkeit von Patchen bis zum Ausrollen*	*z. B. Change-Management*
Angriffe	*Anzahl der Angriffe von Außen: (z. b. Viren, Malware, DoS, ...)*	*z. b. Firewall-log*
Audits	*Anzahl der Autdits pro Jahr*	
Penetrations-test	*Anzahl der durchgeführten Penetrationstests*	
...	...	

Abbildung 2: Beispiel Prozess-Datenblatt

Die Geschäftsprozessvisualisierung schafft Transparenz und Verständnis für Abhängigkeiten und Zusammenhänge. Die graphischen Geschäftsprozessmodelle unterstützen die Identifizierung und Definition der Geschäftsprozesse aus strategischer und organisatorischer Sicht und sind die Basis für flexible, zeitnahe Änderungen.
IuK-Systeme zur Geschäftsprozessmodellierung können zur Integration, Synchronisierung, Beschleunigung und Qualitätssteigerung der Geschäftsprozesse beitragen. Die Tools unterstützen

- die Verwendung vorgefertigter Elemente,
- einheitliche Benennungen,
- Übertragbarkeit der Modelle und
- Simulationen.

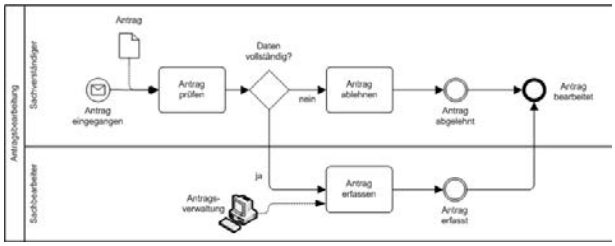

Abbildung 3: Beispiel BPMN2.0

Sie sind Datenbank- und xml-basiert, verfügen über Workflow engines für den Bereich der Prozessumsetzung und Analysetools zur Simulation und Qualitätssicherung. Weiterhin unterstützen sie das Laufzeitmanagement (Task- und Eventmanagement) sowie das Prozesscontrolling. Die Unternehmen können aus einer Vielzahl an BPM-Tools mit unterschiedlichen Funktionsschwerpunkten wählen. [Frauenhofer, 2013]
Grundsätzlich bleibt auch bei Nutzung eines BPM-Tools das Ziel die Erhöhung der Transparenz, deshalb müssen Methoden und Werkzeuge nach den Anforderungen des Unternehmens und den Nutzergruppen ausgewählt werden. Bei Toolnutzung muss das Umfeld und die vorhandene Infrastruktur beachtet werden. Leistungsfähige Schnittstellen zum Datenex- und Import integrieren die BPM-Modelle in die Management-Infrastruktur eines Unternehmens.

Grundlagen des IT-Servicemanagements (ITSM)

Das Hauptziel des ITSM besteht in der Lieferung von qualitativ hochwertigen und durchgehenden IT-Services, die sich an den Erfordernissen des Geschäftsprozesses orientieren. Um die Qualität der IT-Services zu steigern wurde in den 80ziger Jahren im Auftrag der britischen Regierung die Information Technology Infrastructure Library™ (ITIL) entwickelt. ITIL beschreibt Prozesse, Verfahren und Aufgaben innerhalb von IT-Organisationen. ITIL wird ständig verbessert und der jetzt aktuelle Standard ist ITIL V3. Der ITIL V3 Lifecycle beschreibt Prozesse aus fünf zentralen Service-Bereichen – der Service Strategie (Service Strategy), dem Servicedesign (Service Design), der Serviceüberführung (Service Transition), dem Servicebetrieb (Service Operation) und der kontinuierlichen Serviceverbesserung (Continual Service Improvement). Er stellt alle Prozesse zur Verfügung, die für einen effizienten IT-Betrieb erforderlich sind, welcher die Kerngeschäftsprozesse und derer Änderungen unterstützt. [Van Bon, 2004]

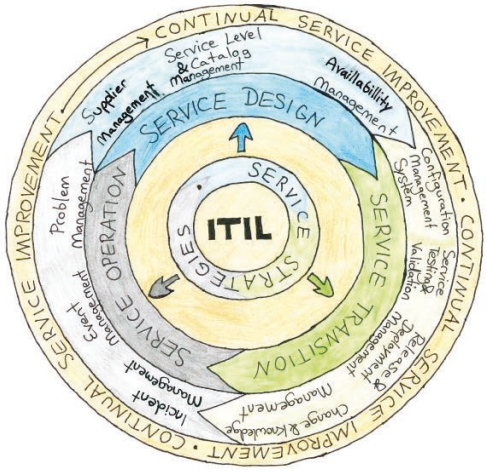

Abbildung 4 ITIL v3 Lifecycle

Unternehmen, die IT Servicemanagement eingeführt und die ITIL-Prozesse implementiert haben, verfügen über eine solide und flexible Servicebasis. Sie kennen ihre Prozesse und steuern sie bewusst. Die zunehmende Komplexität der IT-Infrastrukturen und Anwendungen generiert immer neue Prozesse und es bedarf neuer Lösungen beim Management und dem Schutz dieser Prozesse. Unternehmen entscheiden sich deshalb immer öfter für die Implementierung von Lösungen zur Automatisierung von IT-Prozessen. Workflow-Management-Systeme (WFMS) sind IT-Systeme zur Entwicklung (Modellierungskomponente), zur Ausführung und Steuerung (Laufzeitkomponente) und zur Überwachung (Monitorkomponente) von Prozessen nach spezifischen Vorgaben. Sie können zur Visualisierung, Dokumentation, Editierung, Steuerung und Überwachung von Geschäfts- und IT-Prozessen eingesetzt werden.

Produkte zur Prozessautomatisierung verfügen über Funktionen wie z. B. Inventarisierung, Compliance-Prüfung, Prozessvisualisierung, Ressourcenmanagement, Prozessumsetzung und –überwachung, Prozessanpassung, Reporting und verschiedene Analysemöglichkeiten (was wäre wenn, Simulation, ...). Für den Einsatz intelligenter Automatisierungstools ist es wichtig, dass die einzelnen Prozesse vollständig aufeinander abgestimmt sind. [Kergassner, 2013]

Im Service Desk oder in Self Service-Portalen finden sich besonders viele Beispiele für gelungene Prozessautomatisierungen. Aber auch Sicherheitsservices und –prozesse lassen sich teilweise automatisieren.

Security Management

Von besonderer Bedeutung für die Unternehmen sind heute die Sicherung der Unternehmens- und Kundendaten sowie eine sichere Servicebereitstellung.

Das Security Management gehört wie das Risikomanagement und das Service Continuity Management im Rahmen des ITIL Modells zum Service Design. Ziel aller drei Prozesse ist die Sicherheit und die Aufrechterhaltung der Geschäftsprozesse. Sie beeinflussen permanent alle geschäftlichen Aktivitäten. Die Sicherheitsregeln wie in der IT-Sicherheitsrichtlinie oder der Cloud-Policy von Unternehmen formuliert, basieren auf den Ergebnissen des Risikomanagements sowie den Auswertungen von Systemlogfiles z. B. der Firewall, die aktuelle Angriffe dokumentieren. Viele Unternehmen versuchen, Prozesse im Security Management zu automatisieren, um zeitnah und standardisiert auf Vorkommnisse reagieren zu können.

Produkte für die IT-Prozessautomatisierung ermöglichen zeitnahe, automatisierte Reaktionen auf Systemmeldungen und Vorfälle. Durch integrierte Knowledgebases oder komplexe Analysetools unterstützen sie durch passgenaue Meldung, mit Reports und Dokumentationen die Steuerung und Entscheidungsfindung. Sie liefern Informationen, die für die Diagnose, Behebung und Korrektur von Fehlern oder die Beseitigung von Schwachstellen benötigt werden. Gerade im Sicherheitsbereich spielt die Reaktionsfähigkeit und - geschwindigkeit eine bedeutende Rolle.

Die Diversität der Angriffe auf Unternehmensdaten ist hoch. Sie zu erkennen, erfordert neben dem Einsatz aktueller Security-Techniken auch die Sammlung und Auswertung der verschiedensten Systemlogfiles. Die Überwachung von Systemalarmen ist mit vielen Abhängigkeiten behaftet. Neben der Auswertung von Logfiles sind logische Entscheidungen z. B. mit Hilfe von Expertensystemen zu treffen, um adäquate Reaktionen zu starten.

Mit den neuen Möglichkeiten von Automatisierungslösungen und selbstlernenden Systemen können Prozesse optimiert und Mitarbeiter entlastet werden.

Cloud Computing

Das Cloud Computing eröffnet Chancen, wirft aber viele neue Fragen im Bereich IT-Sicherheit auf.

Die Unternehmen können derzeit aus einer wachsenden Zahl von Cloud-basierten IT-Services wählen. Diese lassen sich in Klassen zusammenfassen.

Bei Software as a Service (SaaS) wird Software als integrierte Dienstleistung netzbasiert über die Cloud bereitgestellt.

Bei Platform as a Service (PaaS) werden neben Software auch Infrastrukturressourcen genutzt

Bei Infrastructure as a Service (IaaS) ersetzt die Cloud die IT-Basis-Infrastruktur des Nutzers.

Die jüngeren Cloud Services sind Business Process as a Service (BpaaS) und Security as a Service (SecaaS).

Bei Bpaas erfolgt die inhaltliche Durchführung von Geschäftsprozessen in der Cloud. SecaaS verlagert Sicherheitsprozesse in die Cloud.

Neue Technologien wie das Cloud-Computing, die zunehmende Verbreitung mobiler Endgeräte und die Vielfalt der IP-basierten oder busgesteuerten Devices verändern die Programmierung und Nutzung von

Geschäftsanwendungen sowie die Datenspeicherung nachhaltig.
Die Anbieter von Entwicklungs-Plattformen müssen neue und sichere Lösungen bereitstellen, um den Anforderungen ihrer Kunden an neue Services gerecht werden zu können. Dies beinhaltet eine hohe Flexibilität bei Kunden und Cloud-Providern.

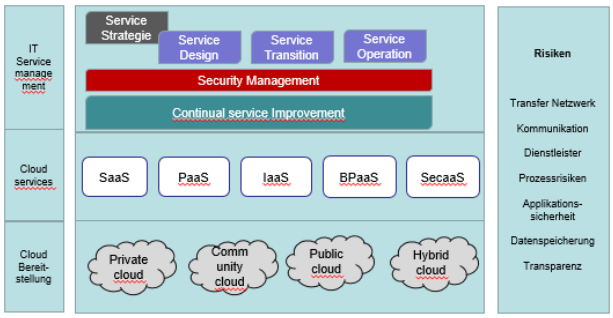

Abbildung 5 - Cloud Umgebungen und Risiken

Die Geschäftsprozesse und die IT-Services werden durch neue Technologien wie das Cloud Computing komplexer. Die Transparenz sinkt und die Steuerbarkeit erfordert zunehmend mehr Aufmerksamkeit. Damit besteht die Gefahr, dass Flexibilität und Sicherheit für die Unternehmen nicht im erwarteten Masse steigt.
Im Folgenden sollen die Auswirkungen des Cloud Computing auf Prozesse und Risiken im Bereich IT-Sicherheit untersucht werden.

Security Management in der Cloud
Cloud Computing bietet den Unternehmen viele Möglichkeiten wie z. B. die Nutzung skalierbarer Rechnerleistung, Software-Anwendungen oder Infrastrukturen ohne eigene Vorhaltung von Ressourcen. Das ermöglicht Flexibilität und Standardisierungseffekte. Des Weiteren können bei sachgerechter Planung Kostenvorteile ("Pay per Use" – nutzungsabhängige Zahlmodelle) genutzt werden.
Im Rahmen der Servicestrategie müssen jedoch zusätzliche Festlegungen zu Serviceprozessen in der Cloud getroffen werden. Aufgrund von gesetzlichen und Compliance-Anforderungen im Bereich IT-Sicherheit müssen die Sicherheits-Richtlinien für das Cloud Computing völlig neu konzipiert werden. Compliance umfasst dabei die Überstimmung mit Reglungen zur IT-Sicherheit und zum Datenschutz, die unternehmensspezifisch sind bzw. von Branchenverbänden als Standards eingeführt wurden. Ein Beispiel dafür ist der Payment Card Industry Data Security Standard (PCI DSS), den alle Unternehmen einhalten müssen, die Zahlungsvorgänge mittels Kreditkarten über ihre IT-Systeme abwickeln. Eine unternehmensspezifische Compliance-Vorgabe könnte sein, dass alle Endgeräte das Betriebssystem Windows 8.1 mit dem aktuellsten Patchlevel und als Endpointsecurity-Tool McAfee mit dem aktuellsten Patternfile installiert haben müssen, bevor sie sich im Unternehmensnetzwerk anmelden dürfen. Leistungsfähige Compliance-Tools können die Compliance vor Anmeldung prüfen und erforderliche Patches und Pattern automatisch installieren und erst danach den Client am Netzwerk anmelden.
Die Cloud Computing-Nutzung erfordert besonders die Ergänzung von Vorgaben für das Security Management, für das Business Continuity Management und für das Risikomanagement in der Cloud-Computing-Richtlinie (Policy).
In Cloud-Verträgen muss unter anderem definiert werden, wer welche Aufgaben übernimmt und welche Kompetenzen und Prozesse für einen sicheren IT-Betrieb benötigt werden. Dies ist besonders für das Unternehmen wichtig, welches Prozesse in die Cloud verlagert, da die Verantwortung für IT-Sicherheit und Datenschutz bei der Unternehmensleitung verbleibt und nicht auf den Cloud-Provider verlagert werden kann.
Mit diesen Trends verschiebt sich die Rolle der IT-Abteilungen immer mehr hin zum Manager von IT-Services und zum Verwalter von Sicherheits-Richtlinien. Vor diesem Hintergrund muss der Passgenauigkeit von IT Servicemanagementprozessen besondere Beachtung geschenkt werden.

Security Risiken
Die ständig steigenden Datenmengen in Clouds und die globale Datenhaltung sind Gründe dafür, dass Unternehmen mehr Transparenz und Kontrolle benötigen. Der Schutz von Unternehmensdaten kann geschäftsentscheidend sein.
Mit der wachsenden Zahl an Cloud-Angeboten und der zunehmenden Bedrohung durch Cyberkriminalität müssen sich Unternehmen zwangsläufig mit Cloud-spezifischen Risiken auseinander setzen. Diese variieren bei den verschiedenen Service-Modellen. Die Gewährleistung von Sicherheit, Kontrolle und Transparenz sind nur einige der Herausforderungen des Cloud Computing. Im Folgenden sollen die derzeit signifikanten Risiken zusammengestellt werden. Im Rahmen des Risikomanagements müssen Unternehmen die Gefährdungslage je Risiko regelmäßig neu bewerten. Die Risikoanalyse beinhaltet im Allgemeinen die Bereiche „Organisatorische Sicherheit“, „Wirtschaftliche Sicherheit“, „Juristische Sicherheit“ und die „Technische Sicherheit“. [Fiebig, 2014]

Technische / Rechenzentrums-Sicherheit
▪ Redundanzen wichtiger Komponenten ▪ Redundantes Rechenzentrum ▪ Schutz gegen Stromausfall, Feuer, Wasser, … ▪ stets aktuelle IT-Sicherheitsarchitektur (Firewall, Virenscanner, URL-/Content-Filter, NAC, Malware-schutz, SPAM-Filter….) ▪ Identity-/Access-Management (IAM) ▪ Verschlüsselung und Schlüsselmanagement ▪ Serversicherheit, Applikationssicherheit ▪ Netzsicherheit und Web-Sicherheit

▪ Datensicherheit inkl. Storage u. Archivierung ▪ Virtualisierung ▪ Frameworks und Tools für das Cloud-Management und für das Reporting ▪ Monitoring und IT-Service-Management ▪ Log-Management ▪ Patch Management ▪ Speicher-/Verarbeitungsort der Daten
Organisatorische Sicherheit
▪ IT-Sicherheits-Richtlinie und regelmäßige Audits ▪ Risiko-Management u. Schutzbedarfsanalyse ▪ Daten-Klassifizierung ▪ Datensicherungskonzepte ▪ Regelmäßige Schulung (Awareness) des Personals ▪ Zutritts- und Zugangs-Schutz ▪ Aufgabentrennung ▪ IT-Service Management Prozesse ▪ IT-Sicherheits-Management-System (ITSM) ▪ Notfall- und Katastrophenplan ▪ Business-Continuity-Management ▪ SLAs und vertragliche Regelungen mit Partnern und Dienstleistern ▪ mehrstufiges Kontrollsystem für die Providersicherheit (Wahrung der Kontroll-pflicht) ▪ Penetrationstest und Sicherheitsrevisionen
Wirtschaftliche Sicherheit
▪ Risikobewertung und –behandlung ▪ Restrisiko-Versicherung ▪ Wirtschaftlichkeitsbetrachtung ▪ Finanzrahmen für IT-Sicherheit u. die IT-Sicherheits-Organisation ▪ Finanzplanung des Unternehmens
Juristische Sicherheit
▪ Feststellung der straf- und zivilrechtliche Haftung ▪ Regelmäßige Prüfung der gesetzlichen u. branchenspezifischen Vorschriften durch Cloud-Nutzer oder unabhängige Organisationen ▪ Sicherung der Vertraulichkeit personen-bezogener Daten ▪ Meldepflichten u. Regelungen zur Umsetzung ▪ Vertraulichkeits- und Betriebsvereinbarung ▪ Festlegung von Zuständigkeiten und Verantwortlichkeiten ▪ Festlegung von Service Level Agreements (SLA) ▪ Vertraulichkeitsvereinbarungen, Versicherungen und Knowhow-Nachweise ▪ Einhaltung landesspezifischer Vorschriften durch Provider und Cloud-Nutzer ▪ Vertragsgestaltung und –Überprüfung (Transparenz) ▪ Compliance (Übereinstimmung mit Vorgaben)

Abbildung 6 - Tabelle der techn., wirt., org. u. jur. Sicherheit

Die Sicherheitsziele Verfügbarkeit, Vertraulichkeit, Integrität und Zurechenbarkeit (Authentizität) müssen in Cloud Umgebungen genauso erreicht werden wie in unternehmenseigenen Rechenzentren.
Global müssen für das Cloud Computing die Risikobereiche der Datenübertragung, der Datenspeicherung und der Zugriffssicherheit (Authentifikation und Autorisation) betrachtet werden. Dazu kommen die Risiken, die in jedem Geschäft mit Dritten, Partnern und Dienstleistern entstehen.

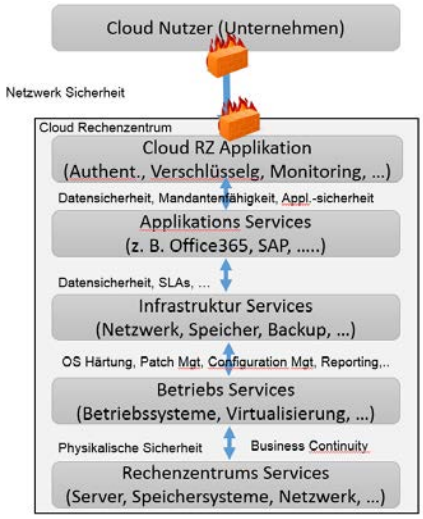

Abbildung 7 - Sicherheitsstufen in Cloud Umgebungen

Netzwerk-/Datentransfer-Sicherheit

Mehr Datenaustausch über Netze und Komponenten von Drittanbietern eröffnet mehr Angriffsmöglichkeiten. Typische Angriffe sind beispielsweise „Man in the middle“ (MITM), Port scans, Packet sniffing, IP spoofing, Ausnutzung der Schwachstellen von Netzwerkkomponenten oder unsicherer Konfigurationen (Standard-Konfiguration/-Passwörter, kurze Passwörter, Gruppenpasswörter) u. a.
Allgemein muss das Risiko von Datenabflüssen (data loss) oder Manipulation durch Verschlüsselung und sichere Protokolle wie Secure Socket Layer (SSL), Transport Layer Security (TSL) oder die Nutzung von Virtual Private Networks (VPN – dedizierte Leitungen) gemindert werden.

Datensicherheit

Im Bereich der Datensicherheit müssen die unternehmenseigenen Sicherheitsrichtlinien auf die Cloud Infrastruktur übertragen bzw. erweitert werden. Ebenso muss die Frage der Datenhoheit vertraglich fixiert werden. Unternehmensdaten sollten ausschließlich in verschlüsselter Form in der Cloud liegen. Eine Schwachstelle stellen Administratoren dar - sowohl eigene als auch die des Providers. Personen mit höherer Berechtigung können unbemerkt Daten kopieren oder manipulieren. Dazu kommen Schwachstellen der Systeme, die Angriffe z. B. mittels Cross-Site Scripting (XSS), SQL-Injection, Cross-Site Request Forgery

(CSRF) oder Cookie Manipulationen zulassen. Weitere Risiken entstehen durch schwache Zugangskontrollen oder unsichere Systeme (älteres Betriebssystem, nicht gepatcht, schwaches Regelwerk, …).

Datenintegrität

Die Datenintegrität ist durch die Nutzung von Cloud- bzw. Webservices permanent gefährdet. Webservices verfügen kaum über Transaktionssicherheitsmechanismen. Die Datenlieferung wird nicht garantiert. Fehlende oder umgeleitete Pakete werden nicht erkannt (http-Protokoll). Das bedeutet, dass die Netzwerksicherheit und die Webservice-Sicherheit durch zusätzliche Komponenten hergestellt werden muss wie z. B. Web Application Firewall (WAF).
Andere Risiken sind die Mandantenfähigkeit und Insider-Informationen (z. B. Zugangsdaten und Strukturinformationen) mit denen z. B. durch kleine Parameteränderungen in Anfragen oder in Applikationen ein Unbefugter Zugriff auf Daten erlangen kann.

Authentifizierung und Autorisierung

Die Benutzeridentitäten-, -rechte- und –rollenverwaltung stellt eine besondere Herausforderung dar. Die Entscheidung für die Realisierung on-premesis, in der Cloud oder in Beiden hat jeweils unterschiedliche Vor- und Nachteile und birgt unterschiedliche Risiken. In jedem Fall muss sichergestellt sein, dass nicht evtl. Personal des Providers Zugriff auf Anmeldedaten haben könnte. Unternehmen, welche schon über eine Passwort-Policy verfügen, müssen die Vorgaben für die Authentifizierung in der Cloud-Umgebung ergänzen. Sicherzustellen ist in jedem Fall, dass Anmeldeinformationen ausschließlich verschlüsselt übertragen und abgelegt werden.

Virtualisierung

Die Virtualisierung und der Hypervisor sind Basiskomponenten für Cloud Infrastrukturen. Wie andere Softwarekomponenten weisen sie u. U. Schwachstellen auf. Schlechte Konfigurationen durch das Provider-Personal können ebenfalls Risiken darstellen. Administratoren, die Zugang zum Hypervisor-Management (z. B. virtual maschine monitor) haben, haben Zugriff auf die gesamten Datenbestand der Mandanten.

Backup

Die Datensicherungen von Daten in der Cloud müssen den Backup&Recovery-Regeln des Cloud-Nutzers entsprechen und durch den Provider umgesetzt werden. Dies muss vertraglich in SLAs fixiert sein. Auch für Backups gilt, die strikte Mandantentrennung und die permanente Verschlüsselung der Daten muss in allen Schritten gesichert sein.

Verfügbarkeit

Die Verfügbarkeit der Cloud Infrastruktur und der Datenanbindung kann nur noch vertraglich fixiert werden. Dieser Kontrollverlust muss durch den Cloud-Nutzer sowohl beim Risikomanagement als auch im Business Continuity Plan (BCM) und im Notfallplan berücksichtigt werden.
Besonders im Web-Server-Bereich müssen Massnahmen gegen Denail of Service-Angriffe (DoS) ergriffen werden.

Prozessfähigkeit

Die Passfähigkeit aller IT-Servicemanagement-Prozesse ist eine Voraussetzung für die Cloud-Nutzung. Sowohl auf Nutzer- als auch auf Provider-Seite müssen für alle Services Prozesse existieren (Service Portfolio). Ein Nachweis dafür wäre z. B. eine Zertifizierung nach ISO20000 (IT Service Management) oder ISO27001 (IT Sicherheits Management System). Wichtiger als eine Rechenzentrums-Zertifizierung ist jedoch der Test, ob die Zusammenarbeit auf der operationalen Ebene klappt beispielsweise im Incidentfall (Incident-Management). Nachweise und ggf. Tests sind zu führen, darüber, dass der Provider einzelne Daten bzw. gesamte Datenbestände aus der Cloud entfernen kann (wichtig für die Datenhoheit und das Recht auf Vergessen).

Übertragbarkeit

Für die Übertragung von Cloud-Datenbeständen oder ganzen Cloud-Umgebungen (virtuellen Maschinen) auf einen anderen Provider oder ins unternehmenseigene Rechenzentrum existieren verschiedene Technologien. Diese sind abhängig von der Virtualisierung und u. U. von der Rechenzentrums-Infrastruktur (z. B. Backup der gesamten VM, Vmotion, Docker). Die Abhängigkeit vom gewählten Provider ist derzeit noch sehr groß. Die Art und Weise einer Vertragsbeendigung muss vertraglich geregelt sein.

Risikomanagement-Prozess

Die vorangegangen Untersuchungen haben gezeigt, dass für das Cloud Computing eine umfassende Risikoanalyse erforderlich ist.
Aufgrund der sich wandelnden Bedrohungen ist diese regelmäßig zu wiederholen. Sinnvoll ist der Vergleich verschiedener Deployment-Varianten.

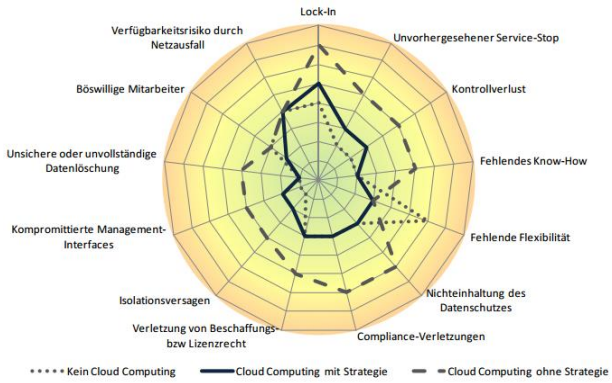

Abbildung 8 - Beispiel Risikoprofil [Schweizer Behörden, 2012]

Das Risikomanagement ist ein ITIL-Prozess. D. h. auch hier ist die Dokumentation, Visualisierung und Automatisierung von Teilaufgaben sinnvoll, um kurzfristig aktuelle Risikozustände ermitteln zu können.

Risikomassnahmen

Die Risikoanalyse zeigt für die unterschiedlichen Risiken unterschiedlich hohe Eintrittswahrscheinlichkeiten und zu erwartende Schadenswerte. Dies erleichtert die Entscheidung für neue Sicherheitsmassnahmen.

Unternehmen finden Hinweise zur Cloud Sicherheit z. B. beim BSI, der Cloud Security Alliance (CSA) oder der Open Group mit dem Open Trusted Technology Provider Standard (O-TTPS; www.opengroup.org) [BSI, 2014, Bedrohungs- und Risikoanalyse …]

Allgemein lassen sich verschieden wiederkehrende Sicherheitslösungen und Prozesse in den Unternehmen finden. Diese sind meist unabhängig voneinander.

Datentransfer
▪ sicherer und verschlüsselter Dateitransfer zum Austausch von Informationen über Internet, LAN oder WAN (ebenso für High-Drive, Foren, social network) ▪ Einsatz leistungsfähiger Datenaustauschprotokolle, Verschlüsselung, Zertifikate, Überwachung von Prüfsummen ▪ VPN (dedizierte Leitung)
Authentisierung
▪ Elektronische Identifikation von Personen mit Passwort, Token und Smartcard (LAN, WLAN, Intranet) ▪ Log-Management ▪ Passwortregel, Identity Access Management (IAM), Zertifikate ▪ Mehrfach-Authentifizierung (Username und Passwort allein sind nicht ausreichend!)
Perimeter /Content gateway security
▪ Sicherheit direkt am Gateway. Bedrohliche Inhalte werden am Perimeter abfangen. Schutz vor Viren, Spyware, Hacker Angriffen etc. ▪ Schutz des Netzwerks vor Eindringlingen und Malware ▪ Remote-Verbindung für mobile Mitarbeiter ▪ Überprüfung des Datenstroms vor Eintritt ins Unternehmensnetz nach diversen Regeln u. Richtlinien ▪ Antivirensoftware, Applikationskontrolle und Sandbox-Test
Firewall / Web Application Firewall (WAF) Applikations-Kontrolle
▪ Firewall-Konzept und Applikationskontrolle zusätzlich zur herkömmlichen Portkontrolle ▪ Firewall überwacht u. beschränkt Datenverkehr gegen unerlaubte Zugriffe u. unbefugte Applikationsnutzung ▪ Filtertechniken und signaturbasierte Lösungen für Anti-Virus u. Anti-Malware, gegen Würmer, Trojaner und Backdoors
Intrusion Detection / Intrusion Prevention
▪ Abschwächung von Angriffen in Echtzeit durch Forensik, interner Netzwerkschutz, ▪ Überwachung von internen Datenströmen, Ports und ggf. Userverhalten
Endpoint
▪ Schutz vor Viren, Spyware, Hacker-Angriffen, Durchsetzung konsistenter Richtlinien für PC, Laptop, externe Speicher, Smartphone ▪ Client-Schutz durch Antiviren-Software, Regelwerke, Rechteverwaltung ▪ Prozesse für Hardware- o. Datenträger-Verlust
LAYER 2, Network Access Control (NAC)
▪ Vollständige Zugangskontrolle über das eigene Netzwerk und Schutz vor Attacken durch fremde, unautorisierte Geräte ▪ Überwachung der internen Ports
Datensicherheit / Verschlüsselung
▪ Gewährleistung der Geheimhaltung von Daten auf PCs und mobilen Geräten ▪ Verschlüsselungssoftware, Zertifikate für Server, Storage, Archive, Cloud-Infrastruktur ▪ Technische Richtlinie BSI-TR-02102 u. ff. ▪ Providerunabhängige Verschlüsselung und Schlüsselservices nutzen
Web- und Datenbank-Sicherheit
▪ Schutz von Web-Anwendungen, SQL-Injection, Spoofing, Ausspähen von Kundendatenbanken ▪ WEB-Applikation-Firewall ▪ Überwachung des gesamten ein- und ausgehenden HTTP-Verkehr
Monitoring, Reporting, Auditing, Change Management
▪ Zentrale Richtlinienkonfiguration, Überwachung, Protokollierung und Analyse, Change Management und Backup ▪ Logging u. Log-Auswertung, gezielte Überwachung von Userverhalten, Datenverkehr, Netzwerk-Anomalien ▪ Session Management, Event-Management

PROXY
▪ dienen als Firewall und Inhaltsfilter für sicheren und effizienten Datenaustausch in der Regel für bestimmt Netzsegmente mit Web-, Content- sowie URL-Filter ▪ Proxy zur Kommunikationsüberwachung Protokoll-/Portebene, URL- und Content-Filter
E-Mail Security
▪ Sicherung und Sicherheit der digitalen Kommunikation gegen Veränderung, Ausspähen und Umleiten. Anti-Virus, Anti-Spam, ▪ E-Mail Verschlüsselung ▪ Mail-Security-Appliance oder Mail-Security – Software als fester Teil der Mail-Lösung mit Verschlüsselung oder Zertifikat und Logging
Tests und Audits
▪ Schwachstellen- und Penetrationstest ▪ Interne und externe Sicherheits-Audits ▪ Monitoring, und Reporting

Abbildung 9 - Elemente der Security-Infrastruktur

Im Cloud Computing spielen besonders die Risiken eine Rolle, die in Beziehung mit Partnern und Lieferanten entstehen d. h. in der Aufgabenverteilung zwischen Kunde und Providern. Diese müssen durch klare vertragliche Regelungen, in SLAs und durch abgestimmte Service-Prozesse minimiert werden. Der Schutz vor Datenverlusten (DLP - data loss protection) kann überlebenswichtig für Unternehmen sein.

Systemlogging

Entsprechend der Spezifik der Unternehmen besteht die IT-Security-Infrastruktur aus unterschiedlichen Komponenten (einer Kombination aus Appliances und Software). Diese Systeme agieren häufig weitgehend unabhängig voneinander. Sie erzeugen Logfiles und Reports mit wichtigen Informationen für die IT-Sicherheit.

Logfiles von Firewall, Netzwerk-Management Analysen, Session- und Event-Management etc. liefern Informationen über alle Aktivitäten im Gesamtsystem wie z. B. Angriffe, Sessions, Ressourcenbelastung, Lastverteilung und das Nutzerverhalten.

Eine gemeinsame Datenbasis für Logdaten (Syslog-Server für die Logfiles aller Management-Systeme) eröffnet die Möglichkeit für unterschiedlichste Analysen und Reports.

Monitoringsysteme erfassen laufend Systemzustände und Ist-Werte (technische und operative KPIs) die als Vergleich mit vorgegebenen Parametern dienen können.

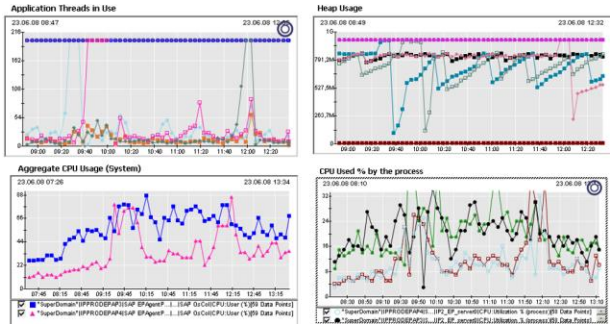

Abbildung 10- Reports verschiedener Überwachungsdaten

Die Logfile-Datenbank liefert die Informationen für einen Soll-Ist-Vergleich. Grundlage ist jedoch die sinnvolle Aufbereitung der Daten und die Erstellung von Templates oder Websites zur Darstellung der Ergebnisse. Eine große Anzahl an Daten erhöht nicht unbedingt die Transparenz und die Sicherheit. Grundsatz muss sein, nur erforderliche und aussagekräftige Werte einzubeziehen und die Reports Zielgruppen gerecht vorzubereiten.

Um ein aussagekräftiges Protokoll zu erstellen, müssen häufig mehrere Logfiles und verschiedene Systemzustände korreliert werden wie z. B. Netzlast, Sessions, CPU-Last, Datenbank-Requests etc.

Messbarkeit von IT-Sicherheit

IT-Sicherheit ist ein Querschnittsbereich und somit tangiert sie viele Geschäftsprozesse. Zur zielgerichteten Steuerung und kontinuierlichen Optimierung der IT-Sicherheit sind adäquate Kennzahlen und Key-Performance Indikatoren (KPI) notwendig.

Hier greift der Grundsatz: *„Was nicht gemessen wird, kann nicht zielgerichtet optimiert werden!“*

Eine zentrale Frage bei der Effizienz von Sicherheitssystemen ist die Messbarkeit ihrer Parameter. Prozess-Parameter oder KPIs sind quantifizierbare Kennzahlen, die der Leistungsmessung und Steuerung dienen. Sie ermöglichen die Einleitung von Reaktionen auf bestimmte Werte oder die Ableitung von bestimmten Massnahmen. KPIs müssen „SMART“ sein. Das bedeutet, dass sie **S**ustainable (nachhaltig), **M**easurable (messbar), **A**chievable (erreichbar), **R**easonable (nachvollziehbar und aussagekräftig) und **T**imely (zeitabhängig und terminierbar) sein müssen. Daraus folgt, dass nicht alle Parameter, die ein Prozess oder Service liefern kann, zur Steuerung und Optimierung einsetzbar sind.

Ausschlaggebend für die Wirksamkeit eines Monitor- und Kennzahlensystems ist die Konzentration auf unternehmensspezifische und prozessrelevante Kenngrößen. [TENABLE, 2014]

KPIs für die IT-Sicherheit sind unternehmensspezifisch. Ausgangsbasis für die Festlegung von KPIs für Sicherheitsprozesse sind Unternehmensvorgaben sowie eine Analyse der vorhandenen Managementtools und der Logfiles, die die unterschiedlichen Sicherheits-

Komponenten schreiben. Des Weiteren sind ggf. die im Einsatz befindlichen Test- und Analysetools nutzbar.
Eine manuelle Erfassung der Daten für Sicherheits-Reports ist aufgrund der Vielzahl verschiedener Komponenten aufwändig und zeitintensiv und damit personalintensiv und langsam.
KPIs lassen entsprechend ihrer Verwendung in Business KPIs (z. B. Durchlaufzeit, IT-Kosten, IT-Anteil an Produktkosten), Service KPIs (SLA-Einhaltung, Time-to-Repair, Response-time, Update-/Patch-Time, Verfügbarkeiten), IT-Prozess und Projekt KPIs (z. B. Anzahl Changes, Anzahl Patches, Umsetzungsdauer von Prozessänderungen) sowie operative IT-KPIs (Auslastung Server, Datenvolumen, Antwortzeiten, Dauer von Ver-/Entschlüsselungsvorgängen) einteilen.
Beispiele für IT-Sicherheits-KPIs könnten sein:

- Anzahl der durchgeführten Sicherheitsaudits- und –tests
- Anzahl von IT-Sicherheits-Trainings
- Aktualität der Antiviren-Software/-Scanner
- Dauer von der Identifikation einer Bedrohung bis zur Implementierung einer geeigneten Gegenmaßnahme
- Dauer von der Veröffentlichung von Patches bis zur Installation im Unternehmen bzw. beim Provider
- Dauer von Produktionsunterbrechungen aufgrund von IT-Sicherheits-Problemen
- Anzahl von Sicherheitsmaßnahmen oder neuen Technologien, die zur Verringerung von identifizierte Bedrohungen implementiert worden sind

Bei der Definition von KPIs muss Klarheit darüber herrschen, was von den vorhandenen Sicherheits-prozessen erwartet wird und was mit der eingesetzten Technologie erreichbar ist.
Nicht alle KPIs sind zur Steuerung und Qualitäts-verbesserung einsetzbar. Deshalb sollten für Reports wenige aber aussagekräftige Werte gewählt werden, um den Aufwand für Ermittlung der KPIs und die Reporterstellung zu verringern. Ziel muss es auch sein, dass Reports im Bedarfsfall kurzfristig, automatisiert erzeugt werden können.
Im Rahmen des Risikomanagements müssen für die gewählten KPIs Sollwerte definiert werden.
KPIs müssen vor der Einführung getestet werden, um festzustellen, wie gut die definierten Ziele erreicht und ob die KPIs Ergebnisse mit der benötigten Aussagekraft liefern.
Im Laufe der Zeit erfolgen besonders im Bereich der KPIs und ihrer Sollwerte häufige Anpassungen.
Einige Unternehmen verfügen über ein IT Sicherheits Management System (ISMS) gemäß ISO/IEC27001. Damit ist in diesen Unternehmen die Transparenz bzgl. der IT-Sicherheitsprozesse, der genutzten Sicherheits-Technologien und der Security-KPIs am größten.
Während im Bereich der Prozessvisualisierung und –automatisierung sehr viele Informationsquellen vorliegen, ist im Bereich der Kenngrößen für die IT-Sicherheit ein Entwicklungsbedarf zu verzeichnen. Eine Informationsquelle ist jedoch die Webseite www.itil.org.

Sicherheitslösungen und neue Technologien

So wie im Entwicklungs- und Projektmanagementbereich mit DevOps und Continuous Delivery [Birk, 2014] müssen im Security Bereich neue Technologien und Prozesse entwickelt und angewendet werden, damit die neuen Technologien wie das Cloud Computing zur Chance und nicht zum Risiko für die Unternehmen werden.

Integrierte Sicherheits-Prozesse

Ziel von integrierten Sicherheits-Prozessen ist die Nutzung der vorhandenen Daten, ihre Aggregation und Verknüpfung zur ganzheitlichen Steuerung und Optimierung der IT-Sicherheit (Prozesse, Parameter, evtl. Technologien).
Die Planung von **Integrierten Sicherheits-Prozessen** für die Optimierung der betrieblichen und der Cloud-IT-Sicherheit umfasst:
1. die Erfassung und Visualisierung aller Prozesse, die Einfluss auf IT-Sicherheitsentscheidungen haben,
2. die Feststellung aller Informationsquellen, die sicher-heitsrelevante Daten für den Soll-Ist-Vergleich liefern können
3. Zusammenfassung aller sicherheitsrelevanten Informa-tionen für das Risikomanagement
4. Feststellung des aktuellen Sicherheitsstatus und des evtl. vorhandenen Handlungsbedarfes
5. Konzeption der erforderlichen Prozesse und Analysen für eine automatisierte Zusammenstellung aller Daten und des Sicherheitsstatus
6. Erarbeitung möglicher Rückkopplungen für eine Übertragung der Ergebnisse aus dem Sicherheitsstatus in die aktuelle Sicherheitsinfrastruktur (organisatorisch, technisch, prozessorientiert)

Im **Schritt 1** (*Visualisierung*) erfolgten die Erarbeitung aller schematischen Übersichten (Prozesslandkarte) und die Prozessvisualisierung aller relevanten Prozesse und Abläufe.

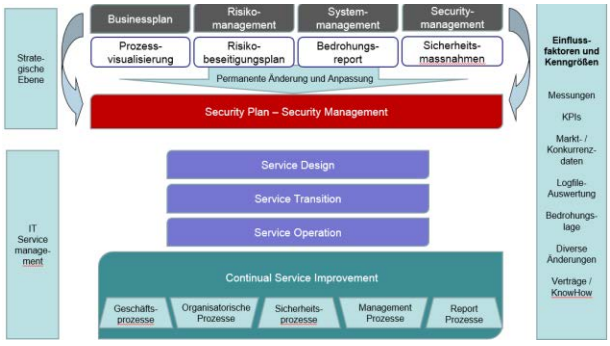

Abbildung 11 – Abhängigkeiten der Steuerungsebenen

Es werden so Abhängigkeiten, Funktionsüberschneidungen und Kommunikationsfehler aufgedeckt. Die Prozessvisualisierung muss mit einem BPMN-Tool erfolgen, damit sichergestellt ist, dass die Prozesse bei Bedarf schnell und unkompliziert editiert werden können und die Einflüsse einer Änderung auf andere Prozesse ersichtlich werden. Je nach eingesetzten Tool sind Simulationen oder Tests möglich.

Sicherheitsrelevante Daten werden im **Schritt 2** *(Messbarkeit und Auswertung)* ermittelt. Ausgehend von den Vorgaben in der IT-Sicherheitsrichtlinie, in der Cloud-Richtlinie und ggf. in Verträgen oder SLAs sowie in gesetzlichen Vorgaben werden alle schon fixierten und messbaren Soll-Werte ermittelt. Aber auch „weiche" und subjektive Bedingungen werden erfasst. Des Weiteren werden alle aktuell eingesetzten Sicherheitslösungen auf ihre Funktionen und Ausgaben (Logs, Reports, etc.) untersucht. Es werden alle erfassbaren oder ermittelbaren Werte hinsichtlich eines möglichen Soll-Ist-Vergleiches analysiert, welcher die Feststellung des Erreichungsgrades der Sicherheitsziele ermöglicht.
Bisher nicht genutzte Daten oder fehlende Analysen und Auswertungen können ergänzt werden.
Die Auswertungen der Logfiles von Firewall und anderen Sicherheitskomponenten liefert beispielweise Hinweise zu Angriffen, zu Transfervolumina, zu genutzten Protokollen sowie zum Nutzerverhalten. Sofern nicht schon ein zentraler Syslog-Server betrieben wird, erfolgt die Konzeption einer zentralen Logfile-Erfassung und die Auswahl der Daten für die Datenbank, welche für die Sicherheitsanalyse genutzt wird. Vorteil der zentralen Logfileerfassung ist, dass kurzfristig neue Werte aus den Logfiles für neue Analysen extrahiert werden können.
Weiterhin dient dieser Schritt zu Festlegung neuer Sollwerte und ihrer Messmethoden. Die Ergänzung neuer Auswertungen und die bessere Ausnutzung von Report- und Analysefunktionen vorhandener Tools wie z. B. Netzwerk-Management, Event-Manager, u. s. w. für aktuelle Fragestellungen bzgl. Sicherheit und Bedrohungen gehören ebenfalls in diesen Schritt.
Ausgehend von Prozess-Datenblättern wird eine Matrix erstellt welche die KPIs je Prozess oder Service enthält. Sie ist Teil des Risikomanagements.

Prozess / Security KPI		Prozess 1	Prozess 2	Prozess 3	Prozess 4	Prozess n	Prozess m
KPI	Soll-Wert				Patch-Mgt		
KPI 1							
KPI 2							
Rollout Time	RT max 4h						
Rollout Durchsatz	100%						
KPI 3							
KPI 4							
KPI 5							
KPI 6							
KPI 7							
KPI 8							
KPI 9							
KPI n							

hohes Risiko bei Nichterreichen
mittleres Risiko bei Nichterreichen
normales Risiko bei Nichterreichen

Abbildung 12: KPI-Matrix

Die Matrix ermöglicht die Zusammenstellung aller wichtiger KPIs der Sicherheitsprozesse und ihrer Soll-Werte sowie die Priorisierung der KPIs.

Im Schritt 3 *(Risikomanagement - innere und äußere Risiken)* wird der Risikomanagement-Prozess optimiert. Hierzu werden die Prozesse, die zur Erstellung der Risikoanalyse benötigt werden, dokumentiert und visualisiert. Die erforderlichen Erfassungsmasken und Reports werden als Templates generiert. Wichtig ist, dass eine Transparenz hergestellt wird, die klare Aussagen über die Risiken und den aktuellen Sicherheitsstatus ermöglichen. Sie sind die Grundlage für die Management-Einordnung der Risiken in tragbare bis nicht akzeptable Risiken. Auf ihrer Basis werden Managemententscheidungen bezüglich der Minimierung von Risiken oder des Umganges mit Restrisiken getroffen.
Beachtet wird dabei, dass das Risikomanagement nicht ausschließlich für IT-Risiken sondern unternehmensweit erfolgen muss. Eine Integration in den unternehmensweiten Risikomanagementprozess ist unabdingbar.

Schritt 4 *(Sicherheitsstatus)* Alle neuen Daten werden in der darauf folgenden **Risikoanalyse** verarbeitet und bewertet. Ergebnis ist der Sicherheitsstatus.
Die Risikoanalyse und der Sicherheitsstatus müssen es dem Management ermöglichen, die richtigen Optimierungsmassnahmen für die IT-Sicherheit zu bestimmen und zu priorisieren.

Schritt 5 *(Automatisierung)* dient zur Realisierung der **Automatisierung** und Wiederholbarkeit aller vorangegangenen Schritte. Um eine Vergleichbarkeit verschiedener Sicherheitsstati zu erreichen und ggf. Verbesserungen sichtbar zu machen, ist es Ziel dies Schrittes, den Prozess soweit zu automatisieren, dass Sicherheitsstati zu beliebigen Zeitpunkten möglichst kurzfristig erstellt werden können.
Dazu wird für die Systemsteuerung ein integriertes Systemmanagement konzipiert. Die Prozessdokumentationen werden zentral bereitgestellt. Die Datenbank für alle verwendeten KPIs und ihre Soll-Werte wird erstellt und die erforderlichen Schnittstellen für alle Datenimporte implementiert.
Des Weiteren werden die Logfiles aller Sicherheitsmanagementsysteme in einer Datenbank erfasst als Basis für die Auswertung und Analyse bzw. eine Schnittstelle zum vorhandenen Syslog-Server erstellt. Somit kann ein Soll-Ist-Abgleich mit den festgelegten Soll-Werten für die IT-Sicherheit erfolgen.
Umfang und Inhalt des Soll-Ist-Vergleiches und der Reports für den Sicherheitsstatus müssen festgelegt werden. Dieser Schritt ist stark vom Unternehmen und den gegebenen Sicherheitsvorgaben und –Technologien abhängig!

Ziel des Konzeptes ist es, die Steuerbarkeit der Sicherheits-Prozesse zu optimieren und damit Verbesserungsprozesse zu unterstützen.

Schritt 6 *(Verbesserung und Optimierung)* beinhaltet die Ergebnisverwertung der Risikoanalyse. Aufgaben und Maßnahmen für eine Verbesserung der IT-Sicherheit können in allen Bereichen des Unternehmens liegen.
Bezogen auf die IT-Sicherheit in der Cloud liegt das Optimierungspotential hauptsächlich in Sicherheitssystemen wie z. B. Firewall und ihrer Konfiguration, in Technologien zur Authentisierung, Verschlüsselung und der Nutzung von Zertifikaten. Hier lassen sich ggf. Automatismen erarbeiten, die eine schnelle Reaktion ermöglichen (z. B. Passwortänderungen, Update-Services, etc.).
Im Prozessbereich ist es sinnvoll, alle Prozessänderungen zu dokumentieren und zu visualisieren. Die erfolgt in der zentralen Prozessablage. Stets aktuelle Prozessdokumentationen erleichtern den Vergleich mit dem Serviceportfolio von Providern bzw. die Verhandlung, wenn seitens Provider Anpassungen im Bereich der IT-Service-Prozesse erforderlich sind.
Zu den häufig erforderlichen Massnahmen gehören auch Einführungs- und Awareness-Schulungen zum Umgang mit Cloud-Services. Auch hier empfehlen sich wiederholbare, editierbare und dokumentierbare Prozesse und Schulungsabläufe.

PDCA-Prozess

Die vorangegangen Schritte ermöglichen die Wiederholung der automatisierten Sicherheitsanalyse und schaffen somit die Voraussetzungen für den *Kontinuierlichen Verbesserungsprozess*. Der auch als Deming Cycle beschriebene Prozess ermöglicht auf Basis einer stetigen Wiederholung der Schritte PLAN-DO-CHECK-ACT eine kontinuierliche Verbesserung.

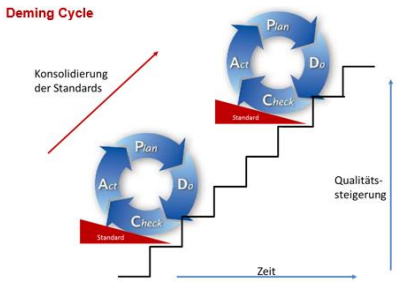

Abbildung 13 - PDCA-Prozess

Nur wenn später die in der Implementierung durchlaufenen Prozesse zur Ermittlung des Sicherheitsstatus wiederholt werden können, ist das Ziel erreicht und die Grundlagen für eine kontinuierliche Optimierung der IT-Sicherheit wurden geschaffen. Dazu müssen möglichst viele Schritte automatisiert und die Ergebnisse in vorgefertigte Templates und Reports integriert werden.

Umsetzung

Die Planung und Einführung integrierter Sicherheits-prozesse ist ein Projekt, welches das Commitment und die Mitarbeit der Geschäftsleitung erfordert, da IT-Sicherheit eine zentrale Leitungsaufgabe ist.
Von besonderer Bedeutung ist, dass die Voraussetzungen und das Ziel von Sicherheitsprozessen klar definiert und mit messbaren Soll-Werten untersetzt wird.

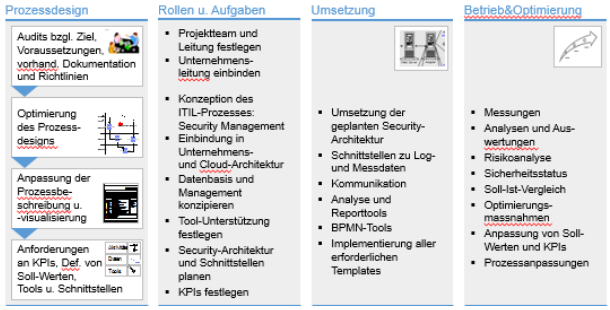

Abbildung 14 - Vorgehen zur organisatorischen und prozessualen Optimierung der Security-Prozesse

Mit der Inbetriebnahme einer Plattform zur integrierten IT-Sicherheit wird der Sicherheits-Prozess gestartet, welcher dauerhaft auf eine kontinuierliche Verbesserung gerichtet ist.
Die Verbesserung betrifft dabei alle Bereiche wie z. B. Organisation, Einzelprozesse aber auch Technologien und Komponenten für IT-Sicherheit.

Integrierte Sicherheitssysteme sind modular aufgebaut. Einzelne Module oder Services können ausgetauscht oder verändert werden.

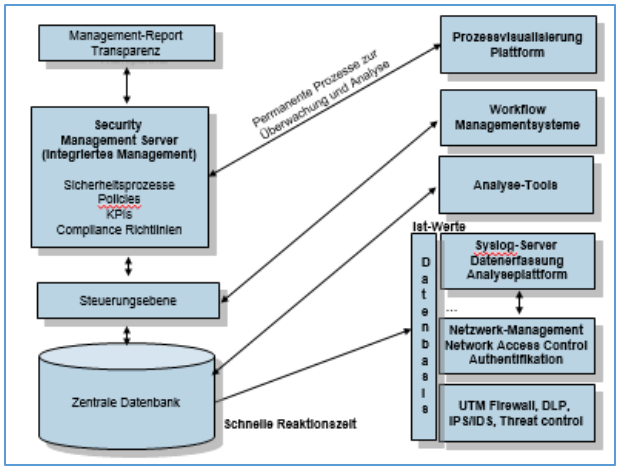

Abbildung 15 - Systemschema für integriertes Sicherheits-management

Komponenten für ein integriertes Sicherheits-management sind:

- Plattform für die Prozessdokumentation und – visualisierung sowie die zentrale Prozess-datenbasis
- zentrale Logfile-Ablage
- Management für KPIs und Policies
- Datenbank für Soll- und Ist-Werte

- Steuerungsebene
- Schnittstellen
- Analyse- und Reporting-Tools

In Anhängigkeit von der zu schützenden Infrastruktur werden zum Aufbau des integrierten Sicherheits-managements unterschiedliche Tools und Komponenten eingesetzt. Wichtig ist die Integration in die vorhandene Systemlandschaft.

Bedeutung integrierter Sicherheits-Prozesse

Die Erfahrungen aus Projekten und Workshops belegen, dass Unternehmen die Vorteile einer integrierten, prozessbasierten Sicherheits-Architektur nutzen wollen oder dies zukünftig planen. Neben der bestehenden Verantwortung für die IT-Sicherheit werden als Gründe die zukünftigen Aufgaben im Rahmen der EU-Daten-schutz-Grundverordnung, des PCI DSS 3.0, des HIPAA (Health Insurance Portability and Accountability Act) oder bevorstehende Zertifizierungen gemäß ISO27001 genannt.

Als Vorteile von integrierten Sicherheits-Prozessen sehen die Unternehmen:

- Erhöhung der Transparenz über Security-Massnahmen und Daten
- Synchronisation von Sicherheitsprozessen
- Synchronisation von Business- und Sicherheitsprozessen
- Strukturierung und Prozessorientierung
- Kapselung von Funktionalitäten
- Kontrolle der heterogenen Sicherheits-Infrastrukturen und Prozesse
- Nachvollziehbarkeit, Prüfbarkeit
- Automatisierung und Wiederholbarkeit
- Umfassende Datennutzung für Entscheidungen
- Qualitätssicherung
- Compliance-Überwachung und Einhaltung gesetzlicher Vorgaben
- Dokumentation
- Mitarbeiter-Awareness

Trotz Zunahme der Bedrohungen und der Schäden durch Cyberkriminelle ist für Unternehmen die Situation aufgrund von globalen Verflechtungen und landes-spezifischen Gesetzeslagen unübersichtlich.

Trotzdem zeichnet sich heute schon ab, dass Unternehmen mit einer wachsenden Zahl an Providern zusammenarbeiten. Deren Steuerung erfordert die Einführung klarer und standardisierter Prozesse sowie eine Angleichung der Prozesskriterien und der Leistungsvereinbarungen (SLAs).

Fazit

Grundsätzlich besteht in den Unternehmen der Bedarf nach effizienteren und effektiveren Prozessen.

Die Ausgangslage für die Planung und Implementierung integrierter Sicherheits-Prozesse ist von Unternehmen zu Unternehmen sehr unterschiedlich.

Während einige Unternehmen noch nicht prozess-orientiert arbeiteten, konnte bei anderen auf IT Service Management-Prozesse aufgesetzt werden. Ähnlich verhielt es sich mit IT-Sicherheits- und Cloud-Richtlinien, die teilweise nicht vorhanden waren.

Eine schwierige Teilaufgabe war die Festlegung von Soll-Werten für die IT-Sicherheit. Dies ist zum einen in unterschiedlicher Ausstattung mit IT-Sicherheitskom-ponenten und Managementtools als auch in fehlenden Knowhow im Bereich Definition und Handling von KPIs zu suchen.

Die Konzeption der integrierten Sicherheit umfasst auch die Auswahl der Hardware und der erforderlichen Toolunterstützung (Datenbanken, BPMN-Software, diverse Analysetools, Risikomanagement-Systeme, …). Hier war es besonders schwierig, die Sicherheits-Architektur in die vorhandene Management-Umgebung zu integrieren bzw. offene Schnittstellen für die spätere Integration weiterer Services zu schaffen.

Häufig ist die Zusammenarbeit von Fachbereichen und Administratoren erforderlich, so dass unterschiedliche Interessen kombiniert werden müssen. Nur die konsequente Führung durch die Geschäftsleitung ermöglicht die Umsetzung effizienter und zukunfts-fähiger Lösungen.

Ebenfalls eine Aufgabe der Unternehmensleitung ist die Ausstattung der IT-Sicherheitsabteilung mit entsprechen-dem Personal (Anzahl und Ausbildung).

Die Umsetzung aller ITIL-Prozesse ist nicht die Voraussetzung für die Implementierung von integrierten Sicherheits-Prozessen und der erforderliche Architektur. In serviceorientierten Organisationen ist jedoch die Planung und Einführung erheblich leichter und die Projektlaufzeiten für die Umsetzung sind erheblich kürzer.

Zukünftig bleibt im Bereich der IT-Sicherheit und der IT-Sicherheitsprozesse ein erheblicher Entwicklungsbedarf. Dieser umfasst beispielsweise:

- die Entwicklung von Prozess-Templates für allgemeingültige Sicherheits-Prozesse
- die Entwicklung und Dokumentation von KPIs im Bereich IT-Sicherheit
- die Integration der KPIs in Templates für eine Prozessmatrix als Grundlage für die Risiko-analyse
- Vorgehensmodelle zur Definition von KPIs
- Modell einer integrierten Sicherheits-Archi-tektur

Allgemein hat sich im Laufe der Projekte gezeigt, dass die Einarbeitung in neue Technologien und ihre operative Nutzung in Unternehmen oft „zu“ lange dauert.

Die Einführung einer durchgängigen Sicherheitslösung und die Messung des Sicherheitsstatus kennzeichnen ein funktionierendes Security Level Management und tragen

zur Qualitätssicherung für die IT-Sicherheit bei. Jedoch kann auch ein professionelles Security Level Management nicht für eine lückenlose IT-Sicherheit garantieren. Durch die geschaffene Transparenz lassen sich jedoch Restrisiko und evtl. offene Sicherheitsmassnahmen schneller erkennen und beheben.

Literatur:

Schmelzer, H. J.; Sesselmann, W., 2006 „Geschäftsprozessmanagement in der Praxis - Kunden zufrieden stellen, Produktivität steigern, Wert erhöhen.“ Hanser Verlag München

Müller, Th., 2011, „Zukunftsthema Geschäftsprozessmanagement“, PricewaterhouseCoopers AG (PwC)

van Bon, J., 2004 „IT Service Management, eine Einführung basierend auf ITIL“ Van Haren Publishing/ IT Service Management Forum®

Richter-von Hagen/Stucky, 2004 „Business-Process- und Work#ow-Management.“ B.G. Teubner Verlag

Schmelzer, H. J.; Sesselmann, W., 2006 „Geschäftsprozessmanagement in der Praxis - Kunden zufrieden stellen, Produktivität steigern, Wert erhöhen.“ Hanser Verlag München

Copargo 2010 „BPMN2.0“ 2010 http://www.copargo.de/

Fraunhofer-Institut für Experimentelles Software Engineering IESE,2013, "BPM Suites 2013" http://www.iese.fraunhofer.de/content/dam/iese/de/dokumente/oeffentliche_studien/Fraunhofer_IESE_Studie_BPM-Suites2013.pdf

Brunnstein, J.; 2006 „ITIL Security Management realisieren“ Vieweg&Sohn Verlag Berlin

Kergassner, R., 2013 „Software für die Prozessautomatisierung“, http://www.it-director.de/home/a/automatisierung-als-allheilmittel.html

Subashini S., Kavitha, V., 2011 „A survey on security issues in the service delivery models of Cloud computing“ Journal of Network and Computer Applications

Birk A., Lukas Ch., 2014 „Eine Einführung in Continuous Delivery, Teil 1: Grundlagen“ http://www.heise.de/developer/artikel/Eine-Einfuehrung-in-Continuous-Delivery-Teil-1-Grundlagen-2176380.html

BITKOM, 2010, „Prozesse und KPI für Rechenzentren“, Bundesverband Informationswirtschaft, Telekommunikation und neue Medien e. V., Berlin

Humble J., Farley D., 2010 „Continuous Delivery: Reliable Software Releases through Build, Test, and Deployment Automation“, Addison-Wesley Professional

Fiebig, D., Karlstetter, F.,2014 „Risikoanalyse mit speziellen Cloud-Risiken“, IT Business, Vogel Verlag

CSA 2011, „Security Guidance V3“ https://Cloudsecurityalliance.org/research/security-guidance/

BSI, 2014,”Bedrohungs- und Risikoanalyse für das SaaS CRM Modell” Teil 2: Bedrohungs- und Risikoanalyse für das SaaS CRM Modell, https://www.bsi.bund.de/DE/Themen/CloudComputing/Sicherheitsprofile/sicherheitsprofil_saas_node.html

Dischl, J., 2012 „Risikoanalyse Cloud-Computing Schweizer Behörden“ http://www.isb.admin.ch/themen/strategien/01603/index.html?lang=de&download=NHzLpZeg7t,lnp6I0NTU042l2Z6ln1acy4Zn4Z2qZpnO2Yuq2Z6gpJCEeYF3e2ym162epYbg2c_JjKbNoKSn6A--&t=.pdf

TENABLE network security, 2014 „Falsche Kennzahlen schaffen Scheinsicherheit in der IT“, STUDIEN, TENABLE

DANIELE FIEBIG studierte Anlagenbau an der Ingenieurhochschule Köthen und promovierte 1990 über Checkroutinen in der rechnergestützten Anlagenprojektierung. Von 1990 bis 1991 arbeitete sie im Rechenzentrum der Isotopen und Strahlenforschung. Seit 1992 ist sie selbständig als IT-Beraterin und Projektleiterin tätig.

Tätigkeitsschwerpunkte sind die Konzeption von IT-Infrastrukturen, Softwareentwicklung, IT-Sicherheit und Geschäftsprozessoptimierung besonders das IT Service Management (ITIL). Ihre Email Adresse lautet daniele.fiebig@yahoo.de.