VO 184.706 - 2018W
Network Engineering
Fragenkatalog ausgearbeitet

25. Januar 2019

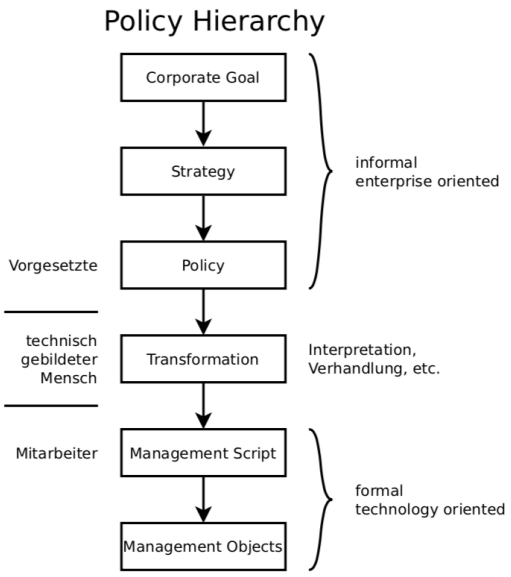
1 Welches Corporate Goal ist für mich das Ziel? Wo will ich arbeiten?

- Corporate Goal: Vision/Mission des Unternehmens
- Strategien: Langzeit-Pläne um das Corporate Goal zu erreichen
- Policy: Unternehmensrichtlinien
- Transformation: führt informale Beschreibungen in formale Anleitungen über. Informale Beschreibungen sind problematisch. Transformation ist Aufgabe des Netzmanagers und erfordert Verhandlungen und Rücksprache nach oben, was wie gemeint ist.
- Management Script: wie ein Kochbuch, sehr detailliert
- Management Objects: Ressourcen (zB Switches, Kabel, Drucker). Wird gemanaged durch Management Scripts.

2 Was ist der Unterschied zwischen Corporate Goal, Strategie und Policy?

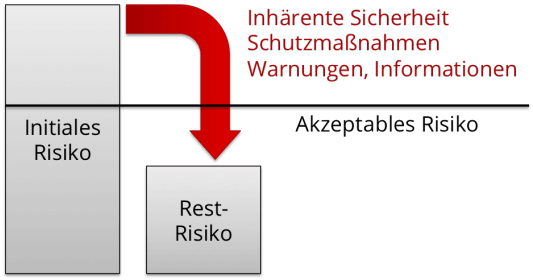
- Corporate Goal: Vision/Mission des Unternehmens z.B. Lehre und Forschung für TU oder Erhaltung der Infrastruktur für die Stadtregierung. Alle Ziele müssen dem Corporate Goal untergeordnet werden.
- Corporate Strategie:
- Corporate Policy: Richtlinien, die festlegen wie ein Unternehmen operiert. Sie regeln das Verhalten von Mitarbeitern, erstellen Verfahren und legen Einschränkungen fest. Alle Entscheidungen und Aktionen finden innerhalb der festgelegten Grenzen statt.

3 Was ist eine Policy Hierarchie?



4 Wie wird Restrisiko definiert?

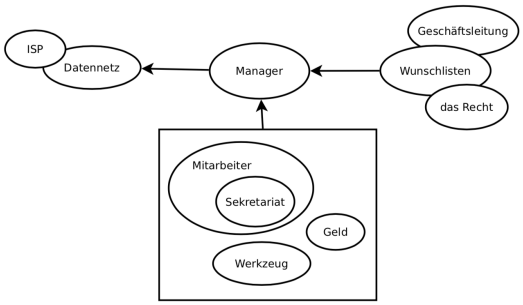
- EN ISO 12100: "Risiko, das verbleibt, nachdem Schutzmassnahmen getroffen wurden".
- Bestandteile: Abschätzbarer und unbekannter Teil.
- Gefahren eines Systems trotz durchgeführter Maßnahmen zur Minderung eines Risikos (akzeptiert).



5 Was unterscheidet Managementressourcen von gewöhnlichen Ressourcen?

- Managementressourcen (Rechteck): Ressourcen, die der Manager benötigt, um seine Aufgabe zu erledigen z.B. Personal, Monitoring
- Gewöhnliche Ressourcen (Nutzer Ressourcen): haben einen direkten Nutzen für den Betrieb, werden daher weniger hinterfragt z.B. Router, kann suggestiv genutzt werden

  Ressource und Repräsentation sollten deckungsgleich sein, aber Kennwerte evtl irreführend, monitoring intensivieren bei Zustandsänderung, hilft Messungenauigkeiten auszugleichen



6 Wie ist mit einem Fehlalarm umzugehen?

- Jemand, der einen Fehler macht/Fehlalarm auslöst darf nicht sanktioniert werden
- Alarme sollten immer ernst genommen und nicht ignoriert werden.

7 Wie sicher ist unsere Welt mit IoT?

- Schlechtes Patch-Management
- Default-Passwörter die nie geändert werden (zB Mirai Botnet)
- Praktisch keine vorhandene Firewall / Securitykonzept
- Geräte hängen frei zugänglich im WWW (zB Hofer Webcams)

8 Welche Bereiche eines Netzwerkmanagers existieren?

- Compliance
- Performance
- Security
- Fault Management (unten)
- Accounting ("Wieviele Ressourcen werden verbraucht?")
- Monitoring (unten)

9 Was sagt die Miller'sche Zahl aus?

- Ein Mensch kann gleichzeitig nur 7 ± 2 Informationseinheiten (Chunks) im Kurzzeitgedächtnis präsent halten
- Größe des Kurzzeitged. ist genetisch festgelegt
- zB schlechtes UI überladen mit Information

10 Ursache von Ausfälle (Störung, etc)

- Störung: System verhält sich *innen* nicht nach Spezifikation z.B. degraded RAID
- Ausfall: System verhält sich *außen* nicht nach Spezifikation z.B. nicht verfügbares RAID

Beispiele:

- Hardwareausfälle z.B. Materialermüdung
- Softwareprobleme z.B. Kompatibilitätsprobleme
- Stromausfall
- Fehlbedienung: kann verhindert werden z.B. unterschiedliche Gewindedurchmesser für direktionales Ventil oder unterschiedliche Größen beim Tanken Benzin/Diesel
- Sicherheit: physisch z.B. Gerätediebstahl oder Software z.B. Hacker-Angriff

11 In welcher Hierarchieebene arbeitet ein Kommunikations- oder IT-Manager?

- Im Stab direkt unter der Geschäftsleitung (CEO)
- Niedriges oder mittleres Management.

12 Was ist ein Incident?

- Unvorhergesehene Unterbrechung eines Services
- NICHT: Geplante Unterbrechungen (Maintenance) / Serverabsturz außerhalb der Verwendungszeiten.
- Incidents müssen sofort gefixt werden durch einen permanenten Fix, temporären fix oder einen Workaround.

13 Was ist ein Problem?

- Die Ursache eines oder mehrerer Incidents.
- Ein Serverabsturz außerhalb der Verwendungszeiten ist ein Problem, da es wieder passieren kann und einen Incident auslösen könnte.

14 Was ist der Unterschied zwischen Problemmanagement und Incidentmanagement?

- Problemmanagement: Problem soll nicht mehr auftreten (strukturelle Änderung notwendig), langsam (Zeit + Ruhe), keine Personalunion mit Incident Management, geht nicht unter Zeitdruck
- Incidentmanagement: Vorfall unmittelbar behandeln, wenig Wissen, rasche Entscheidungen, kein Wegsparen möglich

15 Was ist Fault Management?

- Redundanz aufbauen für den “Fall der Fälle”
- Umgehungslösung um den Betrieb aufrecht zu erhalten

16 Was ist die Configuration Management Datenbank (CMDB)?

- Datenbank die alle relevanten Informationen über Hardware und Software Komponenten (Configuration Items) enthält
- Configuration items werden in der IT einer Organisation verwendet
- Beziehungen und Konfigurationen
- zB: Rechner, Telefone, Netzwerk Komponenten und IT-Services

17 Wozu Monitoring?

überwachung von Computersystemen und Netzwerken für:

- Accounting
- Fehlerfeststellung: frühzeitige Erkennung von Abweichungen vom Soll-Zustand
- Analyse: regelmäßige Berichte
- Monitoring erhöht die Verfügbarkeit, verkürzt Ausfallzeiten und reduziert die Folgekosten von Ausfällen.

18 Vor- und Nachteile der ersten Normalform (Redundante Information)?

- Jede Information in den Tabellen liegt atomar vor (z.B. PLZ und Ort nicht in einer Spalte) und die Relationen sind frei von Wiederholungsgruppen
- Vorteile: Keine Redundanz, Inkonsistenzen vermeiden: keine sich widersprechenden Daten in der Datenbank
- Nachteile: Normalisierungsaufwand, Performance (durch Joins)

19 Warum reicht es nicht nur die Häufigkeit sondern auch die Dauer der Ausfälle zu berücksichtigen?

- Wegen der Wiederanlaufzeit.
- Jede Stunde 5 min Ausfall $\rightarrow$ ganzer Tag verhaut

20 Wie schule ich einen Helpdesk (1st Level Support)?

- Fragen an User stellen: wer/wo sind Sie? Haben Sie es nochmal probiert? Nummer der IT-Dose (Switch).

21 Wieso sind Raumnummern wichtig?

- Räume ändern sich oft z.B. werden Wände eingerissen.

22 Wann führt eine Betriebsunterbrechung zum Abbruch des Arbeitstages?

- Nach ca 1/6 des Arbeitstages
- Anlaufzeit muss miteinbezogen werden
- Anlaufzeit berücksichtigen

23 In welchen Abständen wird der Arbeitsplatz gewechselt?

- Alle 1 bis 3 Jahre z.B. wegen Beförderung.

24 Energieströme

- Energiezufuhr (elektrisch)
- Energieabfuhr (thermisch)

Energieumwandlung

- IT-Systeme: Server, LAN, Speicher
- Schutz: Brandschutz, Zutritt
- Betrieb: Monitoring, Management
- Sonstiges: Licht, Feuchte, etc
- PVC Kabel als Zündschnur

25 Welche Arten von Wartungen existieren?

- Proaktive Wartung: Stichprobe wird geprüft, alles wird getauscht im Fehlerfall
- Reaktive Wartung: Feuerwehrprinzip
- Präventive Wartung: Durchhängen des Drahtes heißt das Einzelstück wird getauscht, jedes Einzelstück wird geprüft

26 Was ist der PUE Wert?

- Power Usage Effectiveness (1 = optimal)
- Der Wert beschreibt wie effizient ein Rechenzentrum Energie nutzt.
- USA DC früher 2,5-3
- 1,05 in DE

$$\text{PUE} = \frac{\text{Total Facility Energy}}{\text{IT Equipment Energy}}, \qquad \text{PUE} > 1$$

27 Was ist der DCIE-Wert?

- Data Center Infrastructure Efficiency Wert

$$\text{PCIE} = \frac{1}{\text{PUE}}, \qquad \text{PCIE} \in (0, 1)$$

28 Wie kann der PUE Wert verbessert werden?

- Reduktion der Verluste bei ET und HKL
- Solarzellen haben mehr Leistung am Tag (billigerer Rechenzentrum Betrieb für lokale Kunden)

29 Wie kann Feuer im Rechenzentrum gelöscht werden?

- Vakuum, CO_2, N_2, Wasser
- Präventiv Sauerstoff O_2 entfernen/verdrängen

30 Wirkungsgrad

$$\eta = \frac{p_{\text{Nutzen}}}{p_{\text{Aufwand}}}, \qquad \eta \in [0, 1]$$

zB Licht $\eta \approx 5\%$ (95% Wärmeverlust)

31 Was ist "Free Cooling"?

- Kühlung, die keinen Energieaufwand verursacht (ohne Kompressor).
- Außentemperatur $<$ Innentemperatur $\rightarrow$ Lüften

32 Warum ist ein Serverraum schützenswert? (Arten, Strategien, ...)

- Zum einen liefert es IT-Services mit geschäftskritischen Daten, zum anderen ist es ein physisches Gebäude und beherbergt IT-Komponenten.

33 Welche Arten von Schutzmaßnahmen existieren?

- Brandschutzmaßnahmen z.B. nicht brennbare Dämmmaterialien, defekte Geräte, Brandmeldeanlage
- Schutz gegen Einbruch, Diebstahl, Sabotage und Vandalismus z.B. durch Zugriffskontrolle, Einbruchmeldeanlage
- Schutz gegen Stromausfall z.B. durch USV
- Schutz gegen Naturgefahren, Wasser z.B. durch bauliche Trennung
- Schutz gegen elektrische Störeinflüsse z.B. Blitz- und Überspannungsschutz

34 Wie können Monitoringmeldungen ausgegeben/angezeigt werden?

- Akustisch
- Optisch, zB verschiedene Farben

35 Wann ist eine Handlung oder Aktion erforderlich?

Incident report, problem report

- Beheben
- Umgehen
- Akzeptieren (Ignorieren → Alternativlösung implementieren "bis dahin geht's halt ned")

36 Fehler, Fehlerzustand, Ausfall, Risiko

- Fehler: Durch Ausführung (Fehler existiert im Programm auch ohne Ausführung)
- Fehlerzustand: Innere Spezifikation verletzt
- Ausfall: Äußere Spezifikation verletzt
- Risiko = Schaden · Eintrittswahrcheinlichkeit

37 Wie sollen die Meldungen des Monitorings angezeigt werden?

- Akustisch
- Optisch
- Farben
- Sprachausgabe?

38 Was sind die 4 Entities von SNMP?

- Manager
- Agent (Software die auf managed Geräten läuft)
- Management Information Base (MIB)
- Protokoll

39 Was ist eine MIB?

- Baumstruktur, info in den Blättern, reine Beschreibung (weder real noch virtuell existent)
- Jeder Knoten hat eindeutige Nummer zB 1.3.6.1.2.1... Pfad durch Knotennummern mit Punkten getrennt
- Manager weiß, was er fragen kann (synchron)
- Datenbank um Entitäten in einem Kommunikationsnetzwerk zu steuern/verwalten.

40 Welche 5 PDUs werden von SNMP unterstützt?

- GET
- GET RESPONSE
- SET, $\rightarrow$ antwort ist auch GET response
- TRAP
- NEXT / GET-NEXT, $\rightarrow$ liefert Wert + OID des nächsten (auch GET response)

41 SNMP Datenstruktur

- 2D-Tabelle (Spalten fix, Reihen dynamisch)
- Idee: schreibe Perl-Code Zeilenweise in Tabelle: erlaubt remote-config des Mid-Level-Managers

42 Was versteht man unter einem OID?

- Object Identifier (OID)
- Definiert einen gobal eindeutigen Objektnamen
- Zu jedem Knoten auch mnemonischer Code

43 Welche Kommunikationsflüsse gibt es bei SNMP?

- Horizontal
- Vertikal
- 1 Manager $\leftrightarrow$ Master Agent (Request, Response)... Manager untereinander nicht definiert
- n Agents $\rightarrow$ Manager (Trap)... Agents können nicht miteinander kommunizieren

44 Personalkosten

- Faktor 2 vom Netto sind Lohnnebenkosten
- Faktor 3-4 für alle Kosten

Reduktion

- Personal einsparen heißt weniger Kreativität
- Hardware hat recht wenig Kosten im Vergleich mit Personal

45 Energieflüsse

- $\overset{\text{Elektrische}}{\text{Energie}} \rightarrow \overset{\text{IT-Systeme}}{\text{HKL}} \rightarrow \overset{\text{Thermische}}{\text{Energie}} \rightarrow$ Umwelterwärmung + Wärmenachnutzung
- Nachnutzung braucht evtl Kompressor für Temperaturunterschied *oder* bereits beim Bau (Gebäude) berücksichtigt

46 Redundanz

- Überflüssiges, im Normalbetrieb nicht benötigt
- Bei Ausfall kann man den Betrieb weiterführen
- zB uptimeinstitute (elektr. Versorgung, Leitungen, Betriebsmittel, USV, Wirkungs- und Scheinleistung)
- USV als Doppelwandler AC/DC $\leftrightarrow$ DC/AC

47 Phasisch

- u und i nicht in Phase, Blindleistung
- Strom fließt hin und her, aber nicht zu Abnehmer
- Netzteil 20W Blindleistung, 2W Wärme

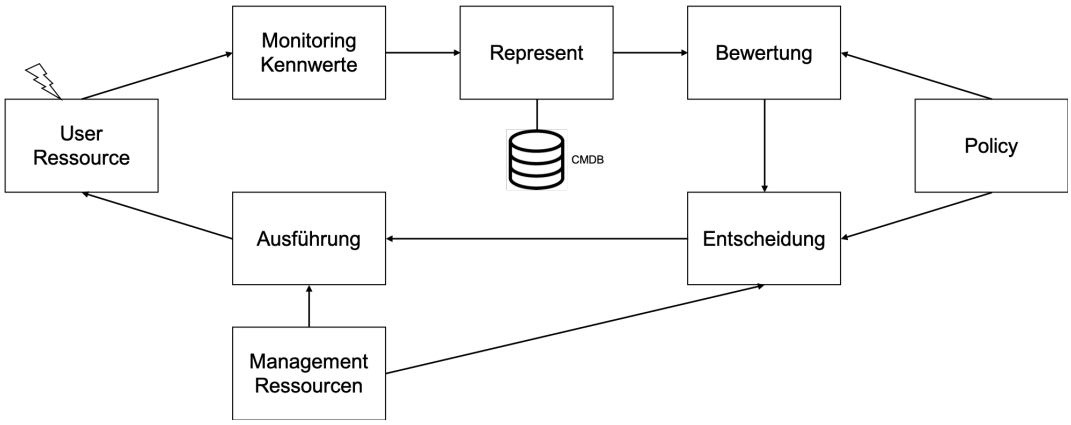
48 Thermische Entsorgung

- Medientransport (Ventilator [2-facher Luftstrom = 2^3 Leistungsaufnahme], Pumpen, Rohre)
- Temperaturänderung
- Medienkurzschlüsse (Wasser)

49 Wieviele Mitarbeiter braucht man für einen IT-Betrieb?

- Kritische Masse, mindestens 5 wegen Urlaub, Krankheit, etc
- Wenn keine kritische Masse vorhanden $\rightarrow$ outsourcing notwendig (+Outsourcing Monitoring Person)

50 Bewertungsgrundlage (???)



- Bewertung: Skala mit Schwellweren notwendig (zB 10-8 OK, 8-6 Warnung, 6-4 Fehler, 4-0 Kritisch) "Schinkenfleckerlskala"
- Mehrere Schwellwerte für Abstufungen

51 Ergebnis der Bewertung? (Monitoring)

- Signalisieren des Ressourcenzustandes
- Gibt es Handlungsbedarf? Wichtig für Management.
- Kickeriki: Wenn Alarm zu oft, wird er einfach ignoriert.

52 Zustände

GRÜN (OK)

- Vermutlich keine Handlung notwendig
- Lange Zeit auf GRÜN = wahrscheinlich teuer, weil viel Zeit und Aufwand notwendig

GELB (Warnung)

- Braucht Gedächtnis, mehrere Warnungen bedingen Aktion
- Handlungsbedarf bei Gelegenheit (zB nach Mittagessen)

ORANGE (Fehler)

- Aktuelle Handlung beenden
- Danach sofort Fehlerbehebung starten

ROT (Kritisch)

- Handlung unterbrechen

- Sofort Fehlerbehebung starten

Zusätzliche Zustände: Wartung, kein Messwert verfügbar, Schwarz = Stromausfall

Schwellwerte in Policy definiert, legt fest wie weiter zu verfahren ist, vom Management festgelegt, reiner Techniker darf das eigentlich nicht

53 Regelkreis

- Schwingen: Warnungen werden mehr
- Dämpfen: Gedächtnis, Warnungen werden weniger

54 Instrumentarium

- Wie komme ich von Hardware zu Wert in Software? Herstellerabhängig